Blockchain mniej bezpieczny niż się wydawało

23 lutego 2019

Blockchain, jeszcze do niedawna uważana za odporną na cyberataki, coraz częściej pada ofiarą cyberprzestępców. Ten typ bazy danych jest tym bardziej atrakcyjnym celem ataków, że opierają się na nim sieci kryptowalut. Statystyki mówią same za siebie. Od początku 2017 roku przestępcy ukradli kryptowaluty o łącznej wartości niemal 2 miliardów dolarów. A mowa tu tylko o kwotach, które zostały publicznie ujawnione. Większości kradzieży dokonano na internetowych giełdach, a atakami zajmują się już nie tylko samotni hakerzy, ale i zorganizowane grupy przestępcze. Firma analityczna Chainalysis informuje, że tylko dwie grupy, które prawdopodobnie wciąż są aktywne, ukradły w sumie około miliarda dolarów.

Na początku lutego firma Coinbase zauważyła dziwną aktywność na blockchainie Ethereum Classic. Cały blockchain był właśnie celem ataku. Napastnik w jakiś sposób przejął kontrolę nad ponad połową zasobów obliczeniowych blockchaina i nadpisywał jej historię. Taki atak, który jeszcze rok temu był czysto teoretyczny, pozwalał na wydanie tych samych pieniędzy więcej niż jeden raz. Ten atak udało się powstrzymać.

Blockchain ma dodatkową zaletę z punktu widzenia przestępców. Oszukańczych transakcji nie można tutaj bowiem odwrócić. W tradycyjnym systemie finansowym, gdy ktoś ukradnie nam pieniądze z konta czy posłuży się naszą kartą płatniczą, możliwe jest cofnięcie transakcji. Tutaj takiej możliwości nie ma.

Blockchain to rozproszona otwartoźródłowa szyfrowana baza danych bez punktu centralnego. Poszczególne dołączone doń komputery, węzły, wykorzystują złożony protoków, który pozwala na weryfikacje transakcji i dodawanie ich do bazy. Protokół

korzysta z szyfrowania i teorii gier oraz wbudowano weń zachęty, które powodują, że bardziej opłaca się wykorzystać moc obliczeniową do współpracy, niż do atakowania sieci. Atak na poprawnie skonfigurowany blockchain powinien być niezwykle trudny i kosztowny, a z drugiej strony weryfikacja prawdziwych transakcji powinna być dość łatwa. Te zalety spowodowały, że blockchain cieszy się coraz większym zainteresowaniem przemysłu. Blockchain jest testowany przez Walmart, a właściciel Giełdy Nowojorskiej, firma Intercontinental Exchange, ma zamiar uruchomić wkrótce swój własny blockchain.

Im jednak blockchain bardziej złożony, tym łatwiej w nim o błędy. Niedawno firma stojąca za kryptowalutą Zcash pinofrmowała, że poprawiła „subtelny błąd kryptograficzny" w blockchainie. Pozwalał on napastnikowi na sfałszowanie dowolnej liczby Zcash. Błędy pojawiają się nie tylko w protokole. We wrześniu deweloperzy Bitcoin Core, głównego klienta kryptowaluty bitcoin poprawili błąd – szczegóły są trzymane w tajemnicy – który pozwalał na wydobycie większej liczby bitcoinów niż to dozwolone.

Większość ataków na kryptowaluty, jak już wspomniano, przeprowadzono na giełdach i można za nie winić same giełdy. Jednak wszystko zmieniło się po styczniowym ataku na Ethereum Classic.

Większość kryptowalut jest podatnych na atak 51%. Dzieje się tak, gdyż wykorzystywane blockchainy uwiarygadniają użytkowników w ten sposób, że każdy z węzłów musi spędzić dużo czasu i zaangażować dużo swojej mocy obliczeniowej na pracę na rzecz całej sieci, by się uwiarygodnić i zyskać prawo dodawania informacji do bazy danych. Teoretycznie więc, jeśli ktoś uzyska kontorlę nad większością (wspomniane 51%) węzłów może uwiarygodnić się wobec całej sieci wysyłając płatności do innych węzłów, a później stworzyć alternatywną wersję blockchaina, w której płatności nigdy nie miały miejsca. Taki fałszywy blockchain staje się całkowicie wiarygodny i możliwe jest wielokrotne wydanie tych samych pieniędzy.

Tego typu ataki mogą być jednak niezwykle kosztowne. Jak mówią specjaliści, wynajęcie mocy obliczeniowej potrzebnej do ataku na Bitcoin kosztowałoby ponad 260 000 USD za godzinę. Jednak obecnie istnieje ponad 1500 kryptowalut, a im mniej popularna kryptowaluta, tym mniejszy blockchain i tym łatwiej się w nim uwiarygodnić. Około połowy 2018 roku rozpoczęła się seria ataków na mniej popularne kryptowaluty. Przestępcy ukradli około 20 milionów UDS. Jesienią podczas serii ataków na Vertcoin skradziono 100 000 dolarów. Atak przeciwko Ehtereum Classic, podczas którego ukradziono ponad milion dolarów był pierwszym przeciwko kryptowalucie znajdującej się wśród 20 największych. Specjaliści uważają, że tego typu ataki będą coraz częstsze i coraz silniejsze.

Jednak 51% to nie jedyny problem blockchainów. Innym są programy typu smart contract. To oprogramowanie automatyzujące przepływ kryptowalut zgodnie z założonymi wcześniej warunkami i zasadami. Jest ono wykorzystywane np. do zawierania umów czy przeprowadzania złożonych transakcji. Pozwala też np. na stworzenie mechanizmu głosowania, który pozwala członkom firmy inwestycyjnej na podjęcie decyzji co do alokacji kapitału.

W 2016 roku w blockchainie Ethereum uruchomiono fundusz o nazwie Decentralized Autonomous Organization. Wkrótce potem napastnik ukradł z niego ponad 60 milionów USD. Wykorzystał bowiem błąd, który pozwalał mu na wycofywanie pieniędzy z kont, a system nie rejestrował, że pieniądze zostały wycofane. W tradycyjnym systemie bankowym wystarczyłoby cofnąć transakcje i zastosować łatę. W blockchainie transakcji nie da się cofnąć, zatem dołączane doń oprogramowania od początku powinno być pozbawione błędów. Istnieją sposoby na częściowe poradzenie sobie z tym problemem. Można bowiem stworzyć kolejne oprogramowanie smart contract, które będzie wchodziło w interakcje z już istniejącym. Możliwe jest stworzenie centralnego wyłącznika, który zatrzymuje całą sieć w momencie, gdy wykryto atak. Jednak transakcje przeprowadzone wcześniej nie mogą zostać cofnięte, a ukradzionych pieniędzy niemal nie

da się odzyskać. Niemal, bo istnieje jedna drastyczna metoda. Można nadpisać historię, cofnąć się do czasu sprzed ataku i w ten sposób stworzyć nowy blockchain. Użytkownicy starego powinni wówczas zgodzić się, że będą używali nowego. To właśnie zrobili w przeszłości twórcy Ethereum. Większość społeczności przesiadła się na nowy blockchain znany obecnie jako Ethereum, ale część pozostała przy oryginalnym, Ethereum Classic.

Smart contracts stają się najpoważniejszym problemem blockchaina. Eksperci twierdzą, że setki, a może nawet tysiące tego typu programów zawierają lub mogą zawierać błędy. Te zaś z pewnością zostaną przez przestępców odnalezione, gdyż, jak już wspomniano, blockchain opiera się na otwartych źródłach, do których dostęp ma każdy.

Powstaje jednak coraz więcej inicjatyw i firm, których celem jest zabezpieczenie blockchaina. Pojawił się też pomysł ustanowienia nagród pieniężnych za odnajdowanie i informowanie o dziurach w oprogramowaniu.

Autorstwo: Mariusz Błoński
Na podstawie: TechnologyReview.com
Źródło: KopalniaWiedzy.pl