Architektura Kryptowalut
Studium Bitcoina i Ethereum

Wojciech Korzeniowski Instytut Informatyki
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Abstrakt

Opis koncepcji i mechanizmów wykorzystanych przy tworzeniu kryptowalut.

I. Wstęp

Niniejszy artykuł przedstawia jakie problemy z pieniędzmi istnieją w dzisiejszym świecie i w jaki sposób pojawienie się kryptowalut może pomóc je rozwiązać. Następnie opiszę matematyczne koncepty które zostały wykorzystane przy projektowaniu kryptowalut oraz samą architekturę kryptowalut. Dalej wyjaśnię czym jest Blockchain, co oznacza kopanie bloków oraz jaki sposób zapewniane jest bezpieczeństwo. Następnie wyjaśnię czym jest fork w kontekście Blockchainu oraz opiszę co nowego wprowadza Ethereum w stosunku do Bitcoina.

A. Historia waluty

Od zarania dziejów na świecie istniał handel. Zanim jednak postały waluty, ludzie wymieniali się między sobą rozmaitymi dobrami w sposób bezpośredni. Jeden z problemów który występuje podczas takiej wymiany jest problem z wydaniem reszty. Przykładowo, jeżeli ktoś kto hodował świnie i potrzebował kostkę masła, musiał wymienić całą świnię na dużą ilość masła. Ewentualnie mógł podzielić świnie i zostać z resztą świni co mogło powodować problem z jej przechowaniem. Rozwiązaniem tego problemu okazały się waluty. Hodowca mógł sprzedać swoją świnie w zamian za określoną ilość danej waluty a następnie część przeznaczyć na zakup masła. Inny problem który istnieje w świecie bez walut to problem z oszacowaniem wartości jednych dóbr w stosunku do innych. Zdecydowanie łatwiej jest sprowadzić wartość dóbr do wspólnej waluty co

pozwala na łatwiejsze określenie w jakim stosunku powinna zostać dokonana wymiana jednego dobra z inne.

B. Rola banków

Jeżeli posiadamy pieniądze, ale nie chcemy być odpowiedzialni za ich przechowywanie możemy skorzystać z usług Banku. Podstawową operacją jaką możemy wykonać w Banku jest możliwość zdeponowania oraz pobrania wcześniej zdeponowanych środków. Kolejną z operacji jest wykonanie transferu środków z jednego konta na inne. Taka operacja umożliwia transfer środków innej osobie bez konieczności bezpośredniego przekazania pieniędzy w postaci monet czy banknotów. W takiej sytuacji Bank poświadcza że właściciel konta przekazał swoje środki innej osobie dzięki czemu ta może z nich skorzystać. Taka rola sprawa że Banki są jedną z instytucji zaufania publicznego. Oznacza to to między innymi fakt że społeczeństwo wierzy, iż w każdej chwili może odebrać powierzone Bankowi pieniądze a to jak pokazuje historia nie zawsze jest prawdą. Za przykład posłuży sytuacja Grecji z 2015 roku gdzie w wyniku kryzysu finansowego greckie Banki zostały zamknięte a wypłaty z bankomatów ograniczone do 60 euro na dzień.[1]

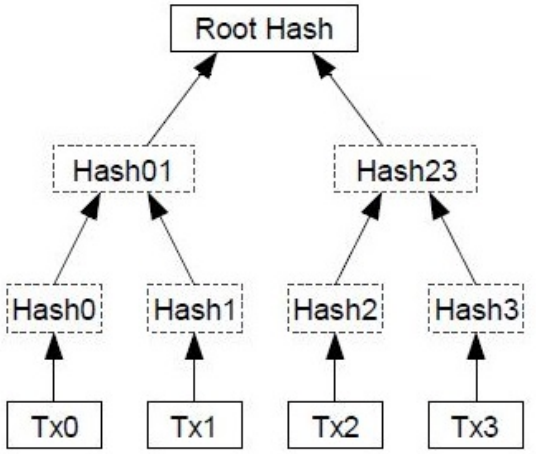
Fakt iż Bank jest odpowiedzialny za weryfikację czy dana osoba posiada odpowiednią ilość środków do wykonania transferu wymusza prowadzenie rejestru. W rejestrze znajduje się historia wszystkim transakcji oraz stan konta przypisany dla każdego użytkownika. Na banku spoczywa odpowiedzialność aby zawartość rejestru nie wpadła w niepowołane ręce oraz aby rejestr nie przepał co spowodowałoby utratę zgromadzonych przez klientów środków gdyż tylko on jest dokumentem poświadczającym stan konta.

II. Matematyka

W tym rozdziale omówię matematyczne koncepty które zostały wykorzystane przy projektowaniu kryptowalut, będę się do nich odnosił w dalszej części artykułu.

A. Funkcja skrótu

Funkcja skrótu jest to funkcja która przyporządkowuje dowolnemu ciągowi znaków, inny ciąg znaków o stałej długości. Jedną z właściwości funkcji skrótu jest fakt iż po niewielkiej zmianie źródłowego ciągu znaków, wynik funkcji zmienia się całkowicie, co widać na poniższych przykładach:



Ryc. 1. Drzewo skrótów

$$\text{SHA256}('Alice') = 3bc5106297\ldots a0699a3043 \tag{1}$$

$$\text{SHA256}('Bob') = cd9fb1e148\ldots bb4bb4e961 \tag{2}$$

$$\text{SHA256}('Bob.') = ec46deb8be\ldots d035fd84a2 \tag{3}$$

Kolejną właściwością funkcji skrótu jest niemożliwość znalezienia źródłowego ciągu znaków posiadając tylko jego skrót. Fakt ten sprawia że funkcję skrótu można wykorzystać do sprawdzania czy dwie wartości są takie same bez potrzeby przechowywania oryginalnej wartości. Jest to wykorzystywane podczas logowania się użytkowników w serwisach internetowych. Dzięki temu w bazie danych nie są przechowywane hasła w sposób jawny, zamiast tego przechowuje się jedynie ich skrót który jest porównywany ze skrótem wprowadzonego hasła podczas logowania.

B. Drzewo skrótów

Jest to bardziej rozbudowana wersja funkcji skrótu dzięki której możemy otrzymać skrót z listy obiektów. W kontekście kryptowalut wykorzystuje się drzewo skrótów do otrzymania skrótu grupy transakcji. Najpierw wyliczany jest skrót dla pojedynczej transakcji później skróty są parowane a następnie z pary obliczany jest kolejny skrót. Operacja jest powtarzana aż otrzymamy jeden skrót który reprezentuje skrót całej listy. Wizualizacja obliczania przedstawiona jest na

diagramie numer 1 gdzie pojedyncza transakcja jest reprezentowana przez symbol *Tx* a skrót całości oznaczony jest jako *Root Hash*.

C. Podpis cyfrowy

Podpis cyfrowy jest techniką która pozwala na weryfikację autora wiadomości. Osoba chcąca skorzystać z podpisu cyfrowego musi posiadać klucz prywatny oraz klucz publiczny. Klucz prywatny służy do podpisywania wiadomości i powinien być znany tylko i wyłącznie autorowi wiadomości. Z kolei klucz publiczny służy do weryfikacji czy wiadomość została podpisana przez odpowiadający mu klucz prywatny. W wyniku podpisu wiadomości powstaje Sygnatura która zostaje przesłana wraz z wiadomością. Odbiorca wiadomości wykorzystując Sygnaturę, klucz publiczny nadawcy oraz samą wiadomość jest w stanie sprawdzić czy wiadomość została podpisana przy użyciu właściwego klucza prywatnego.

III. Kryptowaluty

Kryptowaluta jest to wirtualna waluta która nie ma swojej fizycznej reprezentacji. Jednak nie powinno się jej postrzegać jako byt który ma mniejszą wartość niż waluty tradycyjne. Często można usłyszeć opinię iż kryptowaluty nie mają żadnej wartości ponieważ nie są fizyczne i istnieją tylko wirtualne. Każda waluta sama w sobie nie ma żadnej wartości, nabiera ją dopiero wtedy, kiedy możemy w zamian za nią otrzymać coś innego. Brak posiadania fizycznej postaci rozwiązuje problem przechowywania dużych ilości pieniędzy bez konieczności korzystania z Banków. Z drugiej strony powoduje powstanie nowych problemów z jej przechowywaniem oraz wykorzystaniem jako środek płatności jednak jest to kwestia świadomości jakie istnieją zagrożenia i w jaki sposób można im zapobiec.

A. Portfel

Portfel stanowi para klucz prywatny oraz klucz publiczny. Klucz prywatny służy do podpisywania transakcji w których pieniądze są przelewane z powiązanego portfela na inny portfel wskazany poprzez przypisany do niego klucz publiczny. Klucz publiczny stanowi swego rodzaju adres na który można przesłać pieniądze. Natomiast klucz prywatny jest hasłem do naszego konta bankowego bez którego nie jesteśmy w stanie wykonać przelewu.

Najczęściej klucze reprezentowane są jako ciąg znaków zakodowany przy pomocy base58. Dzięki zastosowaniu base58 klucze są zapisywane w postaci ciągu liter i cyfr z pomięciem

znaków które jest łatwo ze sobą pomylić, takich jak 0 (cyfra zero) oraz O (litera O). Istnieje jednak możliwość zapisana kluczy w dowolny sposób który umożliwia odtworzenie oryginalnego ciągu znaków. Do tego celu może zostać wykorzystany np. kod QR, obraz cyfrowy w którym na najmniej znaczących bitach zapisana jest informacja o kluczach (steganografia), kilkanaście losowo wygenerowanych podczas tworzenia portfela słów które można zapamiętać, zapisać lub dalej zakodować. Możliwości na przechowywanie klucza prywatnego są ograniczone ludzką pomysłowością na zapis informacji w sposób zrozumiały tylko dla autora.

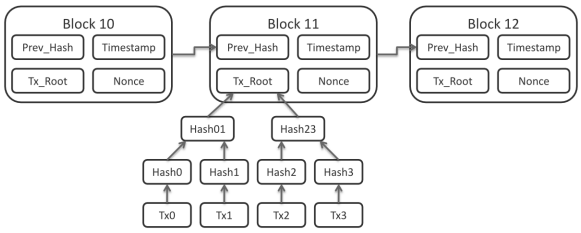
B. Transakcja

W celu wykonania transakcji użytkownik musi posiadać klucz prywatny. Transakcja zawiera w sobie informację na jaki portfel powinna zostać przeniesiona określona ilość waluty. Po utworzeniu Transakcji musi ona zostać podpisana przy pomocy klucza prywatnego powiązanego z portfelem z którego zostaje wykonany transfer. Następnie transakcja wraz z podpisem zostaje wysłana do sieci Blockchain która zajmuje się weryfikacją transakcji oraz zapewnia prawidłowe działanie całego systemu.

Istotny jest fakt iż utworzenie transakcji z podpisem oraz wysłanie jej do sieci nie muszą nastąpić w tym samym momencie. W celu uzyskania najwyższego bezpieczeństwa zalecane jest wykonanie podpisu transakcji na komputerze bez podłączenia do internetu. Następnie skopiowanie transakcji wraz z podpisem na komputer połączony z internetem i wysłanie jej do sieci. W ten sposób zyskujemy większe bezpieczeństwo poprzez fakt iż klucz prywatny nie jest przechowywany ani wprowadzany na komputerze z połączeniem internetowym który jest bardziej narażony na złośliwe oprogramowanie niż odizolowana jednostka.

IV. BLOCKCHAIN

Blockchain jest sercem kryptowalut i stanowi rewolucję w dziedzinie rozproszonych baz danych. Blockchain składa się z bloków który z kolei zawiera listę transakcji. Wielkość bloku jest ustalona i w przypadku Bitcoina wynosi nie więcej niż 1MB, co daje około 2000 transakcji na blok.[2] Bitcoin jest zaprojektowany tak aby nowy blok z transakcjami pojawiał się co 10 minut co daje ostatecznie 3-4 transakcje na sekundę. Dla porównania PayPal realizuje średnio 193 trasakcje na sekundę a Visa 1’667.[3]



Ryc. 2. Schemat Blockchain

A. Blok

Na Rycinie 2 przedstawiony został schemat Blockchainu oraz pojedynczego bloku. Każdy z bloków składa się z listy transakcji oraz jej wartości jej skrótu wyliczonej przy użyciu drzewa skrótów, skrótu z poprzedniego bloku, oraz wartości *Nonce*. Wszystkie z wymienionych elementów są użyte do obliczenia skrótu danego bloku.

Każdy z bloków w Blockchainie musi spełnić warunek aby jego hash zaczynał się op określonej liczby zer. Aby to osiągnąć do bloku została dodana wartość *Nonce*. Zmiana jej wartości całkowicie zmienia wartość hash z bloku.

Podział na bloki i zawieranie wartości funkcji skrótu z poprzedniego bloku przypomina strukturę która została użyta do budowy systemu Git[4]. Całość tworzy liniową strukturę w której dowolna zmiana bloku z przeszłości (taka jak dodanie lub usunięcie transakcji) powoduje zmianę hasha tego bloku co skutkuje przerwaniem łańcucha Blockchain ponieważ kolejny blok zawiera hash zmienionego bloku sprzed modyfikacji. Aby zachować integralność z blokami występującymi dalej w Blockchainie należy dla każdego z tych bloków ustawić nową wartość hash poprzedniego bloku.

B. Kopanie bloków - Proof of work

Jako że nie ma możliwości aby uzyskać źródło funkcji skrótu na podstawie jej wyniku jedyną możliwością na spełnienie wymagania aby hash bloku zaczynał się od określonej liczby zer jest sprawdzanie kolejnych wartości *Nonce* aż trafimy na taką która spełnia to wymaganie. Znalezienie tej wartości jest bardzo czasochłonne i tym zadaniem zajmują się kopacze bloków którzy w zamian za udostępnienie swojej mocy obliczeniowej dostają wynagrodzenie w danej kryptowalucie. To dzięki temu w sieci pojawia się co raz więcej Bitcoinów. Pierwsze bloki w Blockchainie nie zawierały żadnych transakcji a jedynie wynagrodzenie dla kopacza. Nagroda

ta jest zmniejszana o połowę co 4 lat aż do osiągnięcia limitu 21 milionów Bitcoinów w sieci, wtedy kopacze przestaną dostawać wynagrodzenie za samo znajdowanie odpowiedniej liczby *Nonce*. Po osiągnięciu limitu kopacze będą dostawać wynagrodzenie w postaci prowizji za transakcje. Prowizje ustala autor transakcji, im większa prowizja, tym większa szansa na to że jego transakcja znajdzie się w kolejnym bloku. W przypadku ustalenia zbyt małej prowizji istnieje ryzyko że transakcja nigdy nie zostanie zaakceptowania ponieważ kopacze wybiorą transakcje z większą prowizją do następnego bloku. W czasie pisania artykułu w sieci znajdowało się 150'000 transakcji oczekujących na akceptację[5].

Wraz ze wzrostem sieci liczba wymaganych zer może ulec zmianie. W sieci Bitcoin ustalenie liczby wymaganych zer następuje raz na 2 tygodnie i dobierane jest tak aby wydobycie nowego bloku zajmowało średnio 10 minut.

C. Atak 51%

W przypadku gdy ktoś chciałby skompromitować sieć Bitcoin poprzez zmianę jednej z historycznych transakcji, musi wykopać jeszcze raz dany blok oraz wszystkie bloki które po nim występują. Dla przypomnienia, trudność wydobycia bloku jest dostosowana tak aby całej sieci średnio zajmowało to 10 minut. Prawdopodobieństwo wydobycia dwóch lub więcej bloków przez jednego kopacza szybciej niż reszta sieci jest bliska zeru. Warunkiem wymaganym do skutecznego ataku jest posiadanie minimum 51% mocy obliczeniowej sieci. W przeciwnym wypadku reszta sieci będzie w stanie szybciej wydobywać nowe bloki co skutkuje powstaniem dłuższego łańcucha.

W przypadku istnienia wielu łańcuchów brany jest pod uwagę ten który jest dłuższy. Wynika to z teorii gier która zakłada że gracz zyska więcej na przestrzeganiu zasad (akceptacja dłuższego łańcucha i próba wydobycia nowego bloku na jego szczycie) niż na łamaniu zasad (próba kompromitacji łańcucha poprzez nadpisanie istniejącej historii lub wydobywanie bloku na krótszym łańcuchu).

Przez tą niepewność odnośnie końcowych bloków łańcucha które mogą ulec zmianie poprzez zastąpienie go innymi blokami istnieje określenie pewność bloku. Im blok jest dalej od końca łańcucha tym bardziej pewny się staje i maleje szansa na to że zostanie podmieniony. Przyjmuje się że 6. blok od końca jest wystarczająco pewny i jest niewielka szansa na to że w przyszłości ulegnie podmianie.

V. Forki

Istnieje możliwość celowego rozdzielenia łańcucha Blockchain. Najczęstszym z powodów jest zmiana architektury kryptowaluty dzięki której poprawi się jej stabilność. Zazwyczaj po forku właściciele portfeli z bazową kryptowalutą stają się właścicielami takiej samej ilości nowej waluty ile posiadali bazowej przed forkiem.

A. Bitcoin Cash

Jest pierwszym *hard forkiem* Bitcoina. Oznacza to iż jego wersja nie jest kompatybilna wstecz z Bitcoinem. Główną zmianą było zwiększenie wielkości bloku z 1MB do 8MB co według założeń twórców spowoduje iż Bitcoin Cash będzie bardziej użyteczny przy transferach małych kwot. Sytuacja miała miejsce w momencie gdy za transakcję Bitcoina trzeba było zapłacić kilkadziesiąt dolarów.

B. Bitcoin Gold

Kolejny fork Bitcoina który powstał 2.5 miesiąca po forku Bitcoin Cash. Przez wielu uznany za oszustwo i nie powinien być traktowany na poważnie. Wprowadzone zmiany obejmują zmianę algorytmu wykorzystanego do wyliczania skrótu, zmiana z SHA256 na Equihash. Dodatkowo dostosowanie trudności wydobycia bloku następuje po wykopaniu każdego bloku, w oryginalnym Bitcoinie zmiana następuje co 2016 blok czyli około 2 tygodnie.

C. SegWit2x

Fork który nie doszedł do skutku jednak miał wpływ na wahania ceny Bitcoina. Zmiana obejmuje głównie podwojenie bloku w stosunku do Bitcoina z 1MB na 2MB. Został odwołany ponieważ społeczność uznała iż zmiana niewiele wnosi biorąc pod uwagę iż już istnieje Bitcoin Cash ze zwiększoną wielkością bloku i kolejny fork nie wniesie żadnej korzyści.

VI. Ethereum

W przeciwieństwie do forków, Ethereum jest całkowicie nową walutą która wprowadza możliwość wprowadzenia własnego kodu źródłowego do Blockchainu. Dzięki temu Ethereum jest w stanie zaoferować o wiele więcej niż transfery środków.

A. *Kontrakty*

Ethereum umożliwia utworzenie kontraktów. Dzięki temu mechanizmowi możliwe jest wykorzystanie blockchainu jako rozproszonej bazy danych w której istnieje gwarancja że dane nie zostana zmienione ani usunięte. Kontrakt składa się z własnej pamięcie oraz z funkcji które mogą korzystać z tej pamięci i wysyłać walutę na inny adres. Funkcje można porównać do procedur znanych z relacyjnych baz danych przy pomocy których można się czytać z pamięcie kontraktu oraz ją modyfikować. Czytanie pamięci kontraktu odbywa się bezpłatnie, natomiast jeżeli chcemy wprowadzić zmiany w pamięci kontraktu zmuszeni jesteśmy do uiszczenia opłaty za tę operację. Kosz jest proporcjonalny do złożoności obliczeniowej operacji którą chcemy wykonać.

Kontrakt który został umieszczony na Blockchainie nie może zostać już zmieniony. Może zostać utworzony nowy, zmieniony kontrakt, jednak istniejącego nie można zmienić.

Najprostszym przykładem kontraktu jest dystrybucja Tokenów. Każdy może utworzyć swoje własne Tokeny na Blockchainie Ethereum a następnie je sprzedawać za Ethereum. Przykładowo politycy mogą wydawać swoje własne Tokeny które mogą zostać zakupione przez wyborców Dzięki temu politycy zyskują fundusze na działalność a kupujący wierzy w to że polityk jest uczciwy i działa dla dobra społeczeństwa co powinno spowodować wzrost wartości jego Tokenów. Mechanizm został nazwany ICO (Initial Coin Offering) i aktualnie staje się nową formą crowdfoundingu.

Innym kontraktem może być loteria. Uczestnicy wpłacają pieniądze na adres Kontraktu. Następnie dokonuje się losowanie w wyniku którego wybrany zostaje jednej z uczestników który wygrywa całą pulę.

PODSUMOWANIE

Kryptowaluty zdają się być rewolucją w bankowości i podejściu do waluty na miarę rewolucji dokonanej przez internet w dziedzinie komunikacji. Główną z zalet Kryptowalut jest oderwanie ich od fizycznej postaci, możliwość transferu do dowolnego miejsca na Ziemi bez pośredników, przejrzystość oraz brak możliwości dodrukowania. Z góry wiadomo ile maksymalnie może ich powstać oraz jakie są zasady dystrybucji. Według wizji wielu osób Banki, ubezpieczalnie, zakłady bukmacherskie i wszelkie działalności w których występuje transfer pieniędzy będzie można zastąpić odpowiednią Kryptowalutą, Konraktem czy kolejną ideą zbudowaną na na Blockchainie.

Pewne jest to że sama technologia Blockchain zrewolucjonizuje wiele sektorów ponieważ ma wiele do zaoferowania jako szeroko pojęta rozproszona baza danych niekoniecznie związana z pieniędzmi. Już można znaleźć informacje o planowanych migracjach systemów bankowych na Blockchain, wykorzystanie go do przechowywania danych medycznych, czy nawet przeprowadzania wyborów.

BIBLIOGRAFIA

[1] PolskieRadio.pl. (2015) Grecja: bankomaty zaczęły ponownie działać. nie ma limitu wypłat dla zagranicznych turystów. [Online]. Available: https://www.polskieradio.pl/42/273/Artykul/1468946

[2] blockchain.info. [Online]. Available: https://blockchain.info/charts/n-transactions-per-block

[3] PolskieRadio.pl. (2017) Bitcoin and ethereum vs visa and paypal – transactions per second. [Online]. Available: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html

[4] L. Torvalds. Git - system kontroli wersji. [Online]. Available: https://git-scm.com

[5] blockchain.info. [Online]. Available: https://blockchain.info/unconfirmed-transactions