AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Technologia Blockchain na przykładzie kryptowaluty Bitcoin

mgr inż. Konrad Zaworski

Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej
Katedra Informatyka Stosowanej

24.03.2021

Wstęp

- W 2008 roku nieznana osoba pod pseudonimem Satoshi Nakamoto publikuje w internecie dokument o nazwie ”Bitcoin: A Peer-to-Peer Electronic Cash System”.
- Rozwiązanie miało gwarantować wolność od jakichkolwiek wpływów państwowych, eliminować problem dodruku pieniędzy oraz nagłej zmiany zasad użytkowania i własności.
- Bitcoin pozbywa się tych ograniczeń, ponieważ opiera się na dowodzie kryptograficznym przeprowadzonych transakcji, który jest gwarantem ich zajścia i nieodwracalności.
- Technologia, na której jest zbudowany Bitcoin nazwa się Blockchain (zdecentralizowana rozproszona baza danych).

Historia 1/2

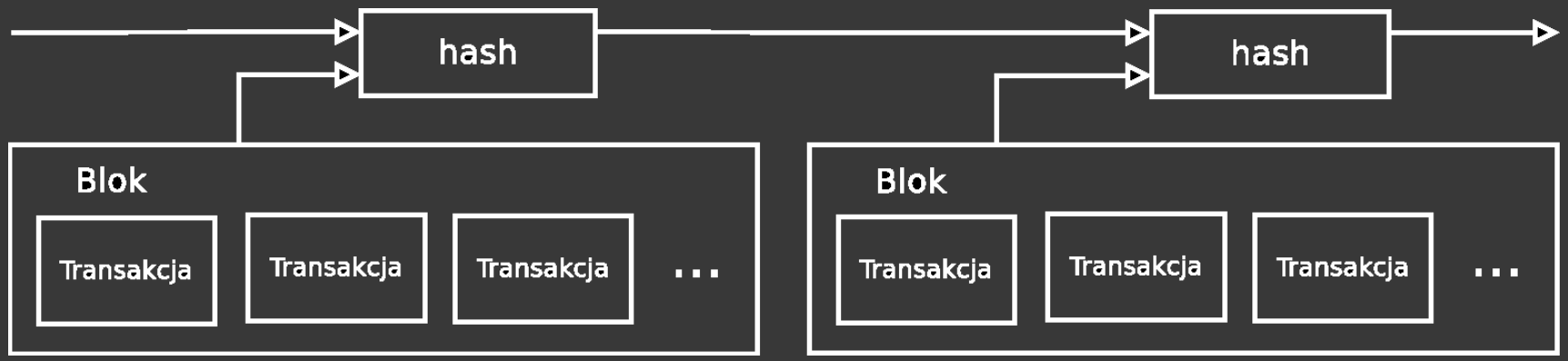
- W 2009 Satoshi Nakamoto publikuje pierwszy kod źródłowy Bitcoina i uruchamia sieć. BTC kosztuje wówczas kilkadziesiąt centów.
- Wąska grupa pasjonatów tworzy wokół Bitcoina ekosystem giełd, kasyn, sklepów z nielegalnym towarem i płatności wirtualnych.
- Większość pieniędzy jest w rękach pierwszych użytkowników.
- W 2011 powstają pierwsze kryptowaluty alternatywne.
- W listopadzie 2013 roku wartość BTC poziom 1000 USD.
- Zwrócenie uwagi polityków - powstają pierwsze regulacje prawne.
- W 2014 upada największa na świecie giełda Mt Gox.
- W 2015 liczba sklepów akceptujących BTC przekracza 100 tys.

Historia 2/2

- W 2016 moc sieci przekracza 1 exahash/s (trylion, tj. 1.000.000.000.000.000.000 operacji podwójnego hashowania SHA-256 na sekundę).
- W 2017 roku cena BTC osiąga poziom 20 tys. USD.
- W 2019 na świecie istnieje ponad 5 tys. bankomatów BTC.
- W 2020 Paypal wprowadza płatności BTC.
- Sieć BTC konsumuje około 121.36 TWh (terawatogodzin) energii elektrycznej w ciągu roku (dla porównania Argentyna 121 TWh, ZEA 113 TWh, Norwegia 122 TWh).
- W marcu 2021 cena przekracza 60 tys. USD.
- Obecnie moc Bitcoina wynosi prawie 200 exahash/s, kapitalizacja ponad 1 bilion USD, handel dobowy wynosi około 50 mld USD.

Ceny historyczne

Podstawowa budowa



- Blockchain składa się z bloków zorganizowanych w kolejności ich dodawania, powiązanych ze sobą przy pomocy skrótów (ang. hash) obliczonych z ich zawartości oraz skrótu poprzedniego bloku.
- Łańcuch jest publicznie dostępny i każdy może go pobrać.

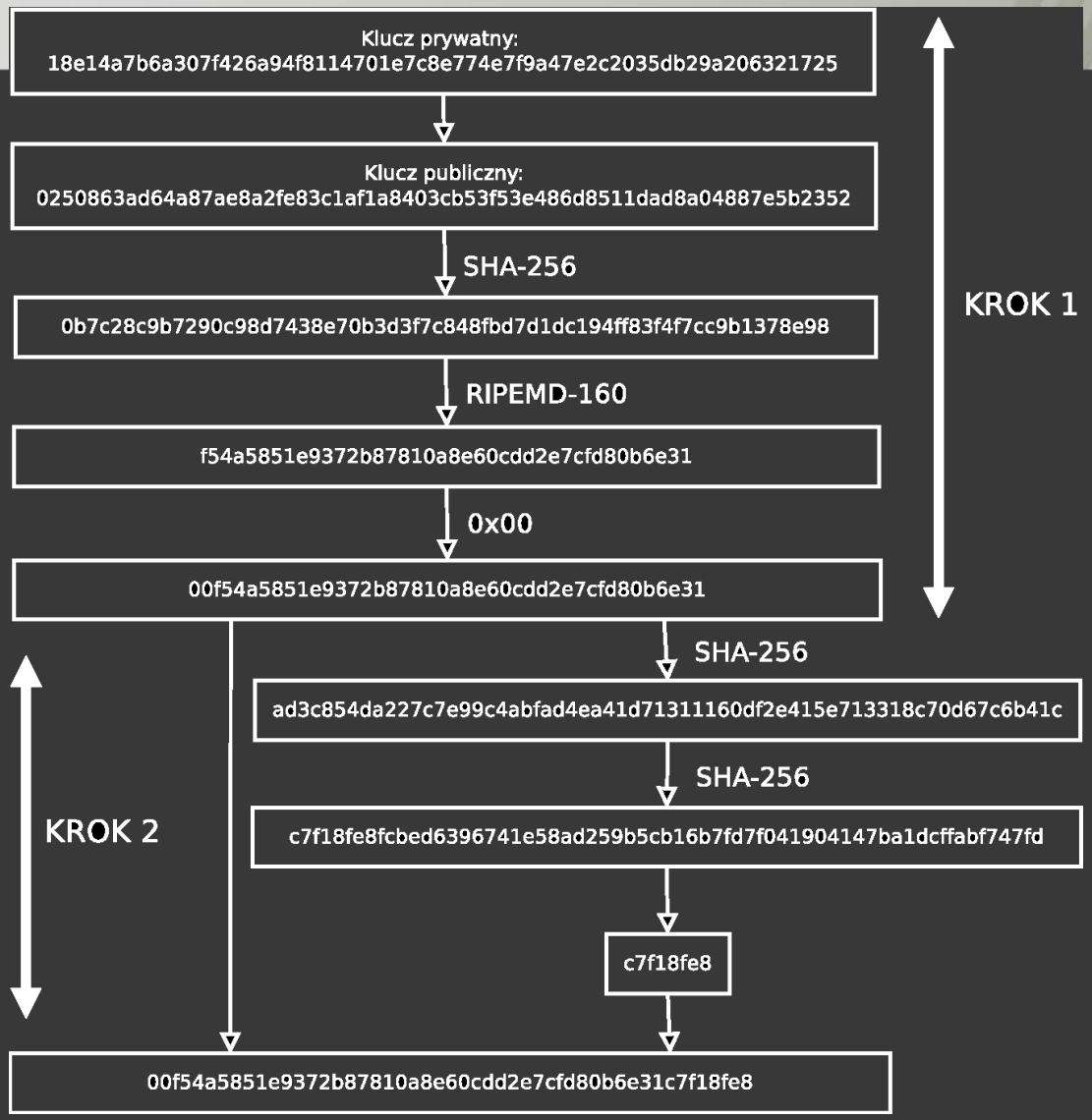
Podstawowa budowa

- Każdy blok zawiera zróżnicowaną liczbę transakcji, które składują istotne z punktu widzenia bazy informacje (np. przepływ pieniędzy).
- Transakcje mogą być dodawane przez wszystkich uczestników sieci.
- Nowe transakcje są grupowane w blok i dodawane do łańcucha po weryfikacji przez górników (dowód pracy).

Klucze, adresy i portfele

- Adresy portfeli są obliczane z kluczy prywatnych ECDSA (kryptografia asymetryczna).
- Klucze publiczne były zbyt długie (65 znaków) oraz byłyby wektorem ataków w przypadku złamania ECDSA, więc adresy nie są nimi, ale są z nich generowane.
- Jest niezwykle nieprawdopodobnym, aby dwie osoby wygenerowały ten sam adres. Sytuacje takie nazywane są kolizjami i nie udokumentowano jeszcze ani jednego przypadku.
- Powstał projekt Large Bitcoin Collider.

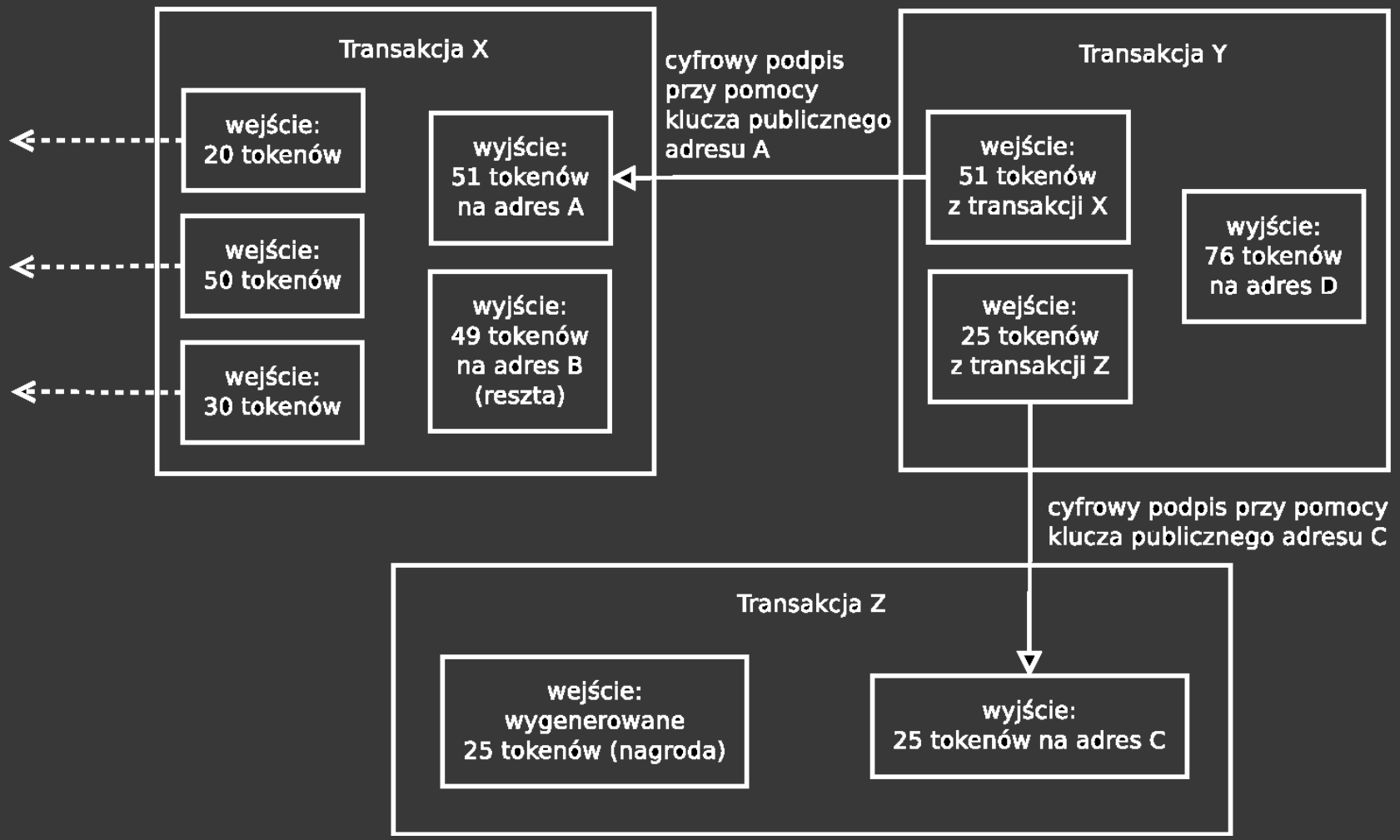
Tworzenie adresu



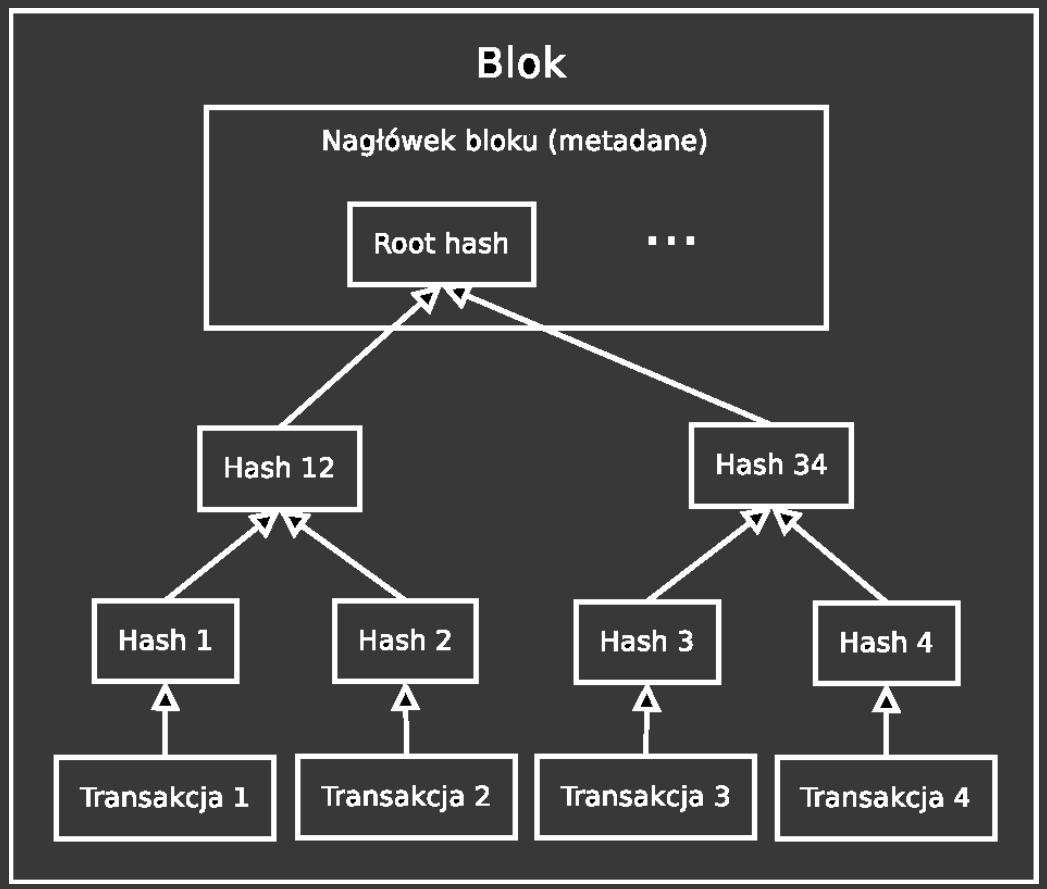
Transakcje

- W Bitcoinie transakcje odpowiadają za przenoszenie monet z jednego adresu na inny.
- Każda transakcja posiada dowolną liczbę wejść i wyjść.
- Wejścia są referencjami do wyjść poprzednich transakcji, z których otrzymane środki zostaną przekazane dalej.
- Wyjścia zawierają instrukcje przesyłu wskazanych środków na inne adresy.
- Suma środków na wyjściach musi być równa sumie na wejściach, aby uniknąć utraty środków.
- Oznacza to, że jedna transakcja może być użyta jako wejściowa tylko raz w całym blockchainie (nie ma double spendingu).

Transakcje


Transakcja X
wejście:
20 tokenów
wejście:
50 tokenów
wejście:
30 tokenów
wyjście:
51 tokenów
na adres A
wyjście:
49 tokenów
na adres B
(reszta)
cyfrowy podpis
przy pomocy
klucza publicznego
adresu A
Transakcja Y
wejście:
51 tokenów
z transakcji X
wejście:
25 tokenów
z transakcji Z
wyjście:
76 tokenów
na adres D
cyfrowy podpis przy pomocy
klucza publicznego adresu C
Transakcja Z
wejście:
wygenerowane
25 tokenów (nagroda)
wyjście:
25 tokenów na adres C

Drzewa hashujące



Bloki w Bitcoinie

- Pierwszy blok (genesis) jest wbudowany do Bitcoina na stałe i jest podstawą łańcucha.
- Bloki posiadają limit 1 MB co pozwala im pomieścić tysiące transakcji. Nagłówek to około 80 bajtów, a transakcja 250 bajtów (1 wejście i 2 wyjścia).
- Rozmiar bloku Bitcoina jest przedmiotem wieloletniej debaty, która wielokrotnie doprowadziła do tzw. hard forka.

Warstwa sieci

- Blockchain bazuje na modelu rozproszonej komunikacji.
- Wszystkie węzły sieci posiadają identyczne uprawnienia.
- Brak podmiotów centralnych lub pośredniczących.
- Jednym z podstawowych zadań każdego węzła jest weryfikacja otrzymanych danych i przekazanie ich dalej, jeżeli zostaną uznane za poprawne.
- Każdy węzeł może przechowywać wszystkie dane sieci, co zapobiega ich utracie w skali globalnej.
- Węzły sieci Bitcoin mogą pełnić cztery różne funkcje: portfela, górnika, routera oraz bazy danych.

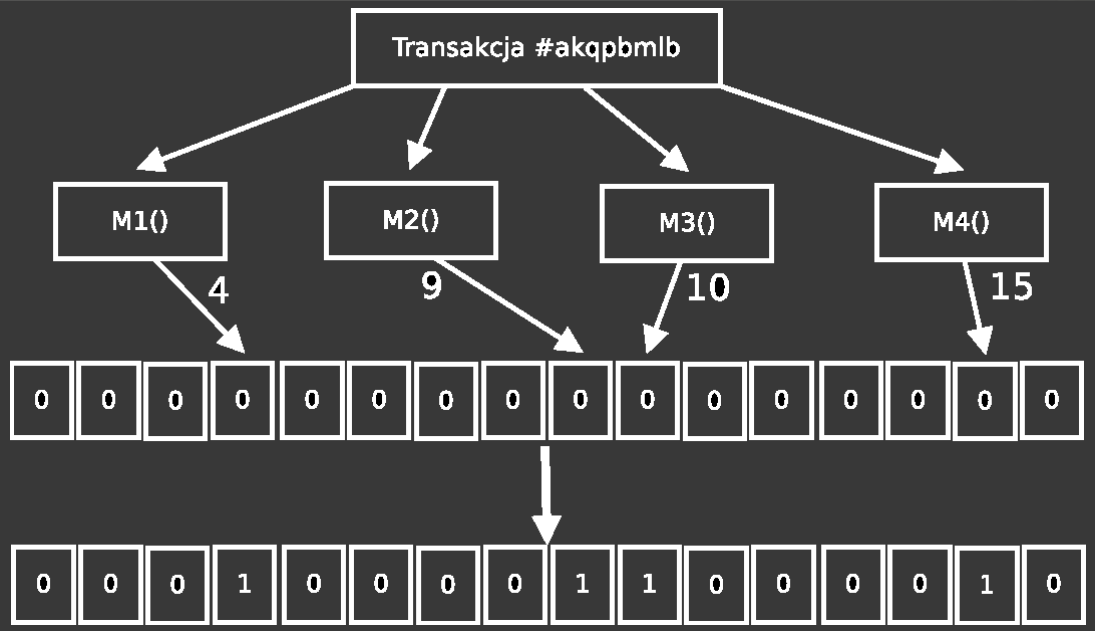
Odkrywanie sieci

- Wszystkie węzły mają takie same uprawnienia, jednakże istnieją wśród nich takie, które działają przez długi czas i uznane są za stabilne (ang. seed nodes).
- Ich lista jest na stałe zapisana w oprogramowaniu blockchaina.
- Pozwalają na uzyskanie informacji o innych użytkownikach i stanowią wrota dostępowe do sieci.
- Powszechnie stosowanym w odkrywaniu sieci protokołem jest DNS, który pozwala na zapisanie adresów seedowych na serwerach DNS.

Filtr Blooma

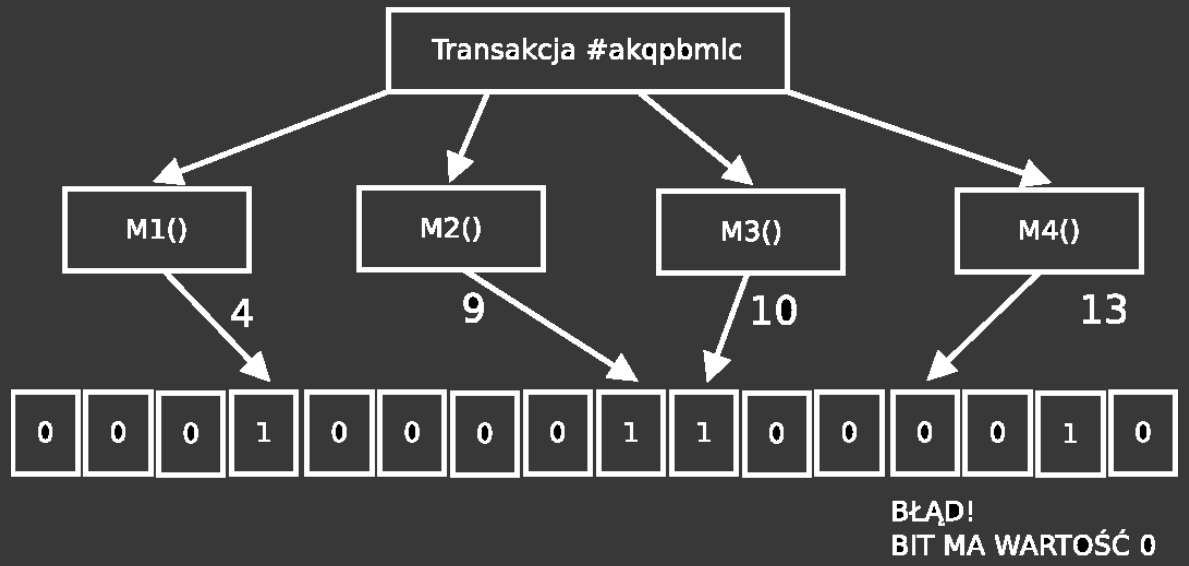
- Portfele mogą używać mechanizm SPV (ang. Simplified Payment Verification), który pobiera z sieci tylko nagłówki bloków i własne transakcje.
- Dzięki temu możliwe jest wysłanie do sieci prośby o własne transakcje bez zdradzania informacji, których adresów dotyczą.
- Przykład: Pytając gdzie jest aleja Mickiewicza zdradzamy rozmówcy dokąd chcemy się udać. W proponowanym rozwiązaniu wystarczy, zapytać o wszystkie ulice kończące się na "icza".

Dodanie wzorca do filtra Blooma



- Filtr Blooma w węzłach SPV jest definiowany jako N-elementowa tablica bitowa i M-elementowy zbiór funkcji hashujących, zwracających wartość z przedziału od 1 do N. Kontrolując parametry N i M można precyzować dokładność filtra.

Sprawdzenie wzorca w filtrze Blooma

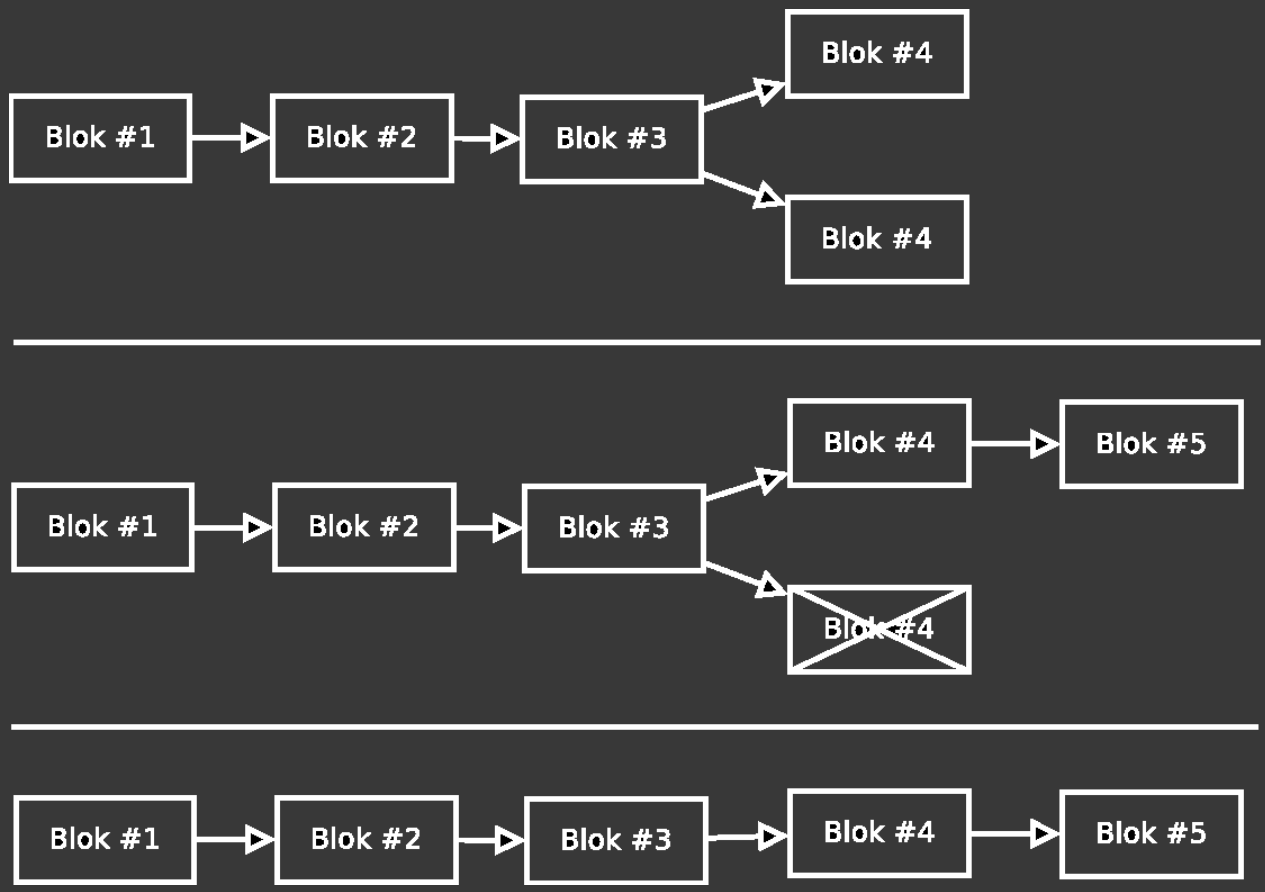


- Sprawdzana jest transakcja inna niż ta, która wchodzi w jego skład. W związku z tym trzy pierwsze funkcje hashujące wskazały bity ustawione na 1, ale ostatnia wskazała bit ustawiony na 0, co oznacza, że transakcja nie pasuje do wzorca.

Wydobywanie bloków i dowód pracy

- Węzły górników przechowują w pamięci podręcznej wszystkie rozgłoszone w sieci transakcje, które nie są jeszcze dodane do bloków.
- Oprogramowanie górnika zbiera z puli głównej "opłacalne" transakcje i grupuje je w blok, tak, aby nie przekroczyć 1 MB.
- Dołożenie nowego bloku do łańcucha w sieci Bitcoin polega na jego weryfikacji (wykopaniu).
- Bitcoin używa jednego z algorytmów konsensusu, zwanego dowodem pracy (ang. Proof of Work).
- W wykopywanym bloku górnik umieszcza adres swojego portfela, na który ma być wydana nagroda w przypadku osiągnięcia celu.

Odgałęzienie w blockchainie



Proof of Work

- W Bitcoinie jest to znalezienie takiego skrótu SHA-256 z bloku, aby liczba zer z przodu wynosiła tyle ile aktualna trudność kopania (ang. difficulty).
- Trudność kopania jest przeliczana co 2016 udanych weryfikacji (około 2 tygodnie) i zapisywana w każdym bloku.
- Obliczany z bloku skrót byłby zawsze taki sam, gdyby nie występujący w jego nagłówku parametr nonce.
- Poziom trudności kopania jest dynamiczny (blok co 10 minut).
- Jak zmodyfikować oprogramowanie, aby szybciej znajdowało skrót?
- Energochłonność :(Czy można użyć Bitcoina w nauce?

Ekonomia

- W sieci Bitcoin liczba tokenów możliwych do wykopania jest ograniczona (występuje deflacja). Docelowo po roku 2100 zostanie wykopany ostatni blok zamykający pulę 21 mln BTC.
- W celu dostosowania poziomu adopcji Bitcoina w realnym świecie do liczby monet w obiegu, wprowadzono mechanizm halvingu.
- Spadek mocy oznacza spadek trudności kopania - zarobki pozostają więc na stabilnym poziomie.
- Wszystkie BTC wykopane? Pozostają jeszcze opłaty za transakcje :)

Na koniec: wady blockchaina i wektory ataków

- Śledzenie historii transakcji
- Ataki 51% (500 najmocniejszych superkomputerów świata razem nie wystarczy)
- Ataki typu Sybil (wiele fałszywych węzłów + śledzenie)
- DoS (wiele nieprawidłowych transakcji wysłanych do węzła)
- Niepotrzebne lub nielegalne dane w sieci

Dziękuję za uwagę :)