Freeman Family

4 Lipiec, 2019

EPIC CASH

PRYWATNY PIENIĄDZ CYFROWY

Elektroniczny system płatności Peer-to-Peer

PRZECHOWYWANIE WARTOŚCI + ŚRODEK WYMIANY + JEDNOSTKA ROZLICZENIOWA

1.7 miliarda dorosłych osób nie ma dostępu do światowego systemu bankowego, a następne 1.3 miliarda nie ma zapewnionej właściwej obsługi. Epic Cash uwalnia potencjał ludzi, łącząc jednostki z rynkiem globalnym. W sposób szybki, praktycznie darmowy i otwarty dla wszystkich.

Version 7.1b **Polish**

Spis treści

I. Abstrakt

Epic Cash jest ostatnim punktem na drodze do stworzenia prawdziwej gotówki cyfrowej P2P, będącej kamieniem węgielnym prywatnego systemu finansowego. Epic Cash ma na celu stać się najskuteczniejszą na świecie formą pieniądza cyfrowego chroniącego prywatność. Aby osiągnąć ten cel, spełnia trzy podstawowe funkcje pieniądza:

1. **Przechowywanie wartości** – można zachować, odzyskać i wymienić w późniejszym czasie; posiada przewidywalną wartość po wymianie
2. **Środek wymiany** – wszystko, co zostało zaakceptowane jako reprezentujące standard wartości i wymienialne na towary lub usługi;
3. **Jednostka rozliczeniowa** – jednostka, według której wartość rzeczy jest rozliczana i porównywana.

	$ USD	BTC	EPIC
Przechowywanie wartości	✗	✓	✓
Środek wymiany	✓	✗	✓
Jednostka rozliczeniowa	✓	✗	✓

W 2009 r. Bitcoin pojawił się jako pierwsza cyfrowa waluta oparta na blockchainie, a wraz z nią trzy cechy definiujące inne kryptowaluty:

- **Zaufanie** – nie musisz ufać scentralizowanemu podmiotowi ani kontrahentowi, aby sieć działała;
- **Niezmiennosc** – transakcje nie mogą zostać cofnięte
  a. Modyfikowanie historii powinno być wysoce nieprawdopodobne lub trudne;
  b. Nikt inny niż właściciel klucza prywatnego nie powinien mieć możliwości przenoszenia środków związanych z tym kluczem prywatnym;
  c. Wszystkie transakcje są rejestrowane w blockchainie.
- **Decentralizacja** – "Łańcuchy bloków są politycznie zdecentralizowane (nikt ich nie kontroluje) i architektonicznie zdecentralizowane (brak konkretnej infrastruktury mogącej być punktem awarii) ... "

Bitcoin wytyczył nowe szlaki technologiczne, jednocześnie przestrzegając sprawdzonych podstaw struktury polityki pieniężnej. Sukces Bitcoina jest ściśle związany z jego ograniczoną podażą w połączeniu z zaufanym, niezmiennym i zdecentralizowanym łańcuchem bloków. Epic Cash naśladuje politykę pieniężną Bitcoina polegającą na zmniejszającej się inflacji i ograniczonej podaży, aby zapewnić, że waluta Epic może służyć jako skuteczny magazyn wartości.

Pomimo sukcesu Bitcoina ujawniono pewne niedociągnięcia od czasu jego powstania 10 lat temu. Inne projekty próbowały pokonać te niedociągnięcia i przeanalizowaliśmy najlepsze z nich, które można wykorzystać jako punkt wyjścia. Postanowiliśmy wykorzystać kod Grin i doskonałą pracę kilku innych projektów, aby pomóc nam w doskonaleniu ciężko zdobytych osiągnięć i odkryliśmy wady poprzedników Epic Cash. Epic Cash ma kluczowe cechy, aby być idealną walutą:

- **Zamienność** – Wartość danej jednostki Epic musi zawsze być równa innej jednostce Epic, tak jak jeden jen lub juan jest zawsze równy i może być zastąpiony innym jenem lub juanem. Osiągnięcie zamienności w dużej mierze zależy od prywatności.
- **Prywatność** – Blockchain Epic Cash chroni anonimowość właścicieli i użytkowników Epic, maskując szczegóły transakcji przed stronami trzecimi, i jest zaprojektowany tak, aby był niewykrywalny i niewidoczny dla organów nadzorujących.
- **Skalowalność** – Epic Cash utrzymuje wydajny pojemnościowo blockchain, w którym nowe węzły mogą powstawać bez konieczności wykorzystania sprzętu wymagającego dużych zasobów mocy. Blockchain Epic Cash jest zdolny do co najmniej dwa razy lepszej wydajności niż Bitcoin.
- **Szybkość** – Transakcje Epic Cash są płynne, ciągłe i wykonywane znacznie szybciej niż w poprzednich generacjach technologii blockchain. Podczas gdy Bitcoin wymaga sześciu 10-minutowych bloków, aby uzyskać pełne potwierdzenie transakcji, transakcje Epic odbywają się po jednym potwierdzeniu bloku, tj. po jednej minucie.

[1] Buterin, Vitalik, *The Meaning of Decentralization*, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Prywatność

Współczesne wykorzystanie pieniędzy można rozumieć jako zbiorowe przeniesienie jednostek rozliczeniowych między ludźmi i instytucjami. Obraz pieniądza w dowolnym momencie można zapisać, odpowiadając na następujące pytania:

1. Kto go posiada i ile go ma?

2. Kto przekazuje komu i za ile?

W przypadku tradycyjnych walut fiducjarnych, a także Bitcoina, możemy odpowiedzieć na te pytania. W ten sposób można ujawnić wiele na temat życia ludzi, takich jak wzorce konsumpcji, status posiadania i kontrahenci. Na podstawie transferów można wyciągnąć dość dokładne wnioski na temat zainteresowań i intencji danej osoby. Bez zachowania prywatności dane transakcyjne mogą być niebezpiecznym narzędziem w rękach bezwzględnych stron trzecich.

Wykorzystanie kryptowalut w ostatniej dekadzie pokazuje stałe poszukiwanie „prywatności" w różnych implementacjach blockchaina. Poziom prywatności rozciąga się od w pełni otwartego dostępu do informacji z jednej strony do pełnej anonimowości z drugiej Gdy prywatność ulega zachwianiu, jeden z podstawowych elementów kryptowalut, zaufanie, ulega degradacji. Jak dowodzi sukces usług analizy blockchaina Bitcoina, Bitcoin jest umiejscowiony bardziej w kierunku przejrzystego, otwartego podejścia do prywatności. Użytkownicy muszą w coraz większym stopniu podejmować kroki, aby mieć pewność, że nie dokonają przypadkowej transakcji na upośledzonym Bitcoinie. Rozwiązanie Epic Cash przesuwa nacisk w stronę anonimowości i przywraca tą istotną właściwość, zapewniając, że zarówno prywatność osoby, jak i prywatność transakcji są zagwarantowane w systemie jako podstawowa funkcja.

Prywatność tożsamości

Prywatność transakcji

Prywatność tożsamości

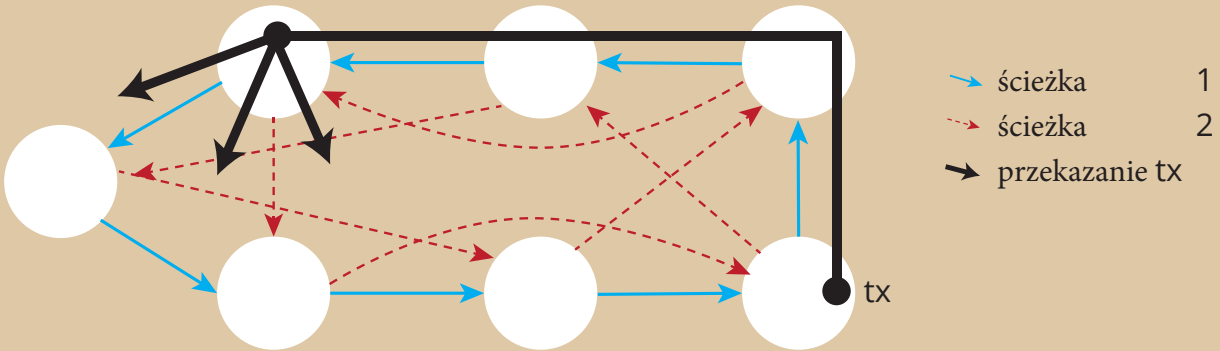
Większość kryptowalut, takich jak Bitcoin, jest przechowywana w portfelach, których adresy to klucze publiczne pochodzące z kluczy prywatnych portfela. Adresy te można traktować jako lokalizatory prywatnego "skarbca" w cyfrowym świecie. Blockchain Epic Cash całkowicie eliminuje adresy i zamiast tego stosuje jedną multisygnaturę z której generowane są jednorazowo wszystkie publiczne i prywatne klucze.

Ponieważ adresy portfeli Bitcoina są tak jakby adresami skarbców w świecie cyfrowym, portfel ten można prześledzić względem adresu IP właściciela, co łączy go z komputerem w określonej lokalizacji w danym momencie. Po prostu: gdy ma miejsce transakcja Bitcoin, jest ona rozgłaszana z centrum komunikacyjnego zwanego „węzłem", a następnie przekazywana do innych węzłów zwanych „równorzędnymi". Informacje te następnie szybko rozprzestrzeniają się na wszystkie węzły równorzędne w całej sieci. Ten proces jest nazwany „protokołem plotek". Po prostu, każdy Bitcoin ma widoczną pozycję online i fizyczną lokalizację, w której można go znaleźć, a raczej właściciela tego Bitcoina. Jak zauważyła dziennikarka Grace Caffyn, Bitcoin nie jest „niczym bardziej prywatnym niż wyszukiwanie na Google z domowego komputera" [2]

Oprócz eliminacji adresów portfeli, łańcuch bloków Epic Cash zapewnia prywatność tożsamości, uniemożliwiając śledzenie adresów IP. Odbywa się to poprzez integrację protokołu Dandelion ++ (tłum. Dmuchawiec). Ulepszając swojego poprzednika, oryginalny protokół Dandelion, protokół Dandelion ++ jest wynikiem ciągłych prac siedmiu badaczy nad zwalczaniem ataków deanonimizacji na blockchain. Za pośrednictwem Dandelion ++ transakcje są przekazywane przypadkowo splecionymi ścieżkami lub „kablami", a następnie nagle przesyłane są do dużej sieci węzłów, takich jak nasiona mniszka lekarskiego po zdmuchnięciu z ich łodygi (ryc. 1). To sprawia, że prawie niemożliwe jest prześledzenie transakcji z powrotem do źródła ich pochodzenia, a tym samym początkowych adresów IP.

Figure 1: Anonimizacja transakcji z wykorzystaniem protokołu *Dandelion++* .

Dandelion++ przesyła wiadomości przez jedną z dwóch splecionych ścieżek na 4-wymiarowym wykresie, a następnie przekazuje je za pomocą dyfuzji. Na rysunku transakcja jest przekazywana po niebieskiej ścieżce stałej[3]. Proces ten bardzo utrudnia śledzenie transakcji z powrotem do ich źródła, a tym samym zapewnia zachowanie prywatności.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Prywatność transakcji

Blockchain Epic Cash zapewnia prywatność transakcji, ukrywając kwoty i relację nadawca-odbiorca transakcji. Osiąga się to poprzez zastosowanie pomysłów znanych z technologii Poufnych Transakcji (CT) [4] i CoinJoin[5], metod w dużej mierze opracowanych przez Gregory'ego Maxwella (programistę Bitcoin Core, współzałożyciela i CTO Blockstream).

CT, pierwotnie stworzony przez Adama Backa, a następnie dopracowany przez Maxwella, działa poprzez dzielenie transakcji na mniejsze części za pomocą szyfrowania homomorficznego, metody wykonywania obliczeń na zaszyfrowanych informacjach bez ich odszyfrowywania w celu zachowania prywatności. Po podzieleniu transakcji obserwatorzy nie widzą rzeczywistych kwot z powodu czynników maskujących, systemu, który rzutuje losowe liczby na mieszankę fragmentów transakcji, aby ukryć wartości tych fragmentów. Ostatecznie tylko strony transakcji znają wartość transferu, podczas gdy transakcja jest weryfikowana przez sieć poprzez potwierdzenie, że suma wartości wyjściowych jest równa sumie wartości wejściowych, a suma czynników maskujących wynik równa się sumie wejściowej tych czynników.

Aby jeszcze bardziej skomplikować zadanie podglądającym, wszystkie transakcje Epic Cash są maskowane za pomocą CT, a następnie mieszane razem, aby ukryć powiązania między stronami transakcji. Odbywa się to poprzez drugą koncepcję Maxwella, *CoinJoin.*

Aby w uproszczeniu zilustrować *CoinJoin*, wyobraź sobie, że A, B i C wysyłają Epic odpowiednio do X, Y i Z. Wysyłając za pośrednictwem *CoinJoin* wiadomo tylko, że A, B i C wysyłają, a X, Y i Z odbierają, a kwoty transakcji pozostają niewidoczne. System *CoinJoin* ma fundamentalne znaczenie dla Epic Cash za pośrednictwem One-Way Aggregate Signatures (OWAS), które łączą wszystkie transakcje wewnątrz bloku w jedną transakcję.

Prywatność: Podsumowanie

Blockchain Epic Cash chroni prywatność osób i ich transakcji poprzez:

- **Eliminowanie adresów portfela** - w blockchainie nie ma identyfikatorów lokalizacji "skarbców" cyfrowych. Transakcje są tworzone bezpośrednio od osoby do osoby na zasadzie portfel do portfela;
- ***Con idential Transactions* –** dzielenie transakcji na wiele części i wprowadzanie czynników maskujących do tych części, aby wartości transferu i inne parametry transakcji nie były znane;
- ***Protokół Dandelion++* –** rozdziela cyfrowe ścieżki transakcji od adresu IP nadawcy transakcji;
- ***CoinJoin* –** łączy transakcje w pakiety, aby zamaskować relacje między stronami transakcji.

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Zamienność

Charlie Lee, twórca Litecoina stwierdził, że zamienność była jedyną właściwością idealnych pieniędzy, której brakowało w Bitcoinie i Litecoinie, przyznając, że prywatność i zamienność były kolejnymi aspektami walki tych monet[6]. Andreas Antonopoulos, jeden z czołowych ekspertów blockchainowych na świecie, stwierdził, że „… naznaczone monety są destrukcyjne. Jeśli naruszasz zamienność i prywatność, psujesz walutę."[7]

Zamienność to właściwość towarów lub aktywów, która zapewnia, że poszczególne jednostki mają taką samą wartość i są równoważne. To właśnie odróżnia najwcześniejsze formy walut od poprzednich systemów wymiany handlowej. Bez zaufania do zamienności pieniędzy, pieniądze szybko tracą swoją użyteczność. Jak zostanie zilustrowane poniżej, zamienność większości kryptowalut jest niepewna, podczas gdy architektura prywatności Epic Cash zapewnia, że jest odporna na te konkretne zagrożenia.

Większość kryptowalut podobnych do Bitcoina, opartych na z natury transparentnych blockchainach, może być dokładnie śledzona tak jak każdy portfel, w którym były przechowywane. Prywatne osoby i firmy, podobnie jak rządy, monitorują blockchain Bitcoina za pomocą coraz bardziej wyrafinowanych metod szybkiego identyfikowania monet używanych w historycznych transakcjach. To naturalnie prowadzi do obaw, że "znaczone" monety mogą zostać kiedyś zablokowane w transakcjach, co spowoduje stratę dla ich aktualnych, niczemu niewinnych posiadaczy.

19 marca 2018 r. Amerykański Urząd Kontroli Aktywów Zagranicznych (OFAC) ogłosił, że rozważa włączenie adresów waluty cyfrowej do listy specjalnie naznaczonych obywateli (SDN, Specially Designated Nationals And Blocked Persons List), czyli podmiotów, z którymi osobom lub firmom z USA nie wolno dokonywać transakcji. Jeszcze bardziej niepokojące jest to, że OFAC nie wykluczył uwzględnienia adresów obecnie trzymających znaczone monety na liście SDN, co skutecznie umieściłoby niewinnych posiadaczy naznaczonych kryptowalut na czarnej liście przestępców z powodu powiązania ze znaczonymi monetami. To spowodowało, że profesor prawa z Uniwersytetu Nowojorskiego, Andrew Hinkes, żartował: „pożegnajmy zamienność" i że społeczeństwo powinno oczekiwać „popytu na świeżo stworzone lub zweryfikowane czyste monety…"[8].

Mając na uwadze te zmiany, nietrudno wyobrazić sobie przewrót na rynku kryptowalut oraz porażkę, a nawet całkowite zapomnienie wielu dobrze ugruntowanych kryptowalut. Jednak Epic jest jedną z niewielu kryptowalut, które całkowicie unikają tego problemu dzięki silnym funkcjom prywatności opisanym wcześniej w tym artykule. Poprzez usunięcie związku między tożsamością a własnością oraz relacji między stronami transakcji, jednostka Epic nigdy nie może być powiązana z konkretną osobą lub działaniem. Jako taka, wartość Epic pozostaje niezależna od jego użytkowników i zapewnia wysoki stopień prywatności i bezpieczeństwa, którym nie mogą łatwo manipulować żadne osoby w celach przestępczych, finansowych lub politycznych.

> **…naznaczone monety są destrukcyjne. Jeśli naruszasz zamienność i prywatność, psujesz walutę.**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Skalowalność

Epic Cash to implementacja blockchaina MimbleWimble która zapewnia najnowsze odkrycia w kwestii skalowalności dzięki oszczędzającemu miejsce blockchainowi, który pomija zbędne dane transakcyjne. Odpowiedzialna za to funkcja Cut-Through zapewnia, że blockchain z czasem zyskuje więcej miejsca, w przeciwieństwie do większości kryptowalut, w tym Bitcoina, i że można tworzyć nowe węzły przy minimalnych inwestycjach w pamięć i moc obliczeniową. Pozostając wydajnym przestrzennie, zapewnia duże rozproszenie sieci i sprzyja decentralizacji. Ponadto, podczas gdy każdy węzeł Bitcoina musi przechowywać cały blockchain, węzły Epic Cash mogą przyczyniać się do bezpieczeństwa sieci w oparciu o niewielki podzbiór bloków.

Większość kryptowalut wymaga nieograniczonego miejsca do przechowywania wszystkich danych transakcyjnych w ich łańcuchach. Blockchain Bitcoina zyskuje obecnie 0,1353 GB pojemności każdego dnia, podczas gdy łańcuch Ethereum rośnie w jeszcze szybszym tempie - o 0,2719 GB dziennie. Jeśli blockchain Bitcoina będzie nadal rósł w obecnym tempie, ostatecznie osiągnie wielkość około 6 TB do czasu wydobycia ostatniego bloku nagrody w roku 2140. Ethereum przekroczy 10 TB do tego czasu[9]. W większości łańcuchów bloków bez MimbleWimble transakcje muszą być weryfikowane przez węzły na całym świecie. Wraz ze wzrostem ilości danych rośnie obciążenie każdego węzła. Nawet przy zaledwie 200 GB (przybliżony rozmiar obecnego łańcucha Bitcoina) synchronizacja danych wymaga stabilnej sieci, a także szybkiego odczytu i zapisu na dysku.

W rezultacie wydobycie staje się coraz bardziej scentralizowane wokół dużych puli-kopalni, wykorzystujących kosztowną moc obliczeniową komputerów. **Jeśli zamiast tego cała historia blockchaina Bitcoina byłaby przechowywana w blockchainie Epic Cash, zmieściłaby się ona na prawie 90% mniejszej przestrzeni.** Mniejszy oznacza szybszy, ponieważ każda transakcja wymaga mniej czasu na przesłanie i zabezpieczenie.

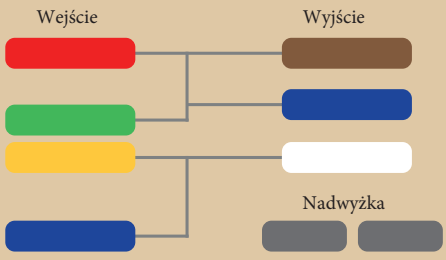
MimbleWimble rozwiązuje problem przechowywania danych za pomocą innowacyjnej metody przycinania bloków, określanej jako „Cut-Through". Aby zrozumieć, jak działa Cut-Through, najlepiej najpierw sprawdzić, w jaki sposób transakcje i bloki składają się w łańcuch bloków MimbleWimble.

Wejście:
Odniesienia do starych danych wyjściowych;

Wyjście:
Dane wyjściowe transakcji poufnych (CT) i **rangeproofs**;

Nadwyżka:
Różnica między danymi wyjściowymi i wejściowymi oraz **podpisy** (dla uwierzytelnienia i potwierdzenia bezinflacyjności).

Rycina 2:
Elementy transakcji MimbleWimble.



[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Każdy blok Epic Cash zawiera:

Drzewa Merkla danych wejściowych transakcji

Drzewa Mekla danych wyjściowych transakcji i rangeproofs;

Lista nadwyżek i podpisów

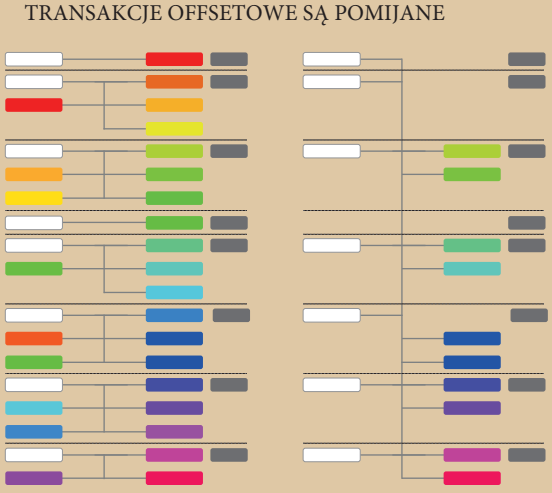
Na rycinach 2 i 3, zaadaptowanych z prezentacji Andrew Poelstry[10], możemy zobaczyć nowo wydobyte Epic przedstawione jako białe komórki wejściowe. Identycznie kolorowe komórki reprezentują wyniki z odpowiadającymi danymi wejściowymi. Dzięki procesowi Cut-Through dane wejściowe i pasujące wyjściowe są usuwane, aby zwolnić miejsce w bloku, co zmniejsza ilość danych, które muszą być przechowywane w blockchainie. Podczas gdy transakcje są pomijane w rozproszonej księdze, pozostałe dane (jądra) nadwyżkowe (zaledwie 100 bajtów) trwale dokumentują, że transakcje miały miejsce.

Jako że bloki są cały czas tworzone, MimbleWimble stosuje Cut-Through między blokami, tak, że w długim okresie pozostają tylko nagłówki poprzednich bloków (około 250 bajtów), niewydane transakcje i jądra transakcji (około 100 bajtów). Grin, druga implementacja MimbleWimble, która została uruchomiona, pokazała, że łańcuch MimbleWimble z podobną liczbą transakcji do łańcucha Bitcoina stanowiłby tylko blisko 10% wielkości łańcucha Bitcoina[11]. Co więcej, rozmiar węzła będzie „rzędu kilku GB nawet dla łańcucha wielkości Bitcoina i potencjalnie można go zoptymalizować do kilkuset megabajtów”.[12]

Stoi to w wyraźnym kontraście do Bitcoina, gdzie cały łańcuch bloków musi być przechowywany przez każdy węzeł. Z biegiem czasu, wraz ze wzrostem efektywności przestrzennej blockchaina Epic Cash w stosunku do blockchaina Bitcoina, wzrośnie również efektywność kosztowa związana z udziałem węzłów w sieci Epic Cash. Niższe progi uczestnictwa pomagają zapewnić kluczową odporność w warstwie projektowania węzłów sieci.

Dzięki wdrożeniu MimbleWimble i zastosowaniu przycinania łańcucha w procesie Cut-Through, blockchain Epic Cash oferuje skalowalność w sposób często pomijany przez społeczność kryptowalut. Jest to taki blockchain, który oddaje istotę Bitcoina i podobnie działających projektów: decentralizację. Niezależnie od tego, ile transakcji na sekundę może przetworzyć moneta, jaką ma to korzyść, jeśli nie może być utrzymywany przez szeroką i różnorodną rozproszoną sieć? Jeśli wymagania dotyczące pamięci są takie, że weryfikacja bloków ostatecznie skłania się ku silnym kompaniom wydobywczym, wówczas wszystkie wysiłki społeczności kryptowalut zmierzające do stworzenia zdecentralizowanego ekosystemu są zmarnowane. W celu zapewnienia dodatkowej przepustowości planowane jest wdrożenie Warstwy 2 w stylu Lightning Network jako krótkoterminowy cel w planie rozwoju Epic Cash.

Rycina 3:
Transakcje MimbleWimble przed i po wykorzystaniu Cut-Through.



[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Polityka monetarna

Polityka pieniężna Epic Cash i Bitcoina są bardzo podobne. Krążąca podaż Epic Cash najpierw szybko się zwiększa, a następnie synchronizuje z podażą Bitcoina w 2028 roku. Następnie rośnie w tempie malejącym, aż do osiągnięcia maksymalnej podaży 21 milionów Epic w 2140 roku. Epic Cash ma wszystkie niezbędne cechy, aby stać się bezpiecznym magazynem wartości, ponieważ ilość monet w obiegu jest znana w każdym punkcie jego cyklu emisji i osiąga szczyt w z góry ustalonym maksymalnym punkcie. Polityka pieniężna Epic Cash charakteryzuje się czterema następującymi cechami:

- Szybka emisja w ciągu pierwszych dziewięciu lat, podczas której ma zostać wydobytych 20 343 750 Epic (96,875% całkowitej podaży). Dokładne poziomy emisji są przedstawione w części Harmonogram emisji w tym dokumencie;
- Krążąca podaż Epic i szybkość emisji synchronizują się z Bitcoinem w czasie Epic Singularity (Wyrównania) około 24 maja 2028 r. Po Singularity, szybkość emisji etapowo spada, dzięki czemu krążąca podaż wzrasta dużo wolniej.;
- Maksymalna podaż 21 milionów Epic zostanie osiągnięta w roku 2140, mniej więcej w tym samym czasie, kiedy Bitcoin osiągnie maksymalną podaż 21 milionów sztuk;
- Epic ma strukturę dziesiętną podzielności, tak że: 1 Epic jest równy 100 000 000 freemanów (tak jak 1 Bitcoin jest równy 100 000 000 satoshi).

Polityka pieniężna Epic Cash jest wzorowana na Bitcoinie z następujących powodów:

- Zgoda z podstawami ekonomicznymi Bitcoina, a mianowicie, że niedostatek i przewidywalność krążącej podaży leży u podstaw silnego trzymania wartości;
- Opinia publiczna zna już model Bitcoina i jego udokumentowane osiągnięcia w ciągu ostatnich dziesięciu lat od powstania. W przybliżeniu synchronizując się z krążącą podażą Bitcoina i odzwierciedlając maksymalną podaż Bitcoina i strukturę podzielności, Epic obiera ścieżkę prostego dostosowania do masowej adopcji.

VI. Harmonogram Emisji

Epic Cash ma w sumie 33 epoki wydobycia, z których każda następna wiąże się ze zmniejszeniem nagród za blok w stosunku do poprzedniej epoki. Epic Genesis, tj. data wydobycia bloku Epic nr 1, odbywa się sierpnia 2019 r. Bloki wydobywane są co minutę. Pierwsze pięć epok wytwarza prawie 97% maksymalnej podaży Epic, odpowiadając 20 latom emisji Bitcoina w około dziewięci lat Można to uznać za szansę aby „cofnąć czas" dla tych, którzy przegapili spektakularny wzrost Bitcoina.

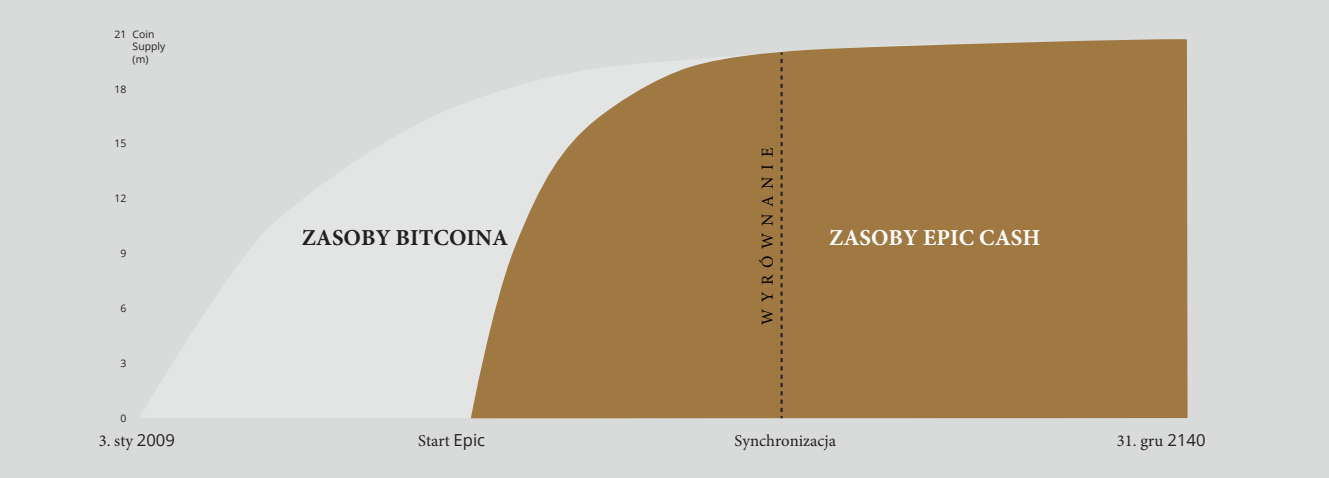
Harmonogram emisji w tabeli 1 określa daty rozpoczęcia i zakończenia pierwszych siedmiu epok wydobycia, odpowiadające im nagrody za wydobycie bloku oraz związaną z nimi podaż w każdej epoce. Okresy od 8 do 33 nie zostały uwzględnione w tabeli ze względu na zwięzłość. W tych epokach wystarczy zrozumieć, że każda kolejna era będzie miała nagrodę za blok, która stanowi połowę nagrody z poprzedniej ery, dokładnie tak jak w Bitcoinie. Ilość podaży Epic emitowanej podczas każdej z tych epok będzie sumą nagród blokowych w ciągu 4 lat (około 1460 dni).

Podczas Epic Singularity (2028), krążąca podaż Epic osiąga liczbę krążącej podaży Bitcoinów, w którym to momencie Epic Cash przyjmuje wzór nagród za bloki i podziałów od Bitcoina, co powoduje, że nagrody blokowe zmniejszają się o połowę co cztery lata. Jedynym wyjątkiem jest to, że bloki Epic są nadal wydobywane w tempie jednego co minutę, w porównaniu do szybkości jednego bloku Bitcoina co dziesięć minut. Dzięki temu krążąca podaż Epic utrzymuje przybliżoną zgodność z krążącą podażą Bitcoina do końca ich istnienia.

Tabela 1: Harmonogram emisji dla pierwszych siedmiu epok górniczych. Daty są przybliżone.

Era	1	2	3	4	5	ZRÓWNANIE	6	7
Nagroda za blok	16	8	4	2	1		0.15625	0.078125
Data startu	1, Sie 2019	29. cze 2020	11. paź 2021	3. cze 2023	10 sie 2025		24. maj 2028	22. maj 2032
Data końca	29. cze 2020	11. paź 2021	3. cze 2023	10. sie 2025	24. maj 2028		22. maj 2032	20. maj 2036
Długość (w dniach)	334	470	601	800	1019		1460	1460
Początkowy zasób	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Końcowy zasób	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% całkowitego zasobu	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Rycina 4: Plany emisji Epic i Bitcoina.



VII. Mining

Blockchain Epic Cash dąży do decentralizacji, przyjmując szeroką gamę sprzętu komputerowego. Wydobycie Epic jest początkowo dostępne dla CPU, GPU, i ASIC, z użyciem trzech algorytmów hashujących: RandomX, ProgPow, i CuckATOO31+. Algorytmy mogą być łatwo zamieniane podczas pracy bez naruszania integralności łańcucha.

1 RandomX i CPU

RandomX to algorytm Proof-of-Work (PoW) zoptymalizowany dla CPU. Wykorzystuje losowe wykonywanie programów z kilkoma technikami memory-hard, aby osiągnąć następujące cele:

- Zapobieganie rozwojowi jednoukładowych ASICów;
- Minimalizacja przewagi wydajności specjalistycznego sprzętu nad procesorami ogólnego przeznaczenia.

Mining Epic procesorami CPU wymaga ciągłego przydzielania 2 GB fizycznej pamięci RAM, 16 KB L1 cache, 256 KB L2 cache, 2 MB of L3 cache na wątek wydobywczy[13]. Urządzenia z systemem Windows 10 wymagają 8 GB lub więcej pamięci RAM. Nie jest wykluczone, że pewnego dnia, w niezbyt odległej przyszłości, telefony komórkowe mogą stać się rentownymi węzłami wydobywczymi. Wczesna integracja procesora z siecią wydobywczą Epic Cash to doskonała okazja dla wielu dysponujących jedynie skromnymi mocami obliczeniowymi, aby zdobyć nagrody blokowe, pomagając jednocześnie zabezpieczyć sieć Epic Cash.

2 ProgPow i GPU

Programmatic Proof-of-Work (ProgPow) to algorytm, który zależy od przepustowości pamięci i obliczeń rdzenia losowych sekwencji matematycznych, które obejmują wiele funkcji obliczeniowych GPU, a tym samym skutecznie wykorzystują całkowity koszt energii sprzętu. Ponieważ ProgPow został specjalnie zaprojektowany, aby w pełni wykorzystać zalety procesorów graficznych dostępnych na rynku, stworzenie specjalistycznych urządzeń jest trudne i kosztowne. W związku z tym algorytm ProgPow zmniejsza potencjał dużych pul ASIC do konkurowania z GPU, co często można zaobserwować w przypadku wielu innych algorytmów PoW, takich jak np. SHA-256 Bitcoina. Procesory graficzne, choć nie tak liczne jak zwykłe procesory, są powszechnie dostępne. Wraz z rozwojem technologicznym napędzanym przez elektrownie, Nvidię i AMD, procesory graficzne są w stanie równolegle przetwarzać więcej obliczeń wydobywczych niż procesory CPU. Z uwagi na to połączenie wszechobecności i wysokiej mocy przetwarzania procesory graficzne zapewnią szkielet dużej części działalności wydobywczej podczas początkowych okresów (Ery), jak wskazano w Tabeli 2.

3 CuckATOO+31 i ASIC

CuckATOO31+ jest przyjazną ASIC wariacją algorytmu Cuckoo Cycle opracowanego przez holenderskiego informatyka Johna Trompa. Powiązany z odpornym na ASICi CuckAROO29, CuckATOO31+ generuje losowe grafy dwudzielne i stawia przed górnikami zadanie znalezienia pętli o danej długości „N" przechodzącej przez wierzchołki tego wykresu.

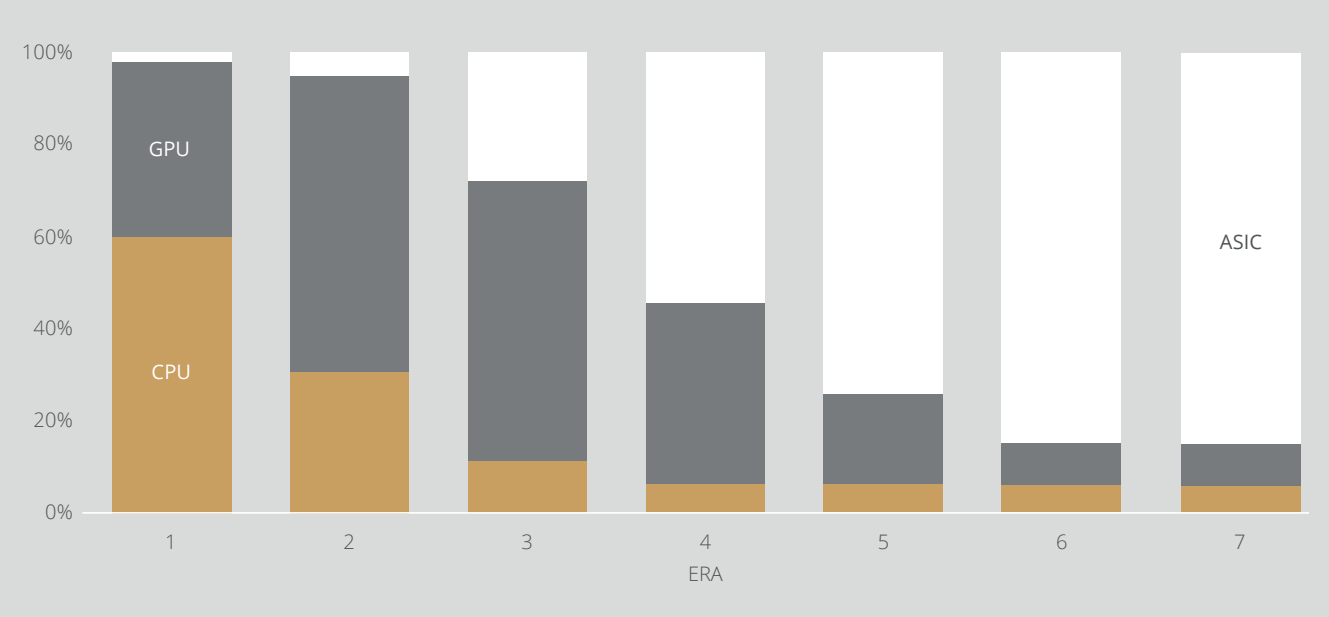
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Jest to zadanie związane z pamięcią, co oznacza, że czas rozwiązania zależy od przepustowości pamięci, a nie od szybkości procesora lub GPU. W rezultacie algorytmy Cuckatoo Cycle wytwarzają mniej ciepła i zużywają znacznie mniej energii niż tradycyjne algorytmy PoW. Przyjazny dla ASIC CuckATоо31 + umożliwia poprawę wydajności w porównaniu z procesorami graficznymi przy użyciu setek MB SRAM pozostając wąskim gardłem przez pamięci I/O[14]. Ostatecznie układy ASIC oferują największe potencjalne korzyści skali z trzech opcji wydobycia. Jednak w interesie dostępności publicznej, choć wcześnie przydzielono im niewielką część nagród wydobywczych w stosunku do procesorów i układów GPU, ostatecznie ASIC przejmują większość udziałów w wydobywanych blokach, przy założeniu, że będzie istnieć konkurencyjny ekosystem producentów urządzeń dla CuckATоо31 +.

Tabela 2: Przydziały nagród górniczych. Możliwość zaistnienia zmian. Przydziały zostaną ukierunkowane na osiągnięcie maksymalnej decentralizacji i będą zgodne z długoterminowymi interesami sieci.

Era	1	2	3	4	5	6	7
Dni	334	470	601	800	1019	1460	1460
CPU	60%	30%	10%	5%	5%	5%	5%
GPU	38%	65%	62%	40%	20%	10%	10%
ASIC	2%	5%	28%	55%	75%	85%	85%

Rycina 5: Przydziały nagrody za wydobycie dla każdej epoki zgodnie z tabelą 2. Możliwość zmiany.



[14] Le Sceller, Quentin, *An Introduction to Grin Proof-of-Work,* 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Podział nagród wydobywczych

Zaczynając razem z Epic Genesis (2019) aż do wydarzenia Epic Singularity - wyrównania (2028), podczas procesu wydobywania część Epic jest przekazywana jako wkład górniczy do EPIC Blockchain Foundation.

EPIC Blockchain Foundation poświęcona jest rozwojowi technicznemu oraz promowaniu świadomości i użyteczności projektu Epic Cash we wczesnych latach jego powstania, poprzez tworzenie działań marketingowych i rozwijanie partnerstw w branży technologii finansowych.

Po Singularity - Wyrównaniu, rolę EPIC Foundation przejmie EPIC Distributed Autonomous Corporation (EDAC), która zostanie opracowana przez fundację przed powyższą zmianą.

EPIC Blockchain Foundation jest finansowany przez procent nagród górniczych, odliczony od nagród za blok, zgodnie z następującymi rocznymi stawkami:

Tabela 3: Roczne stawki składek fundacji wydobywczych jako procent nagród górniczych.

Rok	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% nagród górniczych	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Wnioski

Epic ma na celu zostanie „zdecentralizowanym cyfrowym srebrem", środkiem wymiany będącym odpowiednikiem uznanej pozycji Bitcoina jako zdecentralizowanego cyfrowego złota. Dzięki przywróceniu utraconej zamienności na znacznie bardziej energooszczędnym i ekologicznym rozwiązaniu sprzętowym, Epic Cash przywraca równowagę mocy na korzyść pojedynczych, indywidualnych użytkowników, w przeciwieństwie do najnowszych trendów centralizacji. Połączenie ekonomii Bitcoina, teorii gier i sprawdzonej formuły proof-of-work z najlepszą współczesną technologią blockchain daje w rezultacie niezawodną, niezmienną i zdecentralizowaną walutę (Epic), która jest skalowalna, zamienna i chroni prywatność jej użytkowników. Blockchain Epic Cash jest otwarty, publiczny, bezgraniczny i odporny na cenzurę. Zachowuje prywatność i posiadanie użytkowników oraz nagradza tych, którzy wykorzystują swój sprzęt komputerowy w celu wsparcia sieci poprzez wydobycie. Każdy Epic jest wydobywany przez algorytm proof of work - dowód pracy. Podaż rozpoczyna się od zera, a sieć jest uważana za uczciwie uruchomioną, z działającym już funkcjonalnym testnetem.

Główne fakty Epic Cash:

- **Mining rozpoczyna się sierpnia 2019.**

- **Blockchain Epic Cash oparty jest o MimbleWimble.**

  Kluczowe funkcje protokołu to:

  1. **Cut-Through** – usunięcie zbędnych informacji z łańcucha bloków w celu optymalizacji wydajności zajmowanej przestrzeni, zachęcania do szerokiego uczestnictwa w walidacji sieci i decentralizacji;
  2. ***CoinJoin*** – pakietowanie transakcji w jednym bloku, aby zapewnić zamienność kryptowaluty Epic;
  3. ***Protokół Dandelion++*** – propagacja transakcji poprzez komunikację między splecionymi kanałami i rozpowszechnianie w szerokiej sieci węzłów, maskowanie połączeń między transakcjami i ich źródłem;
  4. **Brak adresów portfeli** – zastosowanie wielozadaniowej multisygnatury do generowania kluczy prywatnych jednorazowego użytku dla stron transakcji, co całkowicie eliminuje potrzebę posiadania adresów portfela.

- **Polityka monetarna Epic Cash** ma na celu zsynchronizowanie podaży Epic dostępnej w obiegu z podażą Bitcoinów za około dziewięć lat i osiągnięcie tej samej maksymalnej podaży 21 milionów jednostek w tym samym czasie co Bitcoin, tj. w 2140 roku. Ta malejąca polityka inflacyjna gwarantuje przejrzystość, przewidywalność podaży, i niedobór, sprzyjający bezpieczeństwu długoterminowego przechowywania wartości.

- **Mining**, który wykorzystuje CPUs GPU, maszyny ASIC poprzez odpowiednio algorytmy RandomX, ProgPow oraz CuckATOO31+, w celu ułatwienia masowej adopcji i wydajności sieci.

IX. Specyfikacja techniczna

Nazwa: Epic Cash
Waluta: Epic
Czas bloku: 60 sekund
Rozmiar bloku: 1 MB
Początkowa ilość monet w obiegu : 0
Ostateczna ilość monet w obiegu : 21,000,000
Blok założycielski : August 2019
Konsensus: RandomX (CPU), ProgPow (GPU) and CuckAToo31+ (ASIC)

Linki:

www.epic.tech

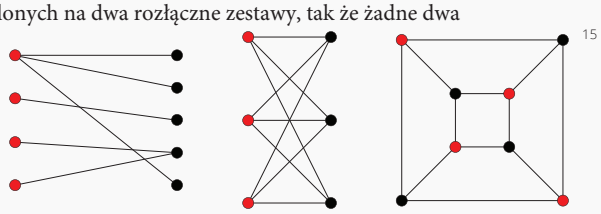
t.me/EpicCash – Telegram

t.me/EpicCashPolski

X. Słowniczek

ASIC Application Specific Integrated Circuits; chipy, które są zaprojektowane do pojedynczego celu

dwudzielny wykres zestaw wierzchołków wykresu podzielonych na dwa rozłączne zestawy, tak że żadne dwa wierzchołki wykresu w tym samym zestawie nie sąsiadują ze sobą.



Czynnik maskujący losowy element wprowadzany do wiadomości cyfrowej w celu ułatwienia szyfrowania; wspólny tajny element między dwiema stronami, który szyfruje dane wejściowe i wyjściowe konkretnej transakcji, a także klucze publiczne i prywatne stron transakcji[16].

Nagroda za blok nowe Epic dystrybuowane przez sieć jako nagrody za obliczenia wykonane w celu zweryfikowania transakcji w nowym bloku.

Cache element sprzętowy lub programowy, który przechowuje dane, dzięki czemu przyszłe żądania dotyczące określonych danych mogą być obsługiwane szybciej.

Monety krążące w obiegu ilość Epic istniejących w danym momencie.

CPU Central Processing Unit: komponent komputerowy odpowiedzialny za przetwarzanie i wykonywanie większości poleceń z innego sprzętu i oprogramowania komputera..

Cut-Through proces blockchaina MimbleWimble, w którym dane wejściowe i pasujące dane wyjściowe są usuwane, aby zwolnić miejsce w bloku, zmniejszając ilość danych koniecznych do przechowywania w blockchainie.

Decentralizacja stan rozproszenia sieci i jej nadzoru.

Emisja stworzenie nowych Epic otrzymywanych przez górników w nagrodach za blok. Epic jest tworzony co 60 sekund, gdy to transakcje są potwierdzane w blockchainie.

Epic Singularity Wyrównanie, punkt, w którym podaż krążąca Epic wyrównuje się z podażą krążącą Bitcoina (Maj 2028)

Nadwyżka (MimbleWimble) różnica między danymi wyjściowymi a danymi wejściowymi oraz podpisy (do uwierzytelnienia i udowodnienia braku inflacji).

Zamienność właściwość towaru lub rzeczy, zgodnie z którą poszczególne jednostki są zasadniczo wymienne, a każdej równej części nie można odróżnić od innej części.

Genesis (wydarzenie) wydobycie pierwszego bloku Epic i oficjalne rozpoczęcie blockchaina.

GPU Graphics Processing Unit: Jednostka zawierająca programowalny układ logiczny (procesor) specjalizujący się w wyświetlaniu. Procesory te mogą dobrze nadawać się do wydobycia kryptowalut.

Halving (dla Bitcoina) występuje co 4 lata. Ilość wydobywanych monet zmniejsza się o 50% po każdym zdarzeniu.

Hash wartość obliczona na podstawie liczb wejściowych za pomocą funkcji mieszającej.

Algorytm hashujący (funkcja) algorytm matematyczny odwzorowujący dane o dowolnym rozmiarze na ciąg o ustalonym rozmiarze, używany do generowania i weryfikacji podpisów cyfrowych, kodów uwierzytelnienia wiadomości (MAC) i innych form uwierzytelniania.

Niezmienność szyfrowania homomorficznego metoda wykonywania obliczeń na zaszyfrowanych informacjach bez ich odszyfrowywania. (W programowaniu) stan, w którym obiekt nie może być modyfikowany po jego utworzeniu.

Wejście (MimbleWimble) składnik transakcji MimbleWimble reprezentujący stronę wysyłającą transakcję; utworzony z wyników poprzednich transakcji.

I/O wejście/wyjście; komunikacja między systemem przetwarzania informacji, takim jak komputer, a światem zewnętrznym, np. człowiekiem lub innym systemem przetwarzania informacji.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Maksymalna podaż	ilość Epic, którą można maksymalnie osiągnąć, powyżej której podaż nie wzrośnie (21 000 000 Epic).
Memory-Hard	użycie dużej ilości pamięci RAM, aby wykluczyć jednoczesne próby uruchamiania równoległych połączeń. Funkcje memory-hard to algorytmy, których czasy obliczeń zależą przede wszystkim od dostępnej pamięci do przechowywania danych. Znane również jako funkcje związane z pamięcią.
Drzewo Merkla	struktura danych wykorzystywana w aplikacjach informatycznych. W blockchainie drzewa Merkla pozwalają na wydajną i bezpieczną weryfikację treści w dużych strukturach danych.
MimbleWimble	protokół przedstawiony przez osobę o pseudonimie Tom Elvis Jedusor w pokoju rozmów deweloperów Bitcoina.
Multisignature	schemat podpisu cyfrowego, który umożliwia grupie użytkowników podpisanie jednego dokumentu. Zwykle algorytm multisignature tworzy wspólny podpis, który jest bardziej zwarty niż zbiór osobnych podpisów od wszystkich użytkowników[17].
Węzeł	komputer, który łączy się z siecią blockchain i propaguje dane na inne węzły w sieci, aby rozpowszechniać informacje o transakcjach i blokach w sposób peer-to-peer.
One Way Aggregate Signature (OWAS)	podpis transakcji złożony z wielu podpisów, który jest zaszyfrowany w taki sposób, że bardzo trudno jest obliczyć poszczególne podpisy, które są częścią agregatu.
Dane wyjściowe (MimbleWimble)	składnik transakcji MimbleWimble reprezentujący odbiór transakcji; wykorzystywane jako dane wejściowe dla kolejnych transakcji.
Pedersen Commitment Scheme	kryptograficzny schemat, który pozwala stronie zaakceptować wybraną wartość bez ujawniania jakichkolwiek informacji na jej temat i bez możliwości anulowania zobowiązania do wartości.
Klucz prywatny	klucz prywatny to niewielki fragment kodu, który jest sparowany z kluczem publicznym w celu uruchomienia algorytmów szyfrowania i deszyfrowania tekstu. Jest tworzony jako część kryptograficzna klucza publicznego podczas szyfrowania kluczem asymetrycznym i służy do odszyfrowywania i przekształcania wiadomości do czytelnego formatu.
Proof of Work (PoW)	fragment danych, których wytworzenie jest trudne (kosztowne i czasochłonne), ale łatwe do zweryfikowania przez innych, i który spełnia określone wymagania. Algorytmy proof of work są często używane do generowania bloków kryptowalut.
Klucz publiczny	klucz publiczny jest tworzony w kryptografii szyfrowania kluczem, która wykorzystuje algorytmy szyfrowania kluczem asymetrycznym. Klucze publiczne służą do konwersji wiadomości na nieczytelny format.
RAM (Random Access Memory)	układy umożliwiające szybki dostęp do przechowywania danych w urządzeniu komputerowym, w którym przechowywany jest system operacyjny, aplikacje i dane będące w bieżącym użyciu, aby procesor urządzenia mógł szybko do nich dotrzeć.
Rangeproof	sprawdzenie poprawności zobowiązania, które weryfikuje, czy suma danych wejściowych transakcji jest większa niż suma danych wyjściowych transakcji i czy wszystkie wartości transakcji są dodatnie. Rangeproofs zapewniają, że podaż waluty nie została zmieniona.
(Cyfrowy) podpis	standardowa część protokołu blockchain, wykorzystywana głównie do zabezpieczania transakcji i bloków transakcji, przekazywania informacji, zarządzania umowami i wszelkimi innymi przypadkami, w których ważne jest wykrywanie i zapobieganie ingerencji z zewnątrz. Zapewnia trzy zalety przechowywania i przekazywania informacji w łańcuchu bloków: • Ujawnia, czy przesyłane dane zostały sfałszowane; • Weryfikuje udział konkretnej strony w transakcji; • Może być prawnie wiążący.
SRAM (Static Random Access Memory)	Random Access Memory (RAM) który zachowuje bity danych w pamięci tak długo, jak długo dostarczane jest zasilanie.
Przepustowość	miara transakcji na sekundę, które mogą być prowadzone przez dany protokół kryptowaluty.
Zaufanie	cecha sieci kryptowalutowej będącej w zgodności z zasadami protokołu bez konieczności nadzoru zewnętrznego urzędu.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPIC PRIVATE INTERNET CASH