BULWARK

CRYPTOCURRENCY

Biała księga

Zespół Projektowy:
Eatbatterys (Koordynator Projektu)
Jack (Dyrektor ds. Marketingu)
SerfyWerfy (Deweloper ds. Blockchain)
Frogman (Kierownik działu Komunikacji)
Patrick (Brand i design)
Stu (Deweloper ds. Ekosystemu)

Bulwark Core Team

Grudzień 2017

My, zespół projektowy kryptowaluty Bulwark, potwierdzamy, że treści zawarte w tej dokumentacji technicznej są naszego autorstwa. W miejscach, w których informacje pochodzą z innych źródeł, zamieściliśmy odpowiednie przypisy.

Streszczenie

Bulwark (ticker: BWK) jest zorientowaną społecznościowo walutą cyfrową, która narodziła się na podstawie spostrzeżenia, że praktykowane obecnie podejście do węzłów głównych (ang. „masternodes") w przypadku walut stawiających na prywatność jest, ogólnie rzecz biorąc, niezbyt sprawiedliwe. Nasza przemyślana, sprawiedliwa strategia startu daje wszystkim jej uczestnikom możliwość włączenia się w obiecujący projekt w fazie jego powstawania. Oferujemy prostą propozycję wartości bez wygórowanych obietnic: dostarczymy nastawioną na prywatność kryptowalutę, która działa już dziś, a w przyszłości będzie się rozwijać, i która korzysta z najlepszych praktyk wypracowanych przez kryptowaluty DASH i PIVX. Nie prezentujemy fantazyjnych wizji, o których realizację będzie potem trudno, lecz funkcjonującą walutę i działającą platformę, wraz ze wsparciem w przyszłości. Nie oznacza to, że nie planujemy innowacji, ale że zamiast skupiać się na szumie medialnym, skupimy się na dostarczaniu rozwiązań. Istnieje już zbyt wiele kryptowalut napędzanych wyłącznie histerią i euforią, lecz kompletnie pozbawionych wewnętrznej wartości. Nie chcemy dołączyć do rosnącej grupy kryptowalut, które — napędzane wygórowanymi obietnicami — nie potrafią ich jednak do końca spełnić. Dzięki cechom i parametrom takim jak: brak oferty ICO, początkowo łagodnie rosnący poziom trudności, niewielki procent waluty wydobytej przed premierą (ang. „premine"), a także faworyzujący górników system przyznawania nagród za bloki, użytkownicy waluty Bulwark mają zapewniony uprzywilejowany dostęp do nastawionej na prywatność kryptowaluty, która łączy w sobie funkcjonalność masternode'ów i najlepsze w branży techniki ochrony prywatności, a także obiecuje rozwój wg. rozsądnie zaplanowanej wizji (ang. „roadmap"). Działające masternode'y będą dostępne już w momencie premiery — są one fundamentalną częścią naszej wizji kryptowaluty Bulwark i będą poprawiać stabilność obiegu waluty, zabezpieczać sieć oraz zapewniać ważne funkcje.

Podziękowania

Projekt Bulwark nie byłby możliwy, gdyby nie poprzedzające go prace zespołów deweloperów walut Bitcoin, Peercoin, Blackcoin, Talkcoin, Dash i PIVX. Oprogramowanie open source i ludzie je tworzący wciąż otwierają drogi do nowych, fascynujących, innowacyjnych rozwiązań. Kiedy informacje i wiedza są darmowe i wolne, społeczeństwo, jako całość, zyskuje. Jesteśmy wdzięczni naszym poprzednikom za możliwość dodania swojego wkładu w ten rosnący ekosystem.

Spis treści

Rozdział 1

Krótkie wprowadzenie do kryptowalut

1.1 Pochodzenie

W 2009 r. Satoshi Nakamoto wydał publikację zatytułowaną „Bitcoin: A Peer-to-Peer Electronic Cash System" (Bitcoin: Elektroniczny system pieniężny oparty na sieci peer-to-peer), szczegółowo przedstawiając swoją wizję systemu pieniężnego w handlu. Wizja Nakamoto pokazywała w detalach system działający na zasadzie sieci P2P (ang. „peer-to-peer" — łączenie się użytkowników równorzędnych) wspierany przez bazujący na funkcji haszującej mechanizm PoW (ang. „proof-of-work" — dowód wykonania pracy). Sieć ta, poprzez haszowanie transakcji, umieszcza ich znaczniki czasowe w uaktualnianym na bieżąco rejestrze, który nie może zostać zmodyfikowany bez ponownego przeprowadzenia dowodu PoW. Węzły sieci wybierają najdłuższy przeliczony łańcuch, poświadczony przez największą pulę obliczeniowej mocy haszującej jako dowód przeprowadzonej transakcji. Dopóki ≥51% mocy haszującej sieci jest kontrolowane przez węzły niezamierzające przeprowadzać jakiegokolwiek ataku na łańcuch, tak długo łańcuch, który one generują, pozostaje łańcuchem najdłuższym (Nakamoto 2009).

1.2 Blok

Każdy blok w sieci jest poprzedzony 80-bajtowym nagłówkiem zawierającym podwójnie zaszyfrowaną algorytmem SHA256 kopię nagłówka poprzedniego bloku, korzeń drzewa haszy (ang. „merkle root" — podwójnie zahaszowaną algorytmem SHA256 pochodną wszystkich haszy występujących w danym bloku), znacznik czasowy, przy którym obliczanie proof-of-work się rozpoczęło, wartość docelową trudności, od której hasz tego nagłówka musi lub mniejszy (lub równy), a także unikalną jednorazową wartość (ang. „nonce"), przy której tzw. górnicy (ang. „miners") osiągnęli wartość docelową trudności. Jako takie, wszystkie próby modyfikacji dowolnej transakcji w dowolnym bloku skutkują odrzuceniem tego bloku przez wszystkich górników (Bitcoin Core Team 2017).

1.3 Łańcuch bloków (ang. „blockchain")

Grupy transakcji są łączone w bloki, które z kolei są chronologicznie umieszczane w łańcuchu, tworząc tzw. „łańcuch bloków" (ang. „blockchain"). Łańcuch bloków tworzy wciąż aktualizowaną historię wszystkich operacji wykonanych w sieci i służy jako

rozproszony model konsensusu, w którym dowolna transakcja może zostać w dowolnym momencie zweryfikowana (Crosby i inni 2015).

1.4 Mechanizm „proof-of-work”

Proof-of-work jest systemem weryfikacji, w którym górnicy muszą poświęcić swoje zasoby materialne (koszty elektryczności i niezbędnego sprzętu), aby znaleźć rozwiązanie pewnej arbitralnej probabilistycznej funkcji. W celu wpisania do blockchainu sfałszowanej transakcji strona przeprowadzająca tego typu atak musiałaby przeliczyć wszystkie dowody proof-of-work znajdujące się w łańcuchu od początku jego istnienia aż do chwili obecnej (Okupski 2016).

Rozdział 2

Przedstawiamy walutę Bulwark

2.1 Solidny fundament

Każdy dom potrzebuje solidnych fundamentów. Kryptowaluta Bulwark nie jest tu wyjątkiem. Jest ona zbudowana w oparciu o kryptowalutę PVIX, która z kolei bazuje na popularnej kryptowalucie DASH. Podczas gdy korzenie wszystkich kryptowalut mogą być prześledzone aż do oryginalnego projektu Satoshiego, projekt każdej kryptowaluty wybrał określony przez siebie kierunek i identyfikuje się z celami i ideami reprezentatywnymi dla społeczności, której ma zamiar się przysłużyć. My zamierzamy kłaść szczególny nacisk na ochronę prywatności i rozszerzać tę funkcję na bazie wymienionych platform naszych poprzedników — w tym celu będziemy eksplorować nowe technologie i tworzyć zestawy narzędzi oraz inne możliwości pozwalające integrować kryptowalutę Bulwark ze współczesnymi platformami technologicznymi.

2.2 Zespół oddany społeczności

W przypadku niektórych projektów aspekt społecznościowy jest dodawany w pewnym momencie ich rozwoju. Jednak w projekcie Bulwark społeczność jest priorytetem numer jeden. Poprzez konkursy, nagrody, żywą platformę dyskusyjną i politykę zera tolerancji w odniesieniu do dokuczania nowoprzybyłym uczestnikom, Bulwark dąży do bycia kryptowalutą odpowiednią dla wszystkich typów użytkowników. Członkowie naszej społeczności już teraz tworzą użyteczne skrypty i poradniki, aby ułatwić posługiwanie się naszą kryptowalutą.

2.3 Sprawiedliwa i zrównoważona

W chwili tworzenie niniejszego dokumentu nastąpił wysyp nowych kryptowalut działających na podobnych zasadach, co Bulwark. O ile technologia, na których są zbudowane, jest godna zaufania, bardzo często przy głębszym przyjrzeniu się specyfikacji parametrów ich blockchainów okazuje się, że stosują one co najmniej wątpliwe dla zwykłych użytkowników praktyki.

2.4 Problem pre-miningu

2.4.1 Studium przypadku: FooBarBazCoin

W świecie kryptowalut istnieje nasilający się trend, aby ustalać pewną arbitralną datę w odległej przyszłości, a następnie opierać procentową liczbę monet utworzonych w procesie tzw. „pre-miningu” (sytuacja, w której część lub całość monet została utworzona przed

uruchomieniem danej kryptowaluty) na liczbie jednostek będących w obiegu tego założonego dnia. Przyjrzyjmy się fikcyjnemu projektowi FBC (*FooBarBaz Coin*), będącego rozgałęzieniem (ang. „fork") kryptowaluty DASH.

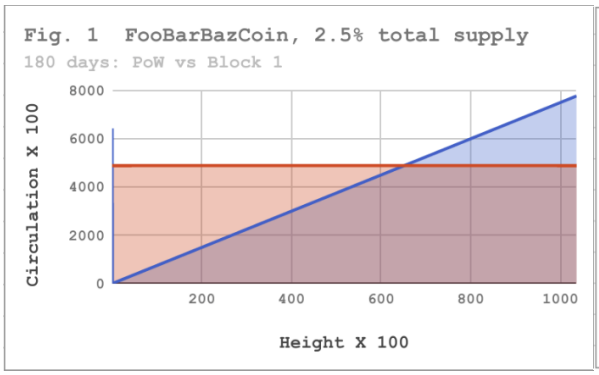
- Nagroda za blok: 15
- Czas między blokami: 2,5 min
- Podział między PoW/masternodes: 50/50%
- Wstępny algorytm ustalania trudności: KGW (Kimoto Gravity Well)
- Liczba generowanych monet zmniejsza się co roku o 12%
- Maksymalna liczba monet: około 25 milionów
- Pre-mine: 2,5%

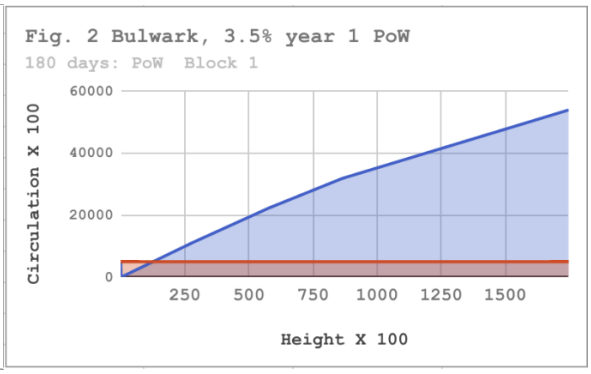
W tym przykładzie reklamowana liczba 2,5% monet wygenerowanych w procesie pre-miningu przekłada się na ok. 643 000 monet (z około 25 milionów), co dla zwykłego obserwatora wydaje się wartością rozsądną. Jednak zarówno w przypadku przeprowadzania obliczeń PoW, jak w przypadków węzłów masternode, wygenerowanie takiej samej liczby monet, jak ta posiadana przez deweloperów, trwałoby około 43 000 bloków. Przy założonym czasie docelowego odstępu między blokami wynoszącym 2,5 minuty, zajęłoby to górnikom mniej więcej 150 dni (lub 75 dni dla PoW i masternode jednocześnie). Po 75 dniach deweloperzy kryptowaluty nadal kontrolowaliby połowę wszystkich istniejących monet.

2.5 Bardziej sprawiedliwa alternatywa

Zespół projektu Bulwark zauważył ten trend i zdecydował się wystąpić przed szereg. Nasz pre-mine w liczbie 489 720 monet (3,5%) reprezentuje niewiele więcej niż 12 dni wydobywania metodą PoW lub nieco ponad 10 dni wspólnego generowania ich obiema metodami. Wierzymy, że posłuży to jako zapewnienie społeczności, iż począwszy od pewnego momentu rynek nie będzie mógł zostać znacząco zdewaluowany w rezultacie posiadania dużej ilości waluty przez zespół deweloperów. Jak możecie zauważyć na poniższych wykresach, z których oba przedstawiają okres 180 dni, różnica jest bardzo wyraźna. Mamy nadzieję, że podchodząc do tego tematu w szczery i otwarty sposób, ustanowimy pewien precedens, który przyniesie korzyść całej społeczności użytkowników kryptowalut.

2.5.1 Porównanie obu podejść





2.5.2 Nasze podejście do „instaminingu”

Projekt DASH (Darkcoin) reprezentuje interesujące studium przypadku, z którego wynika potrzeba chronienia użytkowników przed mechanizmem „instamine” (błyskawicznego miningu wstępnego). Prawie 10–15% całkowitej maksymalnej podaży Dasha, dzięki pewnym przedsiębiorczym użytkownikom (Wiecko 2017), zostało wykreowane w okresie kilku pierwszych dni istnienia nowej waluty. Nasze podejście do instaminingu było dwojakie. Zastosowaliśmy mechanizm powolnego generowania (ang „slow subsidy”), w którym nagroda za pierwsze 960 bloków (1 dzień) wzrasta liniowo do pełnej wysokości, przy czym 100% nagród za bloki wygenerowane tego dnia trafia do górników. W dotychczasowych projektach problem ten rozwiązywano w ten sposób, iż stosowano bardzo niskie nagrody za blok, które w pewnym momencie nagle wzrastały do pełnej wysokości. Jednak takie podejście często owocowało celowymi atakami DDoS na serwery operatorów tzw. „kopalni” (ang. „pool”) lub też po prostu powodowało przytłoczenie tych serwisów wzmożonym ruchem ze strony nowych górników. W przypadku nagrody rosnącej liniowo próby ingerowania w działalność górników czy kopalni nie będą miały żadnego uzasadnienia ekonomicznego.

2.5.3 ICO? Raczej „IC-NO”!

Zmierzmy się z tym zagadnieniem. W czasie tworzenia tego dokumentu jesteśmy ciągle bombardowani nowymi ofertami „ICO” (ang. „initial coin offering”). Choć mają one swoje zasadne miejsce w ekosystemie kryptowalut, to jednak bardzo często służą tylko i wyłącznie skoncentrowaniu kapitału. Uwzględniając fakt, że projekt Bulwark oferuje zarówno nagrody dla węzłów masternode, jak i, w swojej drugiej fazie, nagrody z użyciem algorytmu PoS (ang. „proof-of-stake”), taka koncentracja majątku płynąca z ICO może powodować duże

wahania rynku i mocno przechylać kontrolę nad walutą silnie w stronę najwcześniejszych (i najzamożniejszych) użytkowników. O ile koncentracja kapitału jest, ogólnie rzecz biorąc, nie do uniknięcia, wierzymy, że każda metoda wyrównywania szans dla wszystkich użytkowników jest możliwością wartą wzięcia pod uwagę. Uruchomiliśmy projekt ze strategią skalowanej nagrody za blok, czyli uczciwym mechanizmem mającym na celu promowanie szerokiej dystrybucji waluty Bulwark wśród wielu użytkowników, co w idealnym przypadku pozwoli uniknąć koncentracji kapitału dokonującej się w innych projektach.

2.6 Szybka i funkcjonalna

Dzięki takim parametrom i funkcjom, jak czas między blokami wynoszący 90 sekund, konsensus węzłów masternode i blokowanie transakcji (ang. „transaction locking"), rozsądny harmonogram emisji, a także przyjazny dla środowiska proces „stakingu", Bulwark aspiruje do bycia naprawdę szybką i funkcjonalną kryptowalutą.

Rozdział 3

Parametry naszego blockchaina

3.1 Podsumowanie specyfikacji Bulwark

Tabela 3.1: Podsumowanie specyfikacji Bulwark

Specyfikacja	Opis
Ticker	BWK
Algorytm	NIST5
Port RPC	52541
Port P2P	52543
Czas między blokami	90 sekund
Algorytm trudności	Dark Gravity Wave v3.0
Rozmiar bloku	1 MB
Dojrzałość („maturity") wydobytych monet	67 bloków (ok. 100 minut)
Potwierdzenie	6 bloków (ok. 9 minut)
Liczba monet w obiegu (1 rok)	14 505 720 BWK
Liczba monet w obiegu (5 lat)	27 668 220 BWK
Okres PoW	nHeight ≤ 345 600
Okres PoS	nHeight ≥ 345 601
Wsparcie protokołów	IPv4, IPv6, TOR
PoS	Blackcoin v3.0 PoS, nagrody w funkcji „SeeSaw" projektu PIVX

3.2 Powolny start (SlowStart)

Nasz uczciwy start zapewnia strategia opisana poniższym fragmentem kodu (dziękujemy *Zcash*):

```
int64_t nSlowSubsidy = 50 * COIN;

if (nHeight < 960 / 2) {        // If block height less than 480,
   nSlowSubsidy /= 960;         // Set nSubsidy to .05208333
   nSlowSubsidy *= nHeight;     // Multiply present height by .05208333
} else if (nHeight < 960 {      // ex: Block 200, BR will be 10.41666600
    nSlowSubsidy /= 960;        // Credits: ZCASH Team
    nSlowSubsidy *= nHeight;
```

3.3 Algorytm Dark Gravity Wave 3.0

Algorytm Dark Gravity Wave 3.0 został zaimplementowany w Bulwark od samego początku jako metoda zmiany trudności miningu metodą PoW. Używa on prostej funkcji średniej ruchomej (ang. „moving average"), która może reagować na znaczne wzrosty i spadki mocy obliczeniowej sieci w ciągu zaledwie kilku bloków. Mechanizm ten łagodzi efekt „utknięcia bloku" (ang. „stuck block effect"), często powodowanego przez kopalnie typu „multipool" (czyli wydobywające różne waluty i przełączające się między nimi w zależności od poziomu opłacalności), i zapobiega sytuacji, w której jedna osoba dodająca w pewnym momencie znaczną moc obliczeniową do sieci mogłaby błyskawicznie wydobyć wiele bloków.

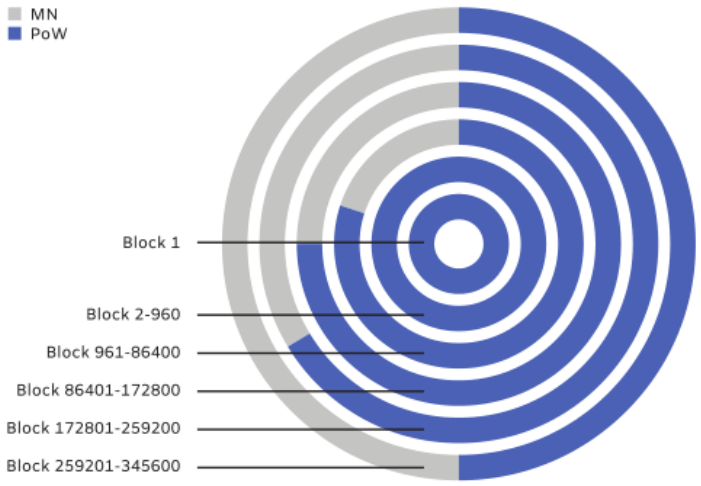
Rozdział 4

Nagroda za blok

4.1 Nagroda za blok w algorytmie PoW

Tabela: Nagroda za blok w okresie działania algorytmu PoW

Liczba tworzonych monet	Blok	PoW	MN	Liczba monet w obiegu
489 720	1	100%	ND.	489 200
ok. 25 (średnio)	2–960	100%	ND.	513 150
50,000	961–28 800	80%	20%	1 953 150
50,000	28 801–57 600	75%	25%	3 393 150
50,000	57 601–86 400	66%	33%	4 833 150
43,750	86 401–172 800	50%	50%	8 613 150
37,500	172 801–259 200	50%	50%	11 853 150
31,250	259 201–345 600	50%	50%	14 553 150



Rys. 4.1 Nagroda za blok w okresie działania algorytmu PoW

4.2 Nagroda za blok w algorytmie PoS

Tabela 4.2: Nagroda za blok w okresie działania algorytmu PoS

Liczba tworzonych monet	Blok	Budżet	PoS/MN	Uwaga
25,000	345 601–432 000	10%	SeeSaw	Rok 2
21,875	432 001–518 400	10%	SeeSaw	Rok 2
18,750	518 401–604 800	10%	SeeSaw	Rok 2
15,625	604 801–691 200	10%	SeeSaw	Rok 2
10,250	691 201–777 600	10%	SeeSaw	Rok 3
10,938	777 601–864 000	10%	SeeSaw	Rok 3
9,3750	864 001–950 400	10%	SeeSaw	Rok 3
7,8120	950 401–1 036 800	10%	SeeSaw	Rok 3
6,2500	1 036 801–1 123 200	10%	SeeSaw	Rok 4
5,4690	1 123 201–1 209 600	10%	SeeSaw	Rok 4
4,6880	1 209 601–1 296 000	10%	SeeSaw	Rok 4
3,9060	1 296 000–1 382 400	10%	SeeSaw	Rok 4
3,1250	1 382 401–1 468 800	10%	SeeSaw	Rok 5
2,7340	1 468 801–1 555 200	10%	SeeSaw	Rok 5
2,3440	1 555 201–1 641 600	10%	SeeSaw	Rok 5
1,9530	1 641 601–1 728 000	10%	SeeSaw	Rok 5
1,6250	1 728 000+	10%	SeeSaw	Na zawsze

Rozdział 5

Haszowanie NIST5

5.1 Dlaczego NIST5

Spopularyzowany przez TalkCoin w roku 2014 algorytm haszujący NIST5 zdobył umiarkowaną popularność. Monety z algorytmem NIST5 można kopać za pomocą szerokiego wachlarza sprzętu dostępnego zwykłym użytkownikom „domowym", włączając w to procesory (CPU) oraz karty graficzne (GPU), zarówno firm AMD, jak i NVIDIA. NIST5 nie jest algorytmem tak trudnym do zaimplementowania w układach ASIC, jak niektóre inne algorytmy mające znacznie większe zapotrzebowanie na pamięć operacyjną. Wierzymy, że ten kompromis jest do zaakceptowania, aby zwiększyć stabilność systemu i zredukować zużycie energii elektrycznej w porównaniu do tych pamięciożernych algorytmów. W przypadku, gdyby przed końcem fazy używania przez nas algorytmu PoW pojawiła się aktualizacja firmware'u dodającego obsługę NIST5 do układów ASIC, jesteśmy na to przygotowani, mając na podorędziu algorytm alternatywny. W takiej sytuacji zwrócimy się do społeczności i zaproponujemy głosowanie w sprawie tego, w którą stronę powinniśmy zmierzać. Jeśli jakieś dodatkowe działania okażą się konieczne, wdrożymy odpowiednie zmiany. Jesteśmy przekonani, że nasza krótka faza PoW i otwartość dla zmiany algorytmu będzie czynnikiem zniechęcającym producentów układów ASIC i nie przewidujemy w tej kwestii żadnych komplikacji.

5.2 Pięciu Finalistów (konkurs NIST SHA-3)

Pięć algorytmów haszujących, które składają się na algorytm NIST5, to finaliści konkursu NIST Hashing Competition (Chang i inni 2012). Są to (w kolejności, w jakiej bloki są haszowane):

Blake (Aumasson 2013), **Grøstl** (Gauravaram i inni 2012), **JH** (Wu 2012), **Keccak** (Bertoni i inni 2012) oraz **Skein** (Ferguson i inni 2010).

5.3 Nowy standard SHA-3

We wspomnianym konkursie do finałowej rundy zakwalifikowany został algorytm Keccak i to właśnie on stał się nową funkcją haszującą SHA-3. Pozostałe cztery algorytmy (pomimo iż uważa się, że są kryptograficznie bezpieczne) straciły po kilka punktów od sędziów z powodu różnych niewielkich niedociągnięć technicznych. Wierzymy, że połączenie nowego standardu SHA-3 (czyli algorytmu Keccak) z pozostałymi finalistami daje w efekcie szybki, bezpieczny i ustandaryzowany algorytm haszujący.

5.4 Dostępność oprogramowania do miningu

W momencie tworzenia tego dokumentu dostępnych jest kilka opcji dla minerów:

Nazwa	Platforma	Łącze
SGMiner-5.0	OpenCL	https://github.com/genesismining/sgminer-gm
ccminer-2.2.2	CUDA	https://github.com/tpruvot/ccminer
cpuminer-opt	CPU	https://github.com/tpruvot/cpuminer-multi

Rozdział 6

Cechy systemu

6.1 Węzły Masternode

Węzły Masternode (węzły główne) są w istocie zdecentralizowaną siecią komputerów, które obsługują sieć Bulwark. Węzły te wykonują ważne funkcje sieciowe i otrzymują cześć nagród za bloki. Służą ekosystemowi Bulwark poprzez stabilizację podaży waluty, przetwarzanie transakcje oraz zabezpieczanie sieci. Aby mógł działać węzeł Masternode, wymagane jest posiadanie 5000 BWK oraz skromnego zasobu wiedzy technicznej. Każdy portfel o saldzie 5000 BWK można skonfigurować do bycia węzłem Masternode.

6.2 Obfuskacja / mieszanie monet

W kryptowalucie Bulwark zaimplementowano mechanizm tzw. „obfuskacji" (z ang. „obfuscation", inaczej: „zaciemniania" transakcji), bazujący na metodzie CoinJoin, ale z kilkoma różnymi usprawnieniami względem oryginału. Mechanizm ten wykorzystuje mieszanie monet w sposób zdecentralizowany sposób, co jest możliwe dzięki sieci węzłów Masternode. W ten sposób zapewniona zostaje dodatkowa warstwa prywatności transakcji. O ile metoda ta nie daje pełnej anonimowości, to jednak obfuskacja za pośrednictwem mieszania wykonywanego przez węzły Masternode jest i tak o wiele lepsza niż w przypadku standardowych transakcji w sieci bitcoin. Dla przykładu, wszystkie transakcje w sieci bitcoin są transparentne. W przypadku sieci Bulwark osoba chcąca prześledzić transakcje musiałaby kontrolować 50% działających węzłów Masternode, aby mieć zaledwie 0,5% szansy na deanonimizację pojedynczej transakcji, która została wymieszana uprzednio 8 rundami obfuskacji (Kiraly 2017b). Ta ważna funkcjonalność zapewnia tym użytkownikom BWK, którzy zdecydują się na zastosowanie obfuskacji swoich transakcji, bardzo wysoki poziom anonimowości.

6.3 SwiftTX

Mechanizm SwiftTX daje węzłom Masternode uprawnienia do blokowania i uzgadniania konsensusu dla transakcji. Kiedy dana transakcja jest przesyłana do sieci, grupa węzłów Masternode ma za zadanie ocenić jej prawidłowość. Jeśli te węzły osiągną konsensus co do prawidłowości tej transakcji, zostanie ona zablokowana w celu późniejszego włączenia jej do łańcucha blockchain, co znacznie zwiększa szybkość transakcji w porównaniu do systemów konwencjonalnych (takich jak bitcoin, w którym wymaganych jest kilka potwierdzeń, a czas między blokami wynosi 10 minut). Mechanizm SwiftTX umożliwia przeprowadzenie wielu transakcji, zanim jeszcze dany blok z tymi sami wejściami zostanie wydobyty w sieci. System ten jest oparty na mechanizmie InstantSend wdrożonym w kryptowalucie Dash (Kiraly 2017a).

6.4 Sporki

W sieci Bulwark stosowany jest specjalny, wielofazowy mechanizm tworzenia forków (czyli, inaczej mówiąc, „odgałęzień" wersji), znany pod angielską nazwą „sporking". Pozwala on sieci BWK na wdrażanie nowych funkcji przy jednoczesnym zminimalizowaniu prawdopodobieństwa wystąpienia w sieci niezamierzonego forka podczas fazy wycofywania starej wersji. W systemie Spork zmiany są wdrażane przez samą sieć i mogą być włączane i wyłączane w miarę potrzeb bez konieczności aktualizacji oprogramowania węzłów (Strophy 2017). Ta cecha jest wyjątkowo użyteczna i pozwala sieci na szybkie reagowanie na ewentualne zagrożenia bezpieczeństwa.

6.5 Węzły Masternode typu TOR oraz IPv6

Sieć Bulwark umożliwia użytkownikom uruchamianie pełnego węzła (ang. „full node") lub węzła Masternode zarówno z adresu typu .onion (sieć TOR), jak i z adresu IPv6. Postaraliśmy się, aby dodać możliwość tworzenia pełnych węzłów typu TOR w celu zarówno wzmocnienia samej sieci TOR, jak i zwiększenia poziomu anonimowości użytkowników sieci Bulwark działających wyłącznie w trybie TOR. Wyjątkową cechą węzła Masternode pracującego w trybie TOR jest możliwość pracy jako usługa ukryta (ang „hidden service") sieci TOR. Węzły TOR umożliwiają użytkownikom dysponującym stabilnym połączeniem z Internetem posiadanie węzła Masternode we własnej sieci domowej bez możliwych implikacji polegających na utracie prywatności na skutek ujawnienia geograficznej lokalizacji tej sieci, czy też niebezpieczeństw wystawienia tej sieci na potencjalne ataki z zewnątrz lub próby przechwycenia jej zasobów.

6.6 Rola społeczności i system zarządzania

Społeczność zgromadzona wokół Bulwark jest najważniejszym czynnikiem stojącym za długoterminowym sukcesem projektu. Jej zdolności do istotnego wpływu na przyszłość kryptowaluty Bulwark są dla nas najistotniejsze. Pod koniec fazy PoW zamierzamy aktywować w sieci tzw. „superbloki budżetowe" (ang. „budget superblocks"). Te superbloki, płatne comiesięcznie, dadzą członkom społeczności znaczącą kontrolę nad wszystkimi aspektami rozwoju projektu Bulwark, jego marką, a także sprawami związanymi z samą społecznością. Opóźniając uruchomienie tego systemu, dajemy sobie czas, aby rozwinąć infrastrukturę niezbędną do zapewnienia prawidłowego działania tego mechanizmu, jak również do zmaksymalizowania nagrody blok dostępnej dla górników i operatorów węzłów Masternode.

Zastosujemy wielofazowy proces kreowania i wdrażania propozycji zmian. Przed przystąpieniem do każdego kolejnego etapu poprzedni będzie musiał być całkowicie zaimplementowany. Niepowodzenie przy realizacji zaplanowanych etapów będzie prawdopodobnie skutkować brakiem aktywacji danej propozycji. Poniżej prezentujemy uproszczony zarys owych etapów:

- Zacznij na naszym czacie Discord. Porozmawiaj z kilkoma doświadczonymi użytkownikami. Oceń zainteresowanie i, jeśli odzew jest pozytywny, przejdź do następnego etapu.
- Skorzystaj z kilku różnych platform mediów społecznościowych, aby nawiązać dyskusje i uzyskać jakiś odzew. Pamiętaj, że projekt Bulwark ma zróżnicowaną bazę użytkowników, a różni użytkownicy w różnym stopniu są zaangażowani w sprawy zarządzania. Dotarcie do części użytkowników będzie wymagało podjęcia pewnych kroków. Zapamiętaj te dyskusję i umiej je później zacytować w formalnej wstępnej propozycji zmian. Im więcej cytatów z wypowiedzi innych użytkowników dostarczysz, tym lepiej.
- Bądź otwarty na sugestie od społeczności i deweloperów. Bądź też elastyczny i gotowy do włączenia dodatkowych pomysłów i sugestii do swojej propozycji.
- Stwórz formalną propozycję wstępną w sekcji Governance > Pre-Proposal naszej strony WWW. Dołącz do niej cytaty ze wszystkich dyskusji, w jakich uczestniczyłeś, zgromadzone w poprzednich krokach. Traktuj swoją propozycję tak, jakby miała być kwestią włączoną do łańcucha blockchain w celu głosowania.
- Po zakończeniu tych kroków przedłożysz swoją propozycję do łańcucha blockchain. Bądź przygotowany na dwie opłaty — jedną w momencie zgłaszania propozycji i drugą jako opłatę za głosowanie przyznawaną deweloperowi, który włączy twoją propozycję do łańcucha blockchain. Opłata za zgłoszenie nie jest refundowana, natomiast opłata za głosowanie zostanie pobrana wyłącznie w przypadku zaaprobowania i aktywowania zaproponowanych przez ciebie zmian.
- Każdy użytkownik ma możliwość dostosowania swojej propozycji w taki sposób, aby uwzględniono w niej zwrot kosztów obu wymienionych powyżej opłat. Upewnij się, że zaznaczyłeś w swojej propozycji żądanie zwrotu poniesionych kosztów.
- Upewnij się, że pozostaniesz w kontakcie ze wszystkimi osobami, z którymi rozmawiałeś, tak aby twój pomysł mógł zostać poddany pod głosowanie. Aby twoja propozycja mogła zostać opłacona, 10% spośród spełniających warunki operatorów węzłów Masternode musi zagłosować na „Tak". Proces uzyskiwania tych 10% zwolenników może być jednak znacznie trudniejszy, niż się to wydaje, więc bądź

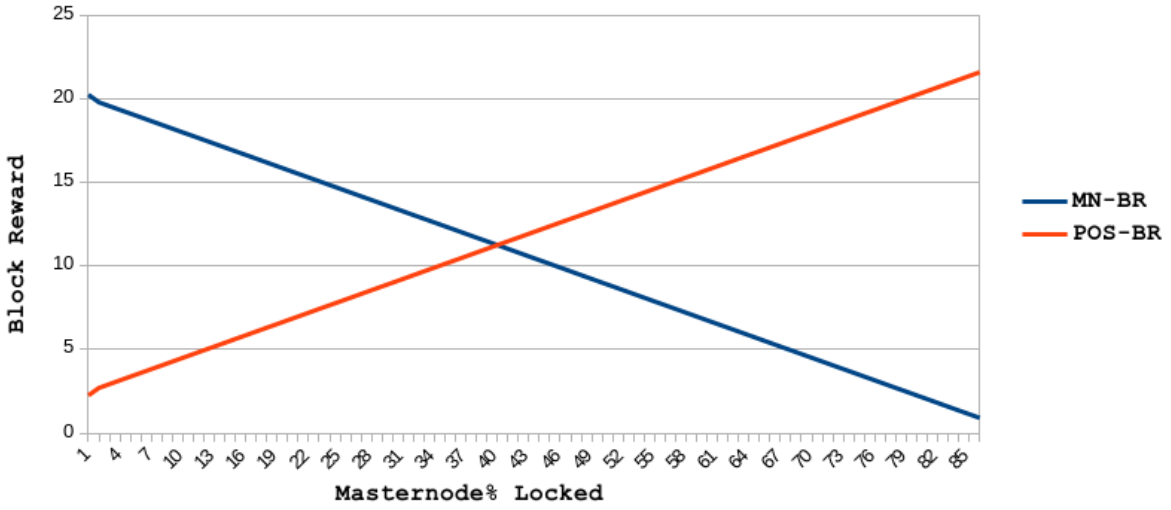
pracowity, komunikatywny i odnoś się do innych z szacunkiem podczas poszukiwania wspierających głosów wymaganych do opłacenia propozycji.

6.7 Mechanizm SeeSaw zmiany nagrody dla PoS/Masternode

Zdecydowaliśmy się na użycie mechanizmu zmiany nagrody o nazwie „SeeSaw" spopularyzowanego przez kryptowalutę PIVX (Jakiman 2017). System zmiany nagrody SeeSaw zaczyna działać przy współczynniku nagrody za blok wynoszącym 9:1 (na korzyść węzłów Masternode), po czym płynnie zmienia ten współczynnik między nagrodą za tzw. „staking" (w algorytmie PoS) a operatorami węzłów, do momentu aż około 41,5% monet w obiegu nie zostanie zablokowanych w węzłach Masternode. W tym momencie nagroda za staking osiąga niewielką przewagę nad nagrodą dla węzłów Masternode, jeśli porównać je na bazie posiadanej liczby monet. Powodem, dla którego ustawiliśmy algorytm SeeSaw na nieznaczne faworyzowanie nagrody za staking, jest chęć uniknięcia problemów takich jak znaczne wahania ceny i niewielka płynność. Problemy tego typu są spotykane w kryptowalutach, w których bardzo duży procent monet będących w obiegu jest zablokowany w węzłach. Strategia taka zmniejszy frustracje użytkowników związane z podażą monet i utrzyma znaczenie naszej odpornej sieci. Jako że jednym z naszych celów jest bycie dobrze wspieraną platformą dla anonimowego handlu, łatwość i szybkość przeprowadzania transakcji są najważniejsze zarówno dla podmiotów akceptujących Bulwark, jak i tych przechowujących monetę.

Fig 3. SeeSaw @ Height 345601 - 432000

(after budget percentage)



Rozdział 7

Przyszłość

7.1 Bulwark Tool Chest

„Bulwark Tool Chest" (w wolnym tłumaczeniu „skrzynka narzędziowa Bulwark") to zbiór fragmentów kodu, interfejsów API, bibliotek, skryptów i innego rodzaju wiedzy, które będą służyć budowaniu środowiska w stylu „bazaru", na którym deweloperzy szukający wsparcia przy dodawaniu obsługi kryptowalut do swoich projektów będą mieli swobodę wymiany wiedzy, informacji i kodu. Wierzymy, że zapewnienie developerom tych narzędzi będzie przypominać zapewnienie narzędzi rzemieślnikowi, tak aby mógł stworzyć ekscytujący, mistrzowski projekt.

7.2 Prywatność i rozszerzenia oprogramowania

Zobowiązujemy się do wdrażania nowych protokołów, które zwiększą poziom prywatności naszych użytkowników. Istnieje kilka ścieżek, które obecnie badamy i oceniamy. Planujemy rozpocząć wewnętrzne testy tych różnych rozwiązań w pierwszej połowie 2018 r. Poniżej prezentujemy listę tylko niektórych spośród tych usprawnień:

- Sieć prywatna I2P
- Protokół Zerocoin lub adresowanie Stealth (kiedy będziemy mieć pewność co do dojrzałości tych rozwiązań)
- Bliższa synchronizacja naszego kodu z główną linią rozwojową bitcoina
- Usprawnianie działania/aktualizowanie portfela QT
- Zintegrowanie biblioteki Libtox
- Wirtualizacja/konteneryzacja portfela Bulwark w celu dodania dodatkowej warstwy bezpieczeństwa

7.3 Bezpieczny węzeł domowy Bulwark

Będziemy współpracować ze specjalistami CAD w celu zaprojektowania niewielkiego, autonomicznego domowego węzła sieci Bulwark. Użytkownicy będą mieli możliwość podłączenia go do swoich sieci domowych i skonfigurować za pośrednictwem interfejsu webowego. Zamierzamy zaimplementować w nim następujące funkcje:

- Dla użytkowników dysponujących stabilnym połączeniem z Internetem — łatwy do skonfigurowania i w pełni zintegrowany z siecią TOR węzeł Masternode (lub pełny węzeł) działający jako usługa ukryta sieci TOR.

- Opcjonalna możliwość działania jako tzw. „przekaźnik TOR" (ang. „TOR relay") w celu usprawnienia ogólnego działania sieci TOR.
- Serwer VPN i/lub proxy, który może być używane do przekierowywania ruchu internetowego w sieci domowej przez sieć TOR/I2P.
- Staking monet Bulwark za pośrednictwem wirtualizacji lub dodatkowego urządzenia.

Trzymając się ducha decentralizacji, pliki do druku na drukarkach 3D oraz pełny kod źródłowy będą dostępne dla społeczności w celu umożliwienia samodzielnego montażu.

7.4 Poszerzanie marki

Będziemy kontynuować wysiłki, aby poszerzać naszą markę i zamierzamy współpracować z dostawcami sprzętu oraz integratorami systemów, którzy dzielą z nami nasze ideały i naszą pasję. Chcemy, aby w ciągu pięciu lat nazwa „Bulwark" stała się synonimem nie tylko kryptowaluty, ale prywatności, bezpieczeństwa i poszanowania wolności użytkowników. Głównym celem projektu Bulwark jest zapewnienie wolności wyboru poprzez ochronę prywatności.

7.5 Aspekty designerskie i wizualne

Poprzez odpowiednie badania i rozwój pragniemy wykreować dla projektu Bulwark własny język wizualny, który będzie wyróżniał ten projekt spośród konkurencji. Nasz zespół designerów planuje wprowadzać innowacje i eksperymentować z bieżącym interfejsem oraz brandingiem, aby ostatecznie osiągnąć doskonały design i wypracować taki styl medialny, który zapewni najlepsze wrażenia użytkownikom oraz innowacyjną i piękną estetykę. Osiągniemy to, analizując produkty konkurencji, śledząc najważniejsze nowoczesne trendy i standardy technologiczne oraz nieprzerwanie dążąc do wnoszenia nowych i ekscytujących elementów wizualnych.

Rozdział 8

Wnioski

8.1 Podsumowanie

Bulwark jest kryptowalutą zorientowaną na prywatność, stosującą węzły Masternode, zarządzaną przez społeczność i oferującą ewoluujący ekosystem narzędzi. Projekt ten rozpoczął się od uczciwego startu i skupienia się na szerokiej dystrybucji monet. Powolny start, rozdzielenie nagród za blok oraz algorytm haszujący zostały celowo wybrane tak, aby stworzyć możliwość znacznego udziału społeczności w projekcie. Bulwark rozpoczął swoje istnienie, posiadając już wiele ważnych funkcji kryptowaluty zapewniającej użytkownikom prywatność. Zespół deweloperów obecnie ciężko pracuje, aby wprowadzić nowe funkcje i tworzyć kolejne rozwiązania na bazie istniejących technologii. Bulwark ma na celu kierunku umożliwienie ludziom wyboru, na co pozwala jego skupienie się na ochronie prywatności. Deweloperzy dołożą wszelkich starań, aby ją należycie zapewniać i wzmacniać wraz z rozwojem technologii.

8.2 Perspektywy na przyszłość

Środowisko nastawionych na prywatność kryptowalut opartych na węzłach Masternode został ostatnio zalany przez waluty kuszące nowych użytkowników obietnicami znaczących zwrotów z inwestycji, gigantycznymi „mapami drogowymi", nieprawdopodobnymi planami i generalnie skupiającymi się na marketingu, zamiast na rzeczywistym udoskonalaniu swoich systemów. Plany dla Bulwark stoją w opozycji do takich projektów. Nie zależy nam na „hype'ie", ale na faktycznym tworzeniu czegoś nowego. Obecne i przyszłe cele projektu będą podążać zgodnie z naszą dewizą bycia precyzyjnym, mierzalnym, dostępnym, istotnym i określonym czasowo.

Bibliografia

Aumasson, L.M., Jean-Phillipe Henzen, 2013. SHA-3 proposal: BLAKE. Pozycja dostępna pod adresem: https://131002. net/blake/blake.pdf.

Bertoni, G., Daemen, J., Peeters, M. & Van Assche, G., 2012. The Keccak SHA-3 submission. Pozycja dostępna pod adresem: https://keccak.team/files/Keccak-submission-3.pdf.

Bitcoin Core Team, T., 2017. Bitcoin developer reference. Pozycja dostępna pod adresem: https://bitcoin.org/en/ developer-reference#block-headers.

Chang, S.-J., Perlner, R., Burr, W.E., Turan, M.S. i inni, 2012. Third-round report of the SHA-3 cryptographic hash algorithm competition. Pozycja dostępna pod adresem: http://nvlpubs.nist.gov/nistpubs/ir/2012/ NIST.IR.7896.pdf.

Crosby, M., Nachiappan, Pattanayak, P., Verma, S. i inni, 2015. BlockChain technology. Pozycja dostępna pod adresem: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

Ferguson, N.L., Schneier, S., Whiting, B., Bellare, D. i inni, 2010. The Skein hash function family. Pozycja dostępna pod adresem: http://www.skein-hash.info/sites/default/files/skein1.3.pdf.

Gauravaram1, P., Knudsen, L.R., Matusiewicz, K., Mendel, F. i inni, 2012. Grøstl – a SHA-3 candidate. Pozycja dostępna pod adresem: http://www.groestl.info/Groestl.pdf.

Jakiman, 2017. PIVX purple paper. Pozycja dostępna pod adresem: https://pivx.org/wp-content/uploads/2017/03/ PIVX-purple-paper-Technincal-Notes.pdf.

Kiraly, B., 2017a. InstantSend. Pozycja dostępna pod adresem: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146928/InstantSend.

Kiraly, B., 2017b. PrivateSend. Pozycja dostępna pod adresem: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/ 1146924/PrivateSend.

Nakamoto, S., 2009. Bitcoin: A peer-to-peer electronic cash system. Pozycja dostępna pod adresem: https://bitcoin.org/ bitcoin.pdf.

Okupski, K., 2016. Bitcoin developer reference., strony 3–4. Pozycja dostępna pod adresem: https://lopp.net/pdf/Bitcoin_ Developer_Reference.pdf.

strophy, 2017. Understanding sporks. Pozycja dostępna pod adresem: https://dashpay.atlassian.net/wiki/spaces/DOC/pages/128319489/Understanding+Sporks.

Wiecko, R., 2017. Dash instamine issue clarification. Pozycja dostępna pod adresem: https://dashpay.atlassian.net/wiki/ spaces/OC/pages/19759164/Dash+Instamine+Issue+Clarification.

Wu, H., 2012. The hash function JH. Pozycja dostępna pod adresem: http://www3.ntu.edu.sg/home/wuhj/research/jh/ jh_round3.pdf.