A primeira criptomoeda de propósito geral, com Algoritmo Hibrido de Consenso, Zerocoin Dinâmico – Prova de Estaca, Prova de Transação e Votação de Masternodes para queima de recompensas baseada em período

WHITE PAPER V1.11

Maik Broemme[1], Novembro 2019

Galilel

TABLE OF CONTENTS

Galilel

SUMÁRIO

Enquanto a moeda fiduciária já definiu e provou os padrões econômicos por centenas de anos, a situação com o dinheiro digital é diferente. O dinheiro digital é um investimento de alto risco com valor imprevisível e equipes de desenvolvimento que estão desaparecendo deixando blockchains órfãos. Os governos identificaram este problema e os regulamentos da Oferta Inicial de Moedas (ICO) irão resolvê-lo nos próximos anos. Além disso, as moedas digitais, que implementam recursos exclusivos de blockchain, têm uma alta probabilidade de definir os padrões futuros de dinheiro digital. A Galilel fará parte desse processo por meio da implementação dos recursos exclusivos descritos neste documento.

INTRODUÇÃO

A Galilel Coin é uma moeda criptográfica dirigida pela comunidade, com total transparência e utilizando um método de desenvolvimento público. A relação de confiança entre os investidores e a equipe do projeto é a chave para o sucesso. Portanto, criamos uma organização do GitHub chamada *Galilel-Project*[2], que monitora todas as nossas atividades de desenvolvimento em repositórios públicos, incluindo todo o nosso código de backend e passou pela verificação pública do *Know Your Developer (KYD)*[3]. O projeto usa principalmente licenças de conteúdo aberto *MIT*[4], *GPLv3*[5] e *CC-BY-NC 4.0*[6] e open content. A tradução e localização usa a plataforma *Transifex*[7].

GALILEL COIN

A Galilel Coin (GALI e zGALI) é uma moeda de criptografia digital Proof-of-Stake de prova pública e privada de código aberto para transações rápidas (usando o SwiftX), privadas (protocolo *Zerocoin*[8]) e micro transações seguras. Nosso principal objetivo é

criar uma rede descentralizada totalmente segura e anônima para executar aplicativos, que não dependem de nenhum controle central do órgão. Por ter um sistema distribuído, milhares de usuários serão responsáveis por manter o aplicativo e os dados, de modo que não haja um único ponto de falha.

PROBLEMAS E SOLUÇÕES

A notoriedade da tecnologia blockchain gera enorme interesse, ganhando popularidade em todo o mundo e é usado por muitas empresas para diferentes propósitos além do dinheiro digital. No entanto, usá-lo como base para serviços de pagamento exige recursos específicos para validar, armazenar e verificar milhares de transações. Embora isso já esteja resolvido usando o algoritmo de consenso existente para gerar blocos na cadeia, existem várias áreas fracas nas implementações atuais de blockchain para atingir a adoção em massa do dinheiro digital.

DINÂMICA ZEROCOIN PROOF-OF-STAKE (dzPoS)

Zerocoin Proof-of-Stake (zPoS) foi o recurso de blockchain mais inovador introduzido em 2018 pela equipe de desenvolvimento da PIVX. No entanto, a implementação técnica feita de uma maneira específica para o seu blockchain, não permite a fácil adoção para os outros projetos pois sua estrutura de recompensa está estaticamente incluída no código-fonte.

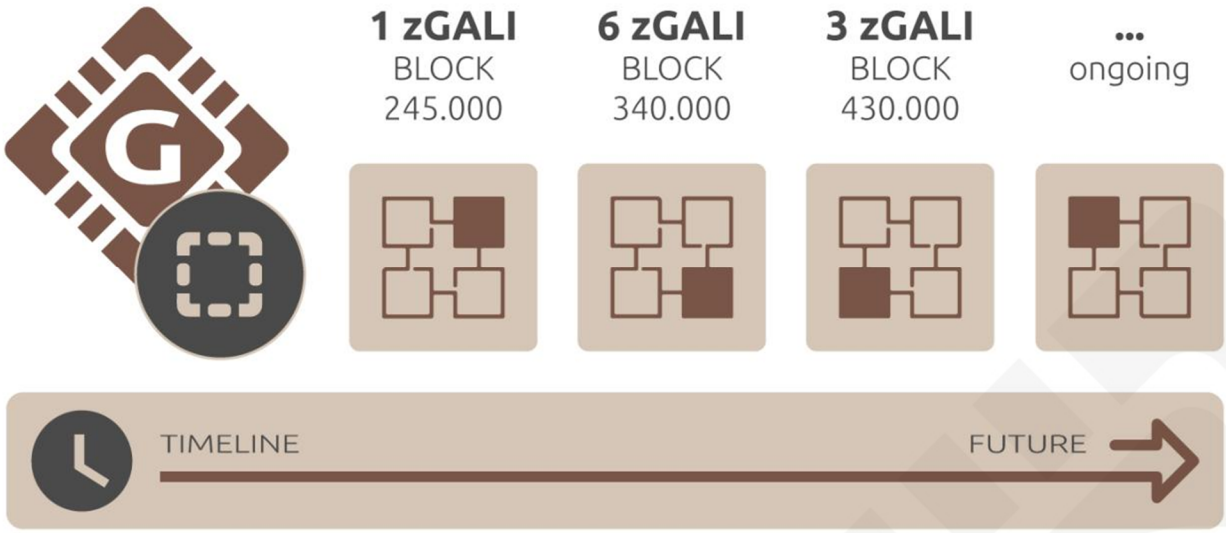

Figura 1. Dinâmica Zerocoin Proof-of-Stake recompensa baseada na fase blockchain.

Na Galilel, nós implementamos uma versão dinâmica do Zerocoin Staking. Zerocoin staking gera recompensas em denominações, que representam um valor inteiro. A menor denominação possível é uma [1]. Na primeira versão - fase de aquecimento - usamos sempre o menor valor de denominação para fins de teste. A desvantagem dessa abordagem é que o Zerocoin staking é muito intensivo em CPU e a probabilidade de gerar um bloco órfão é maior, pois uma stake de moeda pública pode resolver o bloqueio posteriormente, mas distribuí-lo à cadeia anteriormente. Na segunda versão - fase completa - nós determinamos automaticamente a melhor estrutura de denominação com base no valor de recompensa do bloco. Isso reduz significativamente a probabilidade de gerar blocos órfãos.

Galilel

PROVA DE TRANSAÇÃO (ghPoT)

Na economia tradicional, com transferências de dinheiro entre contas bancárias, é possível especificar um assunto para que o destinatário possa atribuir o valor a uma fatura específica. Isso não é possível nas implementações de carteira atuais. Ele permite especificar um comentário ou comentário para o valor, que não faz parte da transação e só é armazenado localmente. Para atribuir uma fatura a um beneficiário específico, é necessário criar um endereço de carteira com um mapeamento de um para um entre os dois interessados.

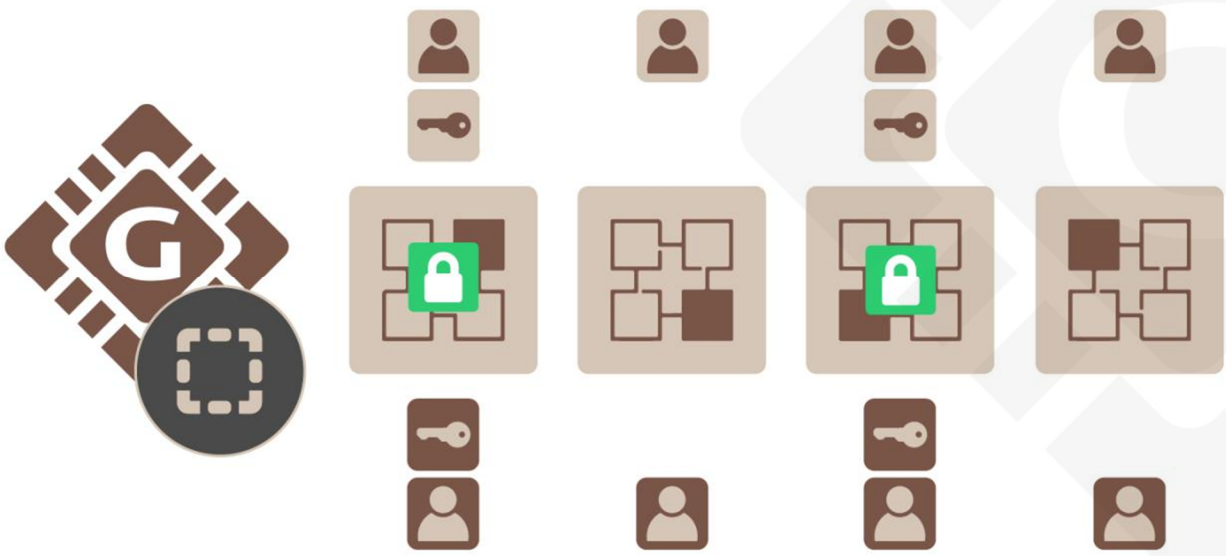

Figura 2. Prova de Transação com assunto criptografado.

Na Galilel, incluímos um campo de dados adicional e anexamos à transação, que é armazenada no bloco. É um campo criptografado e a descriptografia só é possível pelas carteiras, que negociaram a transação. Ele resolve o problema de atribuição de transação e permite que os gateways de processamento de pagamento identifiquem o beneficiário de uma fatura como é com as faturas fiat tradicionais.

PROOF-OF-STAKE HÍBRIDO (ghPoS)

Embora o PoS (Proof-of-Stake) seja um algoritmo de consenso ecologicamente correto, ele cria recompensas apenas enquanto a carteira estiver em execução. Uma solução para esse problema é inscrever-se em qualquer pool de prova de participação compartilhada e participação na nuvem. No entanto, a desvantagem é que o usuário precisa confiar no pool de staking e transferir uma quantidade específica de moedas para ele. Pode levar a uma situação em que uma enorme quantidade de moedas é armazenada em algumas carteiras. Esta é uma situação de risco para uma abordagem de rede descentralizada e é uma parte fundamental para chegar a um consenso. O staking privado, chamado Zerocoin Proof-of-Stake (zPoS), tem os mesmos problemas e limitações.

Figura 3. Possíveis maneiras de ganhar recompensas da rede Galilel.

Em Galilel, a solução para este problema será um algoritmo de consenso híbrido completo denominado Galilel Hybrid Proof-of-Stake (ghPoS). Nós estenderemos a Proof-of-Stake on-line com recursos móvel para o staking tanto público quanto

privado. O staking móvel está sempre ativo, com dez [5] por cento da recompensa em bloco paga se a carteira móvel encontrar um bloco. Neste caso noventa [90] por cento são pagos ao portador do masternode. As carteiras móveis funcionarão como um nó simples do blockchain com quantidade mínima de blocos igual à profundidade de reorganização.

ESTRUTURA HÍBRIDA DE RECOMPENSAS PROOF-OF-STAKE

TIPO DE STAKING[1]	STAKING	MASTERNODE
Online (GALI)	30%	70%
Online (zGALI)	60%	40%
Móvel (GALI)	10%	90%
Móvel (zGALI)	20%	80%

[1] O cálculo é baseado em 5 recompensas GALI > block 430,000

DEPÓSITOS A TERMO (gTD)

Enquanto o staking móvel depende da dificuldade da rede e da quantidade de moedas em carteira, a função *depósito a prazo*[9] permite bloquear moedas por um determinado período e gerar recompensas previsíveis.

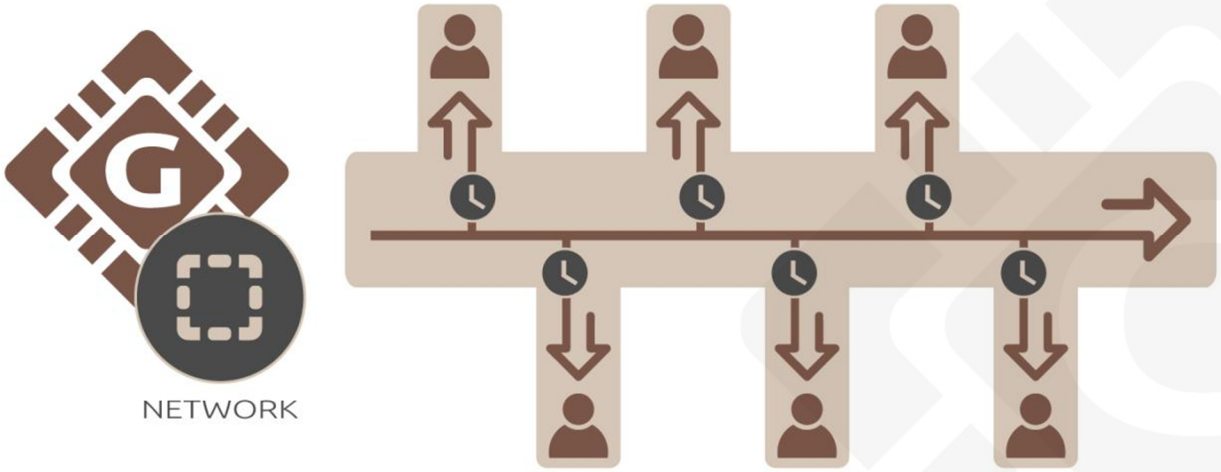

Figura 4. Depósito a prazo baseado em calendário em carteiras.

A quantidade mínima necessária de moedas para usar o Galilel Term Deposit (gTD) é de cinco mil [5,000] GALI. O período de ligação é de um [1] ano. A recompensa do bloco é de dez [10] por cento e as moedas empatadas das diferentes carteiras são ponderadas. Com um novo bloco em carteiras com moedas encadernadas, você obtém a quantia com base no seu peso. Até o final do período de depósito a prazo, esse prêmio é vinculado. Uma vez restrito, mover ou gastar moedas para compras não é possível, o cancelamento do depósito a prazo antes do prazo não é permitido. Isso efetivamente reduzirá o fornecimento de moedas durante o período do vínculo.

CONTROLE DE SUPRIMENTO MONETÁRIO (gMSC)

O controle da inflação é a parte mais desafiadora para o dinheiro digital ser reconhecido e aceito como alternativa ao dinheiro fiduciário. Sem qualquer mecanismo de controle, o valor de qualquer moeda digital é imprevisível. Isso leva a uma situação em que os investidores começam a apostar no valor e isso pode danificar seriamente o mercado em questão de horas e imediatamente elimina a possibilidade de colocar dinheiro digital no mercado como opção de pagamento aceita. Com o controle da inflação, acreditamos que as pessoas fora da esfera do dinheiro digital são atraídas para usá-lo, já que não há a necessidade de olhar todos os dias a sua carteira. Ao contrário dos bancos centrais em caso de moeda fiduciária, não haverá lugar central para assistir e manter a oferta monetária. Na Galilel, implementamos uma abordagem descentralizada para queimar moedas, o chamado mecanismo *Proof-of-Burn*[10] para moedas depositadas em público e privado. Embora este seja um passo necessário para controlar a circulação de dinheiro, os proprietários de masternodes têm a possibilidade de votar pela redução da recompensa ou pela queima completa durante um período específico para reduzir a geração de moedas.

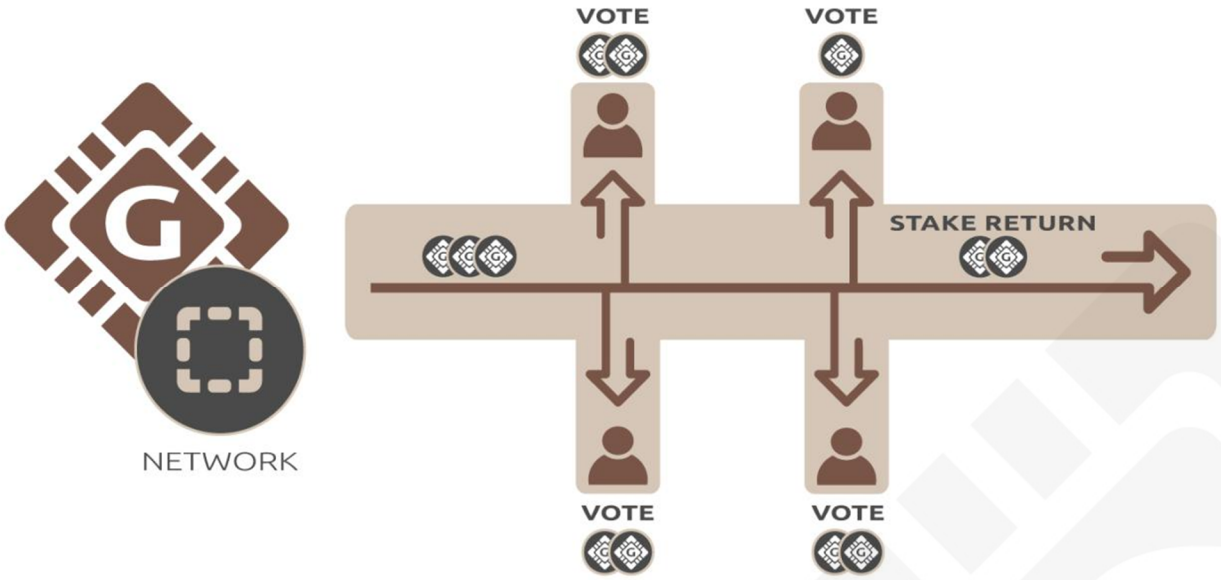

Figura 5. Votação da Masternode para reduzir a geração de recompensas.

Nós nomeamos Galilel Money Supply Control (gMSC), efetivamente Proof-of-Burn v2. Este mecanismo queima apenas recompensas, nunca depósitos a prazo e orçamentos de desenvolvimento. O período para a queima da moeda será de um [1] mês, nas etapas descritas na tabela de estrutura de queima de recompensa, diminuindo a oferta anual. Os detentores do Masternode são aplicáveis para votar todos os meses. A proposta pode ser feita uma vez por mês, começando uma [1] semana antes do término do período atual de vencimento da queima da recompensa. O blockchain aceita qualquer proposta a partir de mil [1000] GALI. Uma vez distribuída a proposta no blockchain, os detentores de masternode podem votar com o gasto adicional de um [1] ou mais GALI. A proposta com a maior quantidade de moedas e com mais de cinquenta [50] por cento de votos de masternode após o término do período da proposta, vencerá. Se o período de proposta terminar e for aceito, moedas trancadas em propostas são queimadas e o período de queima de prêmios começa no próximo

bloco de queima. Se os requisitos mínimos para a aceitação da proposta não forem alcançados, as moedas bloqueadas serão desbloqueadas.

ESTRUTURA DE QUEIMA DE RECOMPENSA

PERCENTUAL DE QUEIMA	QUANTIDADE QUEIMADA POR MÊS[1]
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

[1] O cálculo é baseado na recompensa de 5 GALI reward > block 430,000

INSTANTE EM MASTERNODES (gIOMN)

Masternodes já ganharam muita atenção na esfera do dinheiro digital. Embora muitas novas moedas criptográficas digitais tentem criar moedas de alto retorno (ROI) ridículas e falhem depois que a inflação das moedas entre em ação e distribuam recompensas desequilibradas entre masternodes e carteiras de staking, este não é o objetivo principal da execução de um masternode. Na Galilel, o principal caso de uso dos masternodes é proteger a rede, ao mesmo tempo em que tem a oportunidade de votar em aspectos futuros de desenvolvimento, bem como de manter a circulação de moedas. No entanto, o principal ponto fraco para implementações de masternode disponíveis é o requisito de ter o blockchain sincronizado e indexado em cada máquina que age como um masternode.

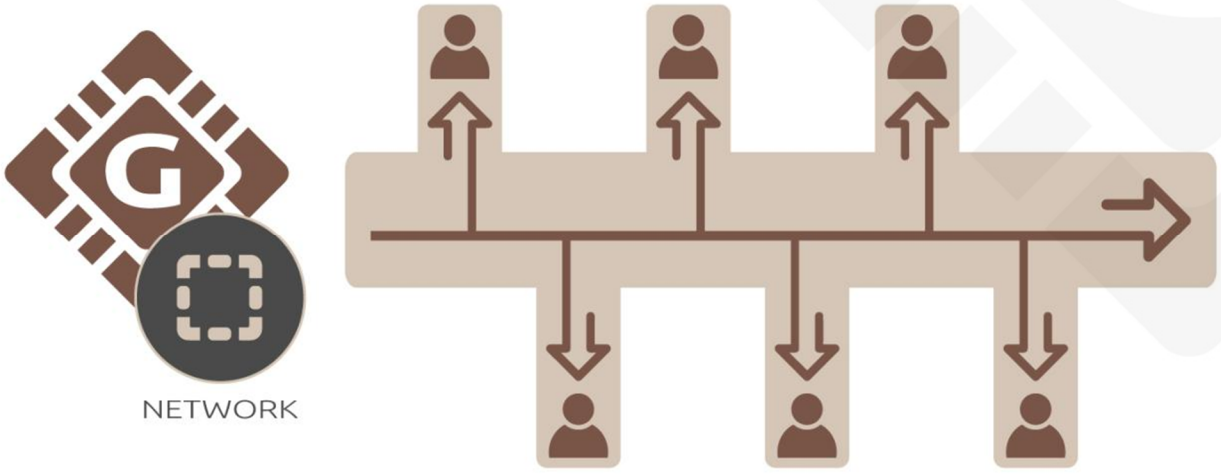

Figura 6. Múltiplos masternodes conectados a um único blockchain na nuvem.

O Galilel Instant On Masternode (gIOMN) resolve esse problema implementando um blockchain compartilhado para executar daemons de carteira *one-to-many*[11] em um

modelo de servidor cliente. É comparável ao modelo “Instant On” disponível no cliente *Electrum*[12].

Galilel

RECURSOS E ESPECIFICAÇÕES

ESPECIFICAÇÕES DA MOEDA	
Nome da moeda	Galilel
Código da moeda	GALI
Algoritmo de hash	Quark
Algoritmo de consenso	PoS + zPoS Hybrid
Tamanho do bloco	2 MB
Tempo por bloco	60 segundos (Recalculado em cada bloco)
RPC Port	36002
P2P Port	36001
Tipo	PoW / PoS / zPoS / MN
Idade mínima para Staking	2 horas
Maturidade	120 confirmações
Elegível para envoi	6 confirmações
Recompensas(até o bloco 1,500)	MN 60%, PoW 40%
Recompensas(até o bloco 205,000)	MN 60%, PoS 40%
Recompensas(desde o bloco 205,001)	MN 70%, PoS 30%
Último bloco PoW	1,500
Garantia por masternode	15,000
Suprimento Máximo de Moedas (Janeiro 2020)	19,035,999 GALI
Suprimento Máximo de Moedas (Janeiro 2030)	45,315,999 GALI

Suprimento Máximo de Moedas (Janeiro 2040)	71,595,999 GALI
Suprimento Máximo de Moedas (Janeiro 2050)	97,875,999 GALI
Suprimento dinâmico de moedas	Taxas de transação e taxas de mineração zGALI são queimadas
Endereço de Doação da Comunidade	UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX
Orçamento Dev (do bloco 250,001)	10% in monthly superblock

ZEROCOIN ESPECIFICAÇÕES

Zerocoin v1 ativação	bloco 245,000
Zerocoin v2 ativação	bloco 245,000
zGALI Automint	10%
zGALI Recompensas(desde bloco 245,001)	1 zGALI
zGALI Recompensas(desde bloco 340,001)	MN 40%, zPoS 60%
zGALI Recompensas(desde bloco 430,001)	MN 40%, zPoS 60%
zGALI Denominadores	1, 5, 10, 50, 100, 500, 1000, 5000
Módulo Acumulador	RSA-2048
Maturidade	240 confirmations
Elegível para envio	20 confirmations
Taxas(mineração)	0,01 GALI por denominação zGALI minerada
Taxas(gasto)	Sem taxa

Galilel

RECOMPENSAS DE PROOF-OF-WORK

ALTURA DO BLOCO	RECOMPENSA	MN	POW	SUPRIMENTO	PERIODO	FINAL DO ESTÁGIO
Bloco 1	220,000	60%	40%	220,000	0 dias	2018-05-25
Bloco 2 – 1,500	1	60%	40%	221,499	1 dia	2018-05-26

RECOMPENSAS DE PROOF-OF-STAKE

ESTÁGIOS	ALTURA DO BLOCO	REC ...	MN	POS	QUANTIA	PERIODO	FINAL DO ESTÁGIO
Estágio 1	1,501-12,000	100	60%	40%	1,271,399	7 dias	2018-06-02
Estágio 2	12,001-22,000	90	60%	40%	2,171,309	7 dias	2018-06-09
Estágio 3	22,001-42,000	80	60%	40%	3,771,229	14 dias	2018-06-23
Estágio 4	42,001-100,000	70	60%	40%	7,831,159	40 dias	2018-08-02
Estágio 5	100,001-160,000	60	60%	40%	11,431,099	42 dias	2018-09-13
Estágio 6	160,001-205,000	50	60%	40%	13,681,049	31 dias	2018-10-14
Estágio 7	205,001-250,000	25	70%	30%	14,806,024	31 dias	2018-11-14
Estágio 8	250,001-340,000	13.5	70%	30%	16,156,009	62 dias	2019-01-15
Estágio 9	340,001-430,000	10	70%	30%	17,055,999	62 dias	2019-03-18
Estágio X	430,001-contínuo	5	70%	30%	contínuo	contínuo	contínuo

ANALISE COMPETITIVA

Todos os dias nascem novos projetos de criptomoedas, principalmente moedas de serviço para uma finalidade específica. Embora seja um cenário válido, isso limita o caso de uso da moeda a um mercado e tamanho específicos. No final, isso limita o valor da moeda. O mercado de criptomoedas que compartilham o mesmo conjunto de recursos com diferentes quantidades de dinheiro digital e diferentes recompensas de bloco é supersaturado. No passado, alguns projetos com ideias únicas e um futuro brilhante nasceram. A Galilel continuará esta tendência e melhorará a blockchain usada para dinheiro digital enquanto constrói uma criptomoeda de uso geral fácil de usar para adoção em massa no mercado.

Galilel

CARACTERÍSTICAS	GALILEL	DASH	PIVX	ROI COIN
Staking Público	✓	✗	✓	✗
Staking Privado	✓	✗	✓	✗
Envio instantâneo	✓	✓	✓	✗
Envio Privado	✓	✓	✓	✗
Masternodes	✓	✓	✓	✗
Votação de Governança Descentralizada	✓	✓	✓	✗
Distribuição de Recompensa Variável[1]	✗	✗	✓	✗
Dinâmica Zerocoin Proof-of-Stake	✓	✗	✗	✗
Prova de Transação	✓	✗	✗	✗
Queima variável de recompensa	✓	✗	✗	✗
Blockchain Desconectado	✓	✗	✗	✗
Móvel Proof-of-Stake	✓	✗	✗	✗
Depósitos a Termo	✓	✗	✗	✓

[1] Possível implementar em Galilel usando o algoritmo Seesaw

ROTEIRO DE DESENVOLVIMENTO

O desenvolvimento da moeda Galilel é crítico para o blockchain do futuro. Algum código já foi escrito e está em teste interno. O recurso Galilel Instant On Masternode (gIOMN) está quase pronto, enquanto o Galilel Hybrid Proof-of-Stake (ghPoS) requer desenvolvimento adicional e ciclos de teste após a ativação planejada do Zerocoin v2 no bloco 245,000. Nosso roteiro inclui principalmente apenas itens de desenvolvimento; nós acreditamos que é necessário definir metas, expectativas e resultados adequados, em vez de colocar itens de marketing bem ajustados nele.

- 2018 – Base de código Fork PIVX e lançamento MAINNET. Criando canal no *Discord*[13] para votação da comunidade e pré-anúncio no forum *BitcoinTalk*[14].
- 2018 – Listagem nos primeiros sites ranking e echanges. Implementação dos resultados de votação da comunidade em relação à distribuição de recompensas, modificação da estrutura de recompensas e garantias de masternode na v2.0. Equipe de design criando a marca e o site da Galilel com cores da marca, logotipos e guia da marca para desenvolvedores de aplicativos. Além do desenvolvimento e do design, passaremos pela verificação pública do Know Your Developer (KYD).
- 2018 – Habilite e libere o TESTNET, dando aos desenvolvedores a capacidade de testar novos códigos blockchain e usuários para testar recursos de ponta. Refatorar a base de código Galilel para a versão mais recente do PIVX 3.1.1 e liberar v3.0 com ativação Zerocoin v1 e v2 no bloco 245.000 e trabalhar com a Organização Autônoma Descentralizada (DAO) para votação de blockchain enquanto mantém o blockchain e a rede compatíveis. Ative o Zerocoin Proof-of-Stake (zPoS) para mineração privada e libere a v3.1. Criação e lançamento de white paper para o Galilel Coin, juntamente com o novo anúncio no fórum do BitcoinTalk.
- 2019 – Conclua a implementação do recurso Galilel Instant On Masternode (gIOMN) e prossiga com a Disponibilidade Geral (GA) da v4.0. Esta atualização irá realizar um

hard-fork da blockchain e é obrigatória. Desenvolvimento de carteira móvel começando no final do primeiro trimestre após o lançamento do Galilel Core.

- 2019 – Concluir a implementação da Galilel Hybrid Proof-of-Stake (ghPoS) público e privado. Publicaremos o bloco de ativação assim que nos aproximarmos da data de lançamento da v5.0. Esta atualização irá criar um hard-fork na blockchain e é obrigatória. Lançamento de carteira móvel da v1.0. No final do segundo trimestre, iniciamos o desenvolvimento da carteira móvel da próxima geração e incluiremos o Galilel Hybrid Proof-of-Stake (ghPoS).
- 2019 – O recurso Galilel Term Deposit (gTD) ficará disponível para o público com a carteira v5.1. Esse recurso depende da Galilel Hybrid Proof-of-Stake (ghPoS) e será desenvolvido posteriormente. Esta atualização criará um hadr-fork na blockchain e é obrigatória. Vamos publicar o bloco de ativação assim que chegarmos perto da data de lançamento.
- 2019 – O Controle de Fornecimento de Dinheiro da Galilel (gMSC) está pronto para produção e prosseguimos com a Disponibilidade Geral (GA) da v6.0. Esta atualização criará um hard-fork na blockchain e é obrigatória. Vamos publicar o bloco de ativação assim que chegarmos perto da data de lançamento. No final do quarto trimestre, publicamos a carteira móvel v2.0 com o recurso Galilel Term Deposit (gTD).
- 2020 – Lançamento de carteira móvel completa da versão v3.0 com Galilel Money Supply Control (gMSC).

Enquanto o roteiro acima é nítido e coloca o foco no blockchain, a equipe tem várias outras idéias em mente para melhorias tecnológicas adicionais para simplificar o uso da carteira. Uma dessas áreas fracas é a carteira Qt embutida. Para uma melhor interoperabilidade de plataforma, é necessário substituí-lo por um servidor web

embutido usando uma estrutura frontend que oferece a melhor experiência ao usuário.

AJUDA

Mesmo que estejamos comprometidos com nossas metas de desenvolvimento de longo prazo, qualquer um pode ajudar ou ajudar nos objetivos do projeto. Embora o desenvolvimento seja uma parte muito importante, qualquer um que possa ajudar com marketing, escrever artigos, explicar recursos para pessoas não técnicas é bem-vindo.

LINKS IMPORTANTES

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

APÊNDICE

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