Informatyczne aspekty systemu kryptowaluty Bitcoin

prof. dr inż. Wojciech Nowakowski
Instytut Maszyn Matematycznych

Co to jest Bitcoin?

Jednostka kryptowaluty?
Idea niezależnego pieniądza?
System informatyczny?

Wszystkie odpowiedzi są prawdziwe!

Bitcoin – to system oprogramowania, oparty na technologii tzw. łańcucha bloków będący próbą realizacji idei niezależnego, społecznego, wirtualnego środka płatniczego, definiujący obrót i przechowywanie jednostek płatniczych o nazwie *bitcoin*.

1. **Uwaga pierwsza: wirtualnymi środkami płatniczymi posługujemy się na co dzień (konta bankowe, karty płatnicze itd.)**

2. **Uwaga druga: Istnieje wiele wirtualnych internetowych środków płatniczych, np. w grach i aplikacjach komputerowych, ostatnio np. BILLON, ale wszystkie one nie są społeczne, tzn. mają emitenta lub zarządcę**

3. **Uwaga trzecia: wartość wszystkich środków płatniczych mających emitenta zależy przede wszystkim od działań tego emitenta (nadmierna emisja, de- lub rewaluacja, wymiany, interwencje itp. Wartość społecznych środków płatniczych zależy wyłącznie od podaży i popytu. Wartość ta może zmieniać się np. tysiąckrotnie w ciągu tygodnia i może podlegać grze spekulacyjnej.**

3.Uwaga czwarta: w oprogramowaniu Bitcoin wykorzystano współczesne metody kryptografii, szereg procedur a także algorytmów matematycznych oraz funkcji obliczeniowych opracowanych w ostatnich latach:

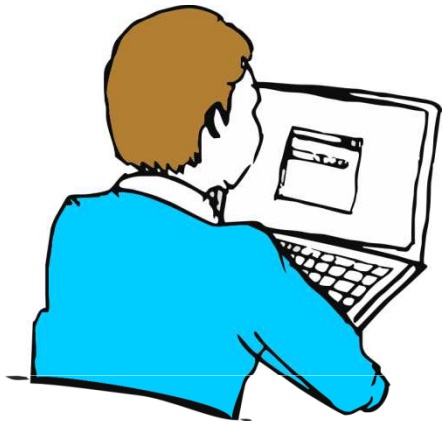
- **kryptografii klucza publicznego**
- **funkcji skrótu (*hash*)**
- **procedury *Proof of Work* (*hashcash*)**

A NA DODATEK NIE WIADOMO, KTO TO ZROBIŁ!

ELEMENTY

KRYPTOGRAFIA SYMETRYCZNA

klasyczna



?

Klucz
0100010101000101

+

WIADOMOŚĆ

=

ĆWDOOMAIŚ

Klucz
0100010101000101

+

ĆWDOOMAIŚ

=

WIADOMOŚĆ

1976

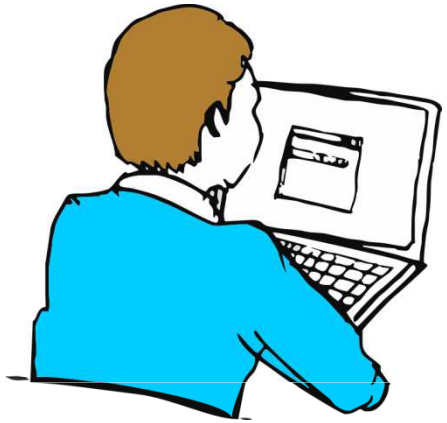
Martin Hellman

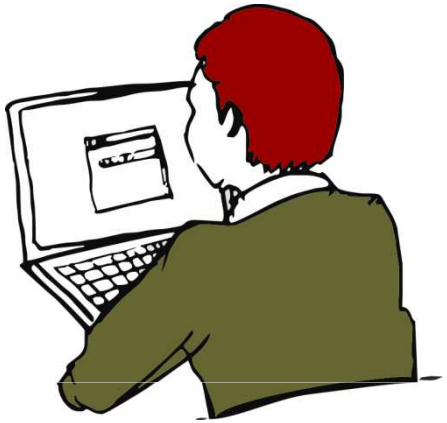
Whitfield Diffie

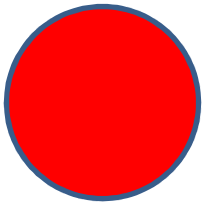
Para różnych kluczy zależnych – **prywatny** i **publiczny**, przy czym klucza prywatnego nie da się (łatwo) odtworzyć na podstawie publicznego.

KRYPTOGRAFIA KLUCZA PUBLICZNEGO

Zwana też: asymetryczną lub z dwoma kluczami







Klucz publiczny
0100010101000101

+

WIADOMOŚĆ

=

ĆWDOOMAIŚ

Klucz publiczny
0100010101000101

ĆWDOOMAIŚ

+

Klucz prywatny (tajny)
0100010101000101

=

WIADOMOŚĆ

KRYPTOGRAFIA KLUCZA PUBLICZNEGO
ZASTOSOWANIA

1991
Poczta elektroniczna, protokół PGP (Pretty Good Privacy - Całkiem Niezła Prywatność) autorstwa Phila Zimmermanna udostępniony przez niego powszechnie i bez wynagrodzenia. PGP jest jeszcze i dziś trudny do złamania nawet przez służby.

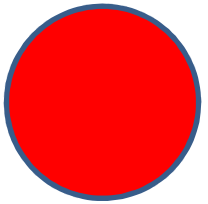
1989 (ISO), 1999 (EC), 2001 (PL)
Podpis elektroniczny. Wdrażany w Polsce i Unii Europejskiej z dużym wysiłkiem prawnym, ale miernym skutkiem.

2008
System kryptograficzny waluty Bitcoin

KRYPTOGRAFIA KLUCZA PUBLICZNEGO
ZASTOSOWANIA c.d.

2011
Silent Circle, Silent Network. Phil Zimmermann, Mike Janke, Jon Callas. System mobilnej cyfrowej łączności szyfrowanej, niemożliwy (jak na razie) do podsłuchu, nawet przez NSA. Umożliwia bezpieczne połączenia głosowe, wideo-czat i połączenia konferencyjne, w jakości HD, w sieciach 3G/4G i Wi-Fi. Połączenia są szyfrowane *on-line* protokołem ZRTP, który jest (pochodną od PGP) wersją RTP (*Real Time Protocol*) rozszerzoną o wykrywanie początku rozmowy i mechanizm uzgadniania kluczy między rozmówcami. Uzgodnienie kluczy odbywa się bezpośrednio w strumieniu danych. Klucze są niszczone z końcem rozmowy.

FUNKCJA SKRÓTU (hash)

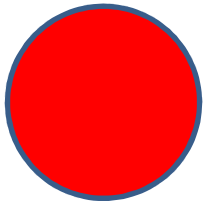


Jest to funkcja, która przyporządkowuje dowolnie dużej liczbie (plik, wiadomość) krótką wartość (skrót wiadomości, sygnatura, hash), zwykle posiadającą stałą długość .

W systemie Bitcoin wykorzystywana jest m. in. funkcja skrótu SHA-256 (tworzy skróty o dlugości 256 bitów).

Porównanie skrótów dwóch plików umożliwia stwierdzenie, czy w pliku zostały dokonane jakiekolwiek zmiany.

PROOF OF WORK (hashcash)

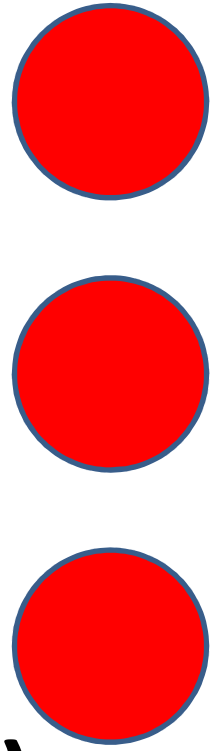


Tzw. ***dowód wykonanej pracy*** lub ***funkcja kosztów***

Procedura ta została wymyślona pierwotnie w celu ograniczania spamu. Polega na asymetrii: praca obliczeniowa musi być żmudna, ale jednocześnie łatwa do sprawdzenia.

W systemie Bitcoin została wprowadzona do **sprawdzania wiarygodności** dokonanych transakcji będąc jednocześnie pierwotnym mechanizmem **emisyjnym** jednostek płatniczych, czyli *bitcoinów*. Mechanizm ten często jest porównywany do wydobywania złota (*mining*).

KRYPTOGRAFIA KLUCZA PUBLICZNEGO



FUNKCJA SKRÓTU (hash)

PROOF OF WORK (hashcash)

Tzw. ***dowód wykonanej pracy*** lub ***funkcja kosztów***

HISTORIA

Prekursorzy

David Chaum (1990). *Untraceable Electronic Cash*.
http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf

Wei Dai (1998). *B-Money*.
http://www.weidai.com/bmoney.txt

Nick Szabo (1998-2005). Decentralized digital currency BitGold.
http://unenumerated.blogspot.co.uk/2005/12/bit-gold.html

Bitcoin: A Peer-to-Peer Electronic Cash System

2008

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

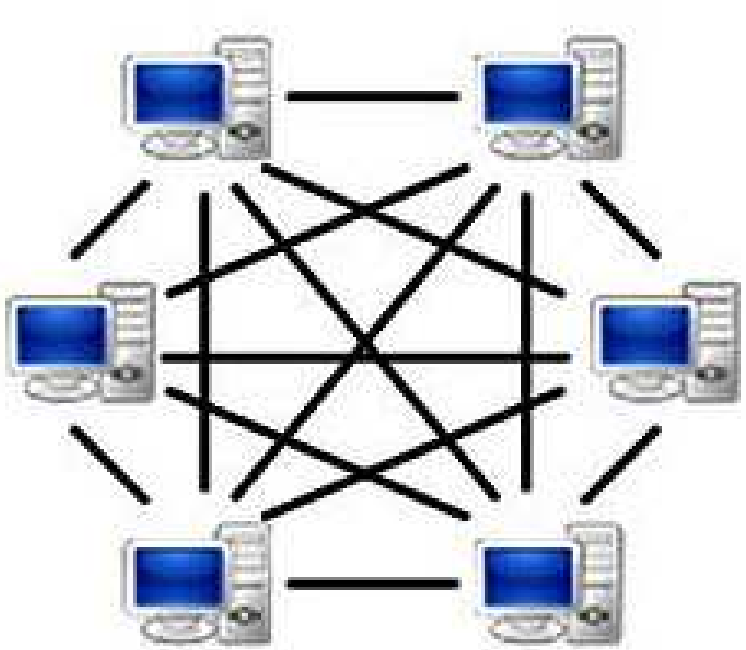
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed...

Sieć typu ***peer-to-peer*** (równy z równym, sieć równoprawnych węzłów) umożliwiająca przekazywanie elektronicznej gotówki *on-line* bezpośrednio od jednego podmiotu (węzła) sieci do drugiego, **bez pośrednictwa jakiekolwiek instytucji finansowej**.

Obok uwiarygodniania niezbędne jest zabezpieczanie przed podwójnym przekazem gotówki. Proponujemy rozwiązanie tego problemu również za pomocą sieci *peer-to-peer*. Sieć dołącza do pliku każdej transakcji **znacznik czasu**, oblicza jej **skrót** (hash) oraz umieszcza go w **łańcuchu bloków** (historii transakcji) **po wykonaniu** obliczeń matematycznych tzw. ***proof of work***, stanowiących dowód wykonania transakcji...

Sieć z serwerem

Sieć *peer-to-peer*



Podstawowe cechy

- W systemie **nie ma emitenta** i administracji centralnej. Nie ma też **administracji** własnej i nadzorcy.

- Baza danych systemu i transakcji **jest rozproszona** w sieci *peer-to-peer.*

- Emisję pieniądza zapewnia **aparat matematyczny** zawarty w oprogramowaniu systemu.

• System **uniemożliwia manipulację** wartością pieniądza przez ingerencję jakiejkolwiek organizacji, firmy czy jednostki.

• Transfer kwot między rachunkami dokonywany jest za pomocą kryptografii klucza publicznego. Wszystkie transakcje są przechowywane w **łańcuchu bloków** czyli publicznie dostępnej, rozproszonej bazie danych.

UWAGA:

W bazie tej nie ma informacji, które umożliwiałyby **identyfikację osób** dokonujących transakcji i przelewów. Identyfikacja taka jakkolwiek teoretycznie możliwa, w praktyce jest niewykonalna ze względu na skalę niezbędnego przetwarzania danych.

POWTÓRZMY:

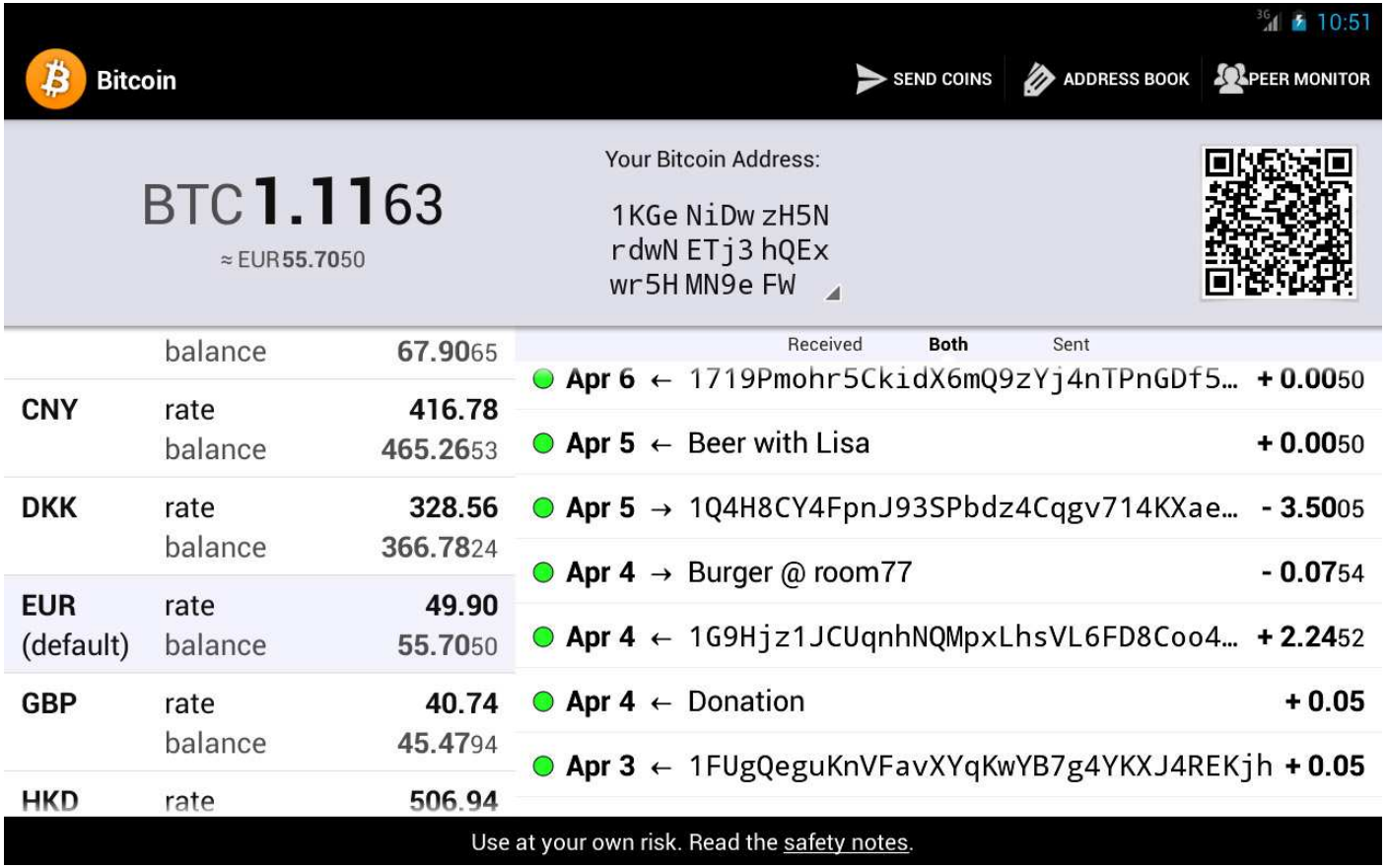
System Bitcoin realizuje transfery kwot między publicznymi rachunkami używając **kryptografii klucza publicznego**.

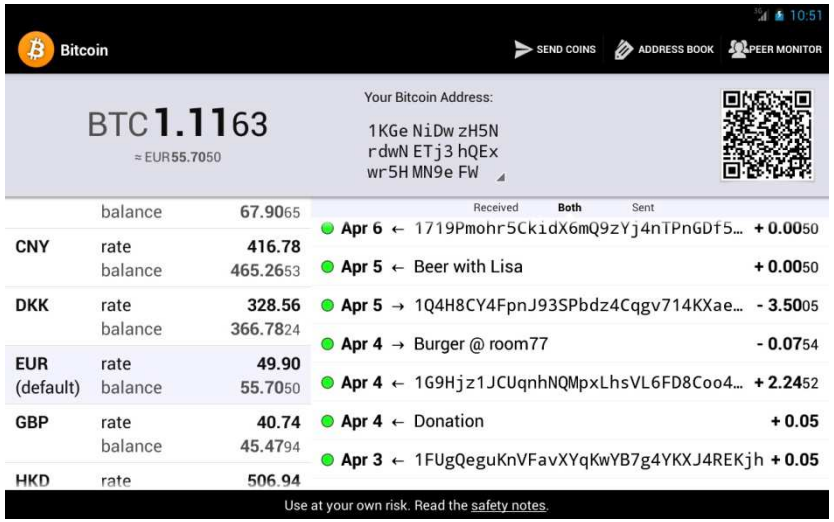
Wszystkie transakcje są publiczne i przechowywane w rozproszonej bazie danych, w **postaci łańcucha wszystkich transakcji** od początku istnienia systemu.

Transakcje są **anonimowe**. System działa **automatycznie** bez emitenta.

Transakcje

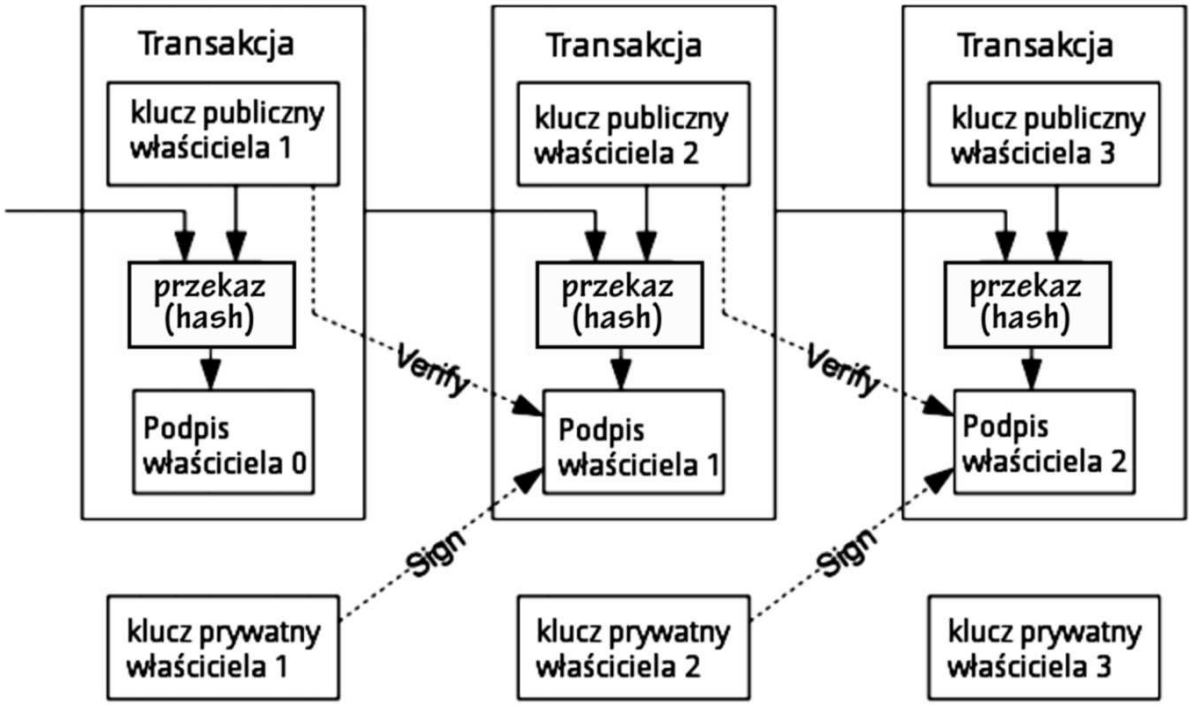
Każda osoba przystępująca do sieci Bitcoin instaluje na swoim smart-fonie, tablecie lub komputerze program kliencki, który generuje portfel (Bitcoin Wallet) zawierający dowolną liczbę **par kluczy kryptograficznych**





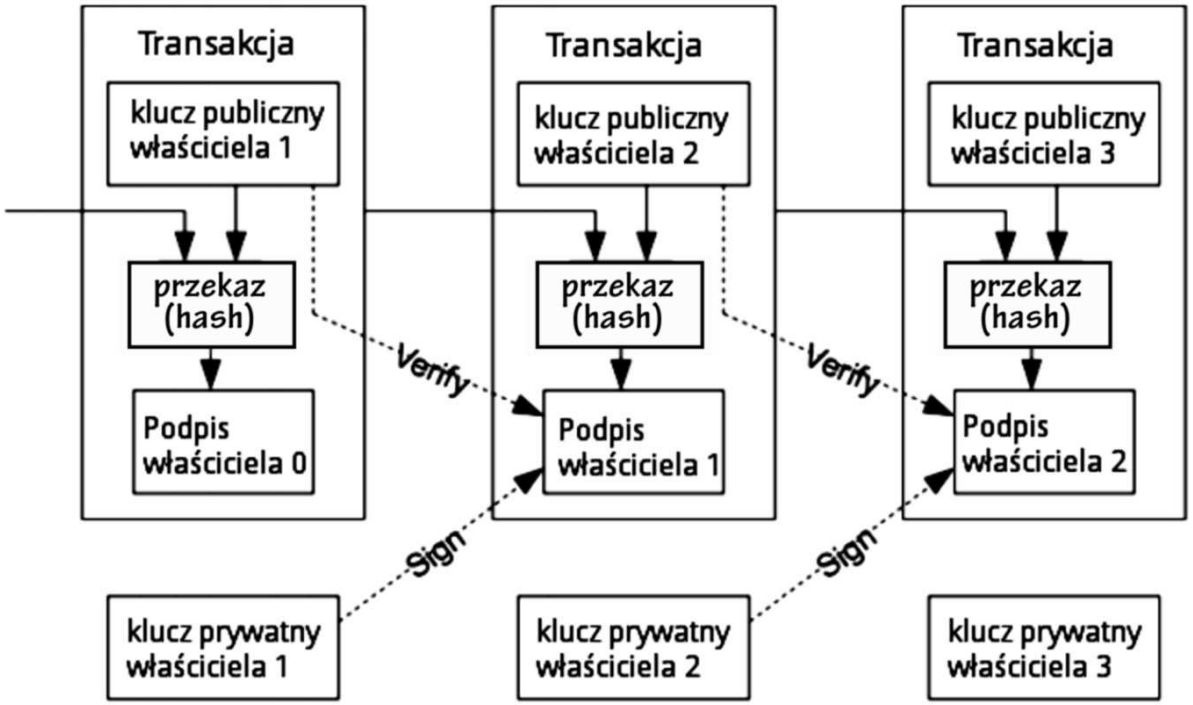
- **Klucze publiczne** to **adresy** odpowiadające numerom kont w klasycznej bankowości dla wszystkich płatności. **Klucze prywatne autoryzują płatności**. Użytkownik może posiadać wiele adresów, nawet do każdej transakcji inny
- Przekazy są wykonywane bezpośrednio, bez operatorów finansowych i osób trzecich.
- Przekazy nie mogą być refundowane.

Transakcja



- Każdy przekaz Bitcoin **jest podpisany cyfrowo kluczem publicznym** jej właściciela (ECDSA)
- Dokonujący przelewu rezygnuje z posiadania przelewanych środków dodając klucz publiczny nowego właściciela i **podpisuje transakcję kluczem prywatnym**

Transakcja (c.d.)

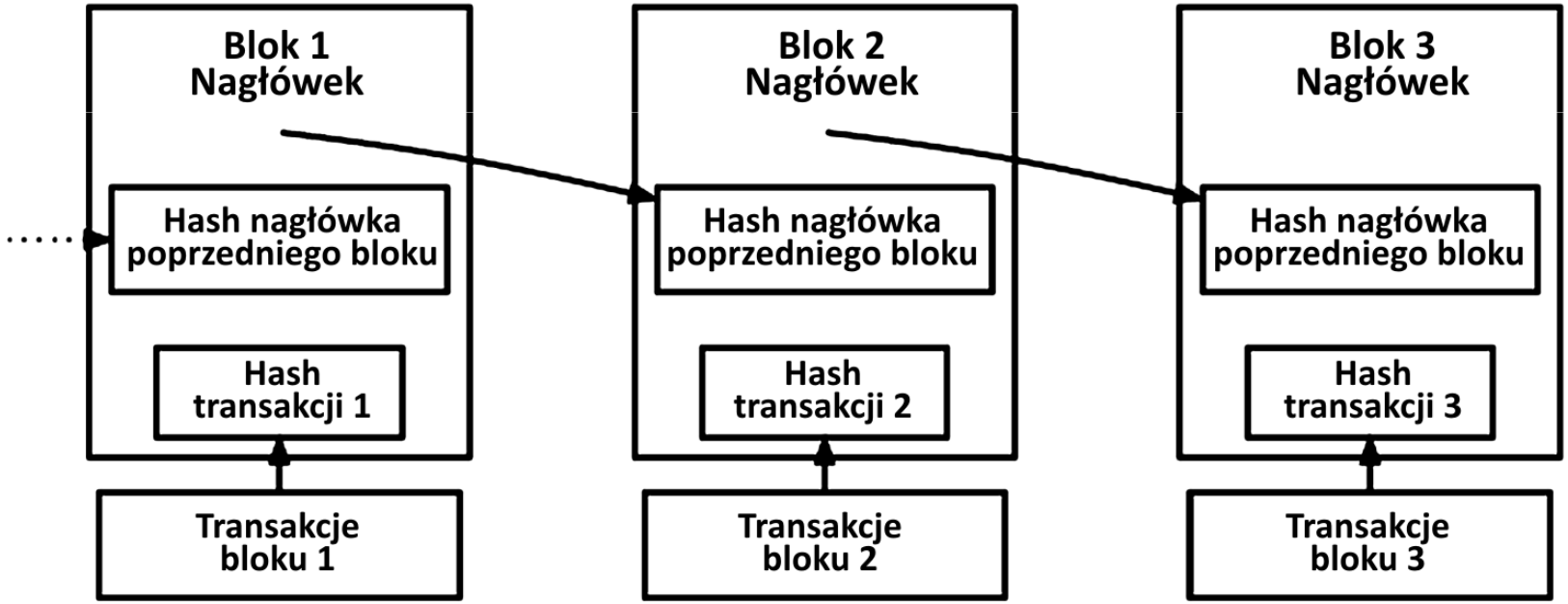


• Następnie **ogłasza wykonaną przez siebie transakcję** w komunikacie wysłanym do sieci. Gdy nowy właściciel zechce zapłacić swoją monetą komuś innemu, **podpisuje ją swoim kluczem prywatnym**, wykorzystując **klucz publiczny kolejnego właściciela**.

Łańcuch bloków

System tworzy w sieci rejestr wszystkich transakcji od początku istnienia sieci, w postaci tzw. łańcucha bloków (*block chain*), który jest upubliczniany przez zapisanie go do powszechnie dostępnego rejestru.

Każdy blok składa się z nagłówka, skrótu nagłówka poprzedniego bloku oraz skrótu transakcji.

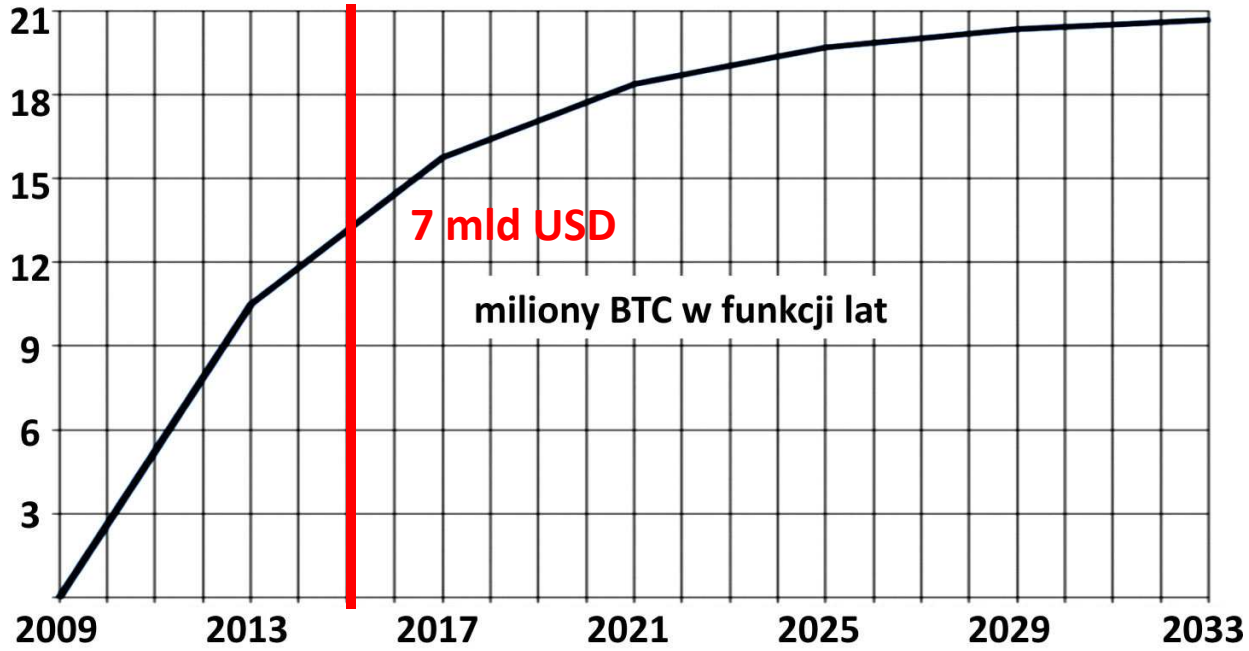


Akceptacja bloków, ***Proof of Work***

- Transakcja przesłana do sieci nie staje się natychmiast „ważna”, tzn. zamieszczona w łańcuchu bloków, oznakowana znacznikiem czasu i potwierdzona.
- Potwierdzenie ważności bloku również dokonuje **sama sieć**. Czyli kto? Po prostu użytkownicy sieci Bitcoin, którzy włączają się w ten proces korzystając z odpowiedniego modułu oprogramowania systemu Bitcoin.
- To oni zbierają wszystkie niepotwierdzone jeszcze transakcje i próbują obliczyć *hash* tego bloku z dodatkowo zadanymi przez system cechami. Kiedy znajdą rozwiązanie, ogłasza je w sieci. Nowo rozwiązany blok, jest sprawdzany przed zaakceptowaniem i dodaniem do łańcucha.
- Sprawdzanie bloków wymaga bardzo silnych maszyn i szybkich obliczeń. Ten trzeci element systemu Bitcoin: wyliczanie takiego superhasha (*hashcash*) z dodatkowymi wymaganiami utrudniajacymi określa się ***dowodem wykonanej pracy*** (ang. *Proof of Work*). Można też tę czynność określić ***sprawdzaniem pracą***.

Emisja jednostek płatniczych, czyli *bitcoinów*

- Emitentem jest procedura systemu informatycznego Bitcoin
- Emisja jest skończona, jednorazowa i wynosi 21 mln jednostek które zostaną wyemitowane stopniowo w latach 2009-2136.
- Emisja, a właściwie **asymptotyczny proces uwalniania** jednostek połączone jest z wykonywaniem procedury sprawdzania *Proof of Work*



Emisja jednostek płatniczych, c.d.

Emisja zachodzi przez **wynagradzanie** użytkowników akceptujących bloki, któremu za zaakceptowany blok sieć dokonuje przelewu.

Jest to trudne zadanie, gdyż sieć utrudnia je przez dodanie wymagań, jakie musi spełnić obliczany *hash* (np. żeby było 10 zer na początku).

Obecnie przeliczenie i akceptacja bloku wymaga obecnie ponad **320 tysięcy** lat pracy lepszego domowego komputera. Dlatego konstruowane są bardzo szybkie maszyny ze specjalizowanymi czipami ASIC, zoptymalizowane i przeznaczone wyłącznie do obliczeń „bitcoinowych".

Sieć *Bitcoin* jest siecią o **cechach homeostatycznych**. Utrzymuje bowiem z góry założone parametry. Jeżeli wydajność sieci w akceptacji bloków zwiększy się, to sieć tak dostosuje trudność obliczania, by blok wydobywany był nie częściej niż co 10 minut.

Obecnie nagroda za akceptację bloku wynosi **25 BTC** i spada o połowę co 210 tysięcy bloków czyli średnio co 4 lata.

A co po zakończeniu emisji?

Już obecnie wysyłający transfery pieniężne w sieci *Bitcoin* mogą wnosić niewielką opłatę transakcyjną. Nie jest to obowiązkowe, ale przyśpiesza autoryzację transakcji, gdyż zachęca do uruchamiania oprogramowania generującego, zwłaszcza, że stopień trudności weryfikacji bloku rośnie, a nagroda spada.

System Bitcoin zakłada, że po zakończeniu emisji węzły weryfikacyjne będą utrzymywać się wyłącznie ze zbierania opłat transakcyjnych.

Obecnie minimalna opłata transakcyjna za transakcje niskiego priorytetu wynosi 0,0005 BTC.

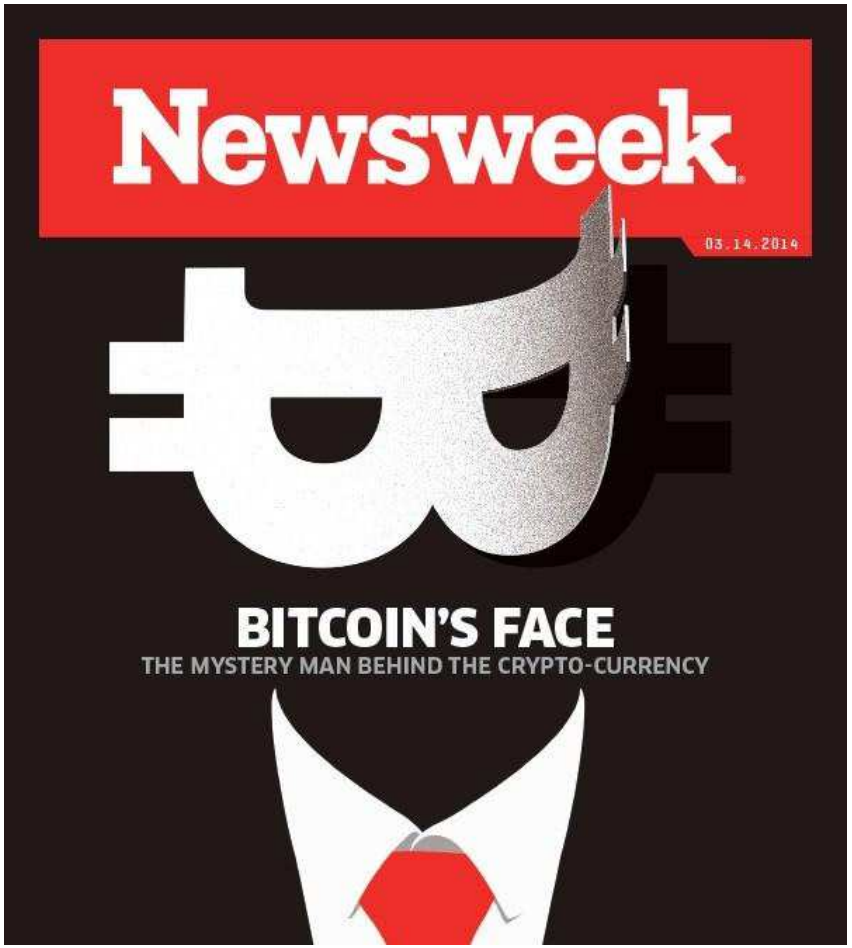
prawie koniec...

Poznając *Bitcoin* nie można się w nim nie zakochać. Jest uwielbiany przez libertarian, podziwiany przez matematyków, spełnia marzenia największych ekonomistów i jednocześnie jest uważany za realne zagrożenie dla monetarnych elit tego świata.

Sam w sobie nie jest niczym innym jak tylko ciągiem zer i jedynek...

Daniel Haczyk, antyweb.pl

Kim jest Satoshi Nakamoto?



Tacitly acknowledging his role in the Bitcoin project, he looks down, staring at the pavement and categorically refuses to answer questions.
"I am no longer involved in that and I cannot discuss it," he says, dismissing all further queries with a swat of his left hand. "It's been turned over to other people. They are in charge of it now. I no longer have any connection.„

Temple City, Los Angeles, California, USA

i… już.