Udany Electronic Cash BitCoin

Andrzej P.Urbański

Wczesne pomysły e-cash

- Transakcje anonimowe jak przy gotówce
- Kryptograficznie generowane liczby jako monety
- Monety mogą brać udział w transakcjach bez pośrednictwa banku
- Program może tylko raz zapłacić jedną monetą
  - Założenie podobnie niemożliwe do zapewnienia jak ochrona oprogramowania przed piractwem

BitCoin

- Waluta cyfrowa
- zaprojektowana w 2009
- autor o pseudonimie Satoshi Nakamoto
- Nie ma emitenta centralnego
- Zaufanie budowane na zasadzie demokratycznej
- Możliwe anonimowe posiadanie i transfery
- Koncept *kryptowaluty* - 1998 przez Wei Dai

Rozwiązanie problemu przez BitCoin

- Publiczne ogłaszanie transakcji w sieci P2P
- Podpisywanie listy transakcji kluczami prywatnymi uniemożliwiające wszelkie fałszowanie

implementacja

- Bitcoin jest implementacją konceptu
  - b-money autorstwa Wei Dai
  - Bitgold autorstwa Nicka Szabo,
  - oparta na sieci P2P.
- Specyfikacja techniczna stworzona w 2008 przez Satoshiego Nakamoto

Adresy

- Każdy klient ma portfel par kluczy
- Klucz publiczny jest jednocześnie adresem
- Klucz prywatny służy podpisywaniu transakcji
- Adresy są anonimowe
- 34 znakowe rozpoczynają się zawsze od liczby 1 lub 3 zawierają wielkie i małe litery oraz cyfry alfabetu łacińskiego z wykluczeniem cyfry *0*, wielkiej litery *O*, wielkiej litery *I* i małej litery *l*.

Transakcje

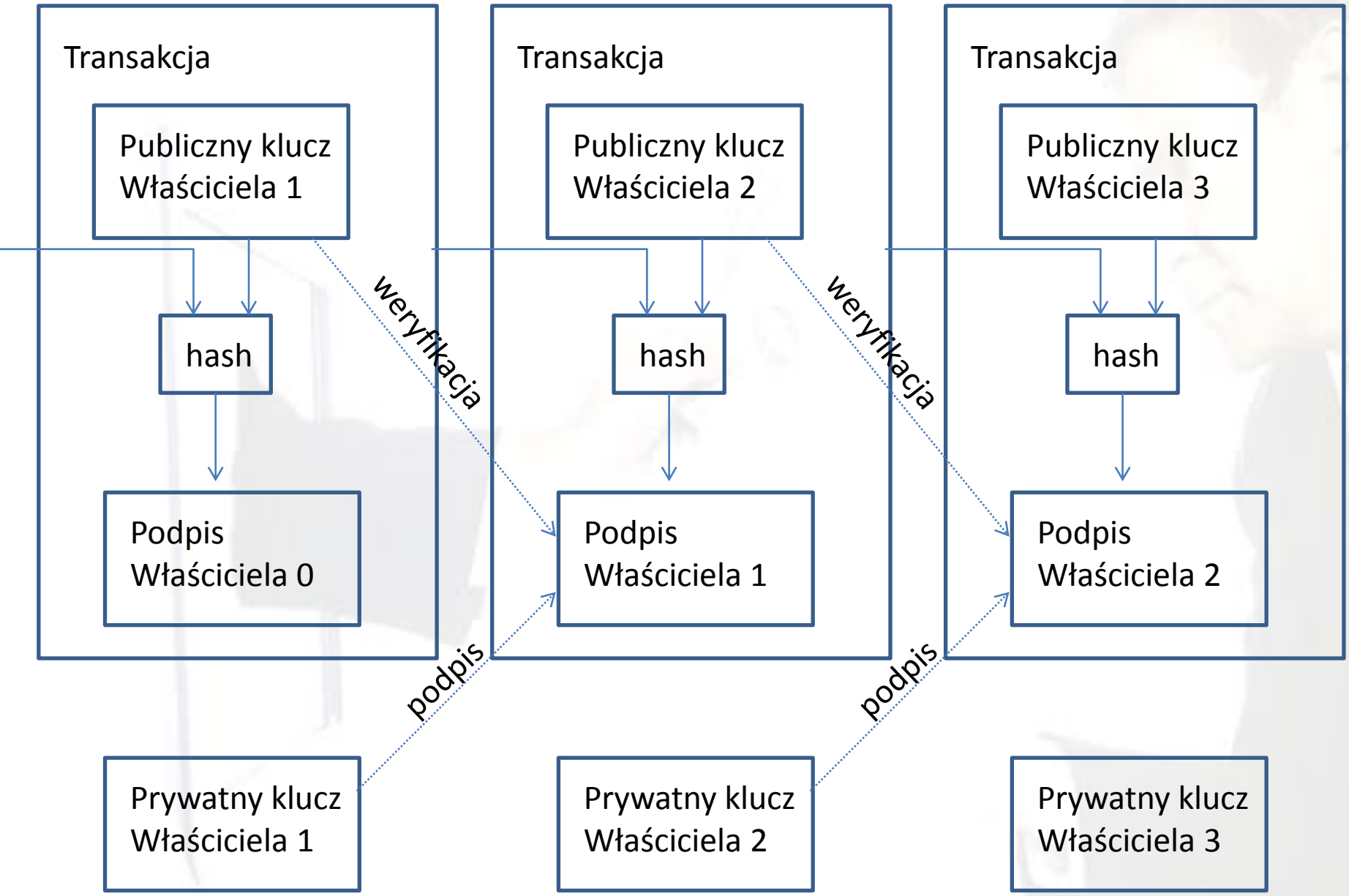
- Bitmonety zawierają klucz publiczny (adres) aktualnego posiadacza.
- Kiedy użytkownik *A* przetransferuje jakąś ilość do użytkownika *B*, *A* rezygnuje z ich posiadania dodając klucz publiczny (adres) *B* do tych monet oraz podpisując je własnym kluczem prywatnym.
- Ogłasza wykonaną przez siebie transakcję w komunikacie wysłanym do sieci peer-to-peer.
- Sieć sprawdza przed zaakceptowaniem transakcji poprawność zastosowanych podpisów cyfrowych oraz ilości monet.

Łańcuch bloków 1

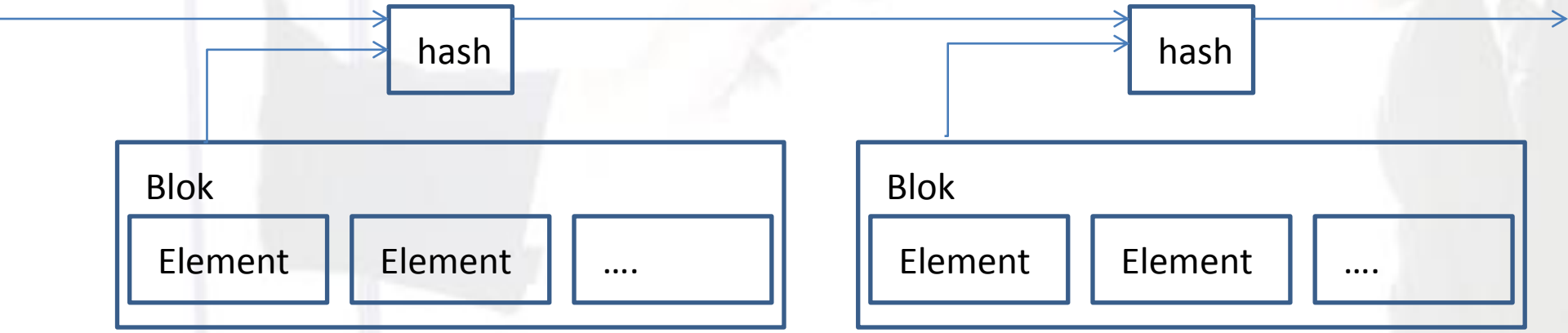
- Rodzaje łańcuchów bloków
  - Czarny to najdłuższa seria bloków od zielonego do aktualnego
  - Zielony to początkujący blok genezy
  - szare bloki istnieją poza głównym łańcuchem Tzw. Osierocone
- Nową transakcję dodaje się do *łańcucha bloków opatrując* znacznikiem czasu
  - To system matematycznych dowodów wykonanych działań, zwanym „proof of work”
  - Zapobiega podwójnemu wydawaniu oraz fałszerstwu.
- Każdy *generujący* węzeł zbiera wszystkie niepotwierdzone transakcje, które zna w kandydacie na *blok* – pliku zawierającym między innymi kryptograficzne hashe poprzedniego poprawnego bloku znanego temu węzłowi.

Łańcuch bloków 2

- Następnie próbuje obliczyć kryptograficzny hash tego bloku z określonymi cechami, co wymaga z góry przewidywalnej liczby prób i błędów.
- Kiedy znajdzie rozwiązanie, ogłasza je reszcie sieci. Węzły otrzymujące nowo rozwiązany blok, sprawdzają jego poprawność przed zaakceptowaniem i dodaniem do łańcucha.
- Ostatecznie łańcuch bloków zawiera kryptograficzną historię zmian posiadania wszystkich monet, poczynając od adresu ich emitenta, aż po adres aktualnego posiadacza.
- Jeżeli użytkownik spróbuje ponownie wykorzystać wydane wcześniej monety, sieć odrzuci próbę wykonania takiej transakcji.


Transakcja
Publiczny klucz Właściciela 1
hash
Podpis Właściciela 0
Prywatny klucz Właściciela 1
weryfikacja
podpis
Transakcja
Publiczny klucz Właściciela 2
hash
Podpis Właściciela 1
Prywatny klucz Właściciela 2
weryfikacja
podpis
Transakcja
Publiczny klucz Właściciela 3
hash
Podpis Właściciela 2
Prywatny klucz Właściciela 3

Serwer znacznika czasu



Pozyskiwanie monet

- nowych bitmonet szacunkowo 6 razy na godzinę w losowych odstępach czasu do jednego z użytkowników.
- Potencjalnie każdy użytkownik może otrzymać partię dzięki użytkowaniu aplikacji lub ekwiwalentnego oprogramowania dostosowanego do posiadanego przez użytkownika wyposażenia. Generowanie bitmonet jest często nazywane „wydobywaniem", poprzez analogię do wydobywania złota Prawdopodobieństwo tego, iż dany użytkownik otrzyma partię monet, zależy od stosunku ilości mocy obliczeniowej wniesionej do sieci za jego pośrednictwem do sumy mocy obliczeniowej wniesionej przez wszystkie węzły. Liczba bitmonet stworzona w partii nigdy nie jest większa niż 25 BTC (dane na luty 2013), a nagrody są zaprogramowane na zmniejszanie się w czasie aż do zera, tak aby nie więcej niż 21 milionów monet mogło kiedykolwiek zaistnieje. W miarę, jak wypłaty będą się zmniejszać, oczekuje się, iż zbieranie opłat transakcyjnych będzie motywacją dla użytkowników do uruchamiania węzłów generujących.
- Wszystkie generujące węzły sieci współzawodniczą w celu bycia pierwszymi w znalezieniu rozwiązania problemu kryptograficznego dla przetwarzanego bloku kandydującego, co wymaga stosowania powtarzających się prób i błędów. Kiedy węzeł znajdzie takie rozwiązanie, ogłasza je reszcie sieci oraz deklaruje się posiadaczem nowej partii bitmonet. Węzły otrzymujące nowo rozwiązany blok sprawdzają jego poprawność przed zaakceptowaniem i dodaniem do łańcucha. Węzły mogą używać CPU,GPU a nawet FPGA[8][13][14]. Użytkownicy mogą także generować bitmonety grupowo[15].
- Tak więc każdy blok jest generowany co 10 minut, każdy węzeł osobno co 2016 bloków (co w praktyce zajmuje średnio 2 tygodnie) rekalkuluje stopień trudności problemu, który próbuje rozwiązać, używając do tego średniej kroczącej, celującej w średnią liczbę bloków na godzinę. Jeżeli bloki są generowane zbyt szybko lub zbyt wolno, co zależy od zwiększającej lub zmniejszającej się mocy obliczeniowej całej sieci, stopień trudności odpowiednio wzrasta lub maleje

Ekonomia

- Eksperymentalna
- Płacenie BitCoinem
- Dotacje BitCoinem
- Kantory BitCoinowe

Fiasko BitCoin

- dewaluację waluty,
- zmniejszającą się bazę użytkowników
- globalne sankcje rządowe, skierowane przeciwko temu oprogramowaniu.

Czy BitCoin jest legalny?

- Problem prawników
- Problem ustawodawców

Ciemne strony

- Nielegalne transakcje
  - Handel narkotykami
- Niebezpieczne wahania kursu


275
250
225
200
175
150
125
100
75
50
25
2013-01-18
2013-01-28
2013-02-07
2013-02-17
2013-02-27
2013-03-09
2013-03-19
2013-03-29
2013-04-08
2013-04-17
Support project: 1L8ULvh3y9Zm9P7Lk6vsfc1H9Ur72SYzqz | Copyright © BitcoinChart.com 2013 | BC: ver.1.0.0 beta