Konsensus Saito: rozwiązanie niedoskonałości rynkowych Bitcoina

David Lancashire, Richard Parris

24 grudzień 2020 roku
wersja 4.0.1

Tłumaczenie: @Szpiegotka; wersja 1.0

Streszczenie

Saito rozwiązuje problemy związane z działaniem zbiorowym, które utrudniają skalowanie w blockchainach typu proof-of-work i proof-of-stake, poprzez sprzężenie okrągłej księgi z mechanizmem konsensusu, który zachęca do zbierania i dzielenia się opłatami za transakcje. W wyniku czego sieć płaci nie tylko za mining czy staking, ale również za wszelkie działania, które wnoszą wartość ekonomiczną do sieci. W procesie tym Saito w pełni eliminuje ataki 51% jak również inne rodzaje ataków.

Saito płaci węzłom infrastruktury skierowanej do użytkownika z otwartego mechanizmu konsensusu. Ponieważ podejście to skaluje się w sposób naturalny, to zachęca ono do przetwarzania dużych ilości danych i może być wykorzystane do budowania zdecentralizowanych wersji wielu usług związanych z dużą ilością danych, takich jak wymiana danych bez zdolności do astroturfingu, aplikacje uwierzytelniające i monetyzujące, rozproszone rejestry kluczy, które są bezpieczne przed atakami MITM, kanały płatności i wiele innych.

W kategoriach ekonomicznych Saito można rozumieć jako rozwiązanie mające na celu skłonieniu wolnego rynku do dostarczania dobra publicznego. Projekt koryguje problemy działania zbiorowego nieodłącznie związanych z mechanizmami proof-of-work i proof-of-stake, dzięki czemu podmioty nastawione na zysk konkurowały o wprowadzenie do sieci jak największej liczby transakcji, co umożliwia naturalną i solidną skalowalność, co pozwala na skalowalność do tego stopnia, że to sprzęt sieciowy, a nie ograniczenia ekonomiczne, stanowią limit dla rozwoju blockchainu. Uważamy, że praktyczny limit dla blockchainu Saito jest dziś rzędu 100 TB danych dziennie, a postępy w zakresie przepustowości routingu sprawi, że w ciągu dekady osiągniemy poziom petabajtów.

W następnej sekcji opisano krótko problemy ekonomiczne, które należy rozwiązać, aby zbudować skalowalny blockchain. W kolejnych częściach przedstawiono sposób, w jaki Saito rozwiązuje te problemy oraz opisano implementacje tych metod.

1. PROBLEMATYKA

Problem ze skalowaniem blockchainu nie leży w warstwie technologii sieciowej: w chwili pisania tego tekstu centra danych na całym świecie wdrażają przełączniki sieciowe o przepustowości 400 Gb/s, a połączenia o przepustowości 100 Gb/s stają się standardem nawet w obiektach kolokacyjnych niższego szczebla. Gdybyśmy mieli środki na opłacenie niezbędnego sprzętu, to nic technicznie nie stoi nam na przeszkodzie, aby zbudować blockchain, który jest zdecentralizowany i otwarty tak jak publiczny szkielet Internetu.

Tym, co ogranicza rozwój sieci, jest problem opłacalności sieci. W przeszłości nie-ekonomiści odżegnali się od tego ograniczenia, twierdząc, że dopóki ktoś zarabia na sieci, to będzie ponosił wszystkie koszty niezbędne do jej utrzymania. Nie jest to jednak prawdą, ponieważ sieci proof-of-work i proof-of-stake są dotknięte dwiema niedoskonałości rynku: tragedią wspólnego pastwiska, który prowadzi do rozrostu blockchainu i ostatecznego upadku oraz problemem gapowicza, który prowadzi do niedostatecznego zaopatrzenia w infrastrukturę sieciową skierowaną do użytkowników przy nadmiernej ilości działalności płatnej, takiej jak staking i mining. Żaden z tych problemów nie jest paraliżujący na małą skalę, ale stają się one obezwładniające w miarę wzrostu kosztów przepustowości i przechowywania danych.

Czy istnieją alternatywy? Stojąc przed koniecznością płacenia za nierekompensowaną infrastrukturę sieciową, informatycy rzucają problem na rynek. Jak wiadomo ekonomistom od lat 60. ubiegłego wieku, żądanie od sektora prywatnego finansowania infrastruktury niewykluczającej wymaga zamknięcia w jakimś modelu ekonomicznym. Podmioty, które płacą za pobieranie opłat, muszą z konieczności zamknąć dostęp do otrzymywanych opłat. Kontrolowany przepływ środków do blockchainu podważa otwartość warstwy konsensusu.

Jedynym realnym rozwiązaniem jest wyeliminowanie tych niedoskonałości rynku na poziomie zachęt. Zanim jednak zrozumie się rozwiązanie, trzeba wyraźnie dostrzec problemy. Główne problemy są następujące.

Problem tragedii wspólnego pastwiska powstaje z powodu istnieniem trwałej księgi, co zachęca węzły do przyjmowanie płatności teraz za koszty przechowywania, które w przyszłości mogą być przeniesione na innych. Ta zachęta prowadzi do rozdęcia blockchainów, a w bardziej subtelny sposób do błędnej wyceny transakcji, ponieważ użytkownicy mogą płacić opłaty, które nie odzwierciedlą kosztów ich transakcji dla całej sieci. Fakt, że jest to podstawowy problem jest ewidentny w sposobie, w jakim rozwiązaniem Satoshiego jest „nie przejmować się", które to podejście przestaje być opłacalne w sieciach działających na poważną skalę ekonomiczną.

Wyeliminowanie problemu tragedii wspólnego pastwiska wymaga, aby wszystkie węzły przesyłające transakcje ponosiły koszty przetwarzania tych transakcji tak długo, jak długo pozostają one w blockchainie. W praktyce wymaga to mechanizmu rynkowego do dokładnego określania ceny przechowywania danych w łańcuchu. Wymaga to również wyeliminowania zjawiska pełzania blockchainu lub odroczenia pobierania opłat, tak aby płatności były dokonywane w czasie,

gdy węzeł kontynuuje wykonywanie pracy wymaganej do zapłaty. Nasze rozwiązanie tego problemu jest opisane w rozdziale 2.

Problem gapowicza jest bardziej podstępny. Pojawia się on w blockchainach, gdzie płatności są dokonywane za jeden konkretny rodzaj pracy (taki jak mining czy staking) kosztem innych niezbędnych działań. To niedopasowanie motywuje uczestników do maksymalizacji swoich wydatków na rzecz płatnej pracy i minimalizacji wydatków na wszystko inne. W przestrzeni blockchain skutkuje to tym, że minerzy i stakerzy „jeżdżą na gapę" na tych, którzy wykonują nieodpłatną pracę polegającą na zbieraniu opłat, tworzeniu aplikacji lub w inny sposób wspierają sieć skierowaną do użytkowników. Problem ten pogłębia się w miarę skalowania sieci, a presja ewolucyjna sprawia, że pułapka staje się nieunikniona: każdy miner Bitcoina, który przeznacza mniejszy procent swoich przychodów na haszowanie niż jego rówieśnicy, straci udział w rynku i w końcu skapituluje.

W ekonomii typowym rozwiązaniem problemu gapowicza jest wyeliminowanie właściwości niewykluczalności związanej z danym dobrem lub usługą: ograniczenie korzyści do tych, którzy ponoszą koszty ich świadczenia. W przestrzeni blockchain jest to niemożliwe do wykonania bez zniszczenia otwartości sieci. Informatycy często rozwiązują ten problem, dodając ochronne oprogramowanie pośrednie, takie jak zawijanie płatności konsensusu w zamknięte pierścienie głosowania, które oczywiście są podatne na te same ataki. Nieuczciwe postępowanie nigdy nie rozwiąże tego problemu ekonomicznego: rynki są wystarczająco silne, by podważyć te struktury właśnie dlatego, że do tego zachęcają.

Bez rozwiązania tego problemu nasz wybór tkwi pomiędzy siecią, która nie może się skalować, ponieważ nie może płacić za operacje sieciowe, a siecią, która się skaluje, za co traci na otwartości, decentralizacji i braku konieczności zaufania użytkowników, czyli cechach czyniących blockchain użytecznym wynalazkiem. Żadne z tych podejść nie jest przydatne do budowania prawdziwie otwartego blockchainu na masową skalę.

Teoretyczne rozwiązanie problemu gapowicza wymaga wyeliminowania możliwości jazdy na gapę poprzez naprawę podstawowej struktury motywacyjnej, tak aby uczestnicy otrzymywali wynagrodzenie za dostarczanie tego, czego sieć faktycznie potrzebuje. Ponieważ blockchain wymaga wymiernego kosztu ataku, wymaga to wyeliminowania miningu i stakingu i przejście na inną formę pracy, która mierzy i płaci węzłom proporcjonalnie do „wartości", jaką dostarczają sieci, a nie do ilości wykonanych przez nie operacji haszowania lub stakingu.

Wymaga to od nas znalezienia nowego sposobu mierzenia wartości, a następnie płacenia węzłom proporcjonalnie do ich wkładu. Aby to osiągnąć, musimy wyprowadzić naszą miarę „pracy" z opłat transakcyjnych, które uiszczają użytkownicy. Praca polegająca na routingu opłat transakcyjnych do sieci jest pracą, do której nasza sieć musi zachęcać. Uczciwe węzły można nakłonić do wykonania tej pracy poprzez udział z pobranych opłat. Trudność polega na zapewnieniu, że mechanizm ten zachowuje właściwości kosztu ataku, tak aby atakujący nie mógł wydać własnych pieniędzy w ataku na sieć i zebrać ich z powrotem w wiecznej pętli. Mechanizm bezpieczeństwa opisany w rozdziale 3. przedstawia techniczną metodę osiągnięcia tego celu.

2. ROZWIĄZANIE TRAGEDII WSPÓLNEGO PASTWISKA

Saito rozwiązuje problem pełzania blockchainu, pozwalając węzłom w sieci na usuwanie najstarszych bloków w księdze w przewidywanych odstępach czasu („epokach"). Długość epok jest określona w kodzie konsensusu. W skrajnym przypadku blockchain przeznaczony do obsługi globalnego ruchu dla aplikacji o rozproszonej wymianie kluczy może mieć epokę tak krótką jak 24 godziny.

Saito precyzuje, że gdy blok wypadnie z bieżącej epoki, to jego niewydane wyjścia transakcyjne (UTXO) nie nadają się już do wydania. Jednak każdy UTXO z tego zestawu, który zawiera wystarczającą ilość tokenów, aby uiścić opłatę za retransmisję, musi zostać ponownie zawarty w następnym bloku. Producenci bloków robią to poprzez „automatyczną retransmisję transakcji" (ang. automatic transaction rebroadcasting, ATR) — transakcji, które zawierają oryginalne dane transakcji, ale mają zupełnie nowe do ponownego wydania UTXO. Po dwóch epokach producenci bloków mogą usunąć wszystkie dane bloku, chociaż 32-bajtowy skrót nagłówka może zostać zachowany, aby udowodnić połączenie z oryginalnym blokiem genesis.

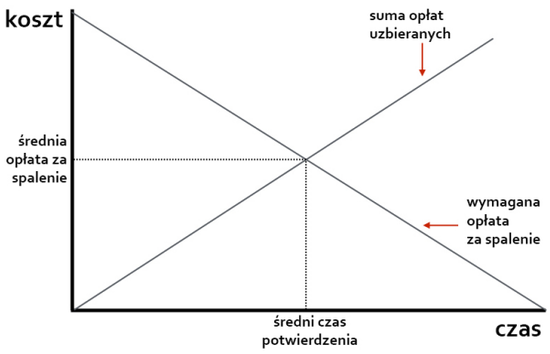
Mechanizm ATR całkowicie rozwiązuje problem tragedii wspólnego pastwiska, uniemożliwiając rozrost blockchainu do rozmiarów powodujących jego upadek. Kluczem jest zapewnienie, że „opłata za retransmisję" uiszczana przez transakcje ATR jest dodatnią wielokrotnością średniej opłaty uiszczanej przez nowe transakcje w poprzedniej epoce. W miarę jak blockchain się rozrasta i jest mniej miejsca na nowe transakcje, konkurencja rynkowa powoduje wzrost opłat wnoszonych przez nowe transakcje. To z kolei wymusza wzrost opłat za starsze transakcje i zwiększa ilość danych usuwanych przez blockchain. Rynek osiąga równowagę, gdy stare dane są usuwane z łańcucha w takim samym tempie, w jakim dodawane są nowe.

Odkrycie przez rynek prawdziwego kosztu przetwarzania danych w blockchainie jest efektem ubocznym tej struktury motywacyjnej, która działa poprzez usunięcie zachęty producentów bloków do dodawania nierentownych danych do łańcucha. Mechanizm ten pozwala uniknąć problemów związanych z twardym kodowaniem zmiennych ekonomicznych przez deweloperów i zapobiega subtelnym formom jazdy na gapę, powszechnie spotykanych w innych łańcuchach (usuwanie danych z łańcucha, odmowa przechowywania lub udostępniania bloków historycznych), w których wycinanie odbywa się w celu zaoszczędzenia pieniędzy. Wszystkie takie formy oszustwa znikają, ponieważ węzły, które nie przechowują całego łańcucha bloków, nie są w stanie produkować nowych bloków, ponieważ nie wiedzą, które płatności muszą być ponownie transmitowane.

Chociaż pozwala to uniknąć problemu, że nasz blockchain urośnie przesadnie, aby węzły sieci mogły go przechowywać, i zapewnia, że przestrzeń na blockchainie może być dokładnie wyceniona, nawet jeśli czas przechowywania zbliża się do nieskończoności, rozwiązanie problemu tragedii wspólnego pastwiska nie dostarcza pieniędzy węzłom w sieci peer-to-peer, które płacą za wszystkie różne działania, które utrzymują sieć w działaniu. Aby rozwiązać ten problem, potrzebny jest nowy mechanizm konsensusu.

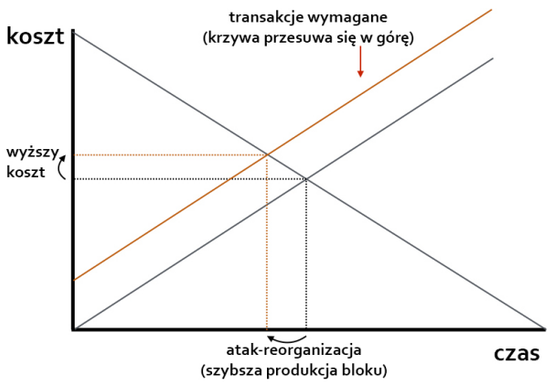
3. ELIMINOWANIE JAZDY NA GAPĘ

W Saito każdy węzeł może stworzyć blok w dowolnym momencie, pod warunkiem, że ma wystarczająco dużo „pracy routingu" w swoim mempoolu. Ilość „pracy routingu" potrzebnej do wyprodukowania bloku zależy od tego, jak szybko blok nastąpi po swoim poprzedniku: zasady konsensusu zwiększają wartość natychmiast po znalezieniu bloku i stopniowo ją zmniejszają, aż do osiągnięcia zera. Skoro producenci bloków wydają bloki, gdy tylko staje się to opłacalne, to tempo produkcji bloków jest determinowane przez całkowitą ilość „pracy routingu" generowanej przez sieć.



Rysunek 1: krzywe kosztu opłaty za spalenie (ang. burn fee) i sumy uzbieranych opłat

Saito wyprowadza pracę routingu z opłaty transakcyjnej wbudowanej w każdą transakcję. Wykorzystanie tej miary pracy do produkcji bloków czyni atakowanie sieci kosztownym, ponieważ reorganizacja kosztuje. Z rysunku 2. wynika, że niemożliwe jest, aby atakujący produkowali bloki w szybszym tempie niż łańcuch główny, chyba że mają dostęp do większej puli opłat transakcyjnych.

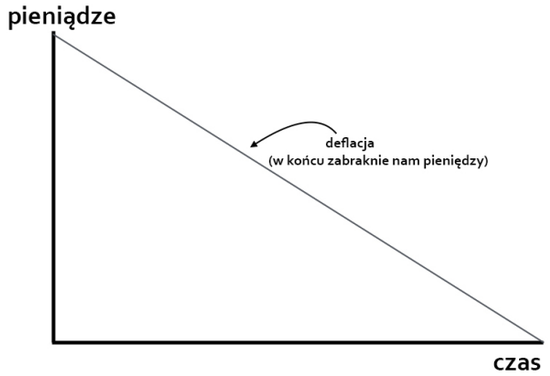


Rysunek 2: koszt opłaty za spalenie w czasie

Aby zabezpieczyć ten mechanizm, Saito wymaga od węzłów routingu kryptograficznego podpisywania transakcji w trakcie ich propagacji w sieci. Zasady konsensusu określają, że ilość "pracy routingu", jaką transakcja zapewnia każdemu węzłowi, spada wraz z liczbą węzłów na jego ścieżce routingu, a transakcje nie zapewniają żadnej użytecznej „pracy routingu" węzłom, które nie znajdują się na ich ścieżce routingu. Praca wykorzystywana do produkcji bloków to efektywne zbieranie i dzielenie się przychodzącymi opłatami sieciowymi.

Tak długo, jak nie ma płatności za produkcję bloku, system ten oferuje porównywalne bezpieczeństwo do Bitcoina: koszt ataku zawsze może być określony ilościowo, a atakujący muszą wydać własne pieniądze, aby zaatakować łańcuch. To pozwala użytkownikom czekać na tyle potwierdzeń, ile potrzeba do spełnienia ich wymogów bezpieczeństwa. Na dodatek sieć może zwiększyć ilość „pracy routingu" potrzebnej do produkcji bloku, aby utrzymać stały czas potwierdzenia w miarę wzrostu wolumenu transakcji, dzięki czemu bezpieczeństwo skaluje się wraz z wolumenem opłat.

Główny problem z tym podejściem leży w konsekwencjach tego, że sieć musi spalać kapitał, aby produkować bloki:



Rysunek 3: deflacja jako wynik opłat za spalenie w czasie

Aby uniknąć krachu deflacyjnego, musimy ponownie wprowadzić tokeny do naszej sieci. Saito nie może jednak po prostu przekazać opłat bezpośrednio producentom bloków: to pozwoliłoby atakującym wykorzystać dochód z jednego bloku do generowania „pracy routingu" potrzebnej do wyprodukowania następnego bloku. Preferowany jest podział płatności pomiędzy różne węzły, ale dopóki producenci bloków mają jakikolwiek wpływ na to, kto otrzymuje wynagrodzenie, sprytny atakujący może przeprowadzać ataki typu grinding lub Sybil, których celem jest mechanizm wydawania tokenów.

Rozwiązanie tego problemu wymaga odwrócenia klasycznego rozwiązania proof-of-work. W Bitcoinie zasady konsensusu powodują, że produkcja bloków jest kosztowna, a opłaty są przekazywane producentowi bloku. Ma to zapewnić, że produkcja bloków jest kosztowna, ale w rzeczywistości gwarantuje, że zawsze istnieją warunki, w których ataki są opłacalne[1]. W Saito rozwiązanie jest odwrotne. Problem pierwszego rzędu zmienia się w zabezpieczenie mechanizmu płatności: zapewnienie, że płatności są proporcjonalne do pracy niezależnie od tego, kto produkuje bloki. Koszt ataku, który tworzy mechanizm z tą właściwością, staje się wtedy kosztem produkcji bloków.

Mechanizm, który to osiąga, nazywamy rozwiązaniem „złotego biletu". Mechanizm ten płaci uczciwym węzłom za pobieranie opłat niezależnie od tego, kto produkuje bloki. Sztuczka polega na dokonaniu tego w taki sposób, że zawsze zapewniony jest wymierny koszt zaatakowania systemu. Praktycznym rozwiązaniem jest zwrot opłat za transakcje do sieci poprzez proces, który nie może być rozegrany przez żadnego z graczy w sieci nie wydając na atak o wiele więcej pieniędzy, niż są oni w stanie zyskać na pobieraniu płatności. Szczegóły realizacji tego rozwiązania są opisane w następnym rozdziale.

[1] Wiele podstawowych problemów z mechanizmami proof-of-work i proof-of-stake wynika z tej decyzji. Pomijając atak 51%, należy zwrócić uwagę, w jaki sposób ograniczenia po stronie podaży na rynkach zewnętrznych (np. nieelastyczna krzywa podaży dla hashrate'u lub kapitału) są wykorzystywane do nałożenia „ograniczenia kosztów" na atakujących. Taka konstrukcja nie tylko pozbawia blockchain możliwość regulowania własnego bezpieczeństwa, ale również zyski dostępne na rynkach zewnętrznych, które w sposób konieczny i nieuchronny utowarowiają funkcję pracy i spłaszczają krzywą podaży czynnika pracy na rynku zewnętrznym.

4. ZŁOTY BILET

Gdy węzeł produkuje blok, może on zebrać różnicę pomiędzy ilością „pracy routingu" zawartej w jego bloku a ilością „pracy routingu" wymaganej do produkcji bloku. Nie dokonuje się żadnych innych płatności.

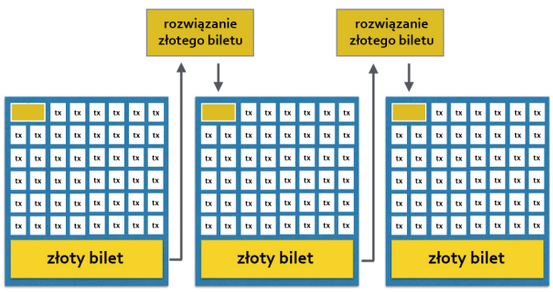
Odblokowanie tych płatności wymaga od sieci rozwiązania zagadki obliczeniowej, którą nazywamy „złotym biletem". Zagadka ta wymaga znajomości hashu bloku i nie może być obliczona z góry. Górnicy w sieci nasłuchują bloków, gdy są one produkowane i zaczynają hashować w poszukiwaniu rozwiązania. Jeśli znajdą transakcję, propagują ją z powrotem do sieci jako normalną transakcję płatniczą.

W każdym bloku może znajdować się tylko jedno rozwiązanie i aby było ono uznane za ważne, musi znaleźć się w następnym bloku. Jeśli te warunki zostaną naruszone lub jeśli złoty bilet nie zostanie rozwiązany, środki, które nie zostały wypłacone w poprzednim bloku, po prostu nie są przydzielane. Trafiają one z powrotem do blockchainu i ostatecznie kończą poza nim, w momencie którym utracone środki są odzyskiwane przez warstwę konsensusu i ostatecznie redystrybuowane jako część przyszłej nagrody za blok.

Jeśli rozwiązanie zostanie znalezione na czas, nieprzydzielone opłaty są uwalniane do sieci; dzielone między górnika, który znalazł rozwiązanie i losowy węzeł w sieci routingu peer-to-peer. Szczęśliwy węzeł routingu jest wybierany za pomocą zmiennej losowej pochodzącej z rozwiązania minera, przy czym szansa każdego węzła routingu na wygraną jest znormalizowana tak, aby była proporcjonalna do całkowitej „pracy routingu", którą wniósł do rozwiązywanego bloku.

W miarę jak transakcje są routowane do sieci, można zauważyć, że wbudowane w nie całkowite roszczenia o zapłatę (suma pracy routingu dostępnej dla wszystkich węzłów na ścieżce routingu) rosną, podczas gdy ilość pracy dostępnej do wyprodukowania bloku (ilość pracy routingu dostępnej dla konkretnych węzłów) maleje. Atakujący, którzy wykorzystują uczciwe transakcje do produkcji bloków, stawiają się w sytuacji, w której muszą zapłacić tę różnicę.

Podział płatności pomiędzy minerów i routerów nazywamy „paysplitem" sieci. Domyślnie jest on ustawiony na 0,5 (połowa dla minerów, połowa dla routerów), ale on może być regulowany w sposób w opisany w rozdziale poniżej. System złotego biletu można zwizualizować w następujący sposób:



Rysunek 4: system złotych biletów

System ten ma kilka istotnych zalet w stosunku do mechanizmów proof-of-work i proof-of-stake. Najważniejszą z nich jest to, że Saito wyraźnie rozdziela opłaty na węzły, które obsługują użytkowników, zbierają transakcje i produkują bloki, i robi to proporcjonalnie do wartości, jaką te podmioty wnoszą do całej sieci. Węzły sieciowe konkurują o dostęp do lukratywnego przepływu transakcji przychodzących i z radością będą finansować wszelkie działania rozwojowe potrzebne do pozyskania użytkowników w sieci. Co warte podkreślenia, usługi świadczone przez węzły brzegowe w celu przyciągnięcia wykorzystania Saito mogą obejmować infrastrukturę publiczną potrzebną dla innych blockchainów.

Jest to fundamentalna zmiana. Tam, gdzie inne blockchainy wyraźnie określają, które działania mają wartość, Saito pozwala użytkownikom zasygnalizować, jakie usługi zapewniają wartość poprzez opłaty, podczas gdy sieć infiltruje, kto zasługuje na płatność. Saito zachęca również do efektywnego dostarczania wartości użytkownikom. A poprzez płacenie za wartość, a nie podzbiór działań sieciowych, zapewnia jedyny sposób zagwarantowania, że samowystarczalna sieć może pozostać otwartą i ekonomicznie niezależną w skali.

Mechanizm konsensusu Saito jest również „dwukrotnie bezpieczniejszy" niż jego odpowiedniki proof-of-work i proof-of-stake. Uczciwe węzły routują transakcje do producentów bloków i w zamian za to pobierają opłaty. Za to atakujący znajdują się w sytuacji paragrafu 22: muszą nie tylko wydać tyle samo opłat, co uczciwa sieć, aby stworzyć konkurencyjny łańcuch, ale muszą również dorównać 100% miningu, aby znaleźć wystarczająco dużo rozwiązań złotych biletów, żeby odzyskać swoje środki. Nawet jeżeli atakujący z powodzeniem przeprowadzają ataki *fee-recycling*, to i tak muszą wydać 100% swoich dochodów na hashowanie.

Niezależnie od tego, która implementacja zostanie zastosowana, znikają problemy ekonomiczne, jakie stwarzają mechanizmy oparte na zewnętrznych krzywych podaży: wydobycie jest czystą funkcją kosztów, a nie funkcją trudności, a blockchain pozostaje bezpieczny nawet wtedy, gdy krzywa podaży haszyszu staje się idealnie płaska.

Podstawowa wersja systemu Saito osiąga 100% bezpieczeństwo w oparciu o opłaty, całkowicie eliminując atak 51%. W rozdziale 5. opisano modyfikację tego mechanizmu, która zwiększa bezpieczeństwo powyżej 100% i gwarantuje, że atakujący stracą pieniądze w każdych okolicznościach. Niezależnie od tego, która implementacja zostanie zastosowana, znikają problemy ekonomiczne wynikające z mechanizmów, które polegają na zewnętrznych krzywych podaży: mining jest czystą funkcja kosztów, a nie funkcją trudności, a blockchain pozostaje bezpieczny nawet wtedy, gdy krzywa podaży hashrate'u staje się idealnie płaska.

5. *POWSPLIT* – ZAAWANSOWANA OCHRONA

Istnieje możliwość zwiększenia kosztów ataku powyżej 100% dostępnych zysków poprzez mechanizm *powsplit*. Należy pamiętać, że w normalnej implementacji Saito ze stałym *paysplitem* wynoszącym 0,5, sieć automatycznie dostosowuje trudność miningu tak, aby na jeden blok przypadało średnio jedno rozwiązanie. Ze względu na to, że minerzy nie mogą kontrolować wariancji, z jaką znajdowane są rozwiązania, trudność sieci może w końcu okazać się średnio niższa, niż jest to konieczne dla optymalnego bezpieczeństwa.

Podejście *powsplit* eliminuje ten problem poprzez dostosowanie trudności miningu tak, aby jedno rozwiązanie było znajdowane średnio co N bloków. Gdy takie rozwiązanie znajdzie się w blockchainie, jeśli poprzedni blok nie zawierał złotego biletu, zmienna lo-

sowa użyta do wybrania zwycięskiego węzła routingu jest ponownie haszowana, aby wybrać zwycięzcę z nierozstrzygniętego bloku, który go poprzedzał lub z tabeli stakerów, jak opisano poniżej. Ze względów praktycznych można zastosować górną granicę rekurencji wstecznej, ponieważ kołowy blockchain będzie odzyskiwał wszelkie środki, które nie zostały wypłacone.

Aby zostać stakerami w sieci, użytkownicy nadają transakcję zawierającą specjalnie sformatowane UTXO. Te UTXO są dodawane do listy oczekujących stakerów w momencie ich włączenia do bloku. Gdy aktualna tabela stakingu zostanie w pełni wypłacona, wszystkie oczekujące UTXO stakingu są przenoszone do aktualnej tabeli stakingu. Aby uniknąć ataków dławiących na mechanizm stakingu, rozsądnie jest nie pozwalać stakerom na wypłacanie lub wydawanie UTXO, dopóki nie otrzymają zapłaty.

Procentowy udział w przychodach sieci przydzielony węzłom stakingu przez mechanizm stakingu podczas poprzedniej rundy, powinien być proporcjonalny do ich udziału w kwocie opłat wpłaconych do skarbca. Limity mogą być nałożone na wielkość puli stakingu, aby wzbudzić konkurencję między stakerami, jeśli jest to pożądane lub celem powstrzymania użytkowników od spamowania mechanizmu stakingu w nadziei na zniechęcenie uczciwych stakerów z udziału w mechanizmie. W normalnych sytuacjach zapętlony blockchain i mechanizm ATR uniemożliwi stakerom rozpoczęcie ataków spamerskich, ponieważ wiele UTXO będzie wnosić opłaty za retransmisję.

Aby zapewnić działanie systemu, producenci bloków, którzy retransmitują UTXO, muszą teraz wskazać w swoich transakcjach ATR, czy określone wyjścia są aktywne w aktualnej lub oczekującej puli stakingu. W każdym bloku można umieścić hash jako reprezentację stanu tabeli stakingu w formie zobowiązania, aby umożliwić węzłom weryfikację dokładności tabeli stakingu, ale mechanizm retransmisji ATR teoretycznie pozwoli wszystkim węzłom odtworzyć stan puli stakingu w ciągu maksymalnie jednej epoki.

Trudność wydobycia może zostać skorygowana w górę, jeśli pod rząd zostaną znalezione dwa bloki zawierające złote bilety, a w dół, jeśli zostaną znalezione kolejno dwa bloki bez złotych biletów. Podobny koszt karny może zdławić wypłatę za staking, jeśli dwa bloki bez złotych biletów zostaną znalezione pod rząd (coraz stale większa część przychodów ze stakingu jest wstrzymana).

6. *PAYSPLIT* – ZAAWANSOWANA OCHRONA

Istnieje kilka modyfikacji mechanizmu paysplit, które można wykorzystać do zwiększenia kosztów ataku. Chociaż wersja Saito wprowadzona do użytku nie zawiera tego mechanizmu, możliwe jest dodanie do Saito dynamicznego systemu głosowania, który pozwoli na dynamiczne zmiany *paysplitu*. W tym rozdziale opisano teoretyczne ulepszenie, które pozwala na uzyskanie zmiennego *paysplitu*, który będzie działał przy pewnych założeniach dotyczących racjonalności sieci.

Implementacja tego systemu modyfikuje bloki tak, aby obejmowały one głosowanie nad zwiększeniem, zmniejszeniem lub utrzymaniem na stałym poziomie *paysplit* sieci. Rozwiązania złotych biletów mogą być następnie zmodyfikowane tak, aby zawierały podobne głosowanie nad trudnością funkcji produkcji złotego biletu. Zmienne konsensusu sieci są aktualizowane wtedy i tylko wtedy, gdy złote bilety są rozwiązane i włączone do blockchainu.

Dostosowując *paysplit* w ten sposób, można w czasie rzeczywistym zmienić podział opłat pomiędzy węzłami routingu i minerami. Dzięki temu sieć osiąga optymalną równowagę, a nie arbitralną. Aby zapobiec sytuacji, w której równowaga ta odzwierciedlałaby jedynie preferencje węzłów routingu i miningu, zalecamy również umożliwienie użytkownikom sieci na oznaczanie swoich transakcji optymalnych głosem *paysplit*: jeśli transakcja zainicjowana przez użytkownika zawiera taki głos, może ona zostać włączona jedynie do bloku, w którym głosuje się w tym samym kierunku. Użytkownicy, którzy opowiadają się po konkretnej stronie trwającej walki między routerami a minerami, poświęcają w ten sposób niezawodność i szybkość potwierdzenia transakcji, uzyskując w zamian marginalny wpływ na sposób alokacji opłat przez sieć. Użytkownicy oddający głosy wstrzymują również swoje opłaty od węzłów głosujących inaczej niż oni sami.

W warunkach, gdy uczestnicy sieci wykazują ograniczoną racjonalność, mechanizm ten przesuwa *paysplit* do punktu, w którym zapewnione bezpieczeństwo jest optymalne dla wszystkich uczestników, biorąc pod uwagę koszty dodatkowego pobierania opłat. Kompakty w stylu De Tocqueville'a zabezpieczają równowagę: dwójka dowolnych graczy w trójstronnej strukturze sieci (routerzy, minerzy i stakerzy) mogą połączyć swoje siły, aby przesunąć *paysplit* z powrotem do pożądanego ideału. Chociaż badania nad tym mechanizmem pozostawiamy na przyszłość, przydatnym eksperymentem myślowym jest zbadanie, w jaki sposób bezpieczeństwo tego trójstronnego systemu degraduje się do bezpieczeństwa klasy Bitcoina, gdy *paysplit* zbliża się do wartości ekstremalnych.

7. DODATKOWE UWAGI DOTYCZĄCE BEZPIECZEŃSTWA SIECI

Projekt Saito rozwiązuje kilka długoletnich problemów, które warto odnotować. Ataki typu „hoarding" są zminimalizowane, ponieważ węzły, które uczestniczą w routingu transakcji, maksymalizują przychody poprzez znalezienie najbardziej efektywnej ścieżki routingu w sieci. Konkurencja zachęca do dzielenia się opłatami, a nie do ich gromadzenia. Dostępność informacji o routingu w blokach pozwala również uczestnikom sprawdzić, czy ich rówieśnicy wiernie propagują swoje transakcje, zamiast je gromadzić.

Ponieważ dodanie kolejnych węzłów do dowolnej ścieżki routingu w sposób obowiązkowy zmniejsza opłacalność routingu dla każdego węzła na ścieżce sprawia, że ataki Sybil są również eliminowane. Bloki dostarczają informacji potrzebnych uczestnikom do identyfikacji i eliminacji „sybili" w ich sieciach peer-to-peer. A presja ewolucyjna zapewnia, że będą oni je eliminować: słabsze węzły, które pozwalają sobie na ataki Sybil, z czasem zostaną wyparte z sieci przez presję konkurencji.

Sieć routingu służy również wyjątkowym mechanizmem obronnym. Węzły routingu w Saito mogą zwiększyć koszt ataku w czasie rzeczywistym, odmawiając kierowania transakcji do atakujących, co wymusza zwiększoną zależność atakującego od własnego portfela w celu sfinansowania produkcji bloków. Ten mechanizm broni również Saito przed subtelnymi atakami, takimi jak monetyzacja przepływów transakcji i routing o zamkniętym dostępie.

Jako ostatnie spostrzeżenie zauważamy, że „trylemat skalowalności" często wymieniany jako podstawowe

prawo blockchainu nie istnieje w projekcie Saito. Istnieje wiele oczywistych konfiguracji sieci, w których przekierowanie opłat od minerów do węzłów routingu może jednocześnie zwiększyć przepustowość, decentralizację i bezpieczeństwo sieci.

8. PODSUMOWANIE

Podstawowe problemy wpływające na skalowanie blockchainu mają charakter ekonomiczny. Saito rozwiązuje te problemy, pozwalając nam zbudować masowo skalowalny blockchain, który osiąga skalowalność poprzez zapewnienie przepływu płatności do węzłów, które wydają pieniądze na infrastrukturę sieci.

Ci, którzy przeanalizują szczegóły techniczne sieci Saito, znajdą w niej co najmniej siedem głównych innowacji w technologii blockchain: automatyczną retransmisję transakcji, opłatę za spalenie, system złotych biletów, *paysplit* i *powsplit*, złote bilety N-bloków, zabezpieczający mechanizm głosowania wielostronicowego oraz łańcuch podpisów kryptograficznych, który pozwala blockchainu identyfikować i nagradzać produktywne węzły w routującej sieci.

Ochrona patentowa na te techniki została zabezpieczona i zapraszamy do kontaktu inne projekty blockchain, które chcą włączyć jedną lub kilka z tych metod do swoich własnych sieci. Zachęcamy również czytelników do odwiedzenia naszej strony internetowej (https://saito.io), która zawiera interfejs działającej sieci, roadmap przedstawiający przyszłe plany rozwoju oraz samouczki, które mogą pomóc każdemu rozpocząć budowę aplikacji Saito **już dziś.**