08 Analiza bezpieczeństwa chmur blockchainowych

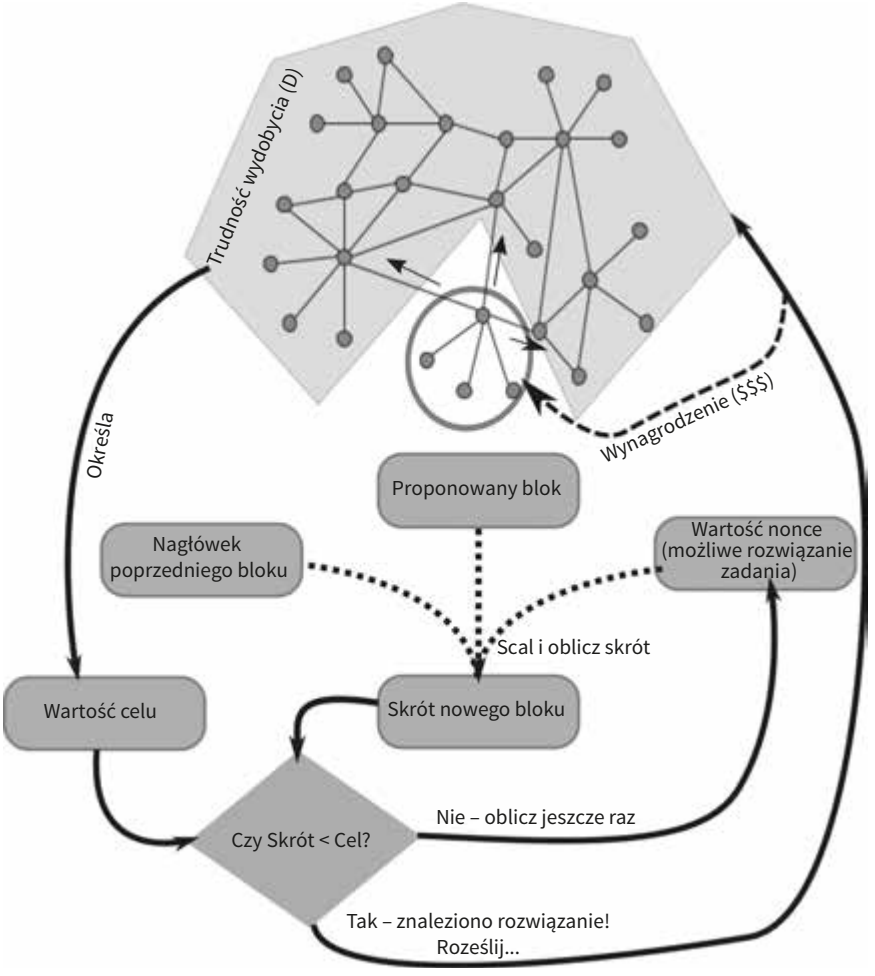
Deepak Tosh [1]***, Sachin S. Shetty*** [2]***, Xueping Liang*** [2]***, Laurent Njilla*** [3]***, Charles A. Kamhoua*** [4] ***i Kevin Kwiat*** [5]

1 University of Texas at El Paso, Department of Computer Science, El Paso, TX, USA
2 Old Dominion University, Virginia Modeling, Analysis and Simulation Center, Norfolk, VA, USA
3 US Air Force Research Lab, Cyber Assurance Branch, Rome, NY, USA
4 US Army Research Lab, Network Security Branch, Adelphi, MD, USA 5 Haloed Sun TEK, LLC, CAESAR Group, Sarasota, FL, USA

8.1. Wprowadzenie

Technologia łańcucha bloków (*blockchain*) cieszy się ogromnym zainteresowaniem w wielu dziedzinach, takich jak finanse, opieka zdrowotna, usługi komunalne, rynek nieruchomości oraz wśród agencji rządowych. Sieci blockchainowe wykorzystują współdzieloną, rozproszoną i odporną na uszkodzenia platformę rejestru danych, który każdy uczestnik sieci może udostępniać i nad którym nie może przejąć samodzielnej kontroli żaden z podmiotów. Blockchain zakłada obecność przeciwników w sieci i niweluje wrogie działania, wykorzystując możliwości obliczeniowych uczciwych węzłów, a informacje przekazywane za jego pośrednictwem są odporne na manipulacje i zniszczenie. Technologia blockchain będzie korzystna dla usług chmury wymagających bezpiecznych narzędzi do śledzenia pochodzenia danych i wsparcia audytowego. Aby zapewnić integralność danych przechowywanych w publicznym rejestrze chmury blockchainowej, tworzone kryptograficznie bloki dołącza się do łańcucha bloków po osiągnięciu konsensusu w zdecentralizowanej sieci, której węzły uwierzytelniają transakcje zawarte w blokach. Ten publiczny rejestr może potencjalnie

zawierać historię wszystkich transakcji związanych z dowolnym rodzajem aktywów – finansowych, fizycznych lub cyfrowych – które mogą być weryfikowane, monitorowane i rozliczane bez udziału administratora chmury. Połączenie mechanizmów kryptograficznych i zdecentralizowanego rejestru publicznego pozwala budować różne aplikacje oparte na łańcuchu bloków, bez obaw o komponenty zaufania użytkowników i o wrogie działania w blockchainowym systemie chmurowym.



Rysunek 8.1. Schemat procesu wydobywania bloków

Ponieważ aktualizacja łańcucha wykonywana jest się w sieci peer-to-peer (P2P), każdy węzeł musi dbać o integralność łańcucha bloków. Aby dołączanie bloku nie zaburzyło stanu łańcucha bloków, konieczne jest zastosowanie rozproszonych mechanizmów