BulenCoin ? projekt sieci i aplikacji w?z?a

1. Cel projektu

BulenCoin jest memcoinem z powa?nym celem technicznym: pokazaniem, ?e dzia?aj?ca sie? kryptowalutowa mo?e by? utrzymywana przez mo?liwie najszersze spektrum sprz?tu, od telefonów i tabletów, przez laptopy i komputery stacjonarne, a? po serwery. Sie? ma by? na tyle lekka, aby mog?a dzia?a? w tle na typowym urz?dzeniu u?ytkownika, a jednocze?nie na tyle op?acalna, ?eby u?ytkownik mia? realn? motywacj?, by utrzymywa? w?ze? online przez wi?kszo?? czasu.

Projekt opisuje architektur? logiczn? sieci BulenCoin, typy w?z?ów, wymagania sprz?towe, model nagradzania za utrzymanie w?z?a, aplikacje dla ró?nych platform oraz pe?ny proces uruchomienia i konfiguracji w?z?a.

2. Ogólny model sieci

Sie? BulenCoin zak?ada istnienie w?asnego ?a?cucha bloków lub warstwy konsensusu, w której wszystkie urz?dzenia mog? uczestniczy? jako w?z?y. Ze wzgl?du na ograniczenia mocy obliczeniowej i baterii na urz?dzeniach mobilnych, sie? nie mo?e opiera? si? na kosztownym Proof of Work. Zamiast tego wykorzystywany jest lekki mechanizm Proof of Stake z losowanymi komitetami walidatorów, który pozwala na udzia? nawet stosunkowo s?abych urz?dze?.

Warstwa logiczna sieci sk?ada si? z kilku g?ównych elementów. Po pierwsze jest to warstwa sieciowa peer to peer odpowiedzialna za wymian? bloków i transakcji. Po drugie warstwa konsensusu, która wybiera, które w?z?y tworz? blok w danym czasie i weryfikuje poprawno?? bloków. Po trzecie warstwa danych zawieraj?ca struktur? bloków, transakcji i stanu kont.
Po czwarte warstwa motywacyjna obejmuj?ca system nagród za utrzymanie w?z?a.

Sie? ma by? dost?pna zarówno z lekkich w?z?ów mobilnych, jak i z pe?nych w?z?ów desktopowych i serwerowych. Aby to osi?gn?? definiuje si? wyra?nie ró?ne role w?z?ów.

3. Typy w?z?ów w sieci BulenCoin

3.1. W?ze? mobilny light

W?ze? mobilny light to aplikacja uruchamiana na telefonie lub tablecie. Nie przechowuje on pe?nej historii ?a?cucha, a jedynie nag?ówki bloków oraz niewielk? cz??? ostatniego stanu potrzebn? do weryfikacji w?asnych transakcji i uczestnictwa w konsensusie. W?ze? mobilny:

? utrzymuje po??czenie z kilkoma w?z?ami pe?nymi, z których pobiera nag?ówki bloków i dowody kryptograficzne potwierdzaj?ce stan,
? uczestniczy w rozproszonym monitorowaniu sieci, potwierdzaj?c dost?pno?? bloków generowanych przez pe?ne w?z?y,
? mo?e by? losowo wybierany do ma?ych komitetów, które zatwierdzaj? bloki poprzez podpisy cyfrowe, je?li u?ytkownik zdeponowa? odpowiedni? ilo?? BulenCoinów jako stake,
? ma wbudowane mechanizmy kontroli zu?ycia baterii i danych, takie jak ograniczanie pracy do godzin nocnych, pauzowanie przy niskim poziomie baterii czy limit transferu w sieci

komórkowej.

3.2. W?ze? desktopowy i serwerowy pe?ny

W?ze? pe?ny uruchamiany jest na komputerach stacjonarnych, laptopach lub serwerach. Jest on odpowiedzialny za utrzymywanie pe?nej kopii ?a?cucha bloków, weryfikacj? wszystkich transakcji i bloków oraz udost?pnianie danych w?z?om light. W?ze? pe?ny:

? przechowuje pe?n? histori? bloków i stan kont,
? utrzymuje rozbudowan? tabel? peerów i bierze udzia? w propagacji nowych bloków i transakcji,
? bierze udzia? w konsensusie jako potencjalny producent bloków, je?li w?a?ciciel zdeponowa? stake,
? obs?uguje lekkich klientów, przygotowuj?c dla nich dowody stanu i reaguj?c na ich zapytania,
? mo?e by? skonfigurowany jako w?ze? bramkowy, udost?pniaj?cy interfejs HTTP lub WebSocket dla aplikacji webowych.

3.3. W?ze? bramkowy

W?ze? bramkowy to logiczna rola pe?nego w?z?a, która udost?pnia interfejsy API dla aplikacji zewn?trznych. W?ze? bramkowy:

? udost?pnia publiczne API do wysy?ania transakcji, odczytu stanu kont, pobierania historii,
? mo?e pe?ni? rol? punktu wej?cia dla u?ytkowników, którzy nie chc? uruchamia? w?asnego w?z?a, ale chc? korzysta? z BulenCoin jako zwyk?ego u?ytkownika,
? mo?e by? u?ywany przez gie?dy, us?ugi p?atnicze oraz integracje z innymi systemami.

3.4. W?ze? ultra lekki tylko portfelowy

Na niektórych urz?dzeniach u?ytkownicy mog? chcie? korzysta? tylko z portfela bez udzia?u w utrzymywaniu sieci. Aplikacja portfelowa korzysta wtedy z API w?z?ów bramkowych lub z funkcji light client w trybie tylko do odczytu. Nie uczestniczy w konsensusie ani dystrybucji nagród.

4. Protokó? konsensusu i motywacja

4.1. Za?o?enia dla konsensusu

Konsensus BulenCoin musi spe?nia? kilka kluczowych wymaga?. Po pierwsze ma by? lekki obliczeniowo, aby nadawa? si? dla urz?dze? mobilnych. Po drugie ma premiowa? ró?norodno?? sprz?tu, tak aby w sieci obecne by?y zarówno telefony, jak i komputery. Po trzecie ma oferowa? przewidywalne nagrody za utrzymywanie w?z?a online.

Wybrany jest model Proof of Stake z losowanymi komitetami. U?ytkownicy deponuj? BulenCoiny jako stake, aby ich w?z?y mog?y bra? udzia? w produkcji bloków i g?osowaniu. W ka?dym kroku czasu wybierany jest producent bloku oraz niewielki komitet w?z?ów, które musz? blok podpisa?, aby by? on uznany za finalny. Proces wyboru opiera si? o deterministyczn? funkcj? losuj?c? z nasionem opartym na poprzednich blokach oraz kluczach uczestników.

4.2. Wp?yw typu urz?dzenia na selekcj?

Aby zach?ci? do udzia?u r??nych klas urz?dze?, sie? mo?e uwzgl?dnia? typ urz?dzenia jako parametr w algorytmie selekcji komitetu. Urz?dzenia mobilne, tablety, komputery i serwery deklaruj? sw?j typ podczas rejestracji w?z?a, a sie? nadaje im wspó?czynniki korekcyjne. Przyk?adowo, je?li w sieci jest bardzo ma?o w?z??w mobilnych, ich wspó?czynnik mo?e by? nieco wy?szy, aby zwi?kszy? szans? udzia?u w komitecie.

Typ urz?dzenia nie mo?e by? jednak jedynym kryterium, ?eby nie by?o zach?ty do fa?szywych deklaracji. Dlatego selekcja uwzgl?dnia tak?e ilo?? zdeponowanego stake, histori? uptime w?z?a i reputacj?. Reputacja to zagregowany wska?nik oceniany na podstawie tego, czy w?ze? poprawnie g?osowa?, nie próbowa? podwójnego podpisu i nie zachowywa? si? podejrzanie.

4.3. Model nagród dla w?z??w

Model nagradzania sk?ada si? z kilku sk?adników. Podstaw? jest nagroda blokowa przydzielana producentowi bloku oraz cz?onkom komitetu, którzy podpisali blok. Dodatkowo istnieje nagroda za utrzymywanie w?z?a online, obliczana na podstawie okien czasowych. W ka?dym oknie czasowym sie? losowo wybiera próbk? w?z??w i sprawdza, czy odpowiadaj? na proste zapytania health check. W?z?y, które konsekwentnie odpowiadaj?, otrzymuj? cz??? nagrody za uptime.

Nagrody za uptime s? proporcjonalne do stake, ale skorygowane wspó?czynnikiem zale?nym od typu urz?dzenia. Dzi?ki temu urz?dzenia o ograniczonej mocy, które nie s? cz?sto wybierane do roli producenta bloków, nadal mog? zarabia? sensowne kwoty, po prostu b?d?c online i pomagaj?c w utrzymaniu sieci. Mechanizm slashing karze w?z?y, które podpisuj? sprzeczne bloki lub próbuj? ataków na konsensus, poprzez utrat? cz??ci stake.

5. Architektura aplikacji BulenNode

5.1. Modu?y aplikacji

Aplikacja BulenNode, niezale?nie od platformy, sk?ada si? z kilku g?ównych modu??w. Modu? komunikacji sieciowej odpowiada za po??czenia peer to peer, wymian? bloków i transakcji oraz wykrywanie nowych peerów. Modu? konsensusu realizuje logik? Proof of Stake, w tym selekcj? bloków, g?osowanie i weryfikacj? podpisów. Modu? przechowywania danych zarz?dza lokaln? baz? danych bloków, stanu i indeksów. Modu? portfela obs?uguje klucze prywatne, podpisywanie transakcji oraz interfejs u?ytkownika do zarz?dzania ?rodkami. Modu? monitoringu i zarz?dzania zasobami nadzoruje zu?ycie CPU, pami?ci, transferu danych i baterii.

Dla r??nych platform modu?y maj? r??ne implementacje, ale interfejsy pozostaj? spójne. Dzi?ki temu ta sama logika sieciowa i konsensusu mo?e by? u?ywana na Androidzie, iOS, Windows, Linux i macOS, a platformowo specyficzne s? jedynie detale zwi?zane z integracj? z systemem operacyjnym.

5.2. Aplikacja mobilna

Aplikacja mobilna BulenNode udost?pnia dwa tryby: tryb pe?nego w?z?a light oraz tryb

wy??cznie portfelowy. W trybie light aplikacja utrzymuje po??czenia P2P w tle, okresowo pobiera nowe nag?ówki bloków i dowody stanu oraz bierze udzia? w konsensusie i pomiarach uptime. U?ytkownik mo?e w ustawieniach okre?li?, w jakich godzinach w?ze? mo?e pracowa?, czy ma dzia?a? tylko po pod??czeniu do ?adowarki i czy mo?e korzysta? z danych komórkowych.

Ze wzgl?du na ograniczenia systemu iOS w pracy w tle, iOS b?dzie typowo wspiera? s?abszy wariant, w którym aplikacja mo?e okresowo wybudza? si?, synchronizowa? nag?ówki i uczestniczy? w uproszczonych pomiarach uptime, a intensywniejsza praca mo?liwa b?dzie w czasie, gdy aplikacja jest otwarta. Na Androidzie mo?liwe jest utrzymywanie trwa?ego procesu w tle z powiadomieniem systemowym informuj?cym u?ytkownika, ?e w?ze? pracuje.

5.3. Aplikacja desktopowa

Aplikacja desktopowa dla Windows, Linux i macOS mo?e dzia?a? jako pe?en w?ze? z pe?n? histori? bloków lub w trybie w?z?a cz??ciowego, przechowuj?cego tylko ostatni? histori? i cz??? stanu. U?ytkownik mo?e w prostym interfejsie graficznym skonfigurowa? ?cie?k? danych, limity zu?ycia dysku oraz porty sieciowe. Aplikacja mo?e równie? dzia?a? bez interfejsu graficznego, jako us?uga systemowa z konfiguracj? w pliku.

Na komputerach stacjonarnych i serwerach uruchamiane b?d? g?ównie w?z?y pe?ne i bramkowe. W?z?y te b?d? równie? cz?sto wykorzystywane jako punkty wej?cia dla w?z?ów mobilnych, zapewniaj?c im szybki dost?p do nag?ówków bloków i dowodów stanu.

5.4. Panel u?ytkownika

Zarówno na urz?dzeniach mobilnych, jak i desktopowych, aplikacja BulenNode oferuje panel u?ytkownika, który prezentuje aktualny stan w?z?a i przychody. U?ytkownik widzi takie dane jak aktualna wysoko?? bloku, liczba po??czonych peerów, przewidywane zu?ycie danych, aktualny stake i ocen? reputacji. Istnieje tak?e prosty wykres nagród otrzymanych w ostatnich dniach, aby u?ytkownik mógª oceni?, czy utrzymywanie w?z?a jest dla niego op?acalne.

6. Wymagania techniczne dla w?z?ów

6.1. Minimalne wymagania sprz?towe

Dla w?z?a mobilnego minimalne wymagania to typowy smartfon z ostatnich 5 lat z co najmniej 3 gigabajtami pami?ci RAM i kilkuset megabajtami wolnego miejsca na dane. Aplikacja nie powinna u?ywa? wi?cej ni? kilku procent CPU w typowych warunkach oraz musi agresywnie ogranicza? zu?ycie baterii poprzez wykorzystanie mechanizmów usypiania i pracy w oknach czasowych.

Dla w?z?a desktopowego minimalne wymagania to komputer z co najmniej 4 gigabajtami RAM, kilkoma gigabajtami wolnego miejsca na dysku oraz sta?ym po??czeniem internetowym. W przypadku konfiguracji serwerowej zalecane jest wykorzystanie dodatkowego dysku na dane ?a?cucha. Dla pe?nego w?z?a przewidywane jest stopniowe zwi?kszanie rozmiaru ?a?cucha, dlatego projekt zak?ada mo?liwo?? przycinania historii i pozostawiania kluczowych punktów kontrolnych, aby ograniczy? zu?ycie dysku.

6.2. Wymagania sieciowe

Sie? BulenCoin wymaga sta?ego dost?pu do internetu dla w?z?ów, które chc? otrzymywa? nagrody za uptime. W?ze? mobilny mo?e dzia?a? na WiFi lub sieci komórkowej, ale u?ytkownik mo?e ograniczy? korzystanie z danych mobilnych. W?z?y desktopowe i serwerowe powinny mie? publiczne lub przekierowane porty, aby mog?y dzia?a? jako pe?noprawne peer to peer nodes, jednak dla u?ytkowników domowych przewidziano mechanizmy przechodzenia przez NAT, takie jak hole punching.

7. Model ekonomiczny w?z?ów

7.1. Sk?adniki przychodów w?z?a

Przychód w?z?a sk?ada si? z nagród blokowych, udzia?u w op?atach transakcyjnych oraz nagród za uptime. W fazie wczesnego rozruchu sie? mo?e mie? wy?sz? nagrod? bazow?, aby silniej wynagradza? pionierów, za? pó?niej nagroda bazowa maleje, a wi?kszy udzia? w nagrodach maj? op?aty z realnego wykorzystania sieci. Celem jest doprowadzenie do sytuacji, w której utrzymywanie w?z?a jest op?acalne pod warunkiem, ?e sie? faktycznie jest u?ywana przez u?ytkowników ko?cowych do przesy?ania warto?ci.

Nagroda za uptime jest rozdzielana na podstawie prób losowych z ca?ego zbioru w?z?ów. Im d?u?ej i stabilniej w?ze? jest online, tym wy?sza jego udzia?owa stawka w puli uptime. U?ytkownik ma w aplikacji prosty kalkulator, który oszacowuje spodziewany przychód na podstawie bie??cych parametrów sieci i jego stake, ale jest wyra?nie informacje, ?e nie jest to gwarancja zysku.

7.2. Koszty po stronie u?ytkownika

Kosztem u?ytkownika jest zu?ycie pr?du, transfer danych i ewentualne zu?ycie sprz?tu oraz ryzyko utraty cz??ci stake w przypadku z?ego zachowania lub b??dnej konfiguracji w?z?a. Aplikacja BulenNode powinna pomaga? u?ytkownikowi zrozumie? te koszty, prezentuj?c szacunkowe zu?ycie energii (na podstawie statystyk systemu operacyjnego), dane o transferze oraz ostrze?enia o ryzyku. W?z?y mobilne domy?lnie dzia?aj? w trybie konserwatywnym, dopóki u?ytkownik nie prze??czy ich w tryb bardziej agresywny.

8. Proces setupu sieci i w?z?ów

8.1. Faza testnet

Pierwszym etapem uruchomienia BulenCoin jest sie? testowa. W testnecie dzia?aj? w?z?y referencyjne utrzymywane przez zespó?, a u?ytkownicy mog? instalowa? aplikacje BulenNode i testowa? utrzymywanie w?z?a bez realnej warto?ci ekonomicznej. Testnet pozwala na sprawdzenie zachowania sieci na ró?nych typach sprz?tu, dopracowanie parametrów konsensusu i modelu nagród oraz wykrycie problemów z wydajno?ci? i stabilno?ci?.

W fazie testnet zbierane s? równie? anonimowe statystyki dotycz?ce rozk?adu urz?dze?, ich uptime i typowych konfiguracji. Dane te s?u?? do skalibrowania wspó?czynników dla ró?nych klas sprz?tu, tak aby rzeczywi?cie zach?ca? do udzia?u urz?dze? mobilnych i domowych komputerów, a jednocze?nie nie tworzy? luk dla ataków.

8.2. Faza mainnet bootstrap

Po zako?czeniu testnetu uruchamiana jest sie? g?ówna. W fazie bootstrap g?ównymi producentami bloków s? w?z?y pe?ne zarz?dzane przez zespó? i spo?eczno??, które posiadaj? znacz?cy stake i stabilne po??czenie z internetem. W tym czasie rozwijana jest sie? w?z?ów mobilnych i desktopowych u?ytkowników, którzy do??czaj? do programu nagród za uptime.

Instrukcja setupu w?z?a mobilnego obejmuje pobranie aplikacji ze sklepu lub z oficjalnej strony, wygenerowanie portfela, wykonanie kopii zapasowej seed phrase oraz w??czenie trybu w?z?a. Aplikacja przeprowadza u?ytkownika przez konfiguracj? zasobów i w razie potrzeby umo?liwia delegowanie stake do sprawdzonych walidatorów, je?li u?ytkownik nie chce samodzielnie by? walidatorem.

Instrukcja setupu w?z?a desktopowego obejmuje pobranie instalatora lub paczki binarnej, konfiguracj? ?cie?ki danych, portów sieciowych i podstawowych parametrów. U?ytkownik wybiera tryb pracy, pe?ny lub cz??ciowy, oraz decyduje, czy w?ze? ma pe?ni? rol? bramki API. W fazie bootstrap dost?pne s? równie? prekonfigurowane pliki konfiguracyjne i skrypty do uruchamiania w?z?ów na serwerach w chmurze.

8.3. Faza pe?nej decentralizacji

Po ustabilizowaniu si? sieci planuje si? stopniowe zmniejszanie udzia?u w?z?ów referencyjnych w konsensusie. Parametry protoko?u s?u??ce do ustalania, jaki procent bloków mo?e by? produkowany przez w?z?y kontrolowane przez zespó?, s? z czasem redukowane a? do poziomu marginalnego. W tym samym czasie ro?nie udzia? w?z?ów spo?eczno?ci, które posiadaj? stake i histori? poprawnego zachowania.

D?ugoterminowym celem jest osi?gni?cie stanu, w którym BulenCoin jest utrzymywany przez rozproszon? sie? w?z?ów nale??cych do u?ytkowników ko?cowych, a w?z?y zespo?u pe?ni? jedynie funkcje in?ynieryjne, takie jak prowadzenie eksploratora, w?z?ów archiwalnych i dodatkowych narz?dzi.

9. Bezpiecze?stwo sieci i w?z?ów

9.1. Ochrona kluczy prywatnych

Wszystkie w?z?y BulenCoin przechowuj? klucze prywatne u?ytkownika, które umo?liwiaj? podpisywanie transakcji i udzia? w konsensusie. Aplikacje musz? stosowa? odpowiednie mechanizmy ochrony kluczy, takie jak szyfrowanie magazynu kluczy mocnym has?em, integracja z bezpiecznymi modu?ami systemowymi na Androidzie i iOS oraz mo?liwo?? u?ycia zewn?trznego portfela sprz?towego w aplikacjach desktopowych.

Aplikacja powinna jasno informowa? u?ytkownika, ?e utrata seed phrase lub klucza prywatnego oznacza utrat? dost?pu do ?rodków. Powinna te? ostrzega?, ?e udost?pnienie klucza lub seeda komukolwiek stanowi bezpo?rednie zagro?enie dla ?rodków, niezale?nie od tego, kto si? za kim podaje.

9.2. Obrona przed atakami Sybil i DDoS

Poniewa? sie? zak?ada du?? liczb? tanich w?z?ów, jest podatna na ataki Sybil, w których

atakuj?cy uruchamia wiele fa?szywych w?z?ów. Aby temu przeciwdzia?a?, udzia? w konsensusie wymaga stake, a selekcja w?z?ów do komitetu uwzgl?dnia zarówno stake, jak i reputacj?. W?z?y, które s? cz?sto niedost?pne lub zachowuj? si? podejrzanie, otrzymuj? ni?sz? reputacj? i mniejsz? szans? na udzia? w komitetach.

Dodatkowo warstwa sieciowa mo?e stosowa? ograniczenia typu rate limiting, losowanie peerów, filtrowanie ruchu oraz ograniczanie liczby po??cze? z jednego zakresu adresów. W?z?y bramkowe mog? korzysta? z mechanizmów takich jak limity zapyta? i konieczno?? rozwi?zania prostych zada? typu proof of work przy nawi?zywaniu sesji, aby utrudni? zalewanie API z?o?liwymi zapytaniami.

9.3. Aktualizacje protoko?u

Sie? BulenCoin musi by? zdolna do aktualizacji protoko?u bez centralnego wy??czania. Aktualizacje oprogramowania w?z?ów odbywaj? si? przez pobieranie nowych wersji klienta z oficjalnych ?ródeł, a zmiany w protokole wymagaj?ce hard forka s? og?aszane z wyprzedzeniem. Aplikacje w?z?ów zawieraj? mechanizmy ostrzegania u?ytkowników o zbli?aj?cych si? aktualizacjach krytycznych oraz o terminach, po których stara wersja klienta przestanie by? kompatybilna z sieci?.

10. Infrastruktura wspomagaj?ca

Do pe?nego dzia?ania ekosystemu BulenCoin potrzebne s? równie? dodatkowe komponenty poza sam? sieci? peer to peer. Nale?y zaplanowa? eksplorator bloków, który pozwoli u?ytkownikom przegl?da? transakcje i bloki przez przegl?dark?. Potrzebny jest tak?e oficjalny serwis statusu sieci, który pokazuje aktualny stan sieci, informacje o ewentualnych problemach i planowanych pracach serwisowych.

Dodatkowo projekt zak?ada istnienie systemu telemetrycznego, który w sposób anonimowy zbiera statystyki dotycz?ce wydajno?ci sieci, rozk?adu typów urz?dze?, ?redniego uptime oraz ruchu. Wszystkie dane telemetryczne powinny by? od samego pocz?tku projektowane w duchu minimalizacji danych, tak aby nie by?o mo?liwe identyfikowanie pojedynczych u?ytkowników.

11. Podsumowanie

BulenCoin jako memcoin z ambicj? techniczn? ma by? dowodem, ?e nowoczesna sie? kryptowalutowa mo?e opiera? si? na szerokim spektrum sprz?tu, a nie tylko na wyspecjalizowanych serwerach i koparkach. Projekt przewiduje lekkie w?z?y mobilne, pe?ne w?z?y desktopowe i serwerowe, w?z?y bramkowe oraz model ekonomiczny, w którym utrzymywanie w?z?a jest potencjalnie op?acalne, ale jednocze?nie zabezpieczone przed nadu?yciami.

Opisany powy?ej projekt obejmuje architektur? sieci, typy w?z?ów, wymagania sprz?towe, model konsensusu i nagradzania oraz proces setupu i bezpiecze?stwa. Stanowi to punkt wyj?cia do dalszego uszczegó?owienia protoko?u, implementacji referencyjnych klientów oraz zaprojektowania dok?adnych parametrów ekonomicznych sieci BulenCoin.