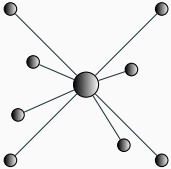
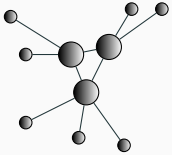
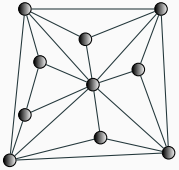
Systemy transakcyjne







Jak zapewnić wiarygodność transakcji?

zaufane jednostki sieci

co zrobić gdy ich nie ma

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

Dla dowolnej wiadomości wartością funkcji jest ciąg bitów o **określonej długości**

→ 01d58360dd9f4f295cd2c09171c798905cd4be3c7fd31d55985eb7c11f2709f6

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

Użytkownik generuje losową parę kluczy: **prywatny** i **publiczny**

Integralny rejestr z uwierzytelnieniem transakcji

⟶ Anna 50 PLN
⟶ Andrzej 50 PLN
dbde8e92f4e44724l8239795a29c0a5e931710c8b7016b2cde25d818c970c41a

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

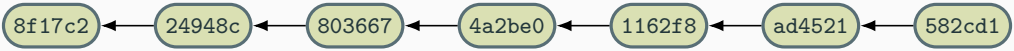
6d340b451... ⟶ 2db36af02... 10 PLN 9604c2c1f51ee2376deb52719e6a678...
2db36af02... ⟶ Marcin 20 PLN d68a612281f4958ebbf5ecb85134575...
065d58a27162f67714b160ec63e39c71b6a1d207d77179d0bc8d109ed0f520f4

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

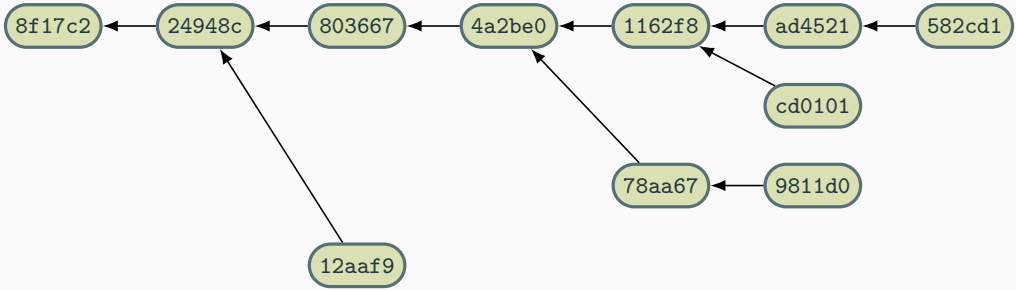
Integralny rejestr z uwierzytelnieniem transakcji

```
⟶ 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
```

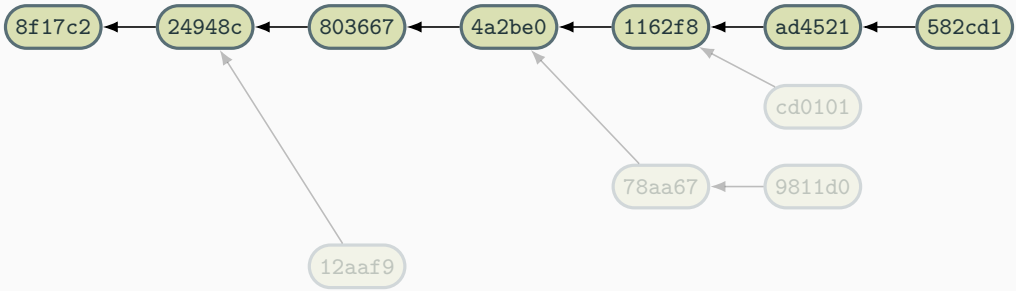
Blockchain



Blockchain


8f17c2
24948c
803667
4a2be0
1162f8
ad4521
582cd1
cd0101
78aa67
9811d0
12aaf9

Blockchain


8f17c2
24948c
803667
4a2be0
1162f8
ad4521
582cd1
cd0101
78aa67
9811d0
12aaf9

Algorytm konsensusu

rozwiązanie problemu uzgadniania przez zbiór jednostek jednej wartości spośród zbioru wartości zaproponowanych wstępnie przez te jednostki

dowód pracy i dowód stawki

Kryptowaluty

system rozliczeń bazujący na mechanizmach kryptograficznych

każdy może utworzyć własną kryptowalutę

problemem jest tylko to **kto będzie chciał jej używać**

Blockchain w skrócie

- blockchain to łańcuch bloków udostępniany w środowisku rozproszonym za pomocą mechanizmów P2P
- każdy z węzłów sieci przechowuje kopię łańcucha
- integralność łańcucha jest zapewniona poprzez wyliczenie funkcji skrótu z uwzględnieniem skrótu poprzedniego bloku
- zlecane transakcje są uwierzytelniane za pomocą mechanizmu podpisu cyfrowego
- utrata klucza prywatnego lub transakcja na nieprawidłowy klucz publiczny może prowadzić do utraty środków/dostępu do środków
- 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

Ethereum

wartością w sieci jest Ether (ETH)

1 ETH = 10^{18} **Wei**

1 Szabo = 10^{12} **Wei**

1 Finney = 10^{15} **Wei**

wraz z transakcją można przechowywać dane

Ether to paliwo dla korzystania z blockchain

sieć publiczna wystartowała 30 lipca 2015

Blok genesis

- każdy blockchain musi mieć swój początek
- blok genesis to pierwszy blok, nie ma poprzednika
- użytkownicy ufają mu z zasady, a zasada jest wbudowana w oprogramowanie

```
{
  "difficulty": "0x4000",
  "gasLimit": "0x8000000",
  "config": { "chainId": 100 },
  "alloc": { "afee6fe96dd557ce8e3cd6d57d7c66eab4a15820": {
    "balance": "10000000000000000000" }
  }
}
```

Dane w blockchain

blockchain to rozproszona baza danych

sens i interpretacja tych danych zależy od konkretnej implementacji

spójny rejestr danych różnego typu

Umieśćmy w nim program komputerowy

Ethereum pozwala na wykonywanie kodu

Inteligentne kontrakty
Smart contracts

tworzony przez wysłanie transakcji z pustym polem odbiorcy
widzą aktualny stan danych w blockchain
zwracają dane do umieszczenia w bloku

nie uruchamiają się same z siebie

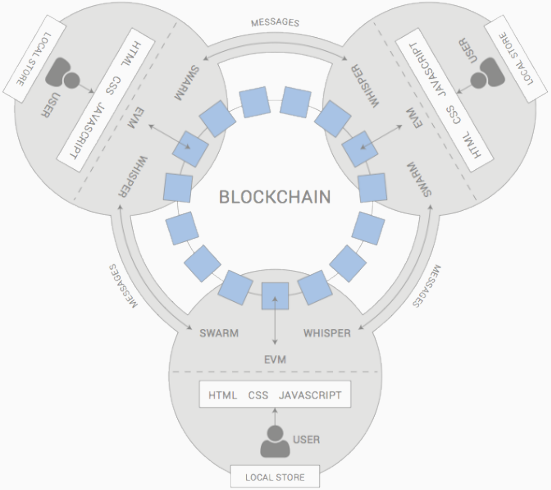
Pierwszy kontrakt

```
pragma solidity >=0.4.0 <0.7.0;

contract Greeter {
    string greeting;

    constructor(string memory _greeting) public {
        greeting = _greeting;
    }

    function greet() public view returns (string memory) {
        return greeting;
    }

    function setGreeting(string memory _greeting) public {
        greeting = _greeting;
    }
}
```

Kontrakt tokenu

```
pragma solidity >=0.4.0 <0.7.0;

contract Token {
    mapping (address => uint256) public balanceOf;

    constructor(uint256 initialSupply) public {
       balanceOf[msg.sender] = initialSupply;
    }

    function transfer(address _to, uint256 _value) public {
        balanceOf[msg.sender] -= _value;
        balanceOf[_to] += _value;
    }
}
```

Ekosystem Ethereum – web3



za *http://ethereum.stackexchange.com*

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
- historia wypożyczeń, lokalizacji, …
- prawa autorskie
- zakłady (loterie)
- ubezpieczenia
- głosowanie

blockchain hype

blockchain do wszystkiego

! to nie technologia ale strategia !

co z danymi poufnymi (dane medyczne, wrażliwe, finansowe)
rozmiar bazy danych (media, filmy, muzyka)
połączenie ze światem realnym

wyrocznia

ĐApps

zdecentralizowana aplikacja

decentralized application

frontend + kontrakty

użytkownik nie musi wiedzieć, że pod spodem jest blockchain

gdzie przechowywać frontend?

częścią blockchain może być kontrakt dbający o spójność frontendu

Trwały nośnik

materiał lub urządzenie umożliwiające przechowywanie informacji w sposób umożliwiający dostęp w przyszłości

pozwala na odtworzenie przechowywanych informacji w niezmienionej postaci

Dowód istnienia

```
struct Document {  uint hash;  uint time; }

uint[] public documentsIds;
mapping(uint => Document) public documents;

function registerDocument(uint _id, uint _hash) public {
    require(!isDocumentExists(_id));
    documentsIds.push(_id);
    documents[_id].hash = _hash;
    documents[_id].time = now;
    emit DocumentRegistration(msg.sender, _id, _hash);
}

function getDocumentsCount() public view returns(uint count) {
    return documentsIds.length;
}

function isDocumentExists(uint _id) public view returns(bool exists) {
    return documents[_id].time != 0;
}

event DocumentRegistration(address _who, uint _id, uint _hash);
```

Podsumowanie

- blockchain to rozproszona baza danych, rozproszony rejestr, sieć P2P wykorzystana do przyrostowego kolekcjonowania danych; blockchain jako gotowe narzędzie
- blockchain to społeczność zbudowana wokół publicznych blockchain, entuzjaści technologii
- blockchain to kryptowaluty i zjawiska w nich zachodzące, rynek inwestycji, narzędzie do zarabiania; blockchain to narzędzie do przepływu środków
- co się stanie po krachu na kryptowalutach, jak to wpłynie na blockchain jako rozwiązanie inżynierskie/bazę danych?
- kto ponosi odpowiedzialność za błędy w kontraktach
- kto ponosi odpowiedzialność za kontrakt niezgodny z prawem
- **baza z gotową kopią zapasową i niezawodną infrastrukturą**