Первая универсальная криптовалюта с Гибридным Алгоритмом Консенсуса, Динамический Zerocoin Proof-of-Stake, Proof-of-Transaction и Голосование Мастернод за период на основании сжигания награды.

WHITE PAPER V1.11

Maik Broemme[1], ноябрь 2019

Galilel

ОГЛАВЛЕНИЕ

Краткий обзор 3

Введение 3

Galilel Coin 3

Проблемы и решения 4

Динамический Zerocoin Proof-of-Stake (dzPoS) 4

Proof-of-Transaction (ghPoT) 6

Гибридный Proof-of-Stake (ghPoS) 7

Срочный депозит (Term Deposits - gTD) 9

Контроль Денежной Массы (Money Supply Control - gMSC) 10

Мгновенные мастерноды (Instant On Masternodes - gIOMN) 13

Характеристики и спецификации 14

Конкурентный анализ 17

План развития 19

Помощь 21

Полезные ссылки 22

Дополнительно 23

Galilel

КРАТКИЙ ОБЗОР

В то время как фиатные деньги уже сотни лет определяют и доказывают экономические стандарты, ситуация с цифровыми деньгами иная. Цифровые деньги - это инвестиции высокого риска с непредсказуемой стоимостью и исчезающими командами разработчиков, оставляющими осиротевшие блокчейны. Правительства определили эту проблему, и правила первоначального предложения монет (ICO) решат ее в ближайшие несколько лет. Более того, цифровые валюты, реализующие уникальные возможности блокчейна, имеют высокую вероятность определить будущие стандарты цифровых денег. Galilel будет участвовать в этом процессе посредством реализации уникальных функций, описанных в настоящем документе.

ВВЕДЕНИЕ

Galilel Coin - это криптовалюта, управляемая сообществом с полной прозрачностью и использующая публичный метод развития. Доверительные отношения между инвесторами и командой проекта - залог успеха. Поэтому мы создали организацию GitHub под названием *Galilel-Project*[2], которая отслеживает всю нашу деятельность по разработке в общедоступных репозиториях, включая весь наш бэкенд-код, и прошла публичную проверку *Know Your Developer (KYD)*[3]. Проект использует в основном лицензии *MIT*[4], *GPLv3*[5] и *CC-BY-NC 4.0*[6] с открытым исходным кодом и открытым контентом. Перевод и локализация использует платформу *Transifex*[7].

GALILEL COIN

Galilel Coin (GALI и zGALI) - это открытая публичная и частная цифровая криптовалюта с Proof-of-Stake для быстрых (с использованием SwiftX), приватных

(протокол *Zerocoin*[9]) и безопасных микро транзакций. Наша главная цель - создать децентрализованную полностью безопасную и анонимную сеть для запуска приложений, которые не зависят от какого-либо центрального органа управления. При наличии распределенной системы тысячи пользователей будут нести ответственность за обслуживание приложения и данных, чтобы не было ни единой точки сбоя.

ПРОБЛЕМЫ И РЕШЕНИЯ

Ажиотаж вокруг технологии блокчейн вызывает огромный интерес, набирает популярность во всем мире и используется многими компаниями для разных целей, помимо цифровых денег. Однако, используя его, в качестве базы для платежных услуг требуются специальные функции для хранения и проверки тысяч транзакций. Хотя это уже решено с использованием существующего алгоритма консенсуса для генерации блоков в цепочке, существует несколько слабых областей в текущих реализациях блокчеин для достижения всеобщего принятия цифровых денег.

ДИНАМИЧЕСКИЙ ZEROCOIN PROOF-OF-STAKE (dzPoS)

Zerocoin Proof-of-Stake (zPoS) была самой инновационной функцией блокчейна, введенной в 2018 году командой разработчиков PIVX. Тем не менее, техническая реализация выполнена определенным образом для их блокчейна и не позволяет легко принять его к другим, поскольку их структура вознаграждения статически включена в исходный код.

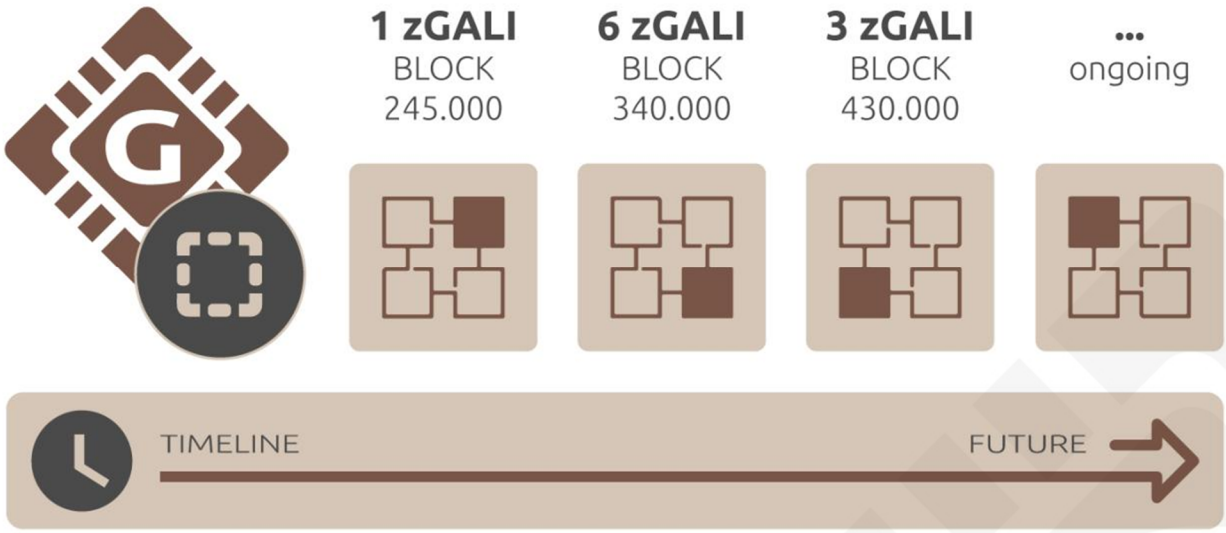

Рис. 1. Динамическое Zerocoin Proof-of-Stake вознаграждение на основе блокчейн фазы.

В Galilel мы реализуем динамическую версию Zerocoin staking, эта версия генерирует награды достоинством, которое представляет целое значение. Наименьший возможный номинал - один [1]. В первой версии – фазе прогрева – мы всегда используем наименьшее значение номинала для тестирования. Недостатком этого подхода является то, что ставка Zerocoin очень интенсивна для процессора, а вероятность создания сиротского блока выше, поскольку публичная монетная ставка может решить блок позже, но распределить его по цепочке раньше. Во второй версии – полной фазе – мы автоматически определяем лучшую структуру номинала на основе суммы вознаграждения блока. Это значительно снижает вероятность генерации сиротских блоков.

PROOF-OF-TRANSACTION (ghPoT)

В традиционной экономике с денежными переводами между банковскими счетами можно указать субъект чтобы получатель мог назначить сумму конкретному счету. Это невозможно в текущих реализациях кошелька. Он позволяет указать значение комментария, которое не является частью транзакции и хранится только локально. Чтобы назначить счет конкретному получателю, необходимо создать адрес кошелька с сопоставлением "один к одному" между обоими заинтересованными сторонами.

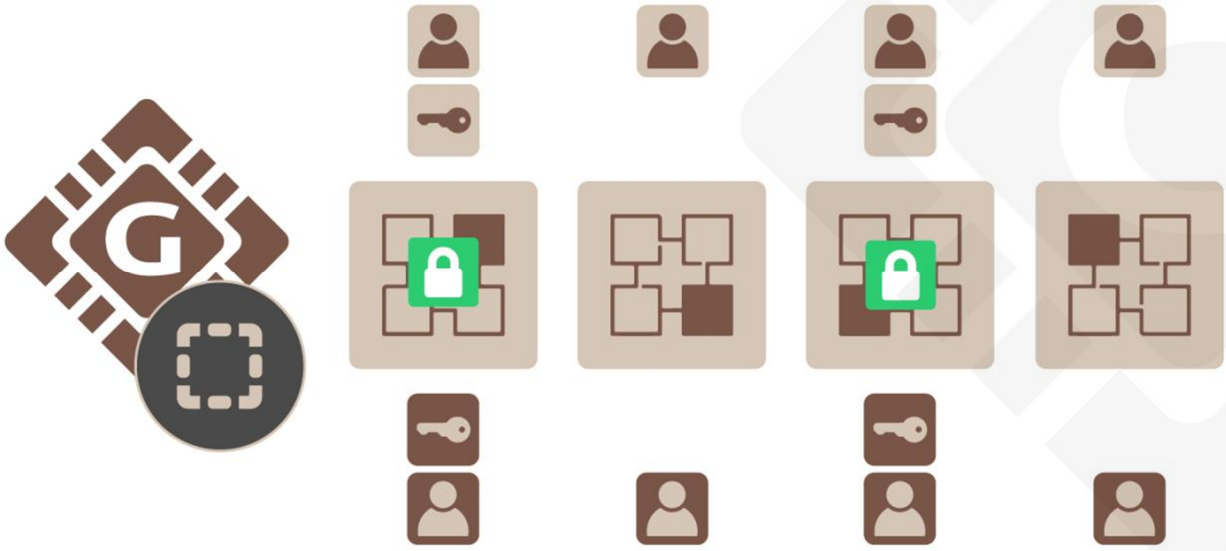

Рис. 2. Proof-of-Transaction с зашифрованным субъектом.

В Galilel мы включаем дополнительное поле данных и прикрепляем его к транзакции, которая хранится в блоке. Это зашифрованное поле и расшифровка возможна только с помощью кошельков, которые указаны в транзакции. Это решает проблему назначения транзакций и позволяет шлюзам обработки платежей идентифицировать счета получателя, как это происходит с традиционными счетами в фиатных валютах.

ГИБРИДНЫЙ PROOF-OF-STAKE (ghPoS)

Хотя Proof-of-Stake (PoS) является экологически чистым алгоритмом консенсуса, он создает вознаграждение только до тех пор, пока работает настольный кошелек. Одним из решений этой проблемы является регистрация в любом общем пуле Proof-of-Stake или в облаке. Однако недостатком является то, что пользователь должен доверять стейк-пулу и передавать ему определенное количество монет. Это может привести к тому, что огромное количество монет будет храниться в нескольких кошельках. Это слабая ситуация для децентрализованного сетевого подхода и является основополагающей частью для достижения консенсуса. Приватный стейкинг, так называемый Zerocoin Proof-of-Stake (zPoS), имеют те же проблемы и ограничения.

Рис. 3. Возможные способы, чтобы заработать награды в Galilel сети.

В Galilel решением этой проблемы будет гибридный алгоритм консенсуса, именуемый Galilel Hybrid Proof-of-Stake (ghPoS). Мы расширим Proof-of-Stake делая мобильный POS возможным для публичного и приватного стейкинга.

Мобильный POS имеет **десять** [10] процентов вознаграждения за блок, если мобильный кошелек находит блок. В этом случае **девяносто** [90] процентов выплачивается владельцу мастерноды. Мобильные кошельки будут работать как легкий узел блокчейна с минимальным количеством блоков, равным возможностям устройства.

ГИБРИДНАЯ СТРУКТУРА ВОЗНАГРАЖДЕНИЯ С PROOF-OF-STAKE

ТИП СТЕЙКА[1]	СТЕЙКИНГ	МАСТЕРНОДА
Online (GALI)	30%	70%
Online (zGALI)	60%	40%
Mobile (GALI)	10%	90%
Mobile (zGALI)	20%	80%

[1] Расчет основан на вознаграждении 5 GALI > блок 430,000

СРОЧНЫЙ ДЕПОЗИТ (gTD)

В то время как мобильный стейкинг зависит от сложности сети и количества монет, функция *Срочный депозит*[9] позволяет блокировать монеты на определенный период и генерировать награды.

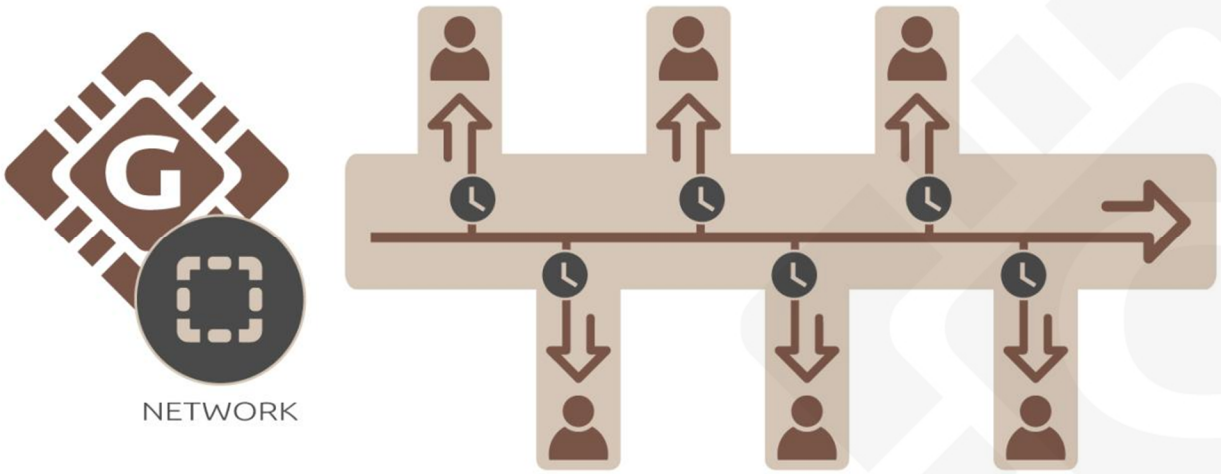

Рис.4. Срочный депозит на основе календаря в автономном кошельке.

Минимальное необходимое количество монет для использования Galilel Term Deposit (gTD) составляет **пять тысяч [5,000] GALI.** Период блокирования - **один [1]** год. Награда за блок составляет **десять [10]** процентов, а заблокированные монеты разных кошельков взвешиваются. С новым блоком в сети кошельки с заблокированными монетами получают сумму в соответствии с их весом. До окончания срока депозита эта награда заблокирована. После блокировки, перемещение или расходование монет невозможно, отмена срочного депозита до истечения срока действия невозможна. Это позволит эффективно сократить предложение монет в период их блокировки.

КОНТРОЛЬ ДЕНЕЖНОЙ МАССЫ (gMSC)

Контроль инфляции является важной частью для цифровых денег, которые должны быть признаны в качестве альтернативы фиатным деньгам. Без механизма управления ценность любых цифровых денег непредсказуема. Это приводит к ситуации, когда инвесторы начинают влиять на стоимость, и это может серьезно повредить рынку и исключает возможность использования цифровых денег на рынке в качестве всеобщего варианта оплаты. С инфляционным контролем мы считаем, что люди за пределами сферы цифровых денег, привлекутся к их использованию, так как не нужно каждый день следить за своим портфолио. В отличие от центральных банков с фиатными деньгами, не будет центрального места для наблюдения и поддержания денежной массы. В Galilel мы реализуем децентрализованный подход к сжиганию монет, так называемый механизм *Proof-of-Burn*[10] (доказательство сжигания) для приватных и публичных монет. Хотя это один из необходимых шагов для контроля денежного обращения, владельцы мастернод получают возможность голосовать за снижение вознаграждения или полное сжигание в течение определенного периода для уменьшения генерации монет.

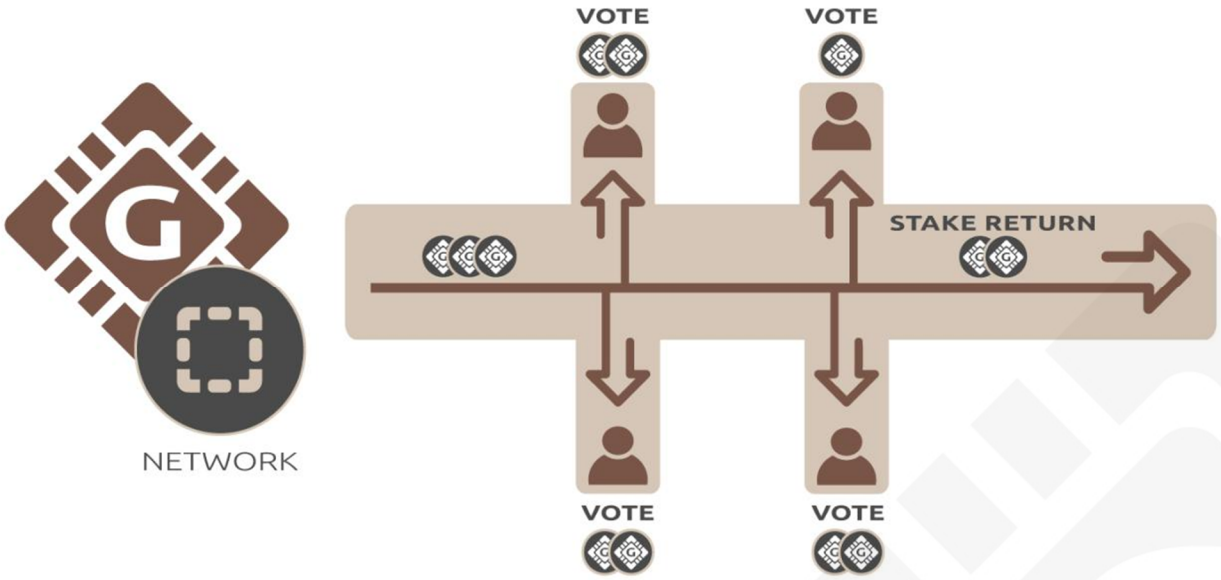

Рис. 5. Голосование мастернод, за уменьшения генерации вознаграждения.

Мы называем его Galilel Money Supply Control (gMSC), эффективный Proof-of-Burn v2. Этот механизм сжигает только вознаграждения, а не срочные депозиты и бюджет разработчиков. Период для сжигания монет один [1] месяц, в количестве, описанном в таблице структуры сжигания вознаграждения, уменьшая годовой запас. Владельцы мастернод могут голосовать каждый месяц. Заявка может быть сделана один раз в месяц, начиная с одной [1] недели до окончания текущего периода записи Proof-of-Burn. Блокчейн принимает любое предложение, начиная с тысячи [1000] GALI. После того, как предложение распространяется в блокчейне, владельцы мастернод могут голосовать дополнительными одним [1] и более GALI. Предложение с наибольшим количеством монет и с более чем пятьюдесятью [50] процентами голосов мастернод после окончания периода предложения выигрывает. Если период предложения заканчивается и принимается, монеты, заблокированные в предложениях, сжигаются, а период сжигания награды начинается с сжигания следующего блока. Если минимальные

требования для принятия предложения не достигнуты, заблокированные монеты будут разблокированы.

СТРУКТУРА СЖИГАНИЯ НАГРАДЫ

ПРОЦЕНТ СЖИГАНИЯ	КОЛ-ВО СЖИГАЕМОЕ В МЕСЯЦ[1]
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

[1] Расчет основан на вознаграждении 5 GALI > блок 430,000

МГНОВЕННЫЕ МАСТЕРНОДЫ (gIOMN)

Мастерноды получили много привлекательности в сфере цифровых денег. В то время как многие новые цифровые криптовалюты пытаются создать глупо высокий возврат инвестиций (ROI) монеты, после этого инфляция монеты "даёт пинка", а также несбалансированное распределение вознаграждения между мастернодами и стейкингом, это не повод для запуска мастернод. В Galilel основным вариантом использования мастернод является обеспечение безопасности сети, имея возможность голосовать за будущие аспекты развития, а также поддержание обращения монет. Однако основным слабым местом для доступных реализаций мастернод является требование синхронизации и индексирования блокчейна на каждой машине, действующей как мастернода.

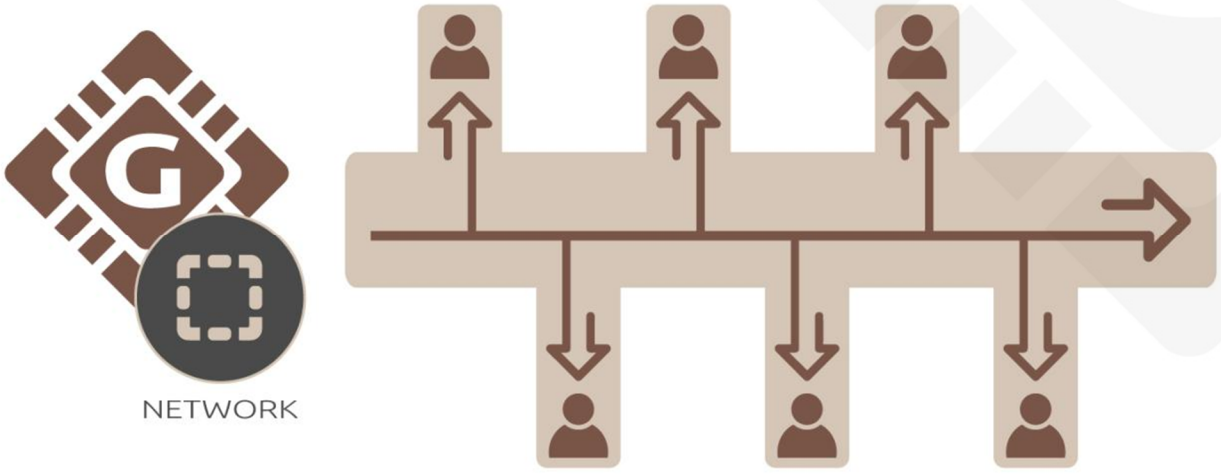

Рис. 6. Несколько мастенод, подключенных к одному блокчейну в облаке.

Galilel Instant On Masternode (gIOMN) решает эту проблему, реализуя общий блокчейн для запуска демонов кошелька *один-к-многим*[11] в модели клиентского сервера. Он сопоставим с моделью "Instant On", доступной в клиенте *Electrum*[12].

Galilel

ХАРАКТЕРИСТИКИ И СПЕЦИФИКАЦИИ

СПЕЦИФИКАЦИИ МОНЕТЫ	
Имя монеты	Galilel
Тикер монеты	GALI
Алгоритм	Quark
Алгоритм консенсуса	PoS + zPoS Гибрид
Размер блока	2 MB
Время блока	60 Секунд (изменяется каждый блок)
RPC Порт	36002
P2P Порт	36001
Тип	PoW / PoS / zPoS / MN
Минимальный возраст монет	2 часа
Зрелость	120 подтверждений
Право на отправку	6 подтверждений
Нрагрда (до блока 1,500)	MN 60%, PoW 40%
Награда (до блока 205,000)	MN 60%, PoS 40%
Награда (с блока 205,001)	MN 70%, PoS 30%
Последний PoW блок	1,500
Монет для мастерноды	15,000
Макс кол-во монет (Январь 2020)	19,035,999 GALI
Макс кол-во монет (Январь 2030)	45,315,999 GALI
Макс кол-во монет (Январь 2040)	71,595,999 GALI

Макс кол-во монет (Январь 2050)	97,875,999 GALI
Динамичный приток монет	Сборы за транзакции и сборы zGALI добычи сжигаются
Адрес пожертвования сообщества	UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX
Бюджет разработчика (с блока 250,001)	10% в ежемесячном суперблоке

ZEROCOIN СПЕЦИФИКАЦИИ

Zerocoin v1 активация	блок 245,000
Zerocoin v2 активация	блок 245,000
zGALI Automint	10%
zGALI Награда (с блока 245,001)	1 zGALI
zGALI Награда (с блока 340,001)	MN 40%, zPoS 60%
zGALI Награда (с блока 430,001)	MN 40%, zPoS 60%
zGALI Знаменатели	1, 5, 10, 50, 100, 500, 1000, 5000
Модуль аккумулятора	RSA-2048
Зрелость	240 подтверждений
Право на отправку	20 подтверждений
Комиссия (mint)	0.01 GALI за отчеканенный zGALI номинал
Сборы (spend)	No fee

Galilel

PROOF-OF-WORK РАСПРЕДЕЛЕНИЕ НАГРАД

ВЫСОТА БЛОКА	НАГРАДА	MN	POW	ВСЕГО МОНЕТ	ПЕРИОД	КОНЕЦ ПЕРИОДА
Блок 1	220,000	60%	40%	220,000	0 дней	2018-05-25
Блок 2 – 1,500	1	60%	40%	221,499	1 день	2018-05-26

PROOF-OF-STAKE REWARDS BREAKDOWN

ЭТАПЫ	ВЫСОТА БЛОКА	НАГРАДА	MN	POS	ВСЕГО МОНЕТ	ПЕРИОД	КОНЕЦ ПЕРИОДА
Этап 1	1,501-12,000	100	60%	40%	1,271,399	7 дней	2018-06-02
Этап 2	12,001-22,000	90	60%	40%	2,171,309	7 дней	2018-06-09
Этап 3	22,001-42,000	80	60%	40%	3,771,229	14 дней	2018-06-23
Этап 4	42,001-100,000	70	60%	40%	7,831,159	40 дней	2018-08-02
Этап 5	100,001-160,000	60	60%	40%	11,431,099	42 дней	2018-09-13
Этап 6	160,001-205,000	50	60%	40%	13,681,049	31 дней	2018-10-14
Этап 7	205,001-250,000	25	70%	30%	14,806,024	31 дней	2018-11-14
Этап 8	250,001-340,000	13.5	70%	30%	16,156,009	62 дней	2019-01-15
Этап 9	340,001-430,000	10	70%	30%	17,055,999	62 дней	2019-03-18
Этап X	430,001- ∞	5	70%	30%	∞	∞	∞

Galilel

КОНКУРЕНТНЫЙ АНАЛИЗ

Каждый день рождаются новые криптовалютные проекты, в основном сервисные валюты для особых целей. И в самом деле, это ограничивает использование монеты определенным рынком и размером. В конце концов, это ограничивает стоимость валюты. Рынок криптовалют, разделяющих один и тот же набор функций с различным количеством цифровых денег и различными вознаграждениями за блок, перенасыщен. В прошлом рождались проекты с уникальными идеями и светлым будущим. Galilel продолжит эту тенденцию и улучшит блокчеин, используемый для цифровых денег, создавая простую в использовании криптовалюту многоцелевого назначения для всеобщего принятия на рынке.

Galilel

ОСОБЕННОСТЬ	GALILEL	DASH	PIVX	ROI COIN
Публичный стейкинг	✓	✗	✓	✗
Приватный стейкинг	✓	✗	✓	✗
Мгновенная Отправка (Instant Send)	✓	✓	✓	✗
Приватная отправка (Private Send)	✓	✓	✓	✗
Мастерноды	✓	✓	✓	✗
Децентрализованное управление голосованием	✓	✓	✓	✗
Переменное вознаграждение[1]	✗	✗	✓	✗
Динамичный Zerocoin Proof-of-Stake	✓	✗	✗	✗
Proof-of-Transaction	✓	✗	✗	✗
Переменная сжигаемая награда	✓	✗	✗	✗
Распределённый Blockchain	✓	✗	✗	✗
Мобильный Proof-of-Stake	✓	✗	✗	✗
Срочные депозиты	✓	✗	✗	✓

[1] Возможно реализовать в Galilel с помощью алгоритма Seesaw

ПЛАН РАЗВИТИЯ

Разработка монеты Galilel имеет решающее значение для блокчейна будущего. Некоторый код уже написан и находится во внутреннем тестировании. Функция Galilel Instant On Masternode (gIOMN) близка к завершению, в то время как Galilel Hybrid Proof-of-Stake (ghPoS) требует дополнительных циклов разработки и тестирования после запланированной активации Zerocoin v2 в блоке 245,000. Наша дорожная карта включает в себя в основном только элементы развития; мы считаем, что необходимо определить правильные цели, ожидания и результаты, а не ставить тонко настроенные маркетинговые элементы.

- 2018 – Форк кодовой базы PIVX и запуск MAINNET. Создание *Discord*[13] для голосования сообщества и предварительного объявления в *BitcoinTalk*[14] форуме.
- 2018 – Листинг на первых биржах и рейтинговых сайтах. Реализация результатов голосования сообщества относительно распределения вознаграждения, модификация структуры вознаграждения и обеспечения мастернод в v2.0. Дизайнерская группа, создаёт бренд Galilel и веб-сайт с фирменными цветами, логотипами и руководством по бренду для разработчиков приложений. Помимо разработки и дизайна, мы пройдем публичную проверку вашего разработчика (Know Your Developer-KYD).
- 2018 – Запуск и релиз TESTNET, дающего разработчикам возможность тестировать новый код блокчеина, а пользователям - тестировать функции bleeding edge. Рефакторинг Galilel код-базы до последнего исхлдника PIVX 3.1.1 и выпуска v3.0 с активацией Zerocoin v1 и v2 в блоке 245,000 и рабочей децентрализованной автономной организацией (DAO) для голосования блокчейном при сохранении обратной совместимости блокчейна и сети.

Включите Zerocoin Proof-of-Stake (zPoS) для приватных ставок и выпуска v3.1. Создание и выпуск whitepaper для Galilel Coin вместе с повторным объявлением на форуме BitcoinTalk.

- 2019 – Завершите реализации Galilel Instant On Masternode (gIOMN) и продолжение работы с общей доступностью (GA) v4.0. Это обновление будет жестко разветвлять цепочку и является обязательным. Разработка мобильного кошелька началась в конце Q1 после выпуска Galilel Core.
- 2019 – Завершение реализации гибридного доказательства Galilel (ghPoS) для публичных и приватных ставок. Мы опубликуем блок активации, как только приблизимся к дате выпуска v5.0. Это обновление будет жестко разветвлять цепочку и является обязательным. Мобильный кошелек v1.0. В конце Q2 мы начинаем разработку мобильного кошелька следующего поколения и включаем Galilel Hybrid Proof-of-Stake (ghPoS).
- 2019 – Функция Galilel Term Deposit (gTD) станет доступной для общественности с кошельком v5.1. Эта функция зависит от Galilel Hybrid Proof-of-Stake (ghPoS) и разрабатывается впоследствии. Это обновление будет жестко разветвлять цепочку и является обязательным. Мы опубликуем блок активации, как только приблизимся к дате релиза.
- 2019 – Galilel Money Supply Control (gMSC) готов к производству, и мы переходим к общей доступности (GA) v6.0. Это обновление будет жестко разветвлять цепочку и является обязательным. Мы опубликуем блок активации, как только приблизимся к дате релиза. В конце Q4 мы публикуем мобильный кошелек v2.0 С Galilel Term Deposit (gTD).
- 2020 – Полноценный релиз мобильного кошелька v3.0 с Galilel Money Supply Control (gMSC).

В то время как дорожная карта выше остра и сосредоточена на блокчейне, у команды есть несколько других идей для дальнейшего совершенствования технологий для упрощения использования кошелька. Одной из таких слабых областей является встроенный Qt кошелек. Для лучшей совместимости платформы необходимо заменить ее тонким встроенным веб-сервером с использованием фреймворка, дающего лучший пользовательский интерфейс.

ПОМОЩЬ

Даже если мы привержены нашим долгосрочным целям развития, любой может помочь или помочь с целями проекта. Хотя разработка является очень важной частью, любой, кто может помочь с маркетингом, написанием статей, объяснением функций нетехническим людям, приветствуется.

Galilel

ПОЛЕЗНЫЕ ССЫЛКИ

Веб-сайт

https://galilel.org/

Блокэксплорер (MAINNET)

https://explorer.galilel.org/

Блокэксплорер (TESTNET)

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

Кошелёк

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

ДОПОЛНИТЕЛЬНО

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