Перша загальноприйнята криптовалюта з Алгоритмом Гібридного Консенсусу, Динамічний Zerocoin Proof-of-Stake, Proof-of-Transaction та Masternode голосування за спалювання винагороди

Технічна Документація V1.11

Maik Broemme[1], Листопад 2019

Galilel

ЗМІСТ

Galilel

РЕЗЮМЕ

Хоча звичні фіатні гроші вже сотні років визначають і підтверджують економічні стандарти, ситуація з цифровими грошима трохи інша. Цифрові гроші - це інвестиції з високим ризиком, які мають непередбачувану цінність і зникаючі команди розробників, які залишають після себе осиротілий блокчейн. Уряди визначили цю проблему і Початкову Пропозицію Монет (ICO) нормативно-правові акти вирішать в найближчі роки. Більш того, цифрові валюти, які реалізують унікальні функції блокчейн, мають високу ймовірність визначення майбутніх стандартів цифрових грошей. Galilel буде частиною цього процесу, шляхом реалізації унікальних особливостей, викладених у цій роботі.

ВСТУП

Galilel Coin - це крипто-валюта, орієнтована на спільноту, з повною прозорістю та методом публічного розвитку. Довірчі відносини між інвесторами та командою проекту є запорукою успіху. Таким чином, ми створили репозиторій GitHub під назвою *Galilel-Project*[2], який освітлює всі наші розробки публічно, включаючи наш серверний код і пройшли публічну перевірку *Знай Свого Розробника (KYD)*[3]. Проект використовує в основному *MIT*[4], *GPLv3*[5] та *CC-BY-NC 4.0*[6] з відкритим вихідним кодом і ліцензіями на відкритий контент. Переклад і локалізація використовує платформу *Transifex*[7].

GALILEL COIN

Galilel Coin (GALI та zGALI) є відкритою та приватною криптовалютою для швидких (з використанням SwiftX), приватних (*Zerocoin*[8] протокол) та безпечних мікро-транзакцій. Наша головна мета - створити децентралізовану, повністю безпечну та анонімну мережу для запуску додатків, які не покладаються на будь-який

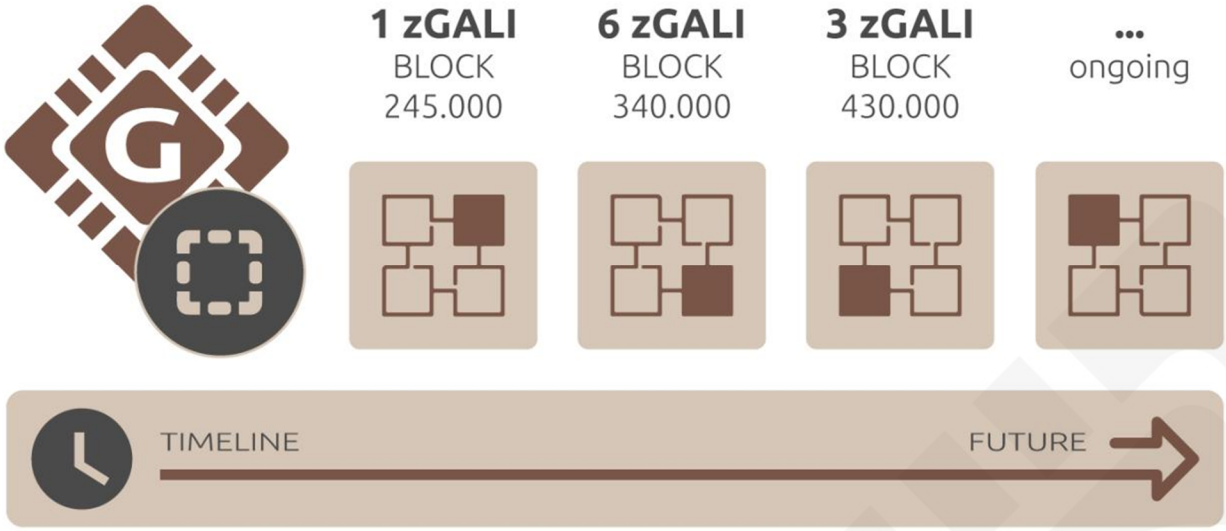
центральний орган управління. Маючи розподілену систему, тисячі користувачів будуть нести відповідальність за підтримку програми та даних, немаючи жодної точки відмови.

ПРОБЛЕМИ ТА РІШЕННЯ

Технологія Blockchain створює величезний інтерес, набуває популярності в усьому світі і використовується багатьма компаніями для різних цілей, крім цифрових грошей. Однак використання її як бази для платіжних послуг вимагає спеціальних функцій для перевірки, зберігання та підтвердження тисяч транзакцій. Хоча це вже вирішено з використанням існуючого алгоритму консенсусу для створення блоків у ланцюжку, в існуючих реалізаціях блокчейн є кілька слабких областей для досягнення основного прийняття її як цифрових грошей.

ДИНАМІЧНИЙ ZEROCOIN PROOF-OF-STAKE (dzPoS)

Zerocoin Proof-of-Stake (zPoS) - найбільш новаторська функція ланцюга блоків, впроваджена в 2018 році командою розробників PIVX. Однак технічна реалізація виконана специфічним чином для їх блокчейна і не дозволяє легко прийняти для інших, оскільки їх структура винагороди статично включена в початковий код.

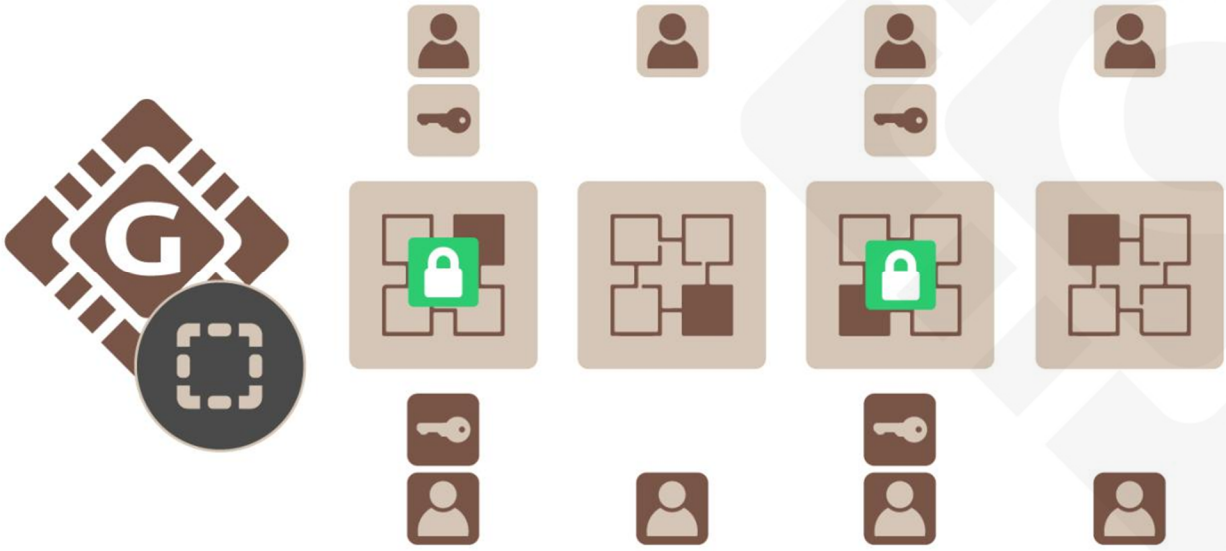


Зображення 1. Динамічний Zerocoin Proof-of-Stake, на основі blockchain фази.

У Galilel, ми реалізуємо динамічну версію ставок Zerocoin. Розклад Zerocoin генерує винагороди в номінаціях, які представляють ціле число. Найменша можлива номінація - один [1]. У першій версії - фазі розігріву - ми завжди використовуємо найменше значення номіналу для цілей тестування. Недолік цього підходу полягає в тому, що ставка Zerocoin дуже ресурсомістка для процесора, і ймовірність генерування сирітського блоку (orphan blocks) вища, оскільки ставка публічної монети може вирішити блок пізніше, але поширити його на ланцюг раніше. У другому варіанті - повна фаза - ми автоматично визначаємо найкращу структуру номіналу на основі суми винагороди за блок. Це істотно знижує ймовірність генерування блоків-сиріт.

PROOF-OF-TRANSACTION (ghPoT)

У традиційній економіці з грошовими переказами між банківськими рахунками, можна вказати умову, щоб одержувач міг присвоїти суму конкретному рахунку. Це не можливо в поточній реалізації гаманця. Вона дозволяє вказувати на коментар або коментар до значення, яке не є частиною транзакції і зберігається лише локально. Щоб призначити рахунок для конкретного одержувача платежу, необхідно створити адресу гаманця з взаємно однозначним відображенням «one-to-one» між обома зацікавленими сторонами.

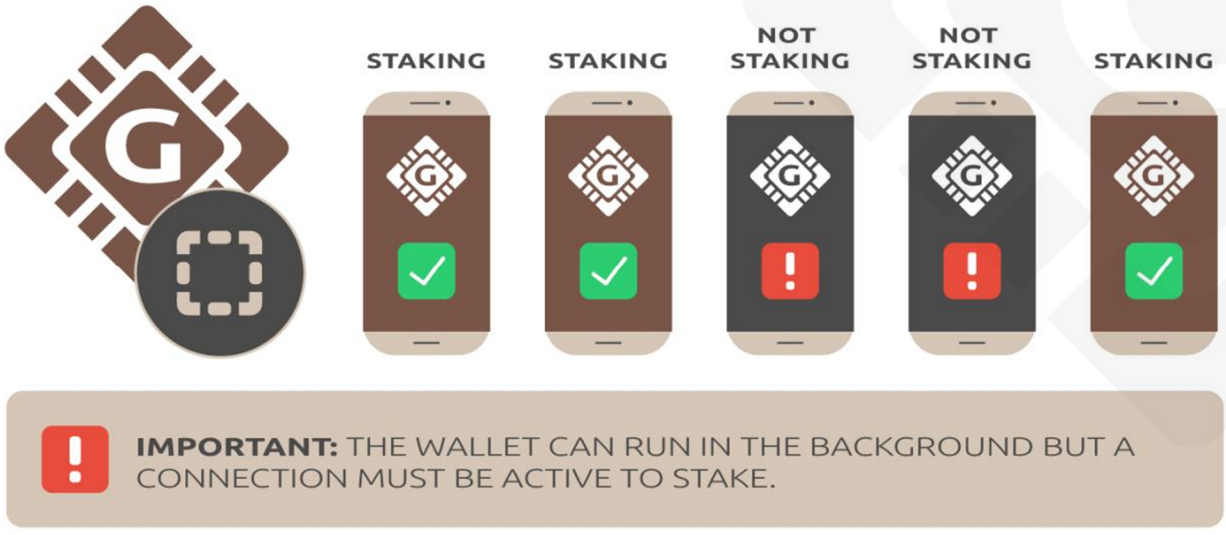


Зображення 2. Proof-of-Transaction з зашифрованим суб'єктом.

У Galilel ми включаємо додаткове поле даних і прикріплюємо його до транзакції, яка зберігається в блоці. Це зашифроване поле і розшифровка можлива тільки за допомогою гаманців, які обговорили транзакцію. Він вирішує проблему призначення транзакцій і дозволяє шлюзам обробки платежів ідентифікувати одержувача платежа, як це відбувається з традиційними рахунками.

ГІБРИДНИЙ PROOF-OF-STAKE (ghPoS)

Хоча Proof-of-Stake (PoS) є екологічно чистим алгоритмом консенсуса, він створює винагороди тільки до тих пір, поки працює гаманець. Одним із шляхів вирішення цієї проблеми є підключення до будь-якого спільного стейк пулу та частки в хмарі. Однак недоліком є те, що користувачеві потрібно довіряти пулу і переносити на нього певну кількість монет. Це може призвести до того, що велика кількість монет зберігається в кількох гаманцях. Це слабка ситуація для децентралізованого мережевого підходу і є фундаментальною частиною для досягнення консенсусу. Приватні ставки, так звані Zerocoin Proof-of-Stake (zPoS), мають ті ж проблеми і обмеження.



Зображення 3. Можливі способи отримання винагород в мережі Galilel.

У Галілелі вирішенням цієї проблеми буде повний гібридний консенсусний алгоритм, названий гібридним доказом Галілеля (ghPoS). Ми будемо розширювати можливості підтвердження ставки за допомогою можливостей мобільного розміщення для публічного та приватного розміщення. Мобільні

ставки завжди включають **десять** [10] відсотків винагороди блоку, що виплачується, якщо мобільний гаманець знаходить блок. У цьому випадку **дев'яносто** [90] відсотків виплачується власнику масової одиниці. Мобільні гаманці працюватимуть як світлий вузол блочного ланцюга з мінімальною кількістю блоків, що дорівнює глибині реорганізації.

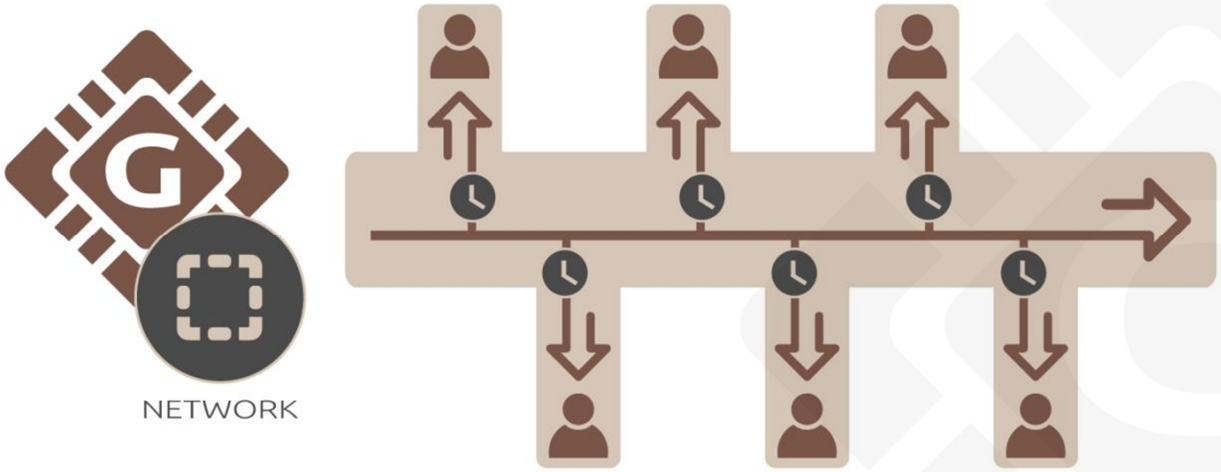
СТРУКТУРА ВИНАГОРОДИ ГІБРИДНОГО PROOF-OF-STAKE

ТИП СТЕЙКІНГУ[1]	СТЕЙК	МАСТЕРНОДА
Онлайн (GALI)	30%	70%
Онлайн (zGALI)	60%	40%
Мобільний (GALI)	10%	90%
Мобільний (zGALI)	20%	80%

[1] Розрахунок базується на винагороді 5 GALI після блоку > 430,000

СТРОКОВІ ДЕПОЗИТИ (gTD)

Хоча мобільний розміщення залежить від складності мережі та кількості закладених монет, функція Строковий депозит *Term Deposit*[9] дозволяє блокувати монети на певний період і створювати передбачувані нагороди.

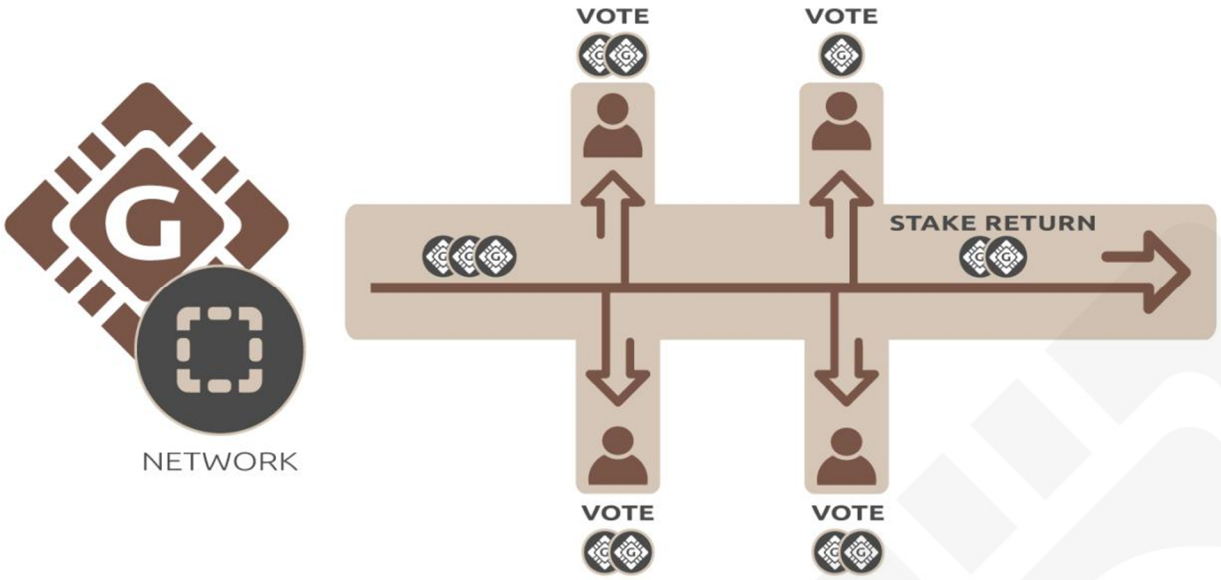


Зображення 4. Календар Строкового депозита в офлайн гаманці.

Мінімальна необхідна кількість монет для використання Galilel Term Deposit (gTD) становить **тисячу** [1000] GALI. Період блокування - **один** [1] рік. Блокова винагорода становить **десять** [10] відсотків, а замкнені монети різних гаманців зважені. З новим блоком в мережі, гаманці з заблокованими монетами отримують суму відповідно до їх ваги. До закінчення строку термінового вкладу ця винагорода блокується. Після блокування, переміщення або витрата монет неможлива, скасування строкового вкладу до закінчення терміну дії неможливе. Це дозволить ефективно зменшити постачання монет протягом періоду блокування.

КОНТРОЛЬ ПОСТАЧАННЯ ГРОШЕЙ (gMSC)

Контроль інфляції є найважливішою частиною для визнання та прийняття цифрових грошей як альтернативи звичним фіатним грошам. Без будь-якого механізму контролю вартість будь-яких цифрових грошей є непередбачуваною. Це призводить до ситуації, коли інвестори починають робити ставку на вартість, і це може серйозно пошкодити ринок протягом декількох годин що негайно виключає можливість висувати цифрові гроші на ринок як прийнятий варіант оплати. З контролем інфляції, ми вважаємо, що люди, які знаходяться поза сферою цифрових грошей, залучаються до її використання, оскільки не буде потреби щодня стежити за своїм портфелем. На відміну від центральних банків у випадку з фіатнимі грошамі, центра для нагляду та підтримки грошової маси не буде. У Galilel, ми реалізуємо децентралізований підхід до спалювання монет, так званий механізм *Proof-of-Burn*[10] для приватних і публічних монет. Хоча це і є необхідним кроком для контролю над грошовим обігом, власники масових мереж отримують можливість голосувати за зменшення винагороди, або повне спалення протягом певного періоду для зменшення генерації монет.



Зображення 5. Голосування Masternode для зменшення генерації винагороди.

Ми назвали його Контроль постачання грошей Galilel Money Supply Control (gMSC), ефективний Proof-of-Burn v2. Цей механізм спалює лише винагороду, і ніколи термінові депозити та бюджет розвитку. Період горіння монет буде один [1] місяць, описаний у таблицях структури винагороди, що знижують річну пропозицію. Власники Masternode мають право голосувати щомісяця. Пропозиція може бути подана один раз на місяць, починаючи з один [1] тижня до закінчення поточного періоду горіння винагороди. Блокчейн приймає будь-яку пропозицію, починаючи з тисячі [1000] GALI. Після того, як пропозиція розповсюджується в блокчейн, власники мастерноди можуть голосувати, витративши додатково один [1] або більше GALI. Виграє пропозиція з найбільшою кількістю монет і з більш ніж п'ятдесят [50] відсотків голосів мастернода після закінчення терміну пропозиції. Якщо термін пропозиції закінчується і приймається, монети, заблоковані в пропозиціях, спалюються, а період спалювання винагороди починається з

наступного згорілого блока. Якщо мінімальні вимоги до прийняття пропозиції не досягнуті, заблоковані монети будуть розблоковані.

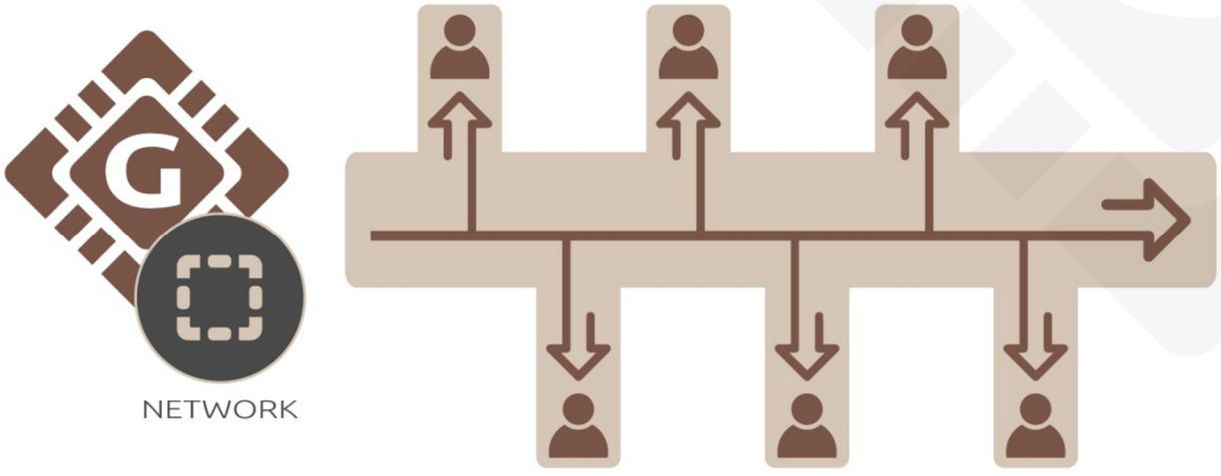
СТРУКТУРА СПАЛЕННЯ НАГОРОД

ВІДСОТОК СПАЛЕННЯ	ОБСЯГ СПАЛЮВАННЯ НА МІСЯЦЬ[1]
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

[1] Розрахунок базується на винагороді 5 GALI після блоку > 430,000

НАЛАШТУВАННЯ MASTERNODES (gIOMN)

Мастерноди отримали вже багато привабливості в сфері цифрових грошей. У той час як багато нових цифрових крипто-валют намагаються створити смішну високу віддачу від інвестицій монет (ROI), зазнають невдачі від інфляції а також незбалансованого розподілу винагороди між мастернодами та гаманцями, це не є основною метою для запуску мастерноди. Основним прикладом використання мастерноди в Galilel є забезпечення мережі, маючи можливість голосувати за майбутні аспекти розвитку, а також підтримувати циркуляцію монет. Проте, головним слабким місцем для доступної реалізації мастерноди є необхідність синхронізувати блокчейн і індексувати його на кожній машині, яка діє як мастернода.



Зображення 6. Кілька мастернод підключених до однієї blockchain в хмарі.

Миттєве налаштування Galilel Instant On Masternode (gIOMN) вирішує цю проблему, реалізуючи спільний блокчейн для запуску «демонів» *one-to-many*[11]

гаманця в моделі клієнтського сервера. Це можна порівняти з моделлю "Instant On", доступною в клієнті *Electrum*[12].

Galilel

ОСОБЛИВОСТІ ТА ТЕХНІЧНІ ХАРАКТЕРИСТИКИ

СПЕЦИФІКАЦІЯ МОНЕТИ	
Назва монети	Galilel
Тикер монети	GALI
Алгоритм хешування	Quark
Алгоритм консенсусу	PoS + zPoS Hybrid
Розмір блоку	2 MB
Час блоку	60 секунд (Перерахування кожен блок)
RPC Порт	36002
P2P Порт	36001
Тип	PoW / PoS / zPoS / MN
Мінімальний вік ставки	2 години
Зрілість	120 підтверджень
Право на отримання	6 підтверджень
Нагорода (до блоку 1,500)	MN 60%, PoW 40%
Нагорода (до блоку 205,000)	MN 60%, PoS 40%
Нагорода (від блоку 205,001)	MN 70%, PoS 30%
Останній PoW блок	1,500
Застава Мастерноди	15,000
Макс. Постачання монет (січень 2020)	19,035,999 GALI
Макс. Постачання монет (січень 2030)	45,315,999 GALI
Макс. Постачання монет (січень 2040)	71,595,999 GALI

Макс. Постачання монет (січень 2050)	97,875,999 GALI
Динамічне постачання монет	Збори за транзакцію і карбування zGALI спалюються
Адреса Пожертвування	UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX
Бюджет розробника (від блоку 250,001)	10% в місячному суперблоку

ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ZEROCOIN

Активація Zerocoin v1	блок 245,000
Активація Zerocoin v2	блок 245,000
zGALI Automint	10%
zGALI Нагорода(від блоку245,001)	1 zGALI
zGALI Нагорода (від блоку 340,001)	MN 40%, zPoS 60%
zGALI Нагорода (від блоку 430,001)	MN 40%, zPoS 60%
zGALI Знаменники	1, 5, 10, 50, 100, 500, 1000, 5000
Модуль акумулятора	RSA-2048
Зрілість	240 підтверджень
Право на отримання	20 підтверджень
Збори (карбування)	0,01 GALI за карбування zGALI
Збори (витрати)	Немає

Galilel

НАГОРОДА PROOF-OF-WORK

ВИСОТА БЛОКУ	НАГОРОДА	MN	POW	ПОСТАЧАННЯ	ПЕРІОД	КІНЕЦЬ ЕТАПУ
Блок 1	220,000	60%	40%	220,000	0 днів	2018-05-25
Блок 2 – 1,500	1	60%	40%	221,499	1 день	2018-05-26

НАГОРОДА PROOF-OF-STAKE

ЕТАПИ	ВИСОТА БЛОКУ	НАГ РОДА	MN	POS	ПОСТАЧАННЯ	ПЕРІОД	КІНЕЦЬ ЕТАПУ
Етап 1	1,501-12,000	100	60%	40%	1,271,399	7 днів	2018-06-02
Етап 2	12,001-22,000	90	60%	40%	2,171,309	7 днів	2018-06-09
Етап 3	22,001-42,000	80	60%	40%	3,771,229	14 днів	2018-06-23
Етап 4	42,001-100,000	70	60%	40%	7,831,159	40 днів	2018-08-02
Етап 5	100,001-160,000	60	60%	40%	11,431,099	42 дня	2018-09-13
Етап 6	160,001-205,000	50	60%	40%	13,681,049	31 день	2018-10-14
Етап 7	205,001-250,000	25	70%	30%	14,806,024	31 день	2018-11-14
Етап 8	250,001-340,000	13.5	70%	30%	16,156,009	62 дня	2019-01-15
Етап 9	340,001-430,000	10	70%	30%	17,055,999	62 дня	2019-03-18
Етап X	430,001-далі	5	70%	30%	далі	далі	далі

Galilel

КОНКУРЕНТНИЙ АНАЛІЗ

Кожен день народжуються нові крипто-валютні проекти, які в основному створюються для конкретної мети. Хоча це вірний сценарій, він обмежує використання монети конкретним розміром і ринком. Зрештою, це обмежує вартість валюти. Ринок криптовалют, що використовують один і той же набір функцій з різною кількістю монет та різними винагородами за блок, перенасичений. У минулому народжувалися деякі проекти з унікальними ідеями і світлим майбутнім. Galilel продовжуватиме цю тенденцію і покращуватиме блокчейн, будуючи просту у використанні крипто-валюту загального призначення для масового використання на ринку.

Galilel

ОСОБЛИВІСТІ	GALILEL	DASH	PIVX	ROI COIN
Публічний Staking	✓	✗	✓	✗
Приватний Staking	✓	✗	✓	✗
Миттєве надсилання	✓	✓	✓	✗
Приватне надсилання	✓	✓	✓	✗
Masternodes	✓	✓	✓	✗
Децентралізоване голосування	✓	✓	✓	✗
Змінний розподіл винагород[1]	✗	✗	✓	✗
Динамічний Zerocoin Proof-of-Stake	✓	✗	✗	✗
Proof-of-Transaction	✓	✗	✗	✗
Змінне спалювання нагороди	✓	✗	✗	✗
Відключений блокчейн	✓	✗	✗	✗
Мобільний Proof-of-Stake	✓	✗	✗	✗
Строкові депозити	✓	✗	✗	✓

[1] Можливе впровадження в Galilel з використанням алгоритму Seesaw

ДОРОЖНЯ КАРТА РОЗВИТКУ

Розвиток монети Galilel Coin має вирішальне значення для блокейна майбутнього. Частка коду вже написана та проходить внутрішнє тестування. Функція Galilel Instant On Masternode (gIOMN) наближається до завершення, тоді як Galilel Hybrid Proof-of-Stake (ghPoS) вимагає додаткових циклів розробки та тестування після запланованої активації Zerocoin v2 на блоці 245,000 Наша дорожня карта включає лише елементи розробки; ми вважаємо, що необхідно визначити належні цілі, очікування та результати, а не встановлювати до нього тонкі маркетингові елементи.

- 2018 – кодування форка PIVX і запуск MAINNET. Створення каналу *Discord*[13] для спільного голосування та анонс на форумі *BitcoinTalk*[14].
- 2018 – Лістинг на перших біржах та сайтах рейтингування. Впровадження результатів голосування спільноти щодо розподілу винагород, модифікації структури винагороди та забезпечення мастерноди у версії 2.0.
- 2018 – Запуск та реліз TESTNET, яка дасть розробникам можливість тестувати новий код blockchain та тестування основних функцій користувачами. Оновлення Galilel до останнього джерела PIVX 3.1.1 випуску v3.0 з активацією Zerocoin v1 і v2 на блоці 245,000 впровадженням Децентралізованої автономної організації (DAO) для голосування, утримуючи блокчейн та мережу сумісно. Увімкнення Zerocoin Proof-of-Stake (zPoS) та випуск v3.1. Створення та випуск білої папери для монети Galilel Coin разом з повторним оголошенням на форумі BitcoinTalk.
- 2019 – Завершення реалізації функції Galilel Instant On Masternode (gIOMN) і виконання загальной доступності (GA) v4.0. Це оновлення ускладнить

ланцюжок і є обов'язковим. Розробка мобільного гаманця, починаючи з кінця Кв.1 після випуску Galilel Core.

- 2019 – Завершення впровадження Galilel Hybrid Proof-of-Stake (ghPoS). Це оновлення буде хард-форком мережі і є обов'язковим. Випуск мобільного гаманця версії 1.0. Наприкінці другого кварталу ми починаємо розробку мобільного гаманця нового покоління що включає гібридний Galilel Hybrid Proof-of-Stake (ghPoS).
- 2019 – функція Galilel Term Deposit (gTD) стане доступною для громадськості з гаманцем v5.1. Ця особливість залежить від Galilel Hybrid Proof-of-Stake (ghPoS) і буде розроблена пізніше. Це оновлення буде хард-форком мережі і є обов'язковим. Ми опублікуємо блок активації після наближення до дати виходу.
- 2019 – Galilel Money Supply Control (gMSC) готовий до виробництва і ми продовжуємо роботу з загальною доступністю (GA) v6.0. Це оновлення буде хард-форком мережі і є обов'язковим. Ми опублікуємо блок активації після наближення до дати виходу. Наприкінці Кв.4 ми опублікуємо мобільний гаманець v2.0 з функцією Galilel Term Deposit (gTD).
- 2020 – повноцінний випуск мобільного гаманця v3.0 з функцією Galilel Money Supply Control (gMSC).

В той час, як дорожня карта є надто строгою і зосереджується на блокчейн, у команди є кілька інших ідей подальшого вдосконалення технології для спрощення використання гаманця. Одним з таких слабких місць є вбудований гаманець Qt. Для кращої взаємодії платформи необхідно замінити його на вбудований веб-сервер, використовуючи структуру зовнішнього інтерфейсу, що дасть кращий досвід роботи з користувачем.

Galilel

ДОВІДКА

Ми віддані нашим довгостроковим цілям розвитку, і вважаємо розвиток дуже важливою частиною проекту. Будь-хто, хто зможе допомогти в реалізації цілей проекту, з маркетингом, написанням статей, поясненням функцій нетехнічним людям, вітається.

Galilel

ВАЖЛИВІ ПОСИЛАННЯ

Website

https://galilel.org/

Block Explorer (MAINNET)

https://explorer.galilel.org/

Block Explorer (TESTNET)

https://explorer.testnet.galilel.org/

Wallet

https://github.com/Galilel-Project/galilel/releases

Discord

https://discord.galilel.org

Twitter

https://twitter.com/GalilelEN

Facebook

https://facebook.com/GalilelEN

YouTube

https://youtube.com/channel/UC26rKBciicXp33dK8NkALmg

BitcoinTalk

https://bitcointalk.galilel.org

Galilel

ДОДАТКИ

1. https://www.linkedin.com/in/mbroemme/

   https://zuppy.pm/
2. https://github.com/Galilel-Project
3. https://review.kydcoin.io/galicoin/
4. https://opensource.org/licenses/MIT
5. https://www.gnu.org/licenses/gpl.txt
6. https://creativecommons.org/licenses/by-nc/4.0/legalcode.txt
7. https://www.transifex.com/galilel-project/galilel-project-translations/
8. http://zerocoin.org/media/pdf/ZerocoinOakland.pdf
9. https://en.wikipedia.org/wiki/Time_deposit
10. https://en.bitcoin.it/wiki/Proof_of_burn
11. https://en.wikipedia.org/wiki/One-to-many_(data_model)
12. https://electrum.org/
13. https://discord.com/
14. https://bitcointalk.org/

galilel.org