Zamykanie transakcji oraz tworzenie konsensusu masternodów:

Mechanizm zapobiegania wydawaniu tych samych środków dwukrotnie.

Data publikacji: 22 września 2014

Wersja dokumentu: 2

Evan Duffield – evan@darkcoin.io

Holger Schinzel – holger@darkcoin.qa

Fernando Gutierrez – gutierrezf@gmail.com

Abstract. *Bitcoin oraz inne kryptowaluty używają rozproszonego systemu zwanego blockchain do osiągnięcia konsensusu całej sieci [Nielsen13]. Sprzedawcy i handlarze zazwyczaj czekają, aż transakcja zostanie potwierdzona przez sieć aby upewnić się, że jest ona autentyczna i nie paść ofiarą ataku wydania tych samych środków dwa razy (double spending attack). Podwójne wydanie tych samych funduszy może nastąpić gdy oszust wyśle dwie sprzeczne ze sobą transakcje, jedną do sprzedawcy (lub kogokolwiek innego) a drugą do samego siebie.*

W Bitcoinie, zwykłe potwierdzenie średnio zajmuję 10 minut. W zależności od tego jak bezpieczny chce być sprzedawca, może on zażądać wielu potwierdzeń tej samej transakcji co może wydłużyć ten czas nawet do 60 minut.

W tym artykule omawiamy rozwiązanie tego problemu trapiącego Bitcoin i inne kryptowaluty. Jak zagwarantować autentyczność transakcji bez czekania na potwierdzenia z blockchain?

1. Wprowadzenie

Stworzony przez Satoshi Nakomoto w 2009 r. Bitcoin [Nakamoto09] jest rozproszonym systemem płatności peer-to-peer. Od samego początku Bitcoin powoli zyskiwał na popularności i wiele przedsiębiorstw zaczęło akceptować Bitcoin jako zapłatę za swoje towary i usługi [Reuters14]. Chociaż Bitcoin okazał się być sukcesem, to w porównaniu do swoich większych konkurentów – kart płatniczych - posiada on jedną poważną wadę. Podczas robienia zakupów, karty płatnicze mają prawie natychmiastową autoryzację płatności, podczas gdy w przypadku Bitciona, trzeba czekać na potwierdzenie transakcji przez sieć. W przypadku dokonywania płatności za pomocą kart płatniczych, informacja zostaje wysłana do firmy która wydała tę kartę i pieniądze są trzymane przez tę firmę dopóki transakcja nie zostaje później potwierdzona, a pieniądze przelane na konto sprzedawcy. W przeciwieństwie do kart płatniczych, klient Bitcoina wysyła wiadomość na ślepo, wierząc że jest ona prawdziwa bez otrzymania żadnych informacji z sieci.

Darkcoin jest kryptowalutą której najważniejszym celem jest dodanie anonimowości do transakcji online. Bazuje on na pracy Satoshi Nakamoto i zawiera wiele różnych usprawnień technologii która została użyta w kliencie Bitcoina. Do wspomnianych usprawnień zaliczają się, funkcje anonimizujące oraz sieć z wbudowanymi zachętami finansowymi do świadczenia usług [Duffield14].

W artykule tym, mamy zamiar przedstawić; sieć węzłów tzw. masternodów jako sieć nadzorująca, używająca; rozproszonego konsensusu oraz algorytmu zamknięcia transakcji ''TX locking" do zabezpieczenia niepotwierdzonych transakcji. Sieć nadzorująca obserwuje każdą transakcję dając im status jako sfinalizowane zaraz po nadaniu ich do sieci. Później, omówimy również różne możliwości ataku na sieć oraz jak sieć masternodów może im zapobiec.

2. Sieć masternodów

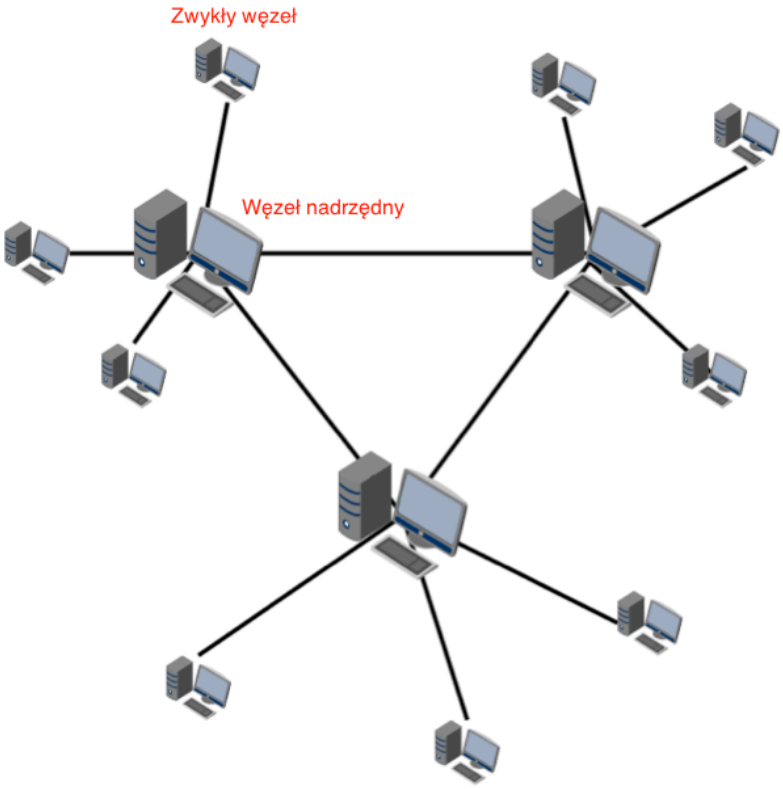
Pierwotnie, masternody zostały wprowadzone do Darkcoin jako wsparcie dla procesu mieszania używanego w implementacji DarkSend. Oryginalne wymagania zostały opisane przez Evan Duffield w kwietniu 2014 roku:

„Węzły te, są fundamentem DarkSend. Wszystkie transakcję będą przez nie przesyłane. Każdy z nich wymaga aby 1000DRK było trzymanych pod ich adresami i za każdym razem kiedy węzeł zostanie wybrany, sieć przeznaczy 10% [podczas gdy pisałem ten artykuł, wynagrodzenie zostało zmienione do 20%] danego bloku dla tego węzła. Jeśli chcesz uruchomić masternoda, musisz być w miarę obeznany z zarządzaniem siecią oraz zabezpieczaniem hosta." [Masternodes]

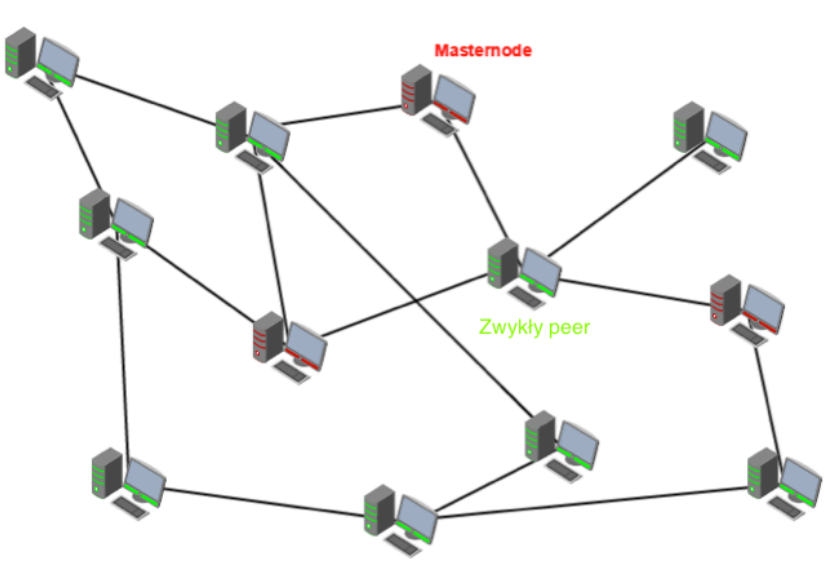
Użytkownicy zarządzający masternodami muszą trzymać 1000DRK jako coś w rodzaju zabezpieczenia. W sieci Darkcoin, zabezpieczenie to, nigdy nie przestaje być w posiadaniu użytkownika oraz jest nie do podrobienia. Może ono zostać wydane, lub przeniesione do innego portfela. Gdy tak się staje masternode zostaje usunięty z listy wszystkich masternodów i nie może otrzymywać prowizji za retransmisje transakcji.

Jądro Darkcoina zostało zmienione w taki sposób aby wspierało drugą sieć P2P, której zadaniem jest rozpowszechnienie wiadomości i synchronizacja wszystkich znanych masternodów w sieci. Dzięki temu dodatkowi, każdy podłączony do sieci klient Darkcoina wie ile jest dostępnych masternodów i może z nich skorzystać dokonując transakcji.

Masternody, - w przeciwieństwie do sieci Gnutella, - która używa hierarchicznej struktury sieci, gdzie węzeł klienta łączy się z tylko jednym węzłem nadrzędnym - są traktowane przez sieć w taki sam sposób oraz są praktycznie identyczne z innymi węzłami, dzięki czemu tworzą one klasyczną sieć P2P.



Rycina 1: Sieć P2P węzłów nadrzędnych



Rycina 2: Sieć masternodów Darkcoin

Jeśli portfel jest uruchomiony i wszystkie warunki są spełnione (statyczne IP, 1000 DRK) to praktycznie każdy węzeł (peer) może stać się masternodem.

Chociaż, w pierwotnym zamierzeniu masternody miały służyć do anonimizowania monet to posiadanie sieci peerów, stwarza możliwość wykorzystania ich w do innych zadań.

3. Zamykanie transakcji

Częstym problemem dużych rozproszonych systemów jest upewnienie się, że tylko jeden węzeł - spośród całej ich puli - przetwarza daną transakcję. Rozwiązanie tego wyzwania

potrzebuje działania różnego rodzaju algorytmów konsensusu np. takich jak Paxos [Chandra07]

Bitcoin na przykład, używa dowodu pracy (proof of work) aby osiągnąć konsensus wśród wszystkich węzłów sieci. Jednakże, z powodu swoich parametrów technicznych, sposób ten ogranicza prędkość z jaką transakcja może zostać uznana za potwierdzoną i zabezpieczoną przed atakiem podwójnego wydania tych samych środków.

Aby zmniejszyć czas jaki transakcja potrzebuje do uzyskania potwierdzenia, możliwym jest przyśpieszenie generacji bloków. Jednak rozwiązanie to, powoduje szybszy rozrost blockchainu oraz z powodu opóźnień w przesyłaniu sygnału przez sieć ograniczony jest do mniej więcej 1 bloku co 30 sekund.

Proponujemy aby połączyć algorytm dowodu pracy z implementacją rozproszonego menadżera zamykania transakcji (distributed lock manager DLM), korzystającego z sieci masternodów.

W przeciwieństwie do Chubby [Burrows06], który potrafi zamknąć (lock) zasoby plików, my mamy zamiar zaimplementować system zamykania transakcji wejściowych.

Klient Darkcoina potrafi lokalnie zamknąć transakcje wejściowe aby nie były one użyte nigdzie indziej. W większości wypadków odbywa się to w specjalnych implementacjach, które używają RPC API klienta, aby ręcznie stworzyć transakcję.

Koncept zamykania transakcji może zostać rozszerzony do zamykania transakcji w całej sieci, zamiast robienia tego tylko na poziomie lokalnym jak to ma miejsce w przypadku wielu inny kryptowalut. Aby skutecznie ochronić się przed atakiem podwójnego wydatku, rozwiązanie to musi poradzić sobie z problemem konsensusu sieci oraz problemem tworzenia wyścigu zamkniętych transakcji.

3.1 Rozwiązanie podwójnego wydatku, przez zamykanie transakcji

W większości implementacji, zalecane jest aby sprzedawca miał jakiegoś rodzaju zabezpieczenie przed oszustami próbującymi wydać te same monety dwa razy. Może to być osiągnięte przez posiadanie klientów, które działają jako obserwatorzy sieci i dają znać sprzedawcy jak tylko zauważą próbę podwójnego wydania tych samych środków [Karame12]. W naszym rozwiązaniu proponujemy aby użyć sieć masternodów jako obserwatorów i zmienić protokół sieci w taki sposób aby dać pewnej grupie masternodów możliwość nadzoru transakcji.

Idea zamykania transakcji polega na tym, że klienci wysyłają chęć zamknięcia transakcji z jednego konkretnego adresu do innego adresu (lub wielu adresów). Dokonuje się to przez transmisję pakietu zawierającego transakcję oraz komendę zamykającą. Użytkownik podpisuje taką wiadomość swoim adresem (lub adresami) wyjściowym i przesyła ją do sieci.

Transaction Lock: (''txlock'', CTransaction, nBlockHeight, Signed Message)

Wiadomość zamykające będą nadawane do wszystkich klientów Darkcoin. Jak już taka wiadomość dotrze do wszystkich, to grupa deterministycznie wybranych masternodów stworzy konsensus. Następnie, po tym jak masternodom uda się osiągnąć konsensus,

nadana zostaje wiadomość do sieci potwierdzająca to wydarzenie i od tego momentu każdy klient Darkcoin uzna tę transakcję za zamkniętą.

3.2 Konsensus sieci oraz zarządzanie zamykaniem przez masternody.

Masternody tworzą sieć dzięki której możemy być pewni, iż dana transakcja jest autentyczna i zostanie dodana do blockchain. Tuż po otrzymaniu przez sieć wiadomości o zamkniętej transakcji, wybrane masternody rozpoczną głosowanie nad autentycznością zamku założonego na tą transakcję.

Jeśli konsensus zostanie osiągnięty przez sieć masternodów, wszystkie sprzeczne transakcje zostaną odrzucone, oprócz tej której ID pasuje do założonego zamka. Zadaniem klientów Darkcoina byłoby odrzucenie sprzecznych zamków oraz odwrócenie transakcji której celem było wydanie dwa razy tych samych monet. Mechanizm ten zadziałałby tylko wtedy gdy atakujący nadałby do sieci wiele zamków na raz i sieć przyjęłaby jeden zamek a drugi odrzuciła.

Jeśli konsensus nie zostanie osiągnięty, to transakcja taka będzie musiała zostać potwierdzona w sposób standardowy, czyli przez blockchain, aby mieć pewność, że jest ona prawidłowa.

3.3 Algorytm wyborów i głosowanie

Aby dokonać pseudo-losowego wyboru masternodów, użyty został specjalny deterministyczny algorytm. W tym systemie to właśnie sieć kopaczy będzie gwarantować bezpieczeństwo tej funkcji, przez używanie haszy dowodu wykonania pracy (proof-of-work) dla każdego bloku,

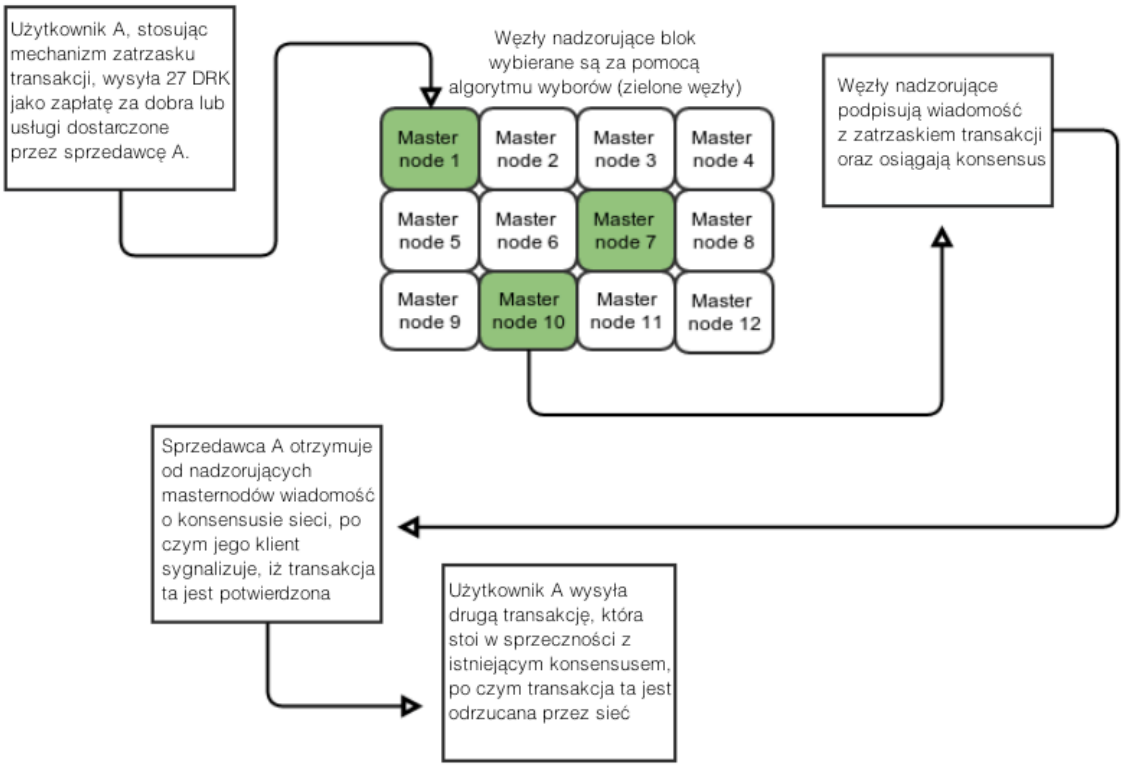
Pseudo kod wyboru masternoda:

```
For(masternode in masternodes){
    n = masternode.CalculateScore();

    if(n > best_score){
          best_score = n;
          winning_node = masternode;
    }
}

Cmasternode::CalculateScore(){
  n1 = GetProofOfWorkHas(nBlockHeight); // get hash of this block
  n2 = x11(n1); //hash the POW hash to increase the entropy
  n3 = abs)n2 – masternode_vin);

  return n3
}
```

W każdej rundzie głosowania wybierany jest jeden masternode do retransmisji transakcji Darksend. Proces ten jest egzekwowany przez pojedyncze masternody używając algorytmu wyboru masternoda niezależnie od innych węzłów. Algorytm ten nie tylko wybiera

zwycięskiego masternoda, ale również decyduje który węzeł jest drugi, trzeci, czwarty… w kolejce.

Przez wdrożenie tego kodu, możemy stworzyć deterministyczną listę masternodów, które będą nadzorowały zamykanie transakcji. To będą te same węzły w całej sieci i będą one głosowały nad autentycznością danej im transakcji. Dla każdego bloku, stworzona zostanie lista dziesięciu różnych węzłów.



Rycina 3: Sieć masternodów osiąga konsensus nad zamkiem transakcji

3.4 Przykładowa Transakcja.

1. Użytkownik A, stosując mechanizm zamknięcia transakcji, wysyła sprzedawcy A 27 DRK jako zapłatę za jego towary lub usługi.

2. Transakcja ta zostaje nadana do całej sieci aż w końcu dociera do grupy wybranych masternodów.

3. Masternody te, kolektywnie nadają do sieci wiadomości, tworząc w ten sposób konsensus co do ważności danej transakcji. Każdy masternode podpisuje wiadomość o „zgodnej transakcji", po czym nadawana jest ona do sieci.

4. Kiedy węzeł zobaczy wszystkie wiadomości mówiące że konsensus został osiągnięty, to wtedy może uznać tę transakcję za potwierdzoną.

4. Bezpieczeństwo

Aby zapewnić bezpieczeństwo sieci musimy być w stanie zapobiec atakom takim jak:

- Atak Sybil
- Atak Finney
- Atak wyścigu zamkniętych transakcji

- Wiadomości z wieloma różniącymi się formami konsensusu

4.1 Atakowanie systemu osiągania konsensusu sieci, przez atak Sybil.

Prawdopodobieństwo wygrania wyborów masternoda jest jak 1 do N gdzie N jest liczbą masternodów. Na chwilę obecną sieć jest wspierana przez 895 masternodów. Każdy masternode ma szanse 1 do N zostania wybranym do przesłania transakcji. Aby atak był skuteczny, sieć musiałaby wybrać masternody kontrolowane przez atakującego.

Rozpatrzmy przykład ataku na system zamykania transakcji, przez kupno masternodów aby móc kontrolować wyniki wyborów. Dla uproszczenia użyjemy przykładu siecią z 1000 masternodów. Obecnie Darkcoin posiada 895 aktywnych masternodów (*podczas tłumaczenia tego artykułu w lutym 2015, istniało już ponad 2100 masternodów – przypisek tłumacza*).

Przy koszcie 1000 DRK za każdego masternoda, próba ataku staje się dosyć kosztowna. Aby mieć 1.72% szansy na zostanie wybranym, atakujący musiałby kontrolować 2/3 wszystkich masternodów (zobacz Tabelę 1) Aby móc kontrolować 2/3 wszystkich masternodów atakujący musiałby kupić 2000 sztuk (co wymagałoby zainwestowania dwóch milionów DRK).

Masternody pod kontrolą atakującego/ Liczba wszystkich masternodów w sieci	Prawdopodobieństwo powodzenia ataku $\prod_{i=1}^{n}(\frac{r-(i-1)}{t-(i-1)})$	Liczba wymaganych DRK
10/1010	3.44e-24	10,000 DRK
100/1100	2.52e-11	100,000 DRK
1000/2000	9.55e-03	1,000,000 DRK
2000/3000	1.72e-02	2,000,000 DRK

Tabela 1: Prawdopodobieństwo powodzenia ataku zakładając, że atakujący kontroluje N masternodów

n - jest długością łańcucha masternodów

t - jest liczbą wszystkich masternodów w sieci

r - jest liczbą masternodów pod kontrolą atakującego przy czym jest większa lub równa n

Wybór masternodów jest losowy.

Biorąc pod uwagę ograniczoną liczbę Darkcoin w obiegu (w czasie pisania tego artykułu istniało około 4.6 miliona) oraz małą płynność rynku, zdobycie wystarczającej ilości monet do przeprowadzenia ataku jest prawie że niemożliwe.

W przypadku próby sfałszowania wyborów masternoda na korzyść nieprawidłowej transakcji (np. Wiadomość o zamku nie została zakomunikowana reszcie sieci), sieć stworzy nieodwracalne zamknięcie powodując odrzucenie transakcji wysłanej do sprzedawcy. Klient Darkcoina po stronie sprzedawcy będzie cały czas pokazywał te transakcje jako niepotwierdzona z powodu próby wydania tych samych monet dwukrotnie i nigdy nie pokaże, że transakcja została uznana za autentyczną.

4.2 Atak Finney

W ataku Finney atakujący wykopuje blok jak każdy inny kopacz i zawiera w nim transakcję w której przesyła fundusze do samego siebie. Kiedy wykopuje ten blok, nie daje o tym znać reszcie sieci, ale zamiast tego wysyła fundusze do sprzedawcy jako zapłatę za jego dobra lub usługi. Natychmiast po otrzymaniu danych dóbr lub usług atakujący wysyła do sieci swój blok na tuż przed pojawieniem się następnego, nadpisując tym transakcję wysłaną do sprzedawcy chwilę wcześniej.

Aby uniemożliwić przeprowadzenie tego ataku, sieć musi być w stanie odrzucić bloki, które naruszają istniejące zamki transakcji. Co więcej musi również być w stanie odróżnić zamek założony na transakcji od transakcji przechodzącej przez system sieci masternodów głosujących nad transakcją. Transakcja może zostać uznana za zamkniętą tylko wtedy kiedy masternode retransmituje zamek dla danej transakcji. W tym wypadku blok ze sprzeczną transakcją zostanie odrzucony.

4.3 Atak wyścigu zamykaniętych transakcji.

W ataku tym klient wysyła do sieci dwie zamknięte i konkurujące ze sobą transakcje. Jedna jako zapłatę dla sprzedawcy, a drugą do samego siebie. Aby zwiększyć prawdopodobieństwo powodzenia tego ataku, atakujący wysła komendy zamknięcia transakcji bezpośrednio do wybranych masternodów, upewniając się, aby rozesłana została wiadomość o tym, że sprzedawca otrzyma obiecane fundusze. W tym samym czasie wysyła on konkurującą transakcję aby wysłać pieniądze do samego siebie.

W tego rodzaju ataku sieć część sieci uznałaby jedną transakcję za ważną a druga część sieci uznałaby drugą transakcję dopóki masternody nie ogłosiłyby wyniku głosowania nad transakcją. Jak tylko to nastąpi, to każdy klient Darkcoin usunie sprzeczną transakcję i wpisze tę autentyczną do pamięci zbiorowej (memory pool). Cały ten proces nie trwałby dłużej niż kilka sekund.

4.4 Nieskończony proces zamknięcia transakcji

Niedomknięta transakcja zdarza się kiedy sieć masternodów nie osiągnie konsensusu w sprawie któregoś z zamków. Brak porozumienia między masternodami mógłby zdarzyć się w rzadkich przypadkach, kiedy wybrany masternode odmawia wzięcia udziału w głosowaniu lub traci połączenie z siecią. W takich przypadkach, transakcja nie zostanie zamknięta i będzie musiała przejść przez standardowy proces potwierdzenia.

4.5 Wielokrotne różniące się, wiadomości konsensusu

Jeśli atakującemu udało się zdobyć kontrolę nad 10 Masternodami nadzorującymi dany blok oraz roześle wiele sprzecznych ze sobą wiadomości, to sieć musi być zdolna do poradzeniu sobie z takim konfliktem. Na przykład, atakujący który kontroluje dużą część masternodów, mógłby wysłać wiadomość tylko i wyłącznie do sprzedawcy A po czym rozesłałby do sieci sprzeczną wiadomość w której zawarta jest transakcja do samego siebie.

W takim wypadku, sprzeczne wiadomości zniwelują siebie nawzajem i klient będzie czekał na normalne potwierdzenie przez blokchain.

5. Dalsze prace

Po implementacji systemu zamykania transakcji i osiągania konsensusu, wiele innych funkcji również staje się możliwe. Między innymi; wstecznie kompatybilna architektura oraz natychmiastowe autoryzacje transakcji pomiędzy klientami Darkcoin bez potrzeby czekania na potwierdzenia.

5.1 Tryb kompatybilność zamku transakcji.

Aby włączyć tryb wstecznej kompatybilności z już istniejącym oprogramowaniem (giełdami, poolami, itp.), klient Darkcoina zacznie pokazywać tylko potwierdzenia transakcji, które zostały pomyślnie zamknięte w ciągu ostatnich 24 godzin. To pozwoli na używanie całego wachlarza funkcji Darkcoina bez żadnych zbędnych implementacji.

Jeśli klient chce aby oprogramowanie działało po staremu, będzie mógł spokojnie wyłączyć ten tryb.

5.2 Natychmiastowe transakcje pomiędzy klientami.

Zazwyczaj klient po otrzymaniu nowych środków musi czekać na przynajmniej jedno potwierdzenie bloku aby móc wydać te środki ponownie. Kiedy zostaną wprowadzone natychmiastowe autoryzacje, klient Darkcoin będzie działał jakby miał w pełni potwierdzoną transakcję i zezwoli na przesłanie funduszy bez żadnego ryzyka dla użytkownika. Pozwoli to na wykonanie całej serii transakcji zanim blok zostanie wykopany.

6. Podsumowanie

Rozwiązanie problemu podwójnego wydania tych samych środków w Bitcoinie oraz innych kryptowalutach, w dużej mierze polega na potwierdzaniu transakcji przez wykopywanie nowych bloków. Chociaż jest to bardzo duży postęp, to dalej nie może równać się z prawie że natychmiastowymi transakcjami wykonanymi przy pomocy kart płatniczych.

Szybkie autoryzacje płatności dzięki zamykanym transakcjom oraz osiąganiu konsensusu sieci masternodów, mogłyby wyeliminować potrzebę czekania na potwierdzenia przez wykopywanie bloków oraz dokonywać płatności z prędkością porównywalną do tej osiąganej przez karty płatnicze. W większości wypadków transakcja powinna zostać potwierdzona przez sieć w ciągu kilku sekund od momentu nadania jej do sieci.

Każdy klient Darkcoin uzna nadzór masternodów i w rezultacie sieć osiągnie konsensus bez potrzeby wykopywania bloku.

Dzięki używaniu sieci masternodów jako nadzorcy oraz wybieraniu masternodów przez deterministyczny algorytm oparty na dowodzie pracy (proof-of-work), możemy stworzyć system, który nie pozwala na dokonywanie transakcji w tempie porównywalnym do kart płatniczych, jest odporny na rożnego rodzaju ataki, jest wstecznie kompatybilny no i bardzo bezpieczny.

Historia rewizji

Wersja 2

- Z powodu komentarzy od niektórych użytkowników, usunięta została sekcja: „Przmyślenia na temat rozmiaru blockchaina". Lepszą metodą na przyszłą redukcję rozmiaru blockchaina, byłoby „okrajanie blockchaina" (blockchain pruning)
- Dodane zostały niektóre informacje o autoryzacjach płatności dokonywanych za pomocą kart płatniczych oraz analogie pomiędzy autoryzacjami i feedbackiem z konsensusu sieci.

Wersja 1

- Pierwsze wydanie

Odnośniki:

[Nakamoto09] Satoshi Nakamoto (2009), Bitcoin: A PeertoPeer Electronic Cash System https://bitcoin.org/bitcoin.pdf

[Reuters14] Reuters (2014), Analysis Bitcoin shows staying power as online merchants chase digital sparkle http://uk.reuters.com/article/2014/08/28/ukusabitcoinretailersanalysisidUKKBN0GS0AQ20140828

[Karame12] Ghassan O. Karame, Elli Androulaki, Srdjan Capkun (2012): Two Bitcoins at the Price of One? DoubleSpending Attacks on Fast Payments in Bitcoin https://eprint.iacr.org/2012/248.pdf

[Duffield14] Evan Duffield (2014): Darkcoin: PeertoPeer CryptoCurrency with Anonymous Blockchain Transactions and an Improved ProofofWork System https://www.darkcoin.io/downloads/DarkcoinWhitepaper.pdf

[Masternodes14] Evan Duffield (2014): https://darkcointalk.org/threads/darkcoinupdatemasternoderequirementsmasternode-payments.225/

[Lo14] Stephanie Lo, J. Christina Wang (2014) Bitcoin as Money? http://www.bostonfed.org/economic/currentpolicyperspectives/2014/cpp1404.pdf

[Nielsen13] Michael Nielsen, How the Bitcoin protocol actually works http://www.michaelnielsen.org/ddi/howthebitcoinprotocolactuallyworks/

[Gnutella03] Chawathe et. al. (2003), Making Gnutellalike P2P Systems Scalable http://www.cs.cornell.edu/people/egs/cornellonly/syslunch/fall03/gnutella.pdf

[Chandra07] Chandra et. al. (2007), Paxos Made Live An Engineering Perspective http://static.googleusercontent.com/media/research.google.com/en//archive/paxos_made_live.pdf

[Burrows06] Mike Burrows (2006), The Chubby lock service for loosely coupled distributed systems http://static.googleusercontent.com/media/research.google.com/en//archive/chubbyosdi06.pdf