sages

Jak działa blockchain?

Wprowadzenie do Ethereum

Piotr Nazimek

8 czerwca 2017

Sages sp. z o.o.

Rejestr transakcji

⟶ Anna 50 PLN
⟶ Andrzej 50 PLN

Andrzej ⟶ Anna 10 PLN
Anna ⟶ Marcin 20 PLN

Marcin ⟶ Marta 10 PLN
Andrzej ⟶ Marta 20 PLN
Anna ⟶ Andrzej 10 PLN

...

Funkcje skrótu

→ 01d58360dd9f4f295cd2c09171c798905cd4be3c7fd31d55985eb7c11f2709f6

- usługa integralności
- dla dowolnej wiadomości wartością funkcji jest ciąg bitów o **określonej długości**
- używamy funkcji dla których jest problemem trudnym znalezienie dwóch dowolnych wiadomości o tym samym skrócie
- funkcje **odporne na kolizje** (ang. *collision resistance*)
- przykłady funkcji skrótu: SHA-256, SHA3-256, Keccak-256, Tiger

Integralny rejestr transakcji

⟶ Anna 50 PLN
⟶ Andrzej 50 PLN
dbde8e92f4e4472418239795a29c0a5e931710c8b7016b2cde25d818c970c41a

Andrzej ⟶ Anna 10 PLN
Anna ⟶ Marcin 20 PLN
3989e7283513c13d72b6b87c7dbcf44db1cf8c68bdc4224395fdee37c185fd38

Marcin ⟶ Marta 10 PLN
Andrzej ⟶ Marta 20 PLN
Anna ⟶ Andrzej 10 PLN
9e4115f10a26506db2cd89279d8aa94b1866bc1c51de72174f03b9139b046386

Integralny rejestr transakcji

⟶ Anna 50 PLN
⟶ Andrzej 50 PLN
dbde8e92f4e4472418239795a29c0a5e931710c8b7016b2cde25d818c970c41a

Andrzej ⟶ Anna 10 PLN
Anna ⟶ Marcin 20 PLN
a4e9436dbd3e889d5dd0f353de31e821fa737876fa131db2df6663af38179f5c

Marcin ⟶ Marta 10 PLN
Andrzej ⟶ Marta 20 PLN
Anna ⟶ Andrzej 10 PLN
9e4115f10a26506db2cd89279d8aa94b1866bc1c51de72174f03b9139b046386

Integralny rejestr transakcji

⟶ Anna 50 PLN
⟶ Andrzej 50 PLN
dbde8e92f4e4472418239795a29c0a5e931710c8b7016b2cde25d818c970c41a

Andrzej ⟶ Anna 10 PLN
Anna ⟶ Marcin 20 PLN
a4e9436dbd3e889d5dd0f353de31e821fa737876fa131db2df6663af38179f5c

Marcin ⟶ Marta 10 PLN
Andrzej ⟶ Marta 20 PLN
Anna ⟶ Andrzej 10 PLN
813b24a5d1075820113835b11efbbd4957b974857fda32a90cbfe7c39d17a4b3

Podpis cyfrowy

- usługa uwierzytelnienia
- użytkownik generuje losową parę kluczy: **prywatny** i **publiczny**

- dla danego klucza do weryfikacji (publicznego) jest operacją trudną obliczeniowo wygenerowanie podpisu dla dowolnej wiadomości
- z podpisu nie da się uzyskać klucza do podpisu (prywatnego)
- jest operacją trudną obliczeniowo (również dla właściciela klucza do podpisu) znalezienie dwóch różnych wiadomości z tą samą wartością podpisu
- przykłady algorytmów podpisu cyfrowego: RSA, DSA, ECDSA

Integralny rejestr z uwierzytelnieniem transakcji

⟶ Anna 50 PLN
⟶ Andrzej 50 PLN
dbde8e92f4e4472418239795a29c0a5e931710c8b7016b2cde25d818c970c41a

Andrzej ⟶ Anna 10 PLN 9604c2c1f51ee2376deb52719e6a678…
Anna ⟶ Marcin 20 PLN d68a612281f4958ebbf5ecb85134575…
065d58a27162f67714b160ec63e39c71b6a1d207d77179d0bc8d109ed0f520f4

Marcin ⟶ Marta 10 PLN 7677e840df3c7343dfb2181761affb7…
Andrzej ⟶ Marta 20 PLN 39c2bc43e65f5157bb8f7b054717f82…
Anna ⟶ Andrzej 10 PLN cf3d2dbfaf9b43903391cde5899faa2…
fa4ae3e527a72bc130db24a253c20b55e14d94242743a009ff23196f2f775810

Integralny rejestr z uwierzytelnieniem transakcji

⟶ 2db36af02... 50 PLN
⟶ Andrzej 50 PLN
dbde8e92f4e4472418239795a29c0a5e931710c8b7016b2cde25d818c970c41a

Andrzej ⟶ 2db36af02... 10 PLN 9604c2c1f51ee2376deb52719e6a678...
2db36af02... ⟶ Marcin 20 PLN d68a612281f4958ebbf5ecb85134575...
065d58a27162f67714b160ec63e39c71b6a1d207d77179d0bc8d109ed0f520f4

Marcin ⟶ Marta 10 PLN 7677e840df3c7343dfb2181761affb7...
Andrzej ⟶ Marta 20 PLN 39c2bc43e65f5157bb8f7b054717f82...
2db36af02... ⟶ Andrzej 10 PLN cf3d2dbfaf9b43903391cde5899faa2...
fa4ae3e527a72bc130db24a253c20b55e14d94242743a009ff23196f2f775810

Integralny rejestr z uwierzytelnieniem transakcji

⟶ 2db36af02... 50 PLN
⟶ 6d340b451... 50 PLN
dbde8e92f4e4472418239795a29c0a5e931710c8b7016b2cde25d818c970c41a

6d340b451... ⟶ 2db36af02... 10 PLN 9604c2c1f51ee2376deb52719e6a678...
2db36af02... ⟶ Marcin 20 PLN d68a612281f4958ebbf5ecb85134575...
065d58a27162f67714b160ec63e39c71b6a1d207d77179d0bc8d109ed0f520f4

Marcin ⟶ Marta 10 PLN 7677e840df3c7343dfb2181761affb7...
6d340b451... ⟶ Marta 20 PLN 39c2bc43e65f5157bb8f7b054717f82...
2db36af02... ⟶ 6d340b451... 10 PLN cf3d2dbfaf9b43903391cde5899faa2...
fa4ae3e527a72bc130db24a253c20b55e14d94242743a009ff23196f2f775810

Integralny rejestr z uwierzytelnieniem transakcji

⟶ 2db36af02... 50 PLN
⟶ 6d340b451... 50 PLN
dbde8e92f4e4472418239795a29c0a5e931710c8b7016b2cde25d818c970c41a

6d340b451... ⟶ 2db36af02... 10 PLN 9604c2c1f51ee2376deb52719e6a678...
2db36af02... ⟶ aa748279f... 20 PLN d68a612281f4958ebbf5ecb85134575...
065d58a27162f67714b160ec63e39c71b6a1d207d77179d0bc8d109ed0f520f4

aa748279f... ⟶ 39927fb83... 10 PLN 7677e840df3c7343dfb2181761affb7...
6d340b451... ⟶ 39927fb83... 20 PLN 39c2bc43e65f5157bb8f7b054717f82...
2db36af02... ⟶ 6d340b451... 10 PLN cf3d2dbfaf9b43903391cde5899faa2...
fa4ae3e527a72bc130db24a253c20b55e14d94242743a009ff23196f2f775810

Blockchain

- łańcuch bloków
- to globalnie współdzielona **baza transakcji** (rozproszona)
- każdy z węzłów sieci przechowuje kopię łańcucha
- nie wymaga **zaufania** pomiędzy korzystającymi z bazy
- wymaga akceptacji **zasad**
- jest jawna, każdy może ją odczytać
- każdy może utworzyć transakcję, ale musi ona być zaakceptowana przez pozostałych
- zatwierdzona transakcja nie może być zmieniona przez nikogo
- transakcje są podpisane przez zlecających
- transakcje łączone są w bloki
- kolejne bloki są zależne od poprzednich

Algorytm konsensusu

- każdy może tworzyć bloki
- który powinien być następny?
- **algorytm konsensusu** to rozwiązanie problemu uzgadniania przez zbiór jednostek jednej wartości spośród zbioru wartości zaproponowanych wstępnie przez te jednostki
- najczęściej wykorzystywane typy algorytmów w blockchain to **dowód pracy** i **dowód stawki**
- wydajne i zarazem efektywne algorytmy konsensusu to obiekt aktualnych poszukiwań

Dowód pracy i kopanie

- ang. *proof of work*, PoW
- dowodem jest wykonanie pewnej pracy, najczęściej zużywanie mocy obliczeniowej
- bazują na losowości
- prawdopodobieństwo wykonania pracy zależy od dostarczonej mocy obliczeniowej
- proces ten nazywany jest zazwyczaj **kopaniem** ang. *mining*
- transakcje trafiają co węzłów sieci, które analizują i potwierdzają blok transakcji
- potwierdzenie bloku polega na rozwiązaniu trudnego problemu matematycznego – wymaga zaangażowania mocy obliczeniowej
- kto pierwszy ten lepszy, kto pierwszy ten dostaje wynagrodzenie
- często kopiący łączą się w grupy (*pools*) i dzielą zyskiem

Dowód stawki

- ang. *proof of stake*, PoS, wirtualne kopanie
- użytkownicy zgłaszają się jako potwierdzający i wnoszą swoje środki
- z odpowiednim prawdopodobieństwem, proporcjonalnym do ilości środków, wybierany jest węzeł zatwierdzający transakcję
- jeśli jej nie zatwierdzi w określonym czasie to wybierany jest kolejny węzeł
- jest wiele wariantów tego typu algorytmów
  - stawka zależna od wieku środków
  - nagrody za blok, kary za nieprawidłowe działanie
  - wprowadzenie głosowania w węzłach
- nie ma potrzeby **zużywania energii** na cele zabezpieczania bloków
- nie ma potrzeby emisji dużej ilości nowych jednostek

Inne mechanizmy

- **dowód aktywności** ang. *proof of activity* – łączy mechanizmy dowodu pracy oraz dowodu stawki
- **dowód spalenia** ang. *proof of burn* – opłata za potwierdzenie bloku
- **dowód pojemności** ang. *proof of capacity* – uzależnienie od posiadanych zasobów przestrzenii dyskowej
- **dowód upływającego** czasu ang. *proof of elapsed time* – wykorzystuje zaufany sprzęt do losowej symulacji dowodu pracy (przez co nie zużywa tyle energii)
- …

Kryptowaluta

- ang. *cryptocurrency*
- system rozliczeń bazujący na mechanizmach kryptograficznych
- przykładem jest bitcoin ₿
- zazwyczaj w jednostkach umownych
- kontrola nad portfelem realizowana jest najczęściej przez mechanizm podpisu cyfrowego
- kryptowaluta nie jest pieniądzem elektronicznym
- w wielu krajach prawnie nie jest walutą
- każdy może utworzyć własną kryptowalutę
- problemem jest tylko to **kto będzie chciał jej używać**
- blockchain jest często wykorzystywany do budowania kryptowalut

Ethereum

- projekt mający na celu uogólnioną implementację bazy transakcyjnej umożliwiającą realizację bezpiecznych transakcji pomiędzy niezaufanymi jednostkami
- założenia projektu i zasady działania opisane są w dokumencie *Yellow Paper*
- wartością w sieci jest wewnętrzna waluta **Ether (ETH)**
  - 1 ETH = 10^{18} Wei
  - 1 Szabo = 10^{12} Wei
  - 1 Finney = 10^{15} Wei
- *New York Times*: *„a single shared computer that is run by the network of users and on which resources are parceled out and paid for by Ether”*
- sieć wystartowała 30 lipca 2015

Architektura Ethereum

- wykorzystywane są algorytmy: Keccak-256 i ECDSA
- system umożliwia **wykonywanie kodu** – rozproszony komputer
- jako algorytm PoW wykorzystywany jest Ethash – algorytm jest skomplikowany pamięciowo (co utrudnia wykorzystanie dedykowanego sprzętu)
- jako algorytm konsensusu wykorzystywany jest GHOST
- wycena realizacji transakcji odbywa się przez naliczenie *gas*
- zlecający proponuje swoją opłatę za *gas* wyrażoną w ETH
- ETH nie należy traktować jak waluty, ale raczej jak **paliwo za korzystanie z blockchain**

Konta w Ethereum

- dwa rodzaje kont
- **konta zewnętrzne** (ang. *external accounts*) – zarządzane są przez operacje na kluczu prywatnym
- **konta kontraktów** (ang. *contract accounts*) – kontrolowane są przez kod, który przechowywany jest razem z kontem
- konta mają swoje adresy:
  - dla kont zewnętrznych adres określany jest na podstawie klucza publicznego
  - dla kont kontraktów adres ma ten sam format i określany jest na podstawie adresu twórcy oraz unikalnej liczby (*nonce*) zleconych przez niego transakcji
  - adresy mogą mieć sumę kontrolną wyrażaną wielkością liter

Inteligentne kontrakty

- ang. *smart contracts*
- przeniesienie **idei prawa, zależności ekonomicznych i społecznych** do świata cyfrowego
- kontrakt jest tworzony przez wysłanie transakcji z pustym polem odbiorcy
- zawiera kod bajtowy do wykonania przez maszynę wirtualną EVM
- widzą aktualny stan danych w blockchain
- zwracją dane do umieszczenia w bloku
- różne narzędzia do tworzenia kontraktów
- języki: Solidity, Serpent, LLL
- http://etherscripter.com
- **wyrocznia** (ang. *oracle*) dla kontraktu

Kontrakt tokenu

```
contract MyToken {
    /* tablica zawierająca salda */
    mapping (address => uint256) public balanceOf;

    /* konstruktor kontraktu */
    function MyToken(uint256 initialSupply) {
        balanceOf[msg.sender] = initialSupply;  // właściciel otrzyma początkowe tokeny
    }

    /* wykonanie transferu środków */
    function transfer(address _to, uint256 _value) {
        if (balanceOf[msg.sender] < _value) throw;           // sprawdzenie salda
        if (balanceOf[_to] + _value < balanceOf[_to]) throw; // sprawdzenie przepełnienia
        balanceOf[msg.sender] -= _value;                     // zmiana salda zlecającego
        balanceOf[_to] += _value;                            // zmiana salda odbierającego
    }
}
```

Zastosowania

- baza jako dowód istnienia, posiadania, przynależności, zdarzenia
- baza zarządzająca kontraktami, baza **tworząca społeczność**
- przechowywanie dowolnych, wymiennych wartości (systemy lojalnościowe, wirtualne waluty, jednostki reprezentujące liczbę biletów, minut)
- powiązania adresów z wartością w świecie realnym (akcje, złoto, banknoty, …), powiązanie przynależności
- prawa autorskie
- historia wypożyczeń
- zakłady (loterie)
- ubezpieczenia
- głosowanie
- ***blockchain hype*** – blockchain do wszystkiego!
- co z danymi poufnymi (dane medyczne, wrażliwe, finansowe)?
- rozmiar bazy danych (media, filmy, muzyka)?

Polecane materiały

Community, Bitcoin. *Bitcoin Wiki*. https://en.bitcoin.it/wiki/Main_Page.

Ethereum Blog. https://blog.ethereum.org/.

Ethereum Frontier Guide. https://www.gitbook.com/book/ethereum/frontier-guide/.

Ethereum Homestead Documentation. http://www.ethdocs.org/en/latest/.

Ethereum Project. https://www.ethereum.org/.

Pietrosanti, Fabio. *Not every elliptic curve is the same: trough on ECC security*. http://infosecurity.ch/20100926/not-every-elliptic-curve-is-the-same-trough-on-ecc-security/.

Solidity. https://solidity.readthedocs.io/en/develop/.

Wardyński i Wspólnicy. *Blockchain, inteligentne kontrakty i DAO*. http://www.codozasady.pl/.

Wood, Gavin. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. http://yellowpaper.io/.

http://www.sages.com.pl/

Jak uruchomić prywatny blockchain i poeksperymentować z kontraktami dowiesz się z naszego bloga

http://www.sages.com.pl/blog/