# Nowoczesne systemy kryptograficzne stosowane w rozproszonych systemach transakcyjnych

Nowoczesne systemy kryptograficzne stosowane w rozproszonych systemach transakcyjnych zwykle opierają się na technologii blockchain. Blockchain to rozproszona baza danych, która jest zabezpieczona przez algorytmy szyfrujące. Każda transakcja jest zapisywana jako blok, a każdy blok jest połączony z poprzednim, tworząc łańcuch bloków

Jednym z najważniejszych aspektów bezpieczeństwa rozproszonych systemów transakcyjnych jest zabezpieczenie przed atakami typu "double-spending". Aby to osiągnąć, algorytm konsensusu jest używany do potwierdzania poprawności transakcji.

Najpopularniejsze algorytmy konsensusu stosowane w blockchain to:

* Proof of Work (PoW) to algorytm konsensusu, w którym użytkownicy (węzły) rozwiązują skomplikowane zadanie matematyczne (puzzle) w celu potwierdzenia transakcji i utworzenia nowego bloku. PoW jest używany w systemie Bitcoin.
* Proof of Stake (PoS) to algorytm konsensusu, w którym użytkownicy (węzły) potwierdzają transakcje, biorąc na siebie ryzyko finansowe. Węzły, które chcą potwierdzać transakcje, muszą "postawić" swoje monety, co oznacza, że tracą je, jeśli potwierdzenie jest nieprawidłowe. PoS jest używany w systemie Ethereum.
* Delegated Proof of Stake (DPoS) to algorytm konsensusu, w którym użytkownicy (węzły) głosują na reprezentantów, którzy potwierdzają transakcje. Reprezentanci są odpowiedzialni za potwierdzanie transakcji i utrzymanie sieci. DPoS jest używany w systemie EOS.

Podpisywanie transakcji jest ważnym elementem rozproszonych systemów transakcyjnych. Mechanizmem często do tego stosowanym jest metoda podpisu cyfrowego - jest to unikalny ciąg znaków, który jest generowany przy użyciu specjalnego klucza i służy do potwierdzenia autentyczności i do uwierzytelnienia nadawcy.

Istnieje kilka różnych metod podpisu cyfrowego, w tym:

1. Podpis cyfrowy z użyciem klucza prywatnego: w tej metodzie podpis cyfrowy jest generowany przy użyciu klucza prywatnego, a jego autentyczność jest potwierdzana przy użyciu klucza publicznego.
2. Podpis cyfrowy z użyciem funkcji skrótu: w tej metodzie podpis cyfrowy jest generowany przy użyciu funkcji skrótu, która jest stosowana do skompresowania danych w krótki ciąg znaków.
3. Podpis cyfrowy z użyciem funkcji skrótu i klucza prywatnego: w tej metodzie podpis cyfrowy jest generowany przy użyciu połączenia funkcji skrótu i klucza prywatnego. Najpierw wybrane dane są skompresowane za pomocą funkcji skrótu, a następnie skompresowane dane są zaszyfrowane przy użyciu klucza prywatnego, a jego autentyczność jest potwierdzana przy użyciu klucza publicznego.

W rozproszonych systemach transakcyjnych stosowane są również czasami szyfry takie jak:

1. Szyfry Symetryczne
   1. AES
   2. Blowfish
   3. Twofish
   4. Serpent
2. Szyfry asymetryczne
   1. RSA
   2. protokół Diffiego-Hellmana
   3. DSA