Bitcoin i blockchain

Karol Janik, Michał Kazanecki

Wydział Inżynierii Materiałowej i Fizyki
Politechnika Krakowska

Luty 3, 2020

Plan

Bitcoin - podstawowe informacje

- Kryptowaluta wprowadzona w 2009 r.
- Twórca: Satoshi Nakamoto - niepotwierdzona tożsamość
- Podział: 100 000 000 satoshi = 1 bitcoin
- Prawdopodobnie nie podlega inflacji, ograniczenie górne ilości: 21mln sztuk
- Nie podlega żadnemu bankowi centralnemu
- Tranzakcje przechowywane w zdecentralizowanej bazie danych
- Wykorzystanie kryptografii w celach bezpieczeństwa
- Praktycznie natychmiastowe tranzakcje w dowolne miejsce na świecie, anonimowość
- Obecna wartość: 1 btc $\approx$ 36 tys. zł

Zdecentralizowana baza danych - blockchain

Porównanie: publiczny dziennik, do którego każdy użytkownik może dodać wpis, wysyłając o tym informację do innych użytkowników. Każdy użytkownik posiada własną wersję dziennika. Do dziennika dodawane są tylko wpisy sygnowane poprawnym podpisem elektronicznym (generowanym za pomocą funkcji haszującej).

- Klucz prywatny - pozwala na wygenerowanie podpisu.
- Klucz publiczny - umożliwia sprawdzenie poprawności podpisu. (adres przypisany do monet)
- Funkcja haszująca - najmniejsza zmiana danych wejściowych zmienia diametralnie wynik. Niemożliwa do odwrócenia.
  SHA-256(Tekst)=5d07abcd8c8c64590e240d2b79...
  SHA-256(tekst)=324d0315d575bf5b4f6c8703f1...

Jak sprawdzić czy każdy ma tą samą wersję dziennika?

Blockchain

Blok 1

Poprzedni hash: 0
Informacje
Hash: 1234

Blok 2

Poprzedni hash: 1234
Informacje
Hash: 4335

Blok 3

Poprzedni hash: 4335
Informacje
Hash: 3445

Kolejne wpisy dodawane są w postaci następujących po sobie bloków. Każdy blok zawiera hash poprzedniego bloku, informacje o tranzakcjach oraz swój własny hash. Zmiana informacji w bloku zmienia jego hash, co wiąże się z koniecznością zmiany wszystkich kolejnych bloków. Zabezpieczenie: “proof of work“

Proof of work, mining, halving

Blok n-ty

Poprzedni hash: 1234
Informacje
Dodatkowa informacja = ?
Hash: 000???

Zanim blok zostanie uznany za poprawny, musi zostać wykonana odpowiednia ilość pracy w celu znalezienia dodatkowej informacji dopisanej do bloku, tak aby jego hash miał z góry określoną postać. Jedyny sposób - metoda prób i błędów.

Węzeł, który znalazł rozwiązanie, rozsyła je do pozostałych (każdy może sprawdzic poprawność) i zostaje nagrodzony określoną ilością monet (mining).
Halving - nagroda zmniejsza się co 210000 bloków (ok 4 lata).
Początkowo: 50 btc, obecnie: 12,5 btc.

Blockchain - możliwe zastosowania

Gdzie blockchain może znaleźć zastosowanie?

- Internet rzeczy
- Systemy głosowania
- Dystrybucja i produkcja energii
- Tożsamość i jej weryfikacja
- Składowanie danych
- Digitalizacja dokumentów
- Usługi rządowe

Bibliografia

- https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/co-to-jest-blockchain-i-jakie-moze-miec-znaczenie-z-punktu-widzenia-ekonomii/ (dostęp: 02.02.2020)
- https://en.wikipedia.org/wiki/Bitcoin (dostęp: 02.02.2020)
- https://en.wikipedia.org/wiki/Blockchain (dostęp: 02.02.2020)
- https://www.youtube.com/watch?v=bBC-nXj3Ng4&fbclid=IwAR0LYbY0rZRHPtrX0_MkZ2mhjTtQK4v61QcXR-Wp9Md6nenLfSYjY4uwOSU (dostęp: 02.02.2020)

Dziękujemy za uwagę