Blockchain
i jego zastosowania w edukacji

Adam Sołtysik

Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki
Seminarium: Systemy Rozproszone

12 października 2017

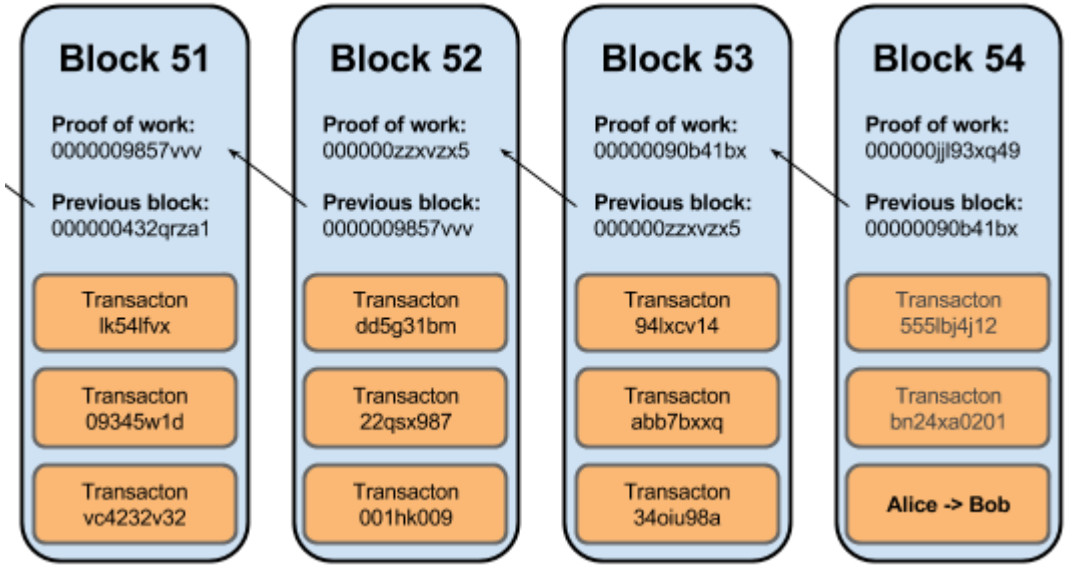
Co to jest blockchain?

Co to jest blockchain?

- łańcuch przechowujący pełną historię transakcji

Co to jest blockchain?

- łańcuch przechowujący pełną historię transakcji



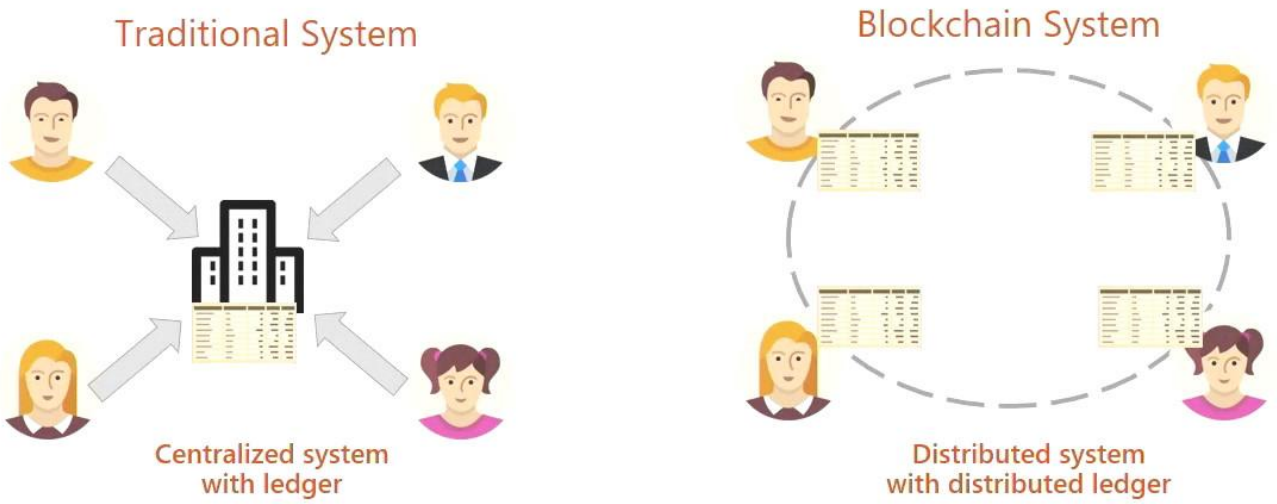
https://www.ybrikman.com/assets/img/blog/bitcoin/bitcoin-block-chain-verified.png

Co to jest blockchain?

- łańcuch przechowujący pełną historię transakcji
- zdecentralizowana baza danych oparta na sieci P2P

Co to jest blockchain?

- łańcuch przechowujący pełną historię transakcji
- zdecentralizowana baza danych oparta na sieci P2P



https://www.youtube.com/watch?v=dPF2jA0JUYc

Co to jest blockchain?

- łańcuch przechowujący pełną historię transakcji
- zdecentralizowana baza danych oparta na sieci P2P
- dane zabezpieczone kryptograficznie, transakcje są niemożliwe do podrobienia ani zmiany po wysłaniu

Trochę historii

http://www.forexnewsnow.com/wp-content/uploads/2016/10/Bitcoin.jpg

Trochę historii

- listopad 2008 – artykuł autorstwa Satoshi Nakamoto

Trochę historii

- listopad 2008 – artykuł autorstwa Satoshi Nakamoto
- styczeń 2009 – powstaje sieć bitcoina

Trochę historii

- listopad 2008 – artykuł autorstwa Satoshi Nakamoto
- styczeń 2009 – powstaje sieć bitcoina
- maj 2010 – pierwsza transakcja ustalająca wartość bitcoina (2 pizze za 10000BTC)

Trochę historii

- listopad 2008 – artykuł autorstwa Satoshi Nakamoto
- styczeń 2009 – powstaje sieć bitcoina
- maj 2010 – pierwsza transakcja ustalająca wartość bitcoina (2 pizze za 10000BTC)

Bitcoin Forum > Economy > Marketplace (Moderators: Cyrus, hilariousandco) > **Pizza for bitcoins?**

« previous topic next topic »

Pages: [1] 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 ... 73 » print

Author	Topic: Pizza for bitcoins? (Read 669949 times)
laszlo Full Member Activity: 199	Pizza for bitcoins? May 18, 2010, 12:35:20 AM #1 I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy! I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire. If you're interested please let me know and we can work out a deal. Thanks, Laszlo BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

https://bitcointalk.org/index.php?topic=137.0

Trochę historii

Trochę historii

- listopad 2008 – artykuł autorstwa Satoshi Nakamoto
- styczeń 2009 – powstaje sieć bitcoina
- maj 2010 – pierwsza transakcja ustalająca wartość bitcoina (2 pizze za 10000BTC)
- 2011 – zaczynają powstawać kolejne kryptowaluty

Trochę historii

http://bitemycoin.com/wp-content/uploads/2017/07/what-is-an-altcoin.jpg

Jak to działa?

Jak to działa?

- transakcja zostaje podpisana kluczem prywatnym i rozesłana w sieci P2P

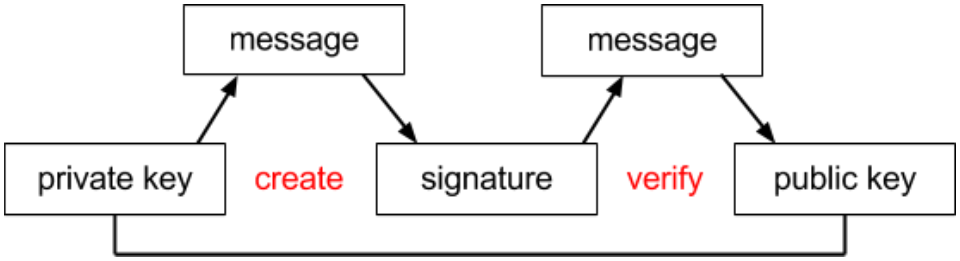
Jak to działa?

- transakcja zostaje podpisana kluczem prywatnym i rozesłana w sieci P2P

Transaction Messages

		Digital Signature
Alice → Bob	5.0 BTC	04323784...
Alice → Dave	12 BTC	88432738...
Alice → Juan	2000 BTC	00328434...
Alice → Bob	14 BTC	19382637...

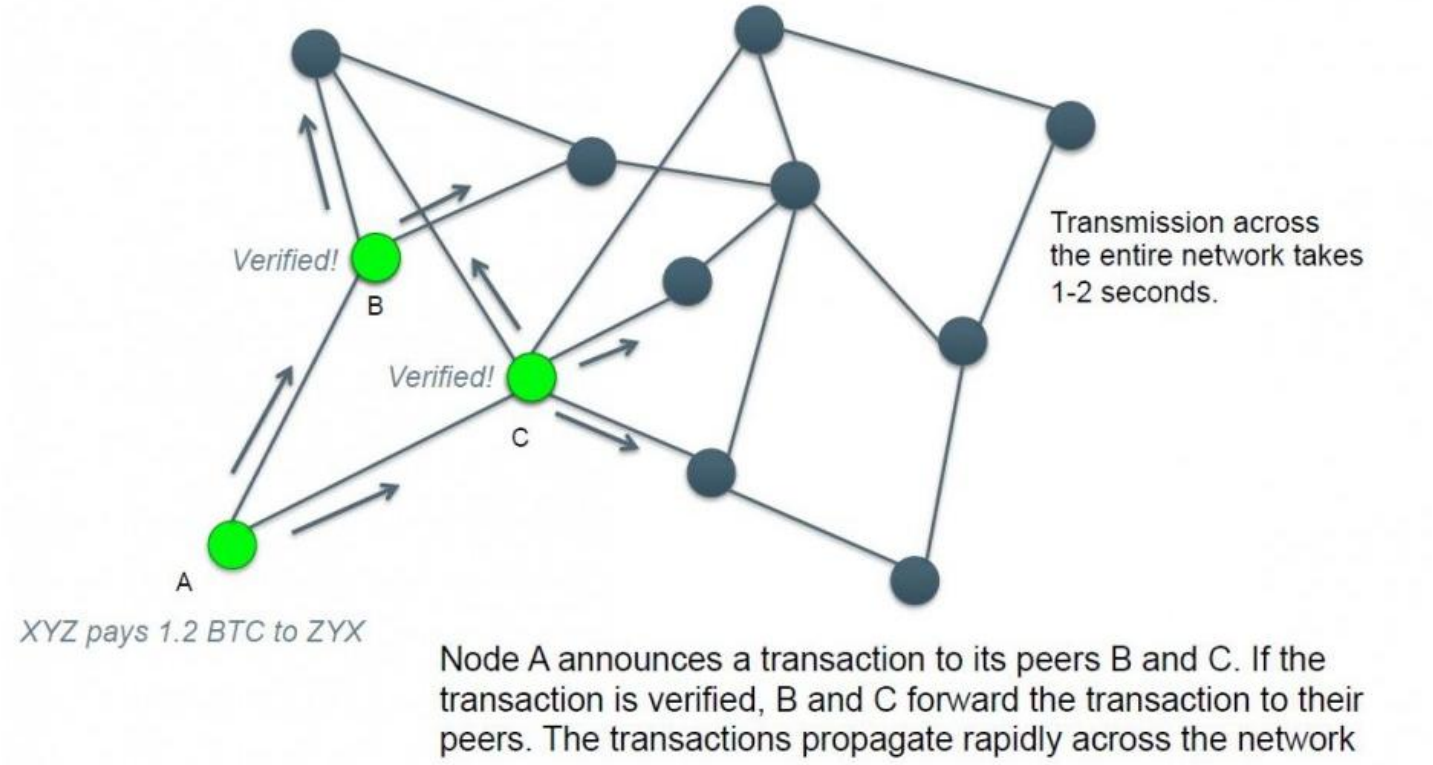
^
different every time



http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Jak to działa?

- transakcja zostaje podpisana kluczem prywatnym i rozesłana w sieci P2P



https://www.actuaries.digital/2015/04/24/bitcoins-banking-and-the-blockchain/

Jak to działa?

- transakcja zostaje podpisana kluczem prywatnym i rozesłana w sieci P2P
- każdy węzeł sieci przechowuje kolejkę wszystkich zweryfikowanych transakcji

Jak to działa?

- transakcja zostaje podpisana kluczem prywatnym i rozesłana w sieci P2P
- każdy węzeł sieci przechowuje kolejkę wszystkich zweryfikowanych transakcji
- stan konta to różnica między otrzymanymi i wydanymi bitcoinami

Jak to działa?

- jak uzgodnić kolejność transakcji?

Jak to działa?

- jak uzgodnić kolejność transakcji?
- każda transakcja zawiera referencje do tzw. inputów i outputów, output jednej transakcji staje się inputem dla następnej

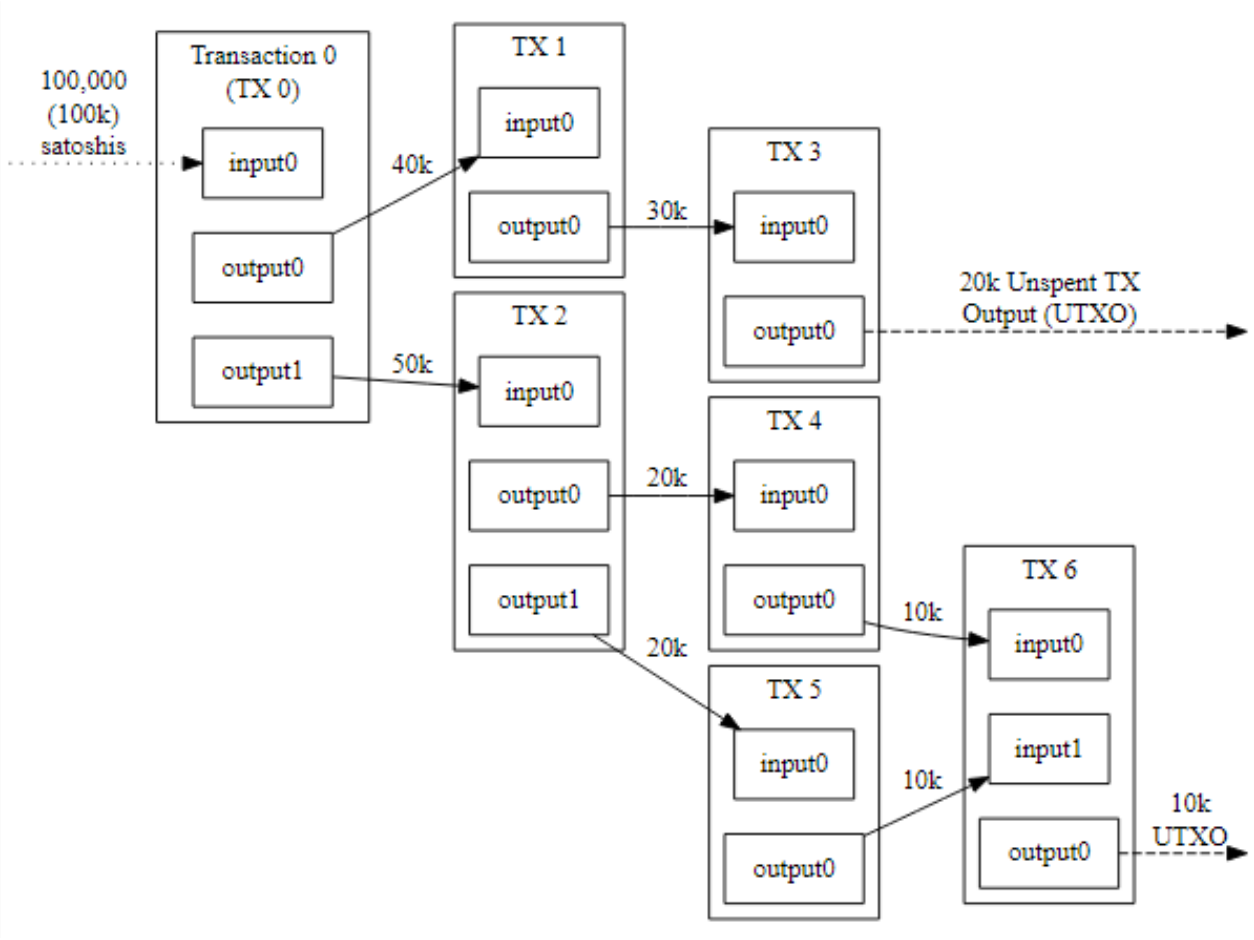
Jak to działa?

- jak uzgodnić kolejność transakcji?
- każda transakcja zawiera referencje do tzw. inputów i outputów, output jednej transakcji staje się inputem dla następnej
- suma inputów = suma outputów + prowizja

Jak to działa?

- jak uzgodnić kolejność transakcji?
- każda transakcja zawiera referencje do tzw. inputów i outputów, output jednej transakcji staje się inputem dla następnej
- suma inputów = suma outputów + prowizja
- zawsze musimy wydać cały input, ale możemy otrzymać resztę

Jak to działa?



https://bitcoin.org/en/developer-guide

Jak to działa?

- jak zapobiec wielokrotnemu wydawaniu tych samych monet?

Proof of Work

Proof of Work

- transakcje są łączone w bloki

Proof of Work

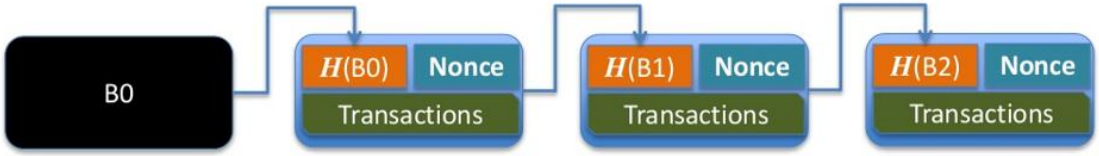
- transakcje są łączone w bloki
- aby blok został dołączony do łańcucha, trzeba go „wykopać”

Proof of Work

- transakcje są łączone w bloki
- aby blok został dołączony do łańcucha, trzeba go „wykopać”
- kopanie polega na znalezieniu takiej wartości dopełnienia (nonce), żeby hash bloku spełniał określony warunek

Proof of Work

- transakcje są łączone w bloki
- aby blok został dołączony do łańcucha, trzeba go „wykopać”
- kopanie polega na znalezieniu takiej wartości dopełnienia (nonce), żeby hash całego bloku spełniał określony warunek



Find a nonce x such that:

SHA-256(SHA-256($r + x$)) < T/d

https://www.slideshare.net/DavidEvansUVa/the-blockchain

Proof of Work

- transakcje są łączone w bloki
- aby blok został dołączony do łańcucha, trzeba go „wykopać”
- kopanie polega na znalezieniu takiej wartości dopełnienia (nonce), żeby hash całego bloku spełniał określony warunek
- jedyna metoda: brute force

Proof of Work

- zwycięzca otrzymuje nagrodę - początkowo 50BTC, dzielone przez 2 co 210000 bloków (aktualnie 12.5BTC), a ponadto prowizje ze wszystkich transakcji

Proof of Work

- zwycięzca otrzymuje nagrodę - początkowo 50BTC, dzielone przez 2 co 210000 bloków (aktualnie 12.5BTC), a ponadto prowizje ze wszystkich transakcji
- łącznie do ~2140 roku zostanie wykopane 21mln bitcoinów

Proof of Work

- zwycięzca otrzymuje nagrodę - początkowo 50BTC, dzielone przez 2 co 210000 bloków (aktualnie 12.5BTC) , a ponadto prowizje ze wszystkich transakcji
- łącznie do ~2140 roku zostanie wykopane 21mln bitcoinów
- co 2016 bloków (2 tygodnie) trudność jest dopasowywana tak, żeby kopanie jednego bloku zajmowało ok. 10 minut

Proof of Work

- wykopany blok jest rozsyłany do sieci i weryfikowany przez pozostałe węzły

Proof of Work

- wykopany blok jest rozsyłany do sieci i weryfikowany przez pozostałe węzły
- górnicy zawsze kopią na szczycie najdłuższego łańcucha jaki znają

Proof of Work

- wykopany blok jest rozsyłany do sieci i weryfikowany przez pozostałe węzły
- górnicy zawsze kopią na szczycie najdłuższego łańcucha jaki znają

https://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/

Proof of Work

- wykopany blok jest rozsyłany do sieci i weryfikowany przez pozostałe węzły
- górnicy zawsze kopią na szczycie najdłuższego łańcucha jaki znają
- wykopany blok nie może zostać zmieniony (ani przepięty na inną gałąź łańcucha) bez ponownego wykonania całej pracy

Zalety

Zalety

- bezpieczeństwo zapewnione dzięki kryptografii

Zalety

- bezpieczeństwo zapewnione dzięki kryptografii
- decentralizacja, brak instytucji pośredniczących

Zalety

- bezpieczeństwo zapewnione dzięki kryptografii
- decentralizacja, brak instytucji pośredniczących
- anonimowość transakcji, brak kontroli przez państwa

Zalety

- bezpieczeństwo zapewnione dzięki kryptografii
- decentralizacja, brak instytucji pośredniczących
- anonimowość transakcji, brak kontroli przez państwa
- niskie opłaty transakcyjne niezależne od wartości przelewu

Zalety

- bezpieczeństwo zapewnione dzięki kryptografii
- decentralizacja, brak instytucji pośredniczących
- anonimowość transakcji, brak kontroli przez państwa
- niskie opłaty transakcyjne niezależne od wartości przelewu
- szybkie przelewy niezależnie od pory dnia

Wady

Wady

- pełna odpowiedzialność zrzucona na użytkowników

Wady

- pełna odpowiedzialność zrzucona na użytkowników
- ograniczona przepustowość, niska wydajność energetyczna

Wady

- pełna odpowiedzialność zrzucona na użytkowników
- ograniczona przepustowość, niska wydajność energetyczna
- mała opłacalność dla transakcji o małej wartości

Wady

- pełna odpowiedzialność zrzucona na użytkowników
- ograniczona przepustowość, niska wydajność energetyczna
- mała opłacalność dla transakcji o małej wartości
- wysoka zmienność cen

Wady

- pełna odpowiedzialność zrzucona na użytkowników
- ograniczona przepustowość, niska wydajność energetyczna
- mała opłacalność dla transakcji o małej wartości
- wysoka zmienność cen
- łatwość wykorzystania do nielegalnych działań

Zagrożenia

Zagrożenia

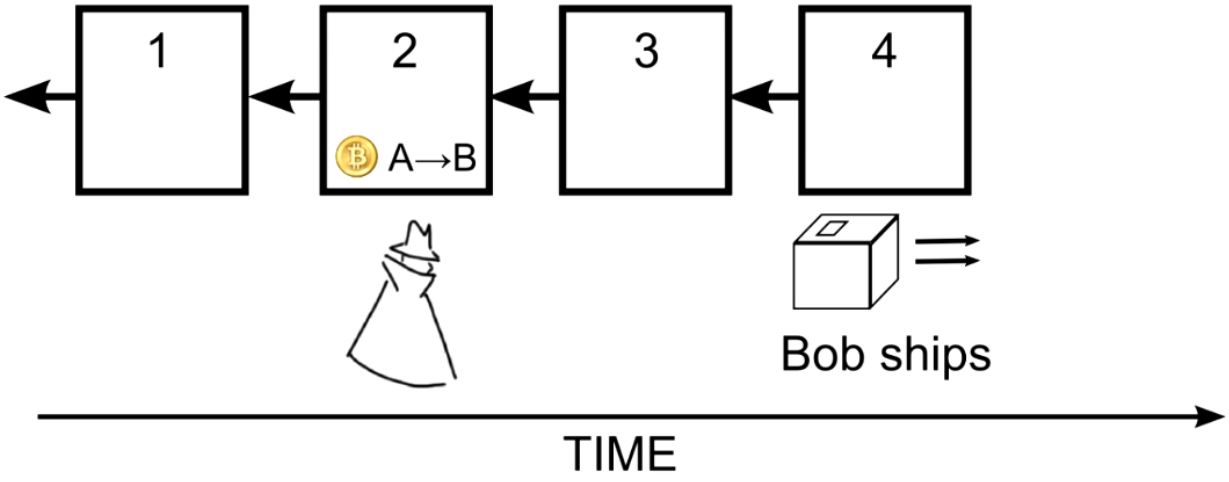
- double spending

Zagrożenia

- double spending
- atak większościowy (51% attack)

Zagrożenia

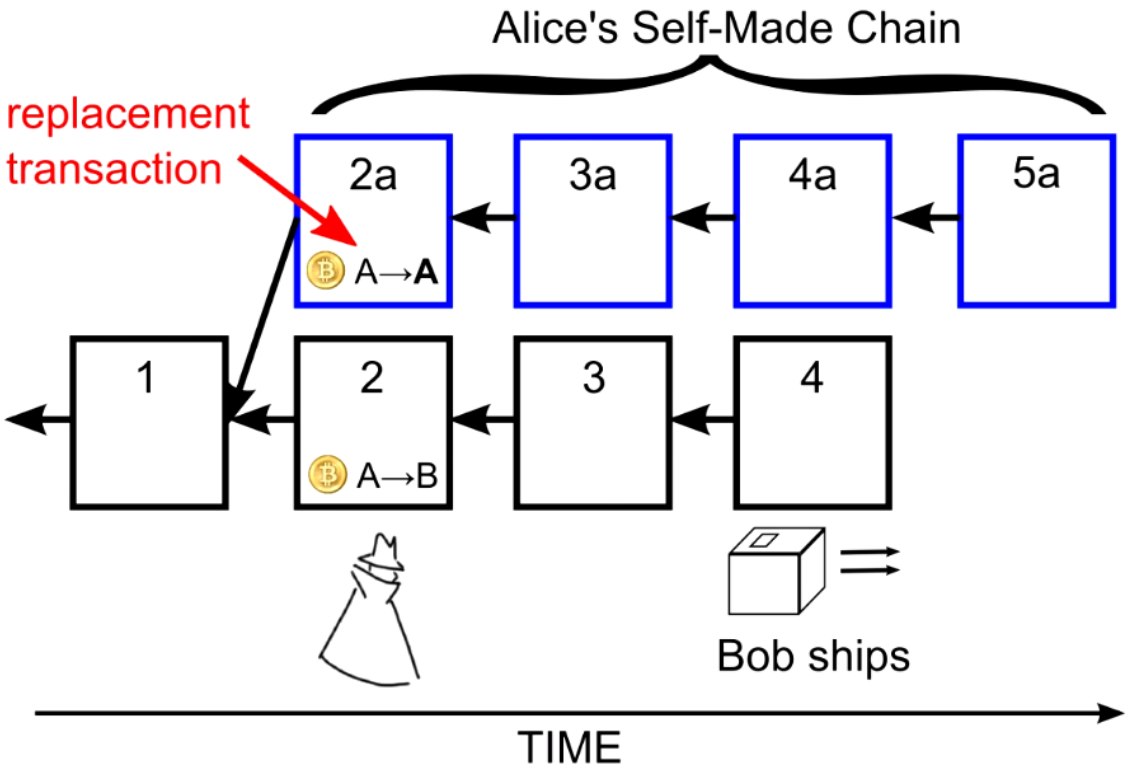
- double spending
- atak większościowy (51% attack)



http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Zagrożenia

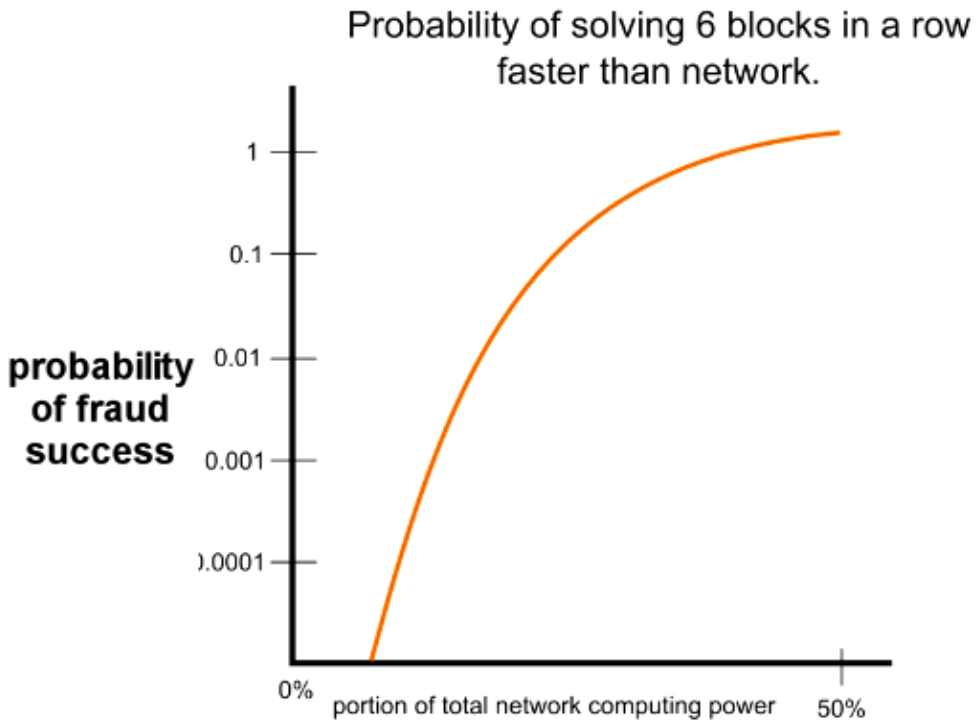
- double spending
- atak większościowy (51% attack)



http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Zagrożenia

- double spending
- atak większościowy (51% attack)



Analysis of hashrate-based double-spending, M. Rosenfield

Zagrożenia

- double spending
- atak większościowy (51% attack)
- komputery kwantowe - np. algorytm Shora: faktoryzacja w czasie $O((\log N)^3)$ zamiast $O(\sqrt{N})$

Zagrożenia

- double spending
- atak większościowy (51% attack)
- komputery kwantowe - np. algorytm Shora: faktoryzacja w czasie $O((\log N)^3)$ zamiast $O(\sqrt{N})$
- ataki na giełdy kryptowalut

Zastosowania

Zastosowania

- szybki przepływ pieniędzy bez pośredników

Zastosowania

- szybki przepływ pieniędzy bez pośredników
- smart contracts – umowy jako programy wykonywane po stronie blockchaina

Zastosowania

- szybki przepływ pieniędzy bez pośredników
- smart contracts – umowy jako programy wykonywane po stronie blockchaina
- rejestry właścicieli aut, ich ubezpieczeń, księgi wieczyste

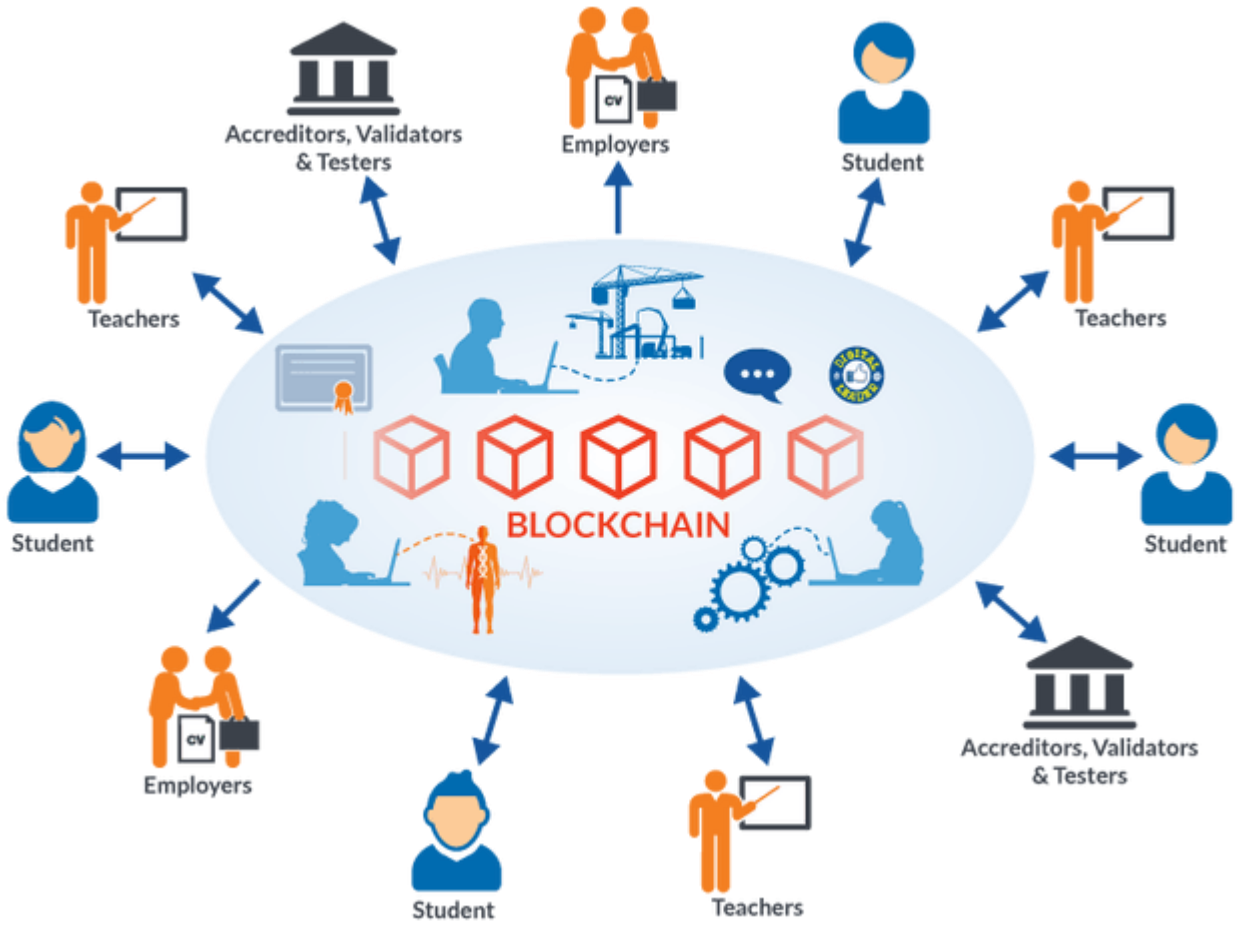
Zastosowania

- szybki przepływ pieniędzy bez pośredników
- smart contracts – umowy jako programy wykonywane po stronie blockchaina
- rejestry właścicieli aut, ich ubezpieczeń, księgi wieczyste
- głosowania przez internet

Zastosowania

- szybki przepływ pieniędzy bez pośredników
- smart contracts – umowy jako programy wykonywane po stronie blockchaina
- rejestry właścicieli aut, ich ubezpieczeń, księgi wieczyste
- głosowania przez internet
- wydawanie dyplomów i zaświadczeń, weryfikowanie osiągnięć

Blockchain w edukacji



http://blockchain.open.ac.uk/

Motywacja

Motywacja

- globalizacja edukacji

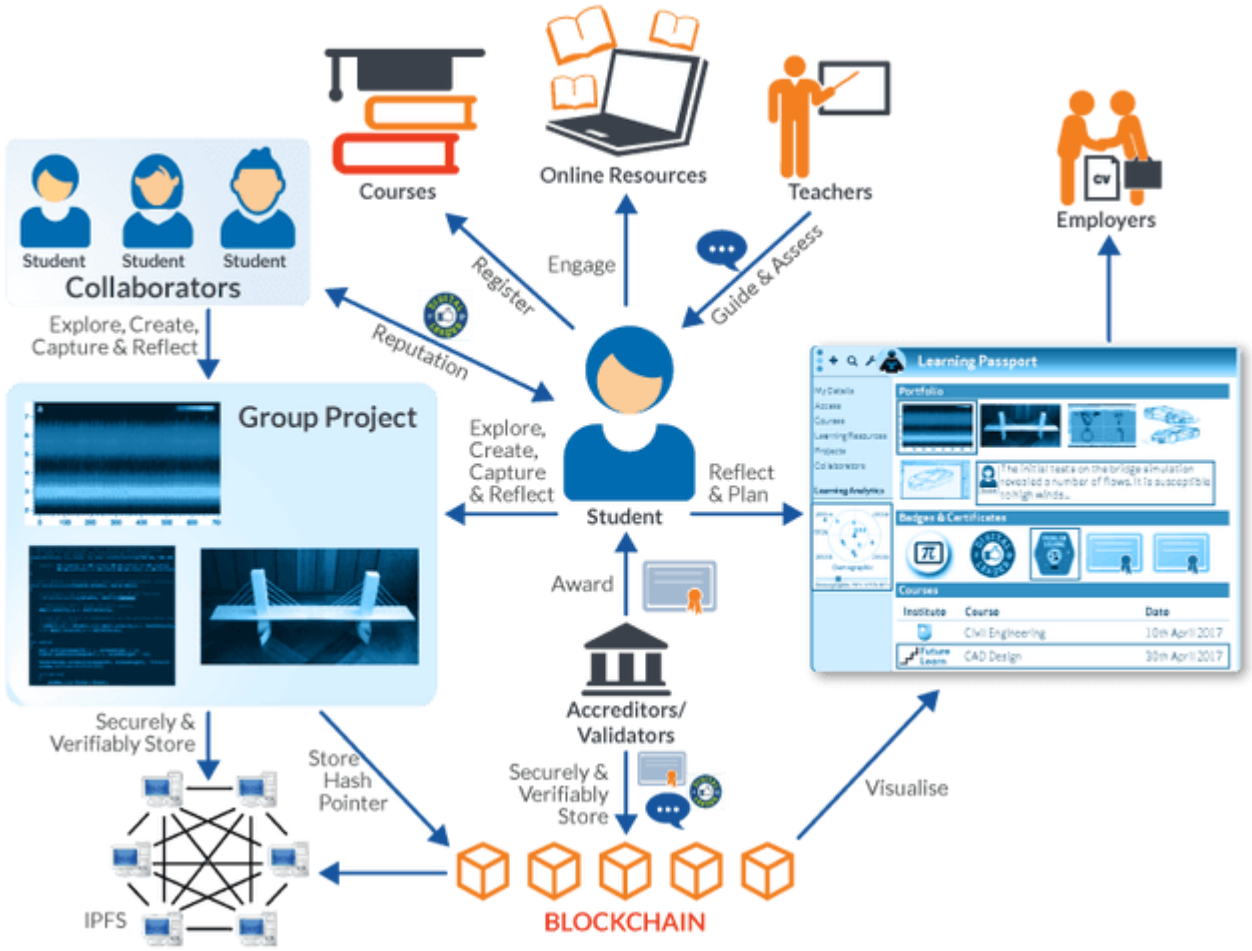
Motywacja

- globalizacja edukacji
- papierowe dokumenty są kłopotliwe i mogą zostać podrobione

Motywacja

- globalizacja edukacji
- papierowe dokumenty są kłopotliwe i mogą zostać podrobione
- chcemy przechowywać informacje nie tylko o wykształceniu, ale także udziałach w projektach, praktykach itp.

E-portfolio



http://blockchain.open.ac.uk/

Ethereum

Ethereum

- platforma oparta o kryptowalutę ether i maszynę wirtualną EVM

Ethereum

- platforma oparta o kryptowalutę ether i maszynę wirtualną EVM
- umożliwia zawieranie inteligentnych umów działających na zasadzie wykonywania skryptów w sieci

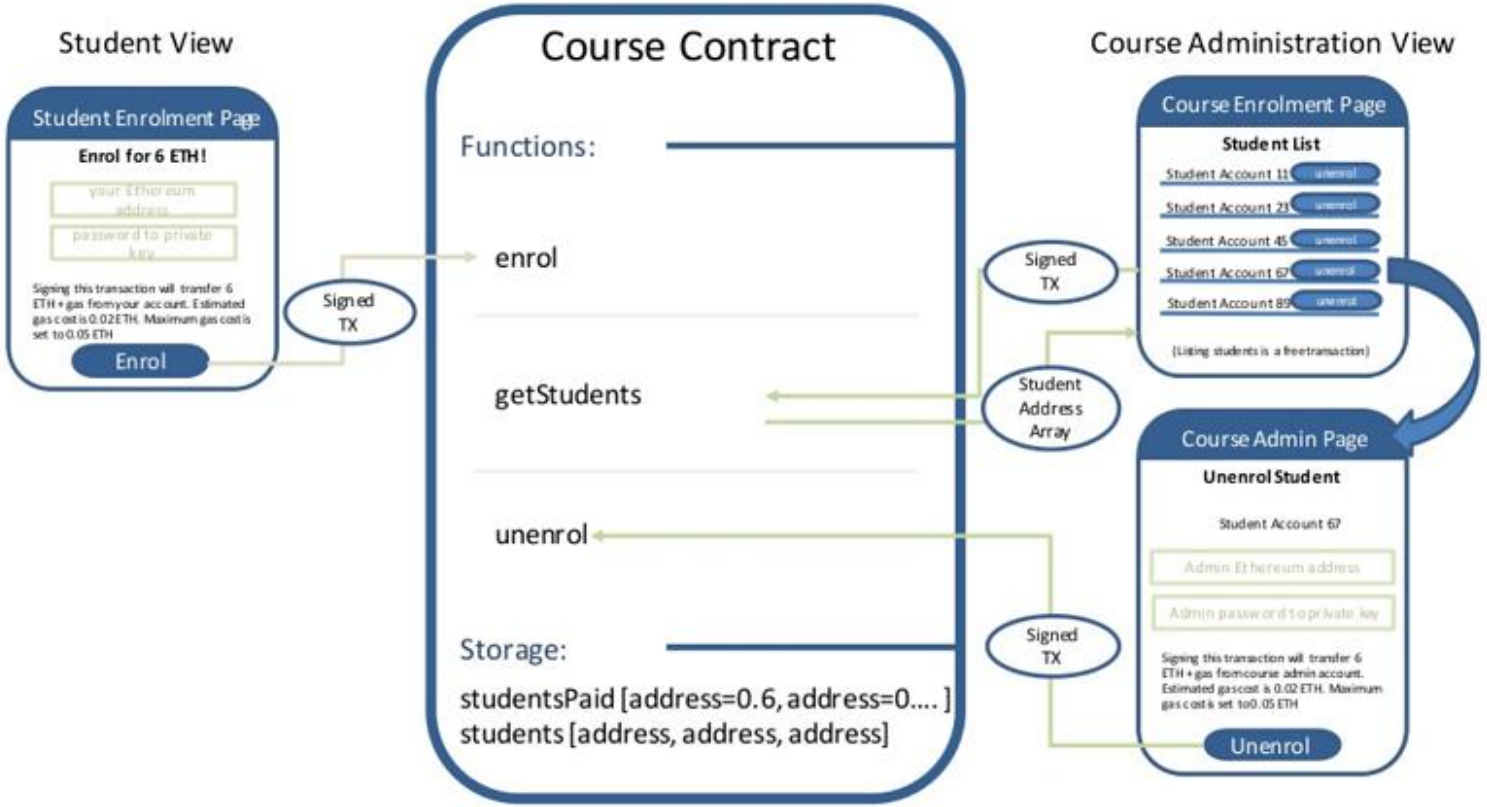
Ethereum

- platforma oparta o kryptowalutę ether i maszynę wirtualną EVM
- umożliwia zawieranie inteligentnych umów działających na zasadzie wykonywania skryptów w sieci
- gas – mechanizm prowizji za wykonywanie obliczeń

Ethereum

- platforma oparta o kryptowalutę ether i maszynę wirtualną EVM
- umożliwia zawieranie inteligentnych umów działających na zasadzie wykonywania skryptów w sieci
- gas – mechanizm prowizji za wykonywanie obliczeń
- DApp (decentralised application) = smart contract (backend) + frontend

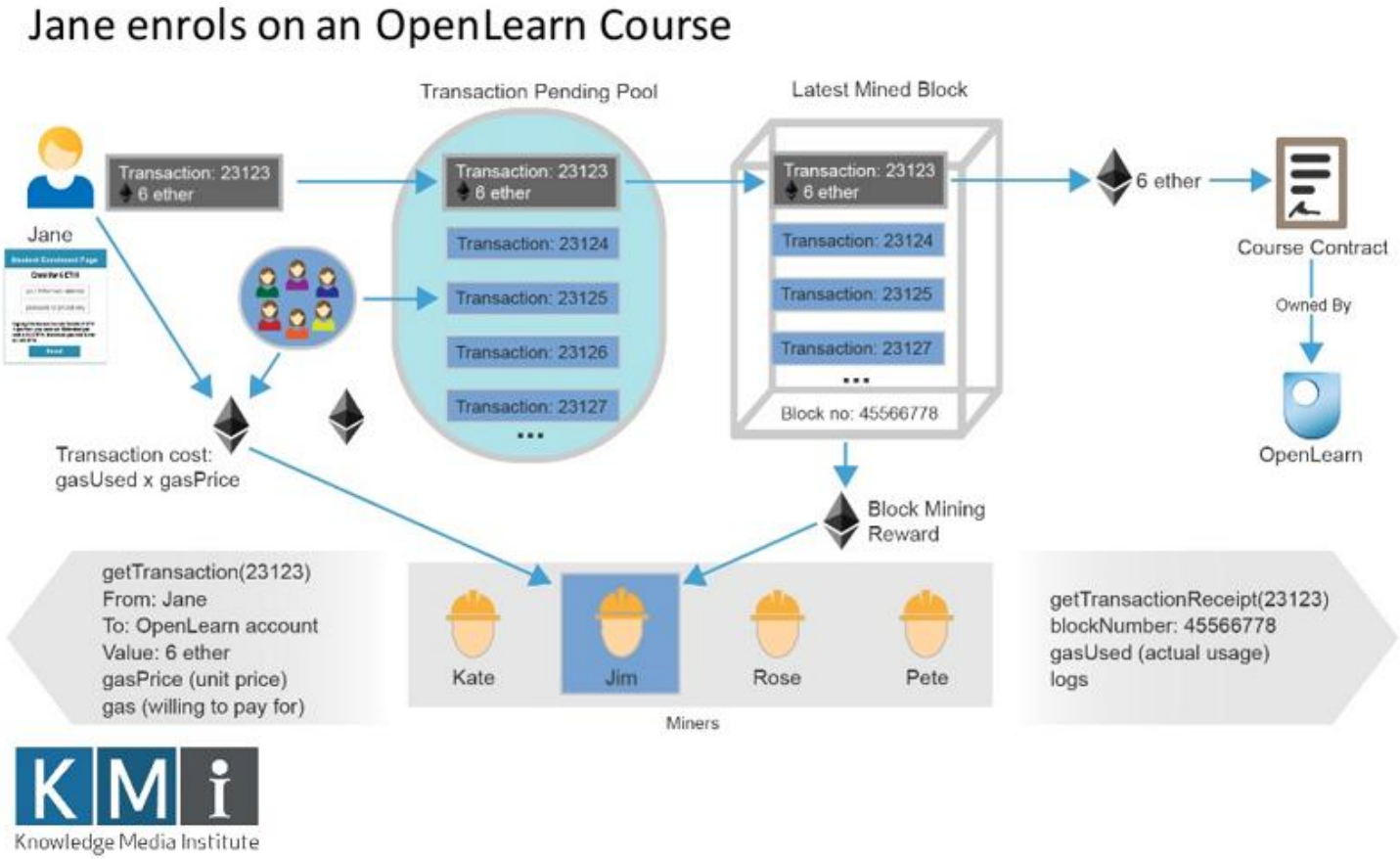
Zdecentralizowane aplikacje



Knowledge Media Institute

https://www.slideshare.net/johndomingue/blockchains-and-adult-education

Zdecentralizowane aplikacje



https://www.slideshare.net/johndomingue/blockchains-and-adult-education

Zdecentralizowane aplikacje

- zintegrowany system płatności

Zdecentralizowane aplikacje

- zintegrowany system płatności
- jedno globalne konto użytkownika do wszystkich aplikacji

Zdecentralizowane aplikacje

- zintegrowany system płatności
- jedno globalne konto użytkownika do wszystkich aplikacji
- open source – zarówno frontend jak i backend

Źródła

- https://bitcoin.org/bitcoin.pdf
- http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html
- https://www.linkedin.com/pulse/blockchains-evolving-clasp-higher-education-david-k-moldoff
- http://blockchain.open.ac.uk

Dziękuję za uwagę ☺

- Pytania?