Inteligentne kontrakty oparte o blockchain

Mateusz Zaborski
M.Zaborski@mini.pw.edu.pl

Plan prezentacji

- Technologia blockchain
  - Bitcoin
  - Rozproszony rejestr
  - Ethereum
- Inteligentne kontrakty
- Symulacja wieloagentowa

Bitcoin i blockchain

Bitcoin

- Satoshi Nakamoto, 2008
- Brak słowa „blockchain”
- Zaprezentowana koncepcja
  - Rozproszony rejestr
  - Transakcja
  - *Proof-of-work*

Bitcoin: A Peer-to-Peer Electronic Cash System

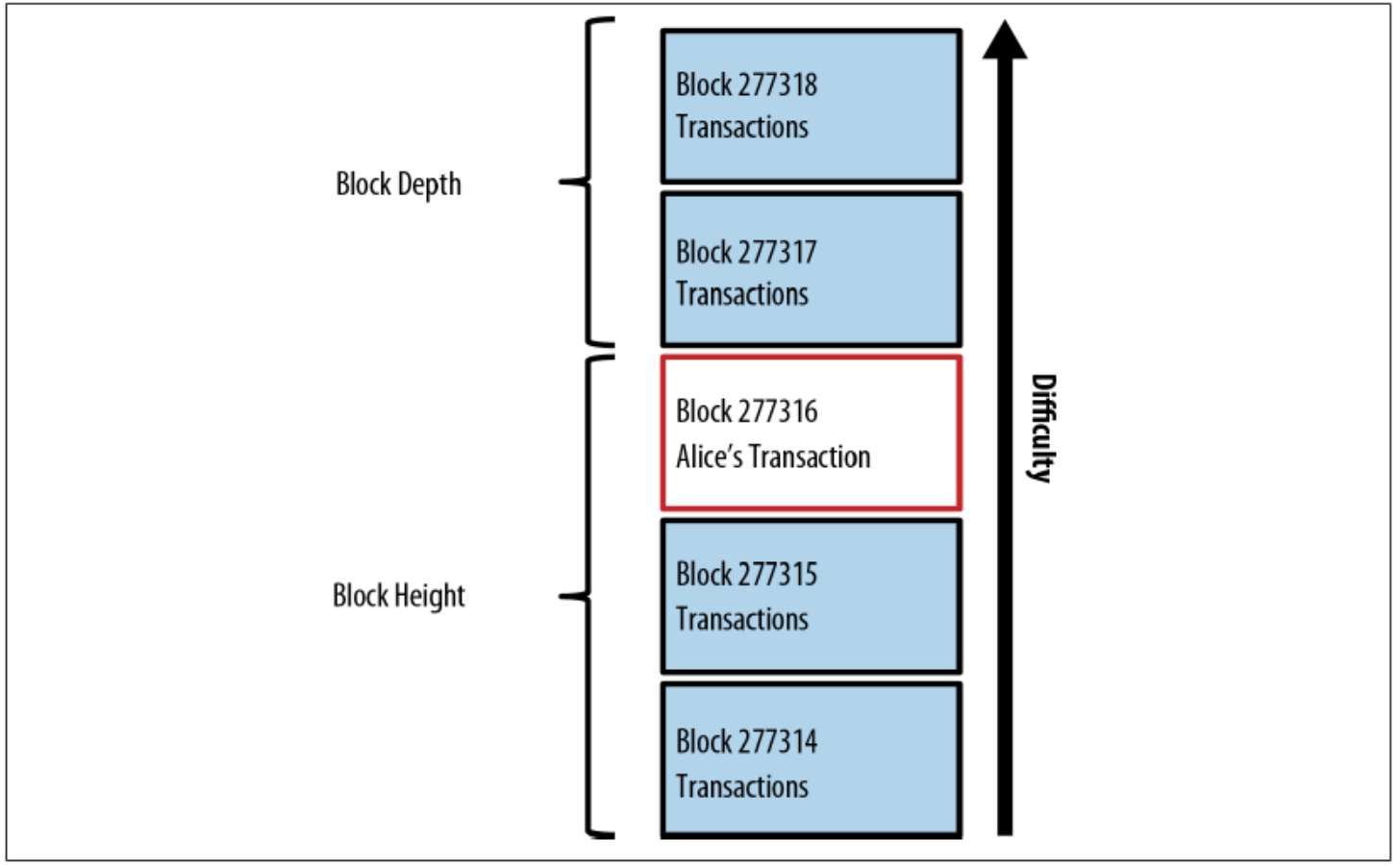
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

„A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.”

Bitcoin – koncepcja blockchain (1)

1. Nowe transakcje są przesyłane do wszystkich węzłów
2. Każdy węzeł gromadzi transakcje w jeden blok
3. Każdy węzeł może pracować nad znalezieniem *proof-of-work* dla jego bloku
4. Gdy węzeł znajdzie *proof-of-work*, przekazuje tę informacje innym
5. Węzeł akceptuje blok, tylko jeśli jest on poprawny
6. Akceptacja oznacza pracę nad nowym blokiem

Bitcoin – koncepcja blockchain (2)

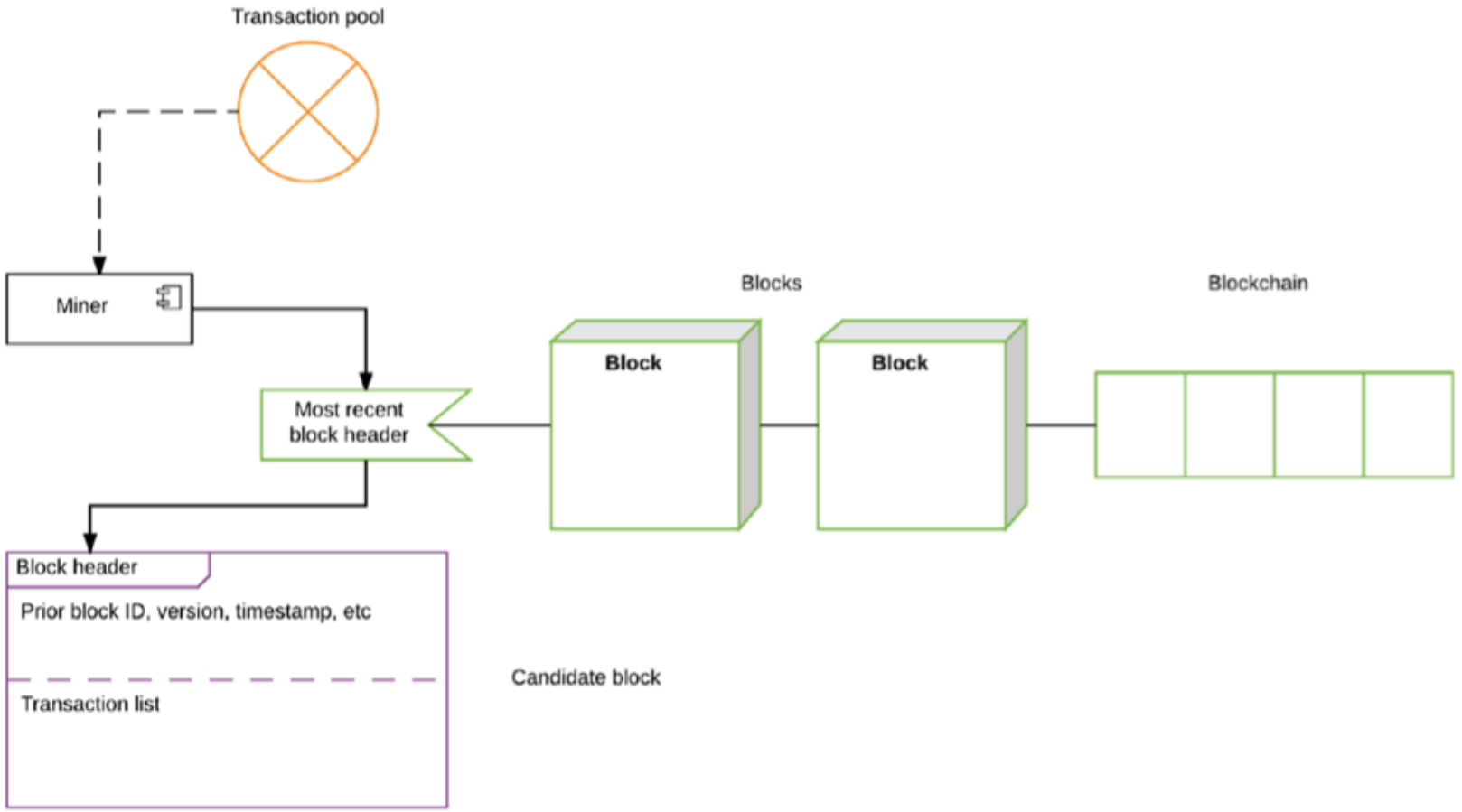


Źródło: A. M. Antonopoulos, Mastering Bitcoin, 2015

Bitcoin – role węzła

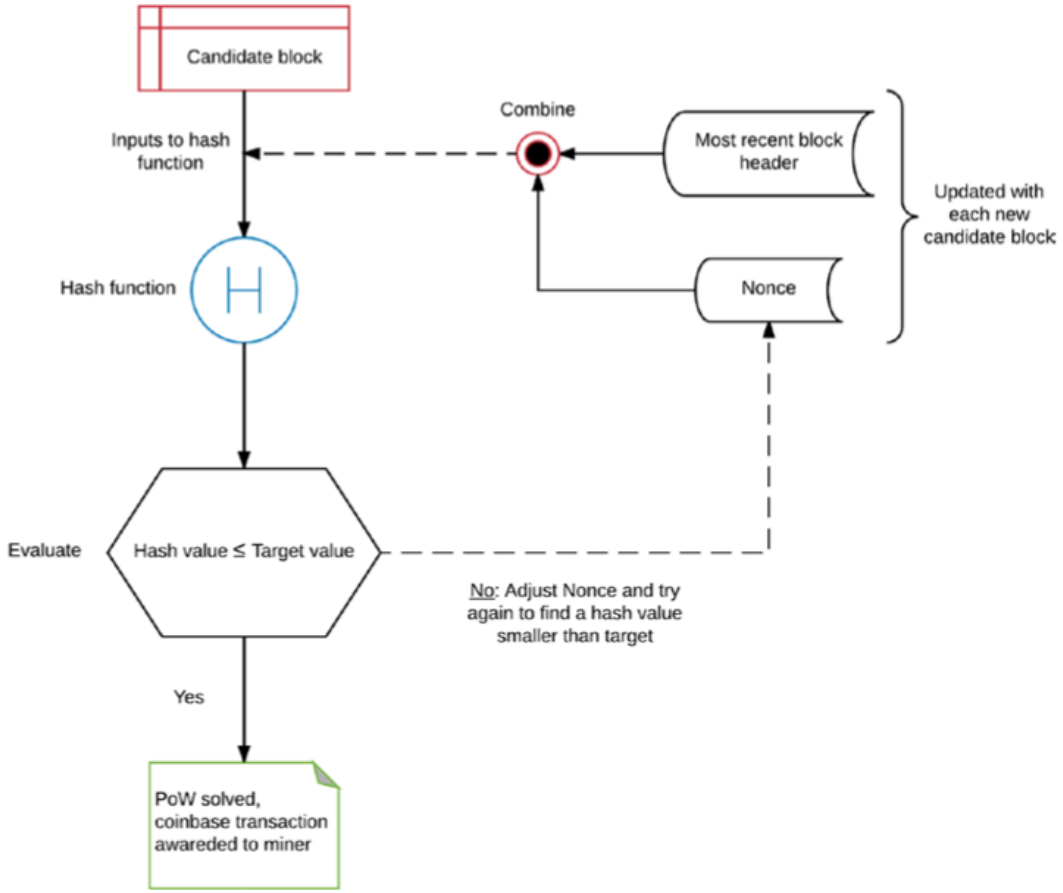
- Portfel
- Górnik
- Baza danych blockchaina
- *Routing*

Bitcoin – kopanie (1)



Źródło: Blockchain Enabled Applications, V. Dhillon, D. Metcalf, M.Hooper, 2017

Bitcoin – kopanie (2)



Źródło: Blockchain Enabled Applications, V. Dhillon, D. Metcalf, M.Hooper, 2017

Blockchain – własności

- Publiczny rejestr
- Anonimowe konta
- Brak centralnego serwera
- Brak centralnego uwierzytelniania
- Zabezpieczenie – kryptografia
- Każda transakcja zostaje na zawsze

Blockchain – Ethereum

- Vitalik Buterin, 2013
- Oparty o Bitcoin
- Platforma do tworzenia zdecentralizowanych aplikacji
- Kryptowaluta – Ether
- Możliwe inteligentne kontrakty
  - *ICO - Initial Coin Offering*

Blockchain – problemy i zagrożenia

- Skalowalność
- Wydajność sieci
- Wyścigi w gałęziach
  - Niepewność transakcji
- Zużycie energii

Inteligentne kontrakty

Inteligentny kontrakt *(ang. smart contract)*

- Program (funkcje i dane)
- Posiada numer – adres, konto
- Jawność
- Duża elastyczność

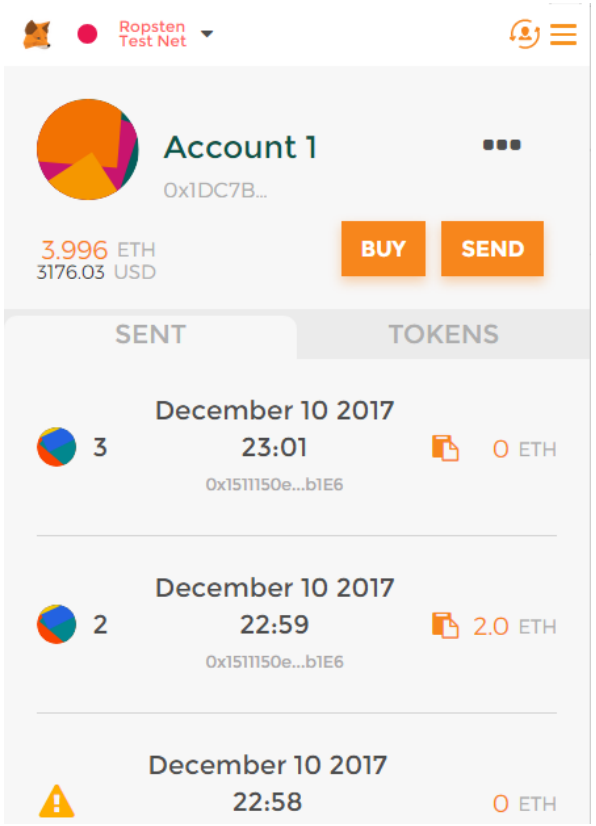
Inteligentny kontrakt – techniczne możliwości

- Przechowywanie danych
- Odbieranie środków (Ether)
- Wysyłanie środków (Ether)
- Sprawdzanie warunków (np. czasu)
- Zmiana swojego stanu

Inteligentny kontrakt – tworzenie (1)

- Prosty kontrakt – *Hello World*
- Wypisuje komunikat przy odebraniu „przelewu”
- Język - Solidity

```
1  contract HelloWorld {
2      event log_string(bytes32 log); // Event
3
4      function () { // Fallback Function
5          log_string("Hello World and MiNI!");
6      }
7  }
```



Inteligentny kontrakt – tworzenie (2)

Adres 0x1DC7BdaE60cDB1b039461E135F61501635502dAb

TxHash	Block	Age	From		To	Value	[TxFee]
0xa0624210ac0e3b...	2241873	9 days 1 hr ago	0x1dc7bdae60cdb1...	OUT	0x1511150eaf4c5bd...	0 Ether	0.000464121
0xaaf4f816d040bd6...	2241864	9 days 1 hr ago	0x1dc7bdae60cdb1...	OUT	0x1511150eaf4c5bd...	2 Ether	0.001136268
0x8d0cacf744cbb6e...	2241861	9 days 1 hr ago	0x1dc7bdae60cdb1...	OUT	0x1511150eaf4c5bd...	2 Ether	0.00042084
0x88a47f5fec1abd6...	2241821	9 days 1 hr ago	0x1dc7bdae60cdb1...	OUT	Contract Creation	0 Ether	0.0018711492
0x802ae90f9dba781...	2241722	9 days 1 hr ago	0x81b7e08f65bdf56...	IN	0x1dc7bdae60cdb1...	1 Ether	0.00042
0xf1da2bed38e62a2...	2241722	9 days 1 hr ago	0x81b7e08f65bdf56...	IN	0x1dc7bdae60cdb1...	1 Ether	0.00042
0x8187c377e6d688...	2241722	9 days 1 hr ago	0x81b7e08f65bdf56...	IN	0x1dc7bdae60cdb1...	1 Ether	0.00042
0x555205676a1507f...	2241721	9 days 1 hr ago	0x81b7e08f65bdf56...	IN	0x1dc7bdae60cdb1...	1 Ether	0.00042

https://ropsten.etherscan.io/

Inteligentny kontrakt – tworzenie (3)

Block #2241821

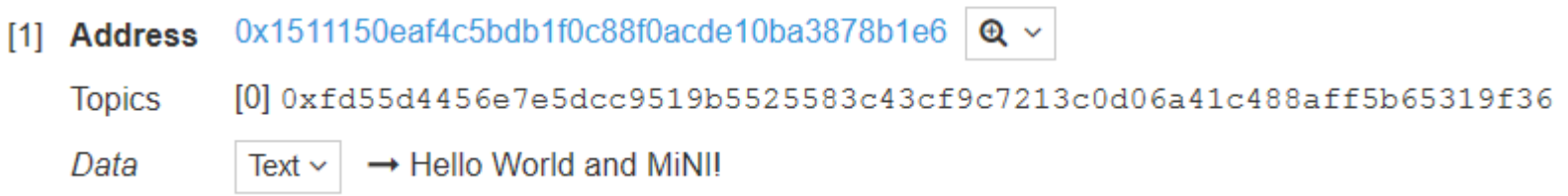
TxHash	Block	Age	From		To	Value	[TxFee]
0xc7f55a8571b8aed...	2241821	9 days 1 hr ago	0x3c41ab9fa4bba5f...		0x527fcb2a7a776af...	0 Ether	0.0011375
0x88a47f5fec1abd6...	2241821	9 days 1 hr ago	0x1dc7bdae60cdb1...		Contract Creation	0 Ether	0.00187114
0x24ed75a157c673...	2241821	9 days 1 hr ago	0xdaa1a6c972d4b8...		0x21ec0699ae84e3...	0 Ether	0.00105189

https://ropsten.etherscan.io/

Inteligentny kontrakt – tworzenie (4)

Adres (kontrakt) 0x1511150eaf4c5bdb1f0c88f0acde10ba3878b1e6

Transaction Receipt Event Logs



https://ropsten.etherscan.io/

Inteligentny kontrakt – inny przykład

```
1  contract Token {
2
3      bool isStarted;
4      mapping (address => uint256) public state;
5
6      function Token() { isStarted = false; }
7
8      function () public payable {
9          if(isStarted == false) {
10             state[msg.sender] = 1000;
11             isStarted = true;
12         }
13         else {
14             state[msg.sender] += 200;
15         }
16         log0(bytes32(state[msg.sender]));
17     }
18 }
```

Transaction Receipt Event Logs

[1] **Address** 0x908e5fea976ee2a7fa40ce03a5c240f4d3d53ac7

Data Num → 1200

https://ropsten.etherscan.io/

Inteligentny kontrakt - *zastosowania*

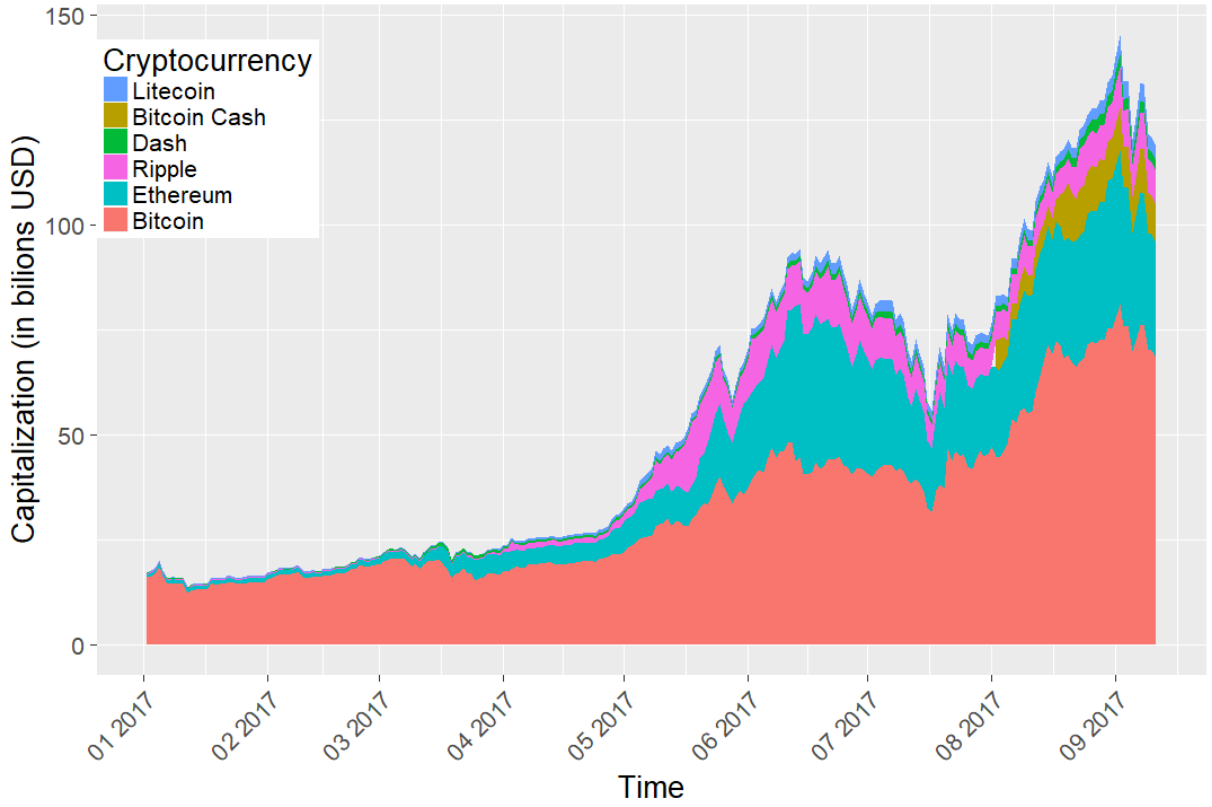
- Przeniesienie własności
- Przekazanie praw / pełnomocnictw
- Głosowanie
- Automatyczne naliczanie opłat
- Tokeny
- *ICO – Initial Coin Offering*
- Rejestr płatności
- Automatyczne płatności
- Licytacje

Inteligentny kontrakt - *zagrożenia*

- Zmienność rynku
- Brak możliwości zmiany
- Możliwość utraty kontroli
  - Strata klucza prywatnego
- Możliwość ataku
  - Przechwycenie klucza prywatnego

Symulacja wieloagentowa

Kapitalizacja rynku kryptowalut



Cel badawczy

- Opracowanie narzędzi i metod do analizy rynków kryptowalut opartych o blockchain
  - Bitcoin
  - Ethereum
- Zagadnienia badawcze
  - Transakcje
  - Zaufanie
  - Cena
  - Decyzje
  - Ryzyko

Przegląd literatury

- Techniczne aspekty mechanizmu rozproszonego konsensusu
- Determinanty rynkowe prowadzące do rozwoju kryptowalut
- Pojawienie się i rozwój rynku Bitcoin
- Modelowanie interakcji aktorów na rynku blockchain

Koncepcja i plan badań

1. Analiza empiryczna rynków opartych o blockchain
2. Stworzenie ogólnego modelu rynku
3. Stworzenie biblioteki do symulacji wieloagentowych rynków (język Julia)
4. Implementacja ogólnego modelu
5. Kalibracja modelu w oparciu o dane empiryczne, weryfikacja
6. Symulacje oraz analiza wyników – determinant mechanizmów cenowych
7. Eksploracja numeryczna przestrzeni parametrów w poszukiwaniu wzorców cenowych

Typy walut

- Pieniądz fiducjarny
  - określenie wartości kryptowaluty
- Kryptowaluta wspierająca inteligentne kontrakty
- Kryptowaluta niewspierająca inteligentnych kontraktów

Hipotezy badawcze

- Wielkość transakcji jest dodatnio skorelowana z zaufaniem
  - Sprzężenie zwrotne pomiędzy wolumenem a zaufaniem
- Mechanizm sprzężenia zwrotnego jest wyznacznikiem ceny
- Symulacja wieloagentowa pozawala analizować złożone zależności oparte o mechanizm blockchain

Niezależni aktorzy

Role / agenty	**Opis / cele**
Górnicy / kopalnie kryptowalut	Osiągają zysk z „kopania” waluty
Konsumenci (użytkownicy kryptowalut)	Dokonują ‚płatności”
Spekulanci	Dokonują szybkich zleceń kupna-sprzedaży
Giełdy wymiany kryptowalut	Łączą kupujących i sprzedających celem ustalenia ceny wymiany
Twórcy inteligentnych kontraktów	Dostarczają inteligentne kontrakty
Uczestnicy inteligentnych kontraktów	Biorą udział w inteligentnych kontraktach
Inwestorzy długoterminowi	Lokują kapitał w kryptowalucie w oczekiwaniu zysku z powodu wzrostu jej wartości

Wnioski

- Inteligentne kontrakty są działającą realizacją pożądanych pomysłów
  - Niebezpieczne rozwiązanie
- Rynki oparte o blockchain oraz blockchain wymaga modelowania
  - Brak dostępnych narzędzi
  - Aktualne, nieznane wcześniej problemy

Źródła

1. Bitcoin: A Peer-to-Peer Electronic Cash System, Nakamoto, 2008
2. Mastering Bitcoin, A. M. Antonopoulos, 2015
3. Blockchain Enabled Applications, V. Dhillon, D. Metcalf, M.Hooper, 2017
4. http://www.ethdocs.org
5. http://www.ethereum.org
6. http://coinmarketcap.com