

La primera criptomoneda de uso general con Algoritmo de Consenso Híbrido, Prueba de Participación Zerocoin Dinámica, Prueba de Transacción y Nodos Maestros, con votación para la quema de recompensas basadas en un período.

WHITE PAPER V1.10

Maik Broemme¹, Mayo 2019



ÍNDICE

Resumen Ejecutivo	3
Introducción	3
Moneda Galilel	3
Problemas y Soluciones	4
Prueba de Participación Dinámica Zerocoin (dzPoS)	4
Prueba de Transacción (ghPoT)	6
Prueba de Participación Híbrida (ghPoS)	
Depósitos a Plazo (gTD)	9
Control de Suministro de Monedas (gMSC)	10
Nodos Maestros al Instante (gIOMN)	
Características y Especificaciones	
Análisis Competitivo	18
Hoja de Ruta de Desarrollo (Roadmap)	20
Ayuda	22
Enlaces Importantes	23
Glosario	24
Apéndice	25



RESUMEN EJECUTIVO

Mientras que el dinero fiat ha sido probado y definido como el estándar económico por cientos de años, la situación con el dinero digital es diferente. Se ha considerado como una inversión de alto riesgo, con valor impredecible y en donde los equipos de desarrollo tienden a desaparecer. Los Gobiernos han identificado este problema, y han comenzado a implementar regulaciones para las (ICO), lo que ayudará a resolverlo en los próximos años. Además, las monedas digitales que implementen características únicas en la blockchain (cadena de bloques) tienen una alta probabilidad de convertirse en el estándar del futuro del dinero digital. Galilel será parte de este proceso, a través de la implementación de características únicas que a continuación se mencionan en este documento.

INTRODUCCIÓN

Galilel es una criptomoneda impulsada por la comunidad, totalmente transparente, y que utiliza un método de desarrollo público. La relación de confianza entre los inversionistas y el equipo desarrollador es la clave para el éxito. Por lo tanto hemos creado una organización en Github llamada *Galilel-Project*², en donde puedes dar seguimiento a todas nuestras actividades de desarrollo en repositorios públicos incluyendo nuestro código back-end, así como la verificación pública obtenida de *Know Your Developer (KYD)*³. El proyecto utiliza principalmente código abierto y licencias de contenido abierto *MIT*⁴, *GPLv3*⁵ y *CC-BY-NC 4.0*⁶. La traducción y localización usa la plataforma *Transifex*⁷.

MONEDA GALILEL

Galilel (GALI y zGALI) es una criptomoneda de código abierto con algoritmo Proof-of-Stake (Prueba de Participación) pública y privada para realizar transacciones



instantáneas, privadas y a bajo costo, utilizando SwiftX y el protocolo *Zerocoin*⁸. Nuestro principal objetivo es crear una red descentralizada, totalmente segura y anónima para ejecutar aplicaciones que no dependan de ningún ente de control central. Siendo un sistema distribuido, miles de usuarios serán responsables de mantener las aplicaciones y datos para que no haya un punto de fallo único.

PROBLEMAS Y SOLUCIONES

El auge de la tecnología blockchain genera un gran interés, ha ganado popularidad en todo el mundo y es utilizado por muchas compañías para diferentes propósitos, además del dinero digital. Sin embargo su uso para pago de bienes y servicios requiere de características específicas para validar, almacenar y verificar miles de transacciones. Si bien esto ya lo han resuelto utilizando los existentes algoritmos de consenso para generar bloques en la cadena, aún existen muchas áreas débiles en la implementación de la actual blockchain para lograr la adopción masiva y su uso como dinero digital.

PRUEBA DE PARTICIPACIÓN DINÁMICA ZEROCOIN (dzPoS)

La Prueba de Participación Zerocoin (Zerocoin Proof-of-Stake) fue la característica de blockchain más innovadora introducida en 2018 por el equipo de desarrollo PIVX, sin embargo la implementación técnica fue hecha de una forma específica para su blockchain y no permite una adopción fácil para otros, ya que su estructura de recompensas está estáticamente incluida en el código fuente.



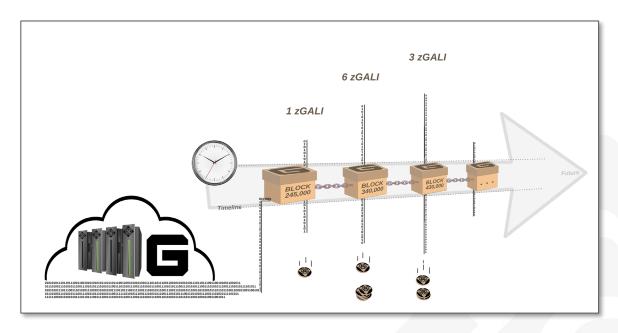


Figura 1. Recompensa Dinámica de Zerocoin Proof-of-Stake, basada en una fase de la cadena de bloques.

En Galilel hemos implementado una versión dinámica de staking Zerocoin. La cual genera recompensas en denominaciones que se representan en un valor entero. La denominación más baja posible es uno [1]. En la primera versión (fase de calentamiento) siempre usamos la denominación más baja para hacer pruebas. La desventaja de esto es que al hacer staking de Zerocoin se utiliza mucho poder de procesamiento del CPU, y la probabilidad de generar un bloque huérfano es mayor, ya que siendo una moneda pública, al hacer stake se puede resolver el bloque tardíamente, pero distribuirlo a la cadena más tempranamente. En la segunda versión (fase completa), se auto determina la mejor estructura de denominaciones basada en la cantidad de recompensas del bloque. Esto reduce significativamente la probabilidad de generar bloques huérfanos.



PRUEBA DE TRANSACCIÓN (ghPoT)

En una economía tradicional con transferencias de dinero entre cuentas bancarias, es posible especificar un concepto, de tal forma que el receptor pueda asignar el monto a una factura específica. Esto no es posible en las actuales implementaciones de billeteras. Permiten especificar un comentario o un "comentario a valor", que no forma parte de la transacción y solo se almacena localmente. Para asignar una factura a un pagador en específico es necesario crear una dirección en la billetera con mapeo uno-a-uno entre ambos individuos.

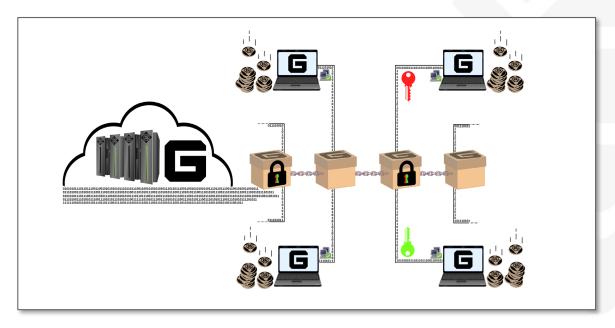


Figura 2. Prueba de Transacción con Concepto encriptado.

En Galilel hemos incluido un campo de datos adicional y lo hemos agregado a la transacción, que se almacena en el bloque. Es un campo encriptado, y solo es posible desencriptarlo por las billeteras que negociaron la transacción. Esto resuelve el problema de asignación de transacción y permite a los portales de procesamiento de



pagos identificar al beneficiario de una factura, de la misma forma que una factura de dinero tradicional.

PRUEBA DE PARTICIPACIÓN HÍBRIDA (ghPoS)

Aunque la Prueba de Participación (PoS) es un algoritmo ambientalmente amigable, solamente genera recompensas mientras la billetera de escritorio esté abierta. Una solución a este problema es inscribirse a una de las pools compartidas que existen en la nube. Esto puede ocasionar que grandes cantidades de monedas estén almacenadas en pocas billeteras. Lo que significa un punto débil para una red descentralizada y su parte esencial de tener consenso. La Prueba de Participación privada, también llamada Zerocoin (zPoS) presenta los mismos problemas y limitaciones.

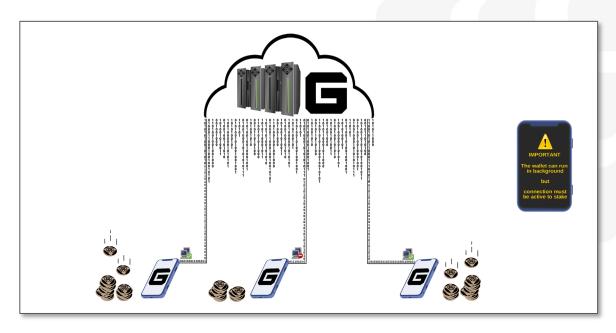


Figura 3. Posibles maneras de obtener recompensas de la red Galilel.

En Galilel, la solución a este problema será un algoritmo de consenso híbrido completo, llamado Prueba de Participación Híbrida Galilel (ghPoS). Expandiremos la Prueba de Participación a móviles con capacidades suficientes para hacer staking, y aplicará para



staking pública como privada. Hacer staking en móviles se obtendrá un diez [10] por ciento de la recompensa del bloque (si la billetera móvil encuentra el bloque). En este caso el noventa [90] por ciento será pagado a los tenedores de nodos maestros (masternodes). La billetera móvil funcionará como un nodo ligero de la blockchain, con una cantidad mínima de bloques, equivalente a la longitud de reorganización de la cadena.

ESTRUCTURA DE RECOMPENSAS DE PROOF-OF-STAKE HÍBRIDA

TIPO DE STAKING ¹	STAKING	MASTERNODE
En línea (GALI)	30%	70%
En línea (zGALI)	60%	40%
Móvil (GALI)	10%	90%
Móvil (zGALI)	20%	80%

¹Cálulo basado en recompensa de 5 GALI > bloque 430,000



DEPÓSITOS A PLAZO (gTD)

Mientras que el staking móvil es dependiente de la dificultad de la red y la cantidad de monedas acumuladas, la función de los *depósitos a plazo*⁹ permite bloquear monedas por un cierto período y generar recompensas.

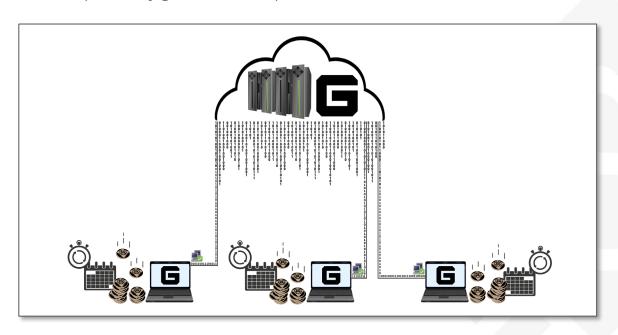


Figura 4. Calendario basado en Depósitos a Plazo en una billetera fuera de línea.

La cantidad mínima de monedas requeridas para usar Depósitos a Plazo (gTD) es cinco mil [5,000] GALI. El período de bloqueo es de un [1] año. La recompensa de bloque es de diez [10] por ciento, y las monedas de diferentes billeteras se usan para ponderar. Con un nuevo bloque en la red, las billeteras con monedas bloqueadas obtendrán la cantidad de acuerdo a su ponderación. Hasta que el período del Depósito a Plazo finalice las recompensas estarán bloqueadas. Una vez bloqueadas, usar las monedas para moverlas o gastarlas para hacer compras es imposible. La cancelación del Depósito a Plazo antes del tiempo de finalización es imposible. Esto reducirá eficazmente el suministro de monedas durante el período bloqueado.



CONTROL DE SUMINISTRO DE MONEDAS (gMSC)

El control de la inflación es uno de los retos más desafiantes para el dinero digital, y poder ser reconocido y aceptado como una alternativa al dinero fiat. Sin ningún mecanismo de control, el valor de cualquier dinero digital es impredecible. Esto pude generar una situación en que los inversores comiencen a apostar en su valor, lo que ocasionaría un serio daño al mercado en cuestión de horas e inmediatamente eliminaría la posibilidad de que el dinero digital sea visto como una opción de pago aceptada. Con el control de inflación creemos que las personas que están fuera de la esfera del dinero digital sean atraídas a usarlo, ya que no sería necesario que tuvieran que estar revisando su portafolio todos los días. A diferencia de los bancos centrales y el dinero fiat, no habrá un lugar central para observar y mantener el suministro de dinero. En Galilel hemos implementado un enfoque descentralizado para la quema de monedas, llamado *Proof-of-Burn*¹⁰ (mecanismo de Prueba de Quema) para monedas acumuladas públicas y privadas. Aunque esto es un paso necesario para controlar la circulación de dinero, los propietarios de masternodes tendrán la posibilidad de votar por una reducción de recompensas o quema completa por un período específico para reducir la generación de monedas.



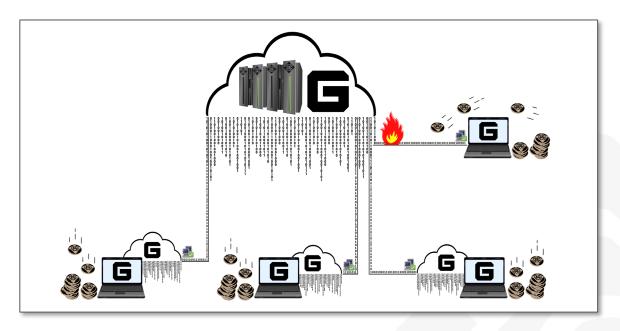


Figura 5. Votación de masternodes para reducir la generación de recompensas.

Le hemos llamado Control de Suministro de Monedas (gMSC), eficazmente Proof-of-Burn v2 (Prueba de Quema v2). Este mecanismo quema únicamente recompensas, nunca los depósitos a plazo ni el presupuesto para desarrollo. El período para la quema de moneda será un [1] mes, en los pasos descritos en la tabla de estructura de quema de recompensas, disminuyendo el suministro anual. Los propietarios de masternodes serán sujetos para votar cada mes. La propuesta podrá ser hecha una vez al mes, comenzando una [1] semana antes de que el período actual de quema de recompensa termine. La blockchain aceptará cualquier propuesta empezando desde mil [1000] GALI. Una vez que la propuesta sea distribuida en la blockchain, los propietarios de masternodes podrán votar haciendo un gasto adicional de uno [1] o más GALI. La propuesta con el mayor número de monedas y con más del cincuenta [50] por ciento de votos de los masternodes después de que el período de propuesta finalice, ganará. Si el período de propuesta termina y es aceptado, las monedas bloqueadas en la propuesta serán quemadas y el nuevo período de quema de recompensa comenzará



desde el siguiente bloque Si los requerimientos mínimos para la aceptación de la propuesta no son alcanzados, las monedas bloqueadas se desbloquearán.

ESTRUCTURA DE QUEMA DE RECOMPENSA

PORCENTAJE DE QUEMA	CANTIDAD A QUEMAR POR MES ¹
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

¹Cálulo basado en recompensa de 5 GALI > bloque 430,000



NODOS MAESTROS AL INSTANTE (gIOMN)

Si bien los masternodes han generado gran atención en el mundo del dinero digital. Muchos de los nuevos proyectos han tratado de crear criptomonedas con retornos sobre la inversión (ROI) ridículamente altos, y fallan después de que la inflación se dispara, de la misma forma, tienen una distribución poco balanceada entre los masternodes y las billeteras staking. Este no es el objetivo principal de tener un masternode. En Galilel el principal uso de los masternodes es asegurar la red y al mismo tiempo tener la oportunidad de votar en aspectos de desarrollo futuros, así como mantener en circulación la moneda. Sin embargo el principal punto débil para la implementación de masternodes disponibles es que se requiere tener sincronizada e indexada la blockchain en cada máquina actuando como masternode.

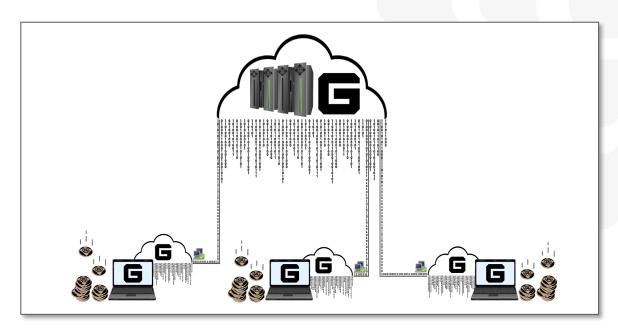


Figura 6. Multiples masternodes conectados a una única blockchain en la nube.



Los masternodes al instante Galilel (gIOMN) resuelven este problema implementando una blockchain compartida que corra *una-a-varias*¹¹ billeteras en un modelo de servidor cliente. Esto es comparable al modelo "Instant On" disponible en *Electrum*¹².



CARACTERÍSTICAS Y ESPECIFICACIONES

ESPECIFICACIONES DE LA MONEDA

Galilel			
GALI			
Quark			
PoS + zPoS Híbrido			
2 MB			
60 Segundos (Re-ajuste cada bloque)			
36002			
36001			
PoW / PoS / zPoS / MN			
2 Horas			
120 confirmaciones			
6 confirmaciones			
MN 60%, PoW 40%			
MN 60%, PoS 40%			
MN 70%, PoS 30%			
1,500			
15,000			
19,035,999 GALI			
45,315,999 GALI			
71,595,999 GALI			



Suministro Máximo (Enero 2050)	97,875,999 GALI
Suministro Dinámico de Moneda	Comisiones de Transacciones y Comisiones de acuñación de zGALI son quemados
Dirección de Donación	UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX
Presupuesto a Desarrollador (desde el bloque 250,001)	10% en súperbloques mensuales

ESPECIFICACIONES ZEROCOIN

Activación Zerocoin v1	bloque 245,000
Activación Zerocoin v2	bloque 245,000
Autoacuñación zGALI	10%
Recompensas zGALI (desde el bloque 245,001)	1 zGALI
Recompensas zGALI (desde el bloque 340,001)	MN 40%, zPoS 60%
Recompensas zGALI (desde el bloque 430,001)	MN 40%, zPoS 60%
Denominadores zGALI	1, 5, 10, 50, 100, 500, 1000, 5000
Módulo Acumulador	RSA-2048
Madurez	240 confirmaciones
Eligibilidad de envío	20 confirmaciones
Comisiones (acuñación)	0.01 GALI por denominación
	zGALI acuñada
Comisiones (gasto)	No fee



DESGLOSE DE RECOMPENSAS DE PRUEBA DE TRABAJO (PROOF-OF-WORK)

ALTURA DEL BLOQUE	RECOMPENSA	MN	POW	SUMINISTRO	PERÍODO	FINALIZACIÓN
Bloque 1	220,000	60%	40%	220,000	0 días	2018-05-25
Bloque 2 – 1,500	1	60%	40%	221,499	1 día	2018-05-26

DESGLOSE DE RECOMPENSAS DE PRUEBA DE PARTICIPACIÓN (PROOF-OF-STAKE)

ETAPAS	ALTURA DEL BLOQUE	REC	MN	POS	SUMINISTRO	PERÍODO	FINALIZACIÓN
Etapa 1	1,501-12,000	100	60%	40%	1,271,399	7 días	2018-06-02
Etapa 2	12,001-22,000	90	60%	40%	2,171,309	7 días	2018-06-09
Etapa 3	22,001-42,000	80	60%	40%	3,771,229	14 días	2018-06-23
Etapa 4	42,001-100,000	70	60%	40%	7,831,159	40 días	2018-08-02
Etapa 5	100,001-160,000	60	60%	40%	11,431,099	42 días	2018-09-13
Etapa 6	160,001-205,000	50	60%	40%	13,681,049	31 días	2018-10-14
Etapa 7	205,001-250,000	25	70%	30%	14,806,024	31 días	2018-11-14
Etapa 8	250,001-340,000	13.5	70%	30%	16,156,009	62 días	2019-01-15
Etapa 9	340,001-430,000	10	70%	30%	17,055,999	62 días	2019-03-18
Etapa X	430,001-En adelante	5	70%	30%	En adelante	En adelante	En adelante



ANÁLISIS COMPETITIVO

Cada día nuevos proyectos de criptomonedas nacen, la mayoría son monedas de servicio para un propósito específico. Aunque es un escenario válido, la utilidad de estas monedas se limita a un mercado en particular. Y al final se limita el valor de la moneda. El mercado de las criptomonedas compartiendo las mismas características, con diferentes suministros y diferentes recompensas por bloque está sobresaturado. En el pasado nacieron algunos proyectos con ideas únicas y un futuro brillante. Galilel continuará esta tendencia y mejorará la blockchain usado para dinero digital, construyendo una criptomoneda de uso general y fácil de utilizar para la adopción en masa.



CARACTERÍSTICA	GALILEL	DASH	PIVX	ROI COIN
Staking Público	Ø	8	Ø	8
Staking Privado	Ø	8	Ø	8
Envío instantáneo	Ø	Ø	Ø	8
Envío Privado	②	Ø	Ø	8
Masternodes	Ø	Ø	Ø	8
Voto de Gobernanza Descentralizada	②	Ø	Ø	8
Distribución Variable de Recompensa ¹	8	8	Ø	8
Proof-of-Stake Zerocoin Dinámico	②	8	8	8
Proof-of-Transaction	Ø	8	8	8
Quema de Recompensa Variable	Ø	8	8	8
Blockchain Desconectado	Ø	8	8	8
Proof-of-Stake Móvil	Ø	8	8	8
Depósitos a Plazo	②	8	8	•

¹Posible implementar en Galilel usando el algoritmo Seesaw.



HOJA DE RUTA DE DESARROLLO (ROADMAP)

El desarrollo de la moneda Galilel es crítico para la blockchain del futuro. Una parte del código ha sido escrita y se encuentra en pruebas internas de testeo. La característica de Galilel Instant On Masternode gIOMN (Nodos Maestros al instante) está casi completada, mientras que la función Hyrbid Proof-of-Stake ghPoS (Prueba de Participación Híbrida) requiere aún de desarrollo y ciclos de testeo antes de la planeada activación de Zerocoin v2, en el bloque 245,000. Nuestra hoja de ruta incluye principalmente elementos de desarrollo. Creemos que es necesario definir objetivos, expectativas y resultados claros y adecuados, en lugar de enfocarnos únicamente en elementos de mercadeo.

- 2018 Bifurcación del código PIVX y lanzamiento de MAINNET (Red Principal).
 Creación del canal *Discord¹³* para votación de la comunidad, y preanuncio en el foro *Bitcointalk¹⁴*.
- 2018 Listado en el primer Exchange y sitios de rankeo. Implementación de votos de la comunidad, independientemente de la distribución de recompensas, modificación de la estructura de recompensas y colateral de masternode en v2.0.
 Creación de la marca Galilel y el sitio web con colores, logotipos y guía de la marca para desarrolladores de aplicaciones. Además del desarrollo y diseño, aplicaremos para pasar la verificación pública Know Your Developer (KYD) (Conoce a tu Desarrollador (KYD)).
- 2018 Habilitación y lanzamiento del TESTNET (Red de Testeo), dando a los desarrolladores la posibilidad de testar un nuevo código blockchain y a los usuarios probar características innovadoras. Reestructuración del código Galilel a la última versión de PIVX 3.1.1 y lanzar la v3.0 con activación de Zerocoin v1 y v2 en el bloque 245,000. Y trabajar la Organización Autónoma Descentralizada (DAO) para votación



del blockchain y red compatible con versiones anteriores. Habilitar Zerocoin Proof-of-Stake (zPoS) para staking privado y lanzar v3.1. Creación y lanzamiento de la hoja técnica (whitepaper) para la moneda Galilel, junto con el re-anunciamiento en el foro Bitcointalk.

- 2019 Finalizar la implementación de la característica Instant On Masternodes (gIOMN) y proceder con la Disponibilidad General (GA) de v4.0. Esta actualización es obligatoria ya que se hará una bifurcación en la cadena. Se comenzará con el desarrollo de la billetera móvil a finales del T1, después de lanzar Galilel Core.
- 2019 Finalización de la implementación de Proof-of-Stake Híbrido (ghPoS) para staking público y privado. Publicaremos la activación del bloque una vez que estemos cerca de la fecha de lanzamiento de v5.0. Esta actualización es obligatoria ya que se hará una bifurcación en la cadena. Lanzamiento de la billetera móvil en versión v1.0. A finales del T2, comenzaremos a desarrollar la nueva generación de la billetera móvil e incluiremos Proof-of-Stake Híbrido (ghPoS).
- 2019 La característica de Depósitos a Plazo (gTD) estará disponible en la versión de la billetera v5.1. Esta característica depende de Proof-of-Stake Híbrido (ghPoS) y será desarrollado posteriormente. Esta actualización es obligatoria ya que se hará una bifurcación en la cadena. Publicaremos la activación del bloque una vez que estemos cerca de la fecha de lanzamiento.
- 2019 Control de Suministro de Dinero Galilel (gMSC) estará listo para producción y procederemos con la Disponibilidad General (GA) de v6.0. Esta actualización es obligatoria ya que se hará una bifurcación en la cadena. Publicaremos la activación del bloque una vez que estemos cerca de la fecha de lanzamiento. A finales del T4, publicaremos la billetera móvil v2.0. con la característica de Depósitos a Plazo (gTD).



• 2020 – Lanzamiento de la billetera móvil versión **v3.0**, completamente desarrollada, con Control de Suministro de Dinero (gMSC).

Aunque la hoja de ruta es precisa y pone énfasis en la blockchain, el equipo tiene muchas otras ideas en mente para futuras mejoras tecnológicas para simplificar el uso de la billetera. Una de estas áreas débiles es la billetera qt. Para una mejor interoperabilidad de la plataforma, es necesario reemplazarla con un servidor web incorporado ligero que use un marco de front-end para brindar la mejor experiencia de usuario.

AYUDA

Aun cuando estamos comprometidos con nuestros objetivos de desarrollo a largo plazo, cualquiera puede aportar o ayudar con los objetivos del proyecto. Si bien, el desarrollo es una parte muy importante, cualquier persona que pueda ayudar con el marketing, escribir artículos, explicar las características a personas no técnicas, es bienvenida.



GLOSARIO

Back-end code: Código secundario o de fondo.

Blockchain: Cadena de Bloques.

DAO: Organización Autónoma Descentralizada.

Exchange: Casa de cambio.

Front-end code: Código primario o de interfaz.

Mainnet: Red principal.

Masternode: Nodo Maestro.

Minted: Acuñado / Acuñación.

Proof-of-Burn: Prueba de Quema.

Proof-of-Stake (PoS): Prueba de Participación.

Proof-of-Transaction (PoT): Prueba de Transacción.

Proof-of-Work (PoW): Prueba de Trabajo.

Q (Quarter): Trimestre (T1, T2, T3, T4)

Roadmap: Hoja de ruta.

Stake: Acumulación.

Staking: Se refiere a la acción de hacer Prueba-de-Participación.

Whitepaper: Informe técnico.



ENLACES IMPORTANTES

Página web

https://galilel.cloud/

Explorador de bloques

https://explorer.galilel.cloud/

Repositorio de versiones de la billetera

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

Discord

https://discord.galilel.cloud

Twitter

https://twitter.com/GalilelEN

https://twitter.com/GalilelES

Facebook

https://facebook.com/GalilelEN

YouTube

https://youtube.com/channel/UC26rKBciicXp33dK8NkALmg

BitcoinTalk

https://bitcointalk.galilel.cloud



APÉNDICE

- 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.cloud