GALILEL CORE

Dynamic Zerocoin Proof-of-Stake, Proof-of-Transaction e votazione
Masternode per la distruzione delle ricompense nel tempo

White Paper v1.9

Maik Broemme[1], Gennaio 2019

Sommario

Sintesi

Mentre le valute fiat hanno già definito e mostrato gli standard economici per centinaia di anni, la situazione con il denaro digitale è diversa. Il denaro digitale è un investimento ad alto rischio con un valore imprevedibile e team di sviluppo in via di estinzione che lasciano blockchain orfane. I governi hanno identificato questo problema e le nuove regolamentazoni per le ICO (Initial Coin Offering) lo risolveranno nei prossimi anni. Inoltre, le valute digitali, che implementano caratteristiche uniche nella propria blockchain, hanno un'alta probabilità di definire gli standard della moneta digitale del futuro. Galilel sarà parte di questo processo implementando le caratteristiche uniche descritte in questo documento.

Introduzione

Galilel Coin è una cryptovaluta spinta dalla comunità con piena trasparenza e che utilizza un metodo di sviluppo pubblico. Le relazioni di fiducia tra gli investitori e il team di progetto sono la chiave del successo. Perciò, abbiamo creato un'organizzazione GitHub denominata *Galilel-Project*[2], che tiene traccia di tutte le nostre attività di sviluppo in archivi pubblici, includendo tutto il nostro codice back-end e superando la verifica pubblica *Know Your Developer (KYD)*[3]. Il progetto utilizza principalmente open source *MIT*[4], *GPLv3*[5] e *CC-BY-NC 4.0*[6] e licenze open content. La traduzione e la localizzazione utilizzano la piattaforma *Transifex*[7].

Galilel Coin

Galilel Coin (GALI and zGALI) è una cryptovaluta digitale pubblica e privata open source, basata su Proof-of-Stake per micro transazioni rapide (tramite SwiftX), private (protocollo Zerocoin[8]) e sicure. Il nostro obiettivo principale è creare una rete decentralizzata completamente sicura e anonima per eseguire applicazioni che non si basano sul controllo da parte di un organismo centrale. Avendo un sistema distribuito, migliaia di utenti saranno responsabili della manutenzione dell'applicazione e dei dati, in modo da non avere un singolo punto debole.

Problemi e Soluzioni

Il clamore per la tecnologia blockchain genera enorme interesse, guadagnando popolarità in tutto il mondo ed è utilizzata da molte aziende per diversi scopi oltre quello del denaro digitale. Tuttavia, utilizzandolo, come base per i servizi di pagamento sono richieste caratteristiche specifiche per convalidare, archiviare e verificare migliaia di transazioni. Sebbene questo sia già stato risolto utilizzando l'algoritmo di consenso esistente per generare blocchi nella catena, esistono diverse aree deboli nelle attuali implementazioni della blockchain per ottenere un' adozione di massa della moneta digitale.

Dynamic Zerocoin Proof-of-Stake (dzPoS)

Zerocoin Proof-of-Stake (zPoS) è stata la funzione di blockchain più innovativa introdotta nel 2018 dal team di sviluppo PIVX. Tuttavia, l'implementazione tecnica è fatta in un modo specifico per la loro blockchain e non consente una facile adozione ad altri in quanto la loro sistema di ricompense è staticamente incluso nel codice sorgente.

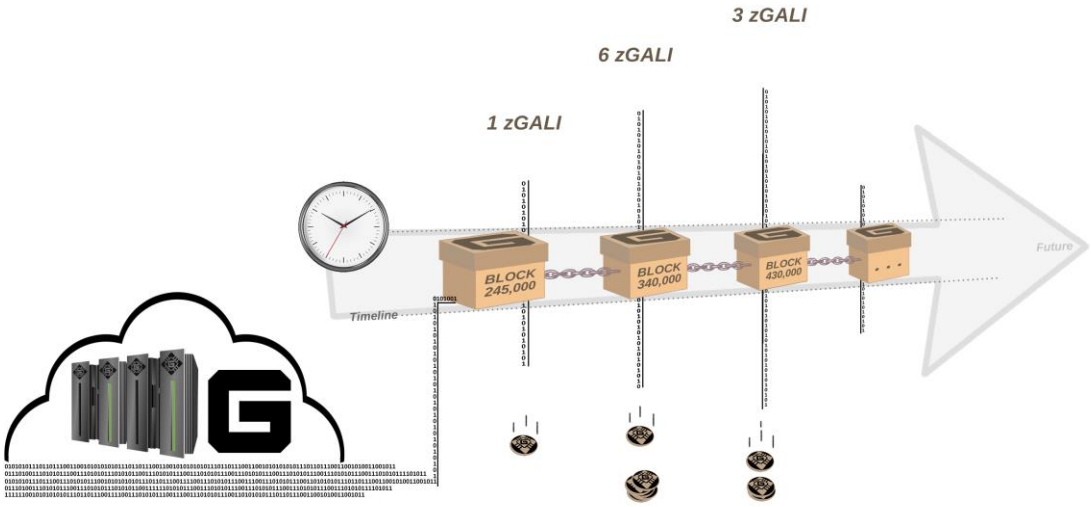

Figura 1. Dynamic Zerocoin Proof-of-Stake ricompense basate sulla fase della blockchain.

In Galilel, implementiamo una versione dinamica dello staking di Zerocoin. Lo staking di Zerocoin genera ricompense in denominazioni, che rappresentano un valore intero. La denominazione più piccola possibile è uno [1]. Nella prima versione - fase di riscaldamento - usiamo sempre il valore di denominazione più piccolo a scopo di test. Lo svantaggio di questo approccio è che lo staking di Zerocoin è molto intenso per la

CPU e la probabilità di generare un blocco orfano è più alta in quanto una moneta pubblica può risolvere il blocco in seguito, ma distribuirlo alla catena in anticipo. Nella seconda versione - fase completa - determiniamo automaticamente la struttura di denominazione ottimale in base all'importo della ricompensa del blocco. Ciò riduce significativamente la probabilità di generare blocchi orfani.

Proof-of-Transaction (ghPoT)

Nell'economia tradizionale con i trasferimenti di denaro tra conti bancari, è possibile specificare un argomento in modo che il destinatario possa assegnare l'importo a una specifica fattura. Nelle attuali implementazioni del portafoglio non è possibile. È permesso specificare un commento o un valore da commentare, che non fa parte della transazione ed è solo memorizzato localmente. Per assegnare una fattura a un particolare beneficiario è necessario creare un indirizzo del portafoglio con una mappatura one-to-one tra le due parti interessate.

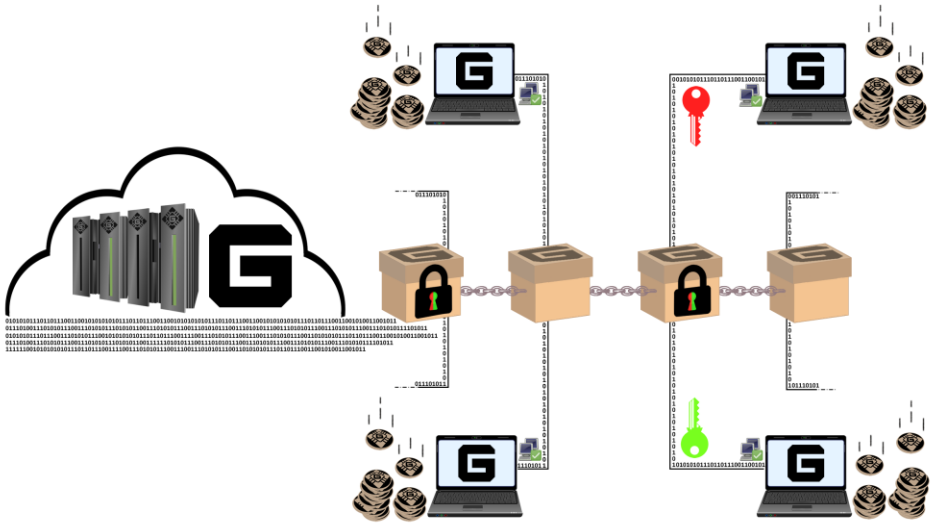

Figura 2. Proof-of-Transaction con contenuto criptato.

In Galilel, è previso un campo dati aggiuntivo collegato alla transazione, che è memorizzata nel blocco. È un campo crittografato e la decrittografia è possibile solo tramite i portafogli, che hanno generato la transazione. Risolve il problema dell'assegnazione delle transazioni e consente ai gateway di elaborazione dei pagamenti di identificare il beneficiario di una fattura come avviene con le fatture tradizionali in valuta fiat.

Hybrid Proof-of-Stake (ghPoS)

Sebbene Proof-of-Stake (PoS) sia un algoritmo di consenso rispettoso dell'ambiente, genera ricompense solo se il wallet desktop è in esecuzione. Una soluzione a questo problema è iscriversi a qualsiasi pool di Proof of Stake condiviso e partecipare al cloud. Tuttavia, lo svantaggio è che l'utente deve fidarsi della staking pool e deve trasferirvi una quantità specifica di monete. Ciò può portare a situazioni in cui un'enorme quantità di monete viene memorizzata in pochi portafogli. Questo è uno scenario debole per un approccio di rete decentralizzata ed è una punto fondamentale per raggiungere il consenso. Il sistema di staking privato, il cosiddetto Zerocoin Proof-of-Stake (zPoS), ha gli stessi problemi e limiti.

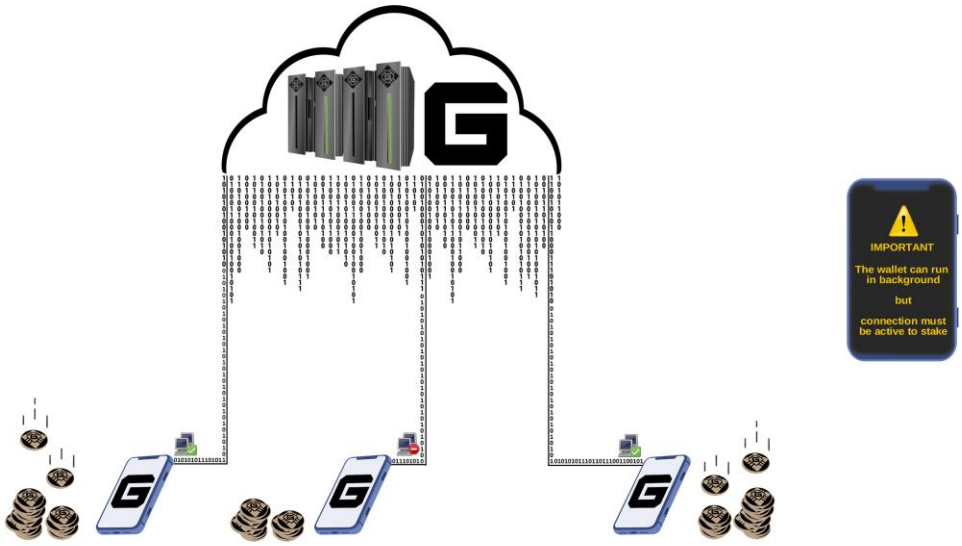

Figura 3. Possibili modi per guadagnare premi dalla rete Galilel.

In Galilel, la soluzione a questo problema sarà un algoritmo di consenso ibrido completo denominato Galilel Hybrid Proof-of-Stake (ghPoS). Estenderemo Proof-of-Stake con funzionalità di mobile staking sia per le monete pubbliche che per quelle private. Il mobile staking è sempre attivo con il dieci [10] percento della ricompensa del blocco pagato se il mobile wallet trova un blocco. In questo caso il novanta [90] percento è stato pagato al detentore del masternode. I portafogli mobili funzioneranno come un nodo leggero della blockchain con una quantità minima di blocchi pari alla profondità della riorganizzazione.

Sistema delle ricompense Hybrid Proof-of-Stake		
Tipo di Staking[1]	Staking	Masternode
Online (GALI)	30%	70%
Online (zGALI)	60%	40%
Mobile (GALI)	10%	90%
Mobile (zGALI)	20%	80%

[1] Calcoli basati su ricompensa di 5 GALI > blocco 430000

Term Deposits (gTD)

Mentre il mobile staking dipende dalla difficoltà della rete e dalla quantità di monete impiegate, la funzione *Term Deposit*[9] consente di vincolare le monete per un certo periodo e generare ricompense.

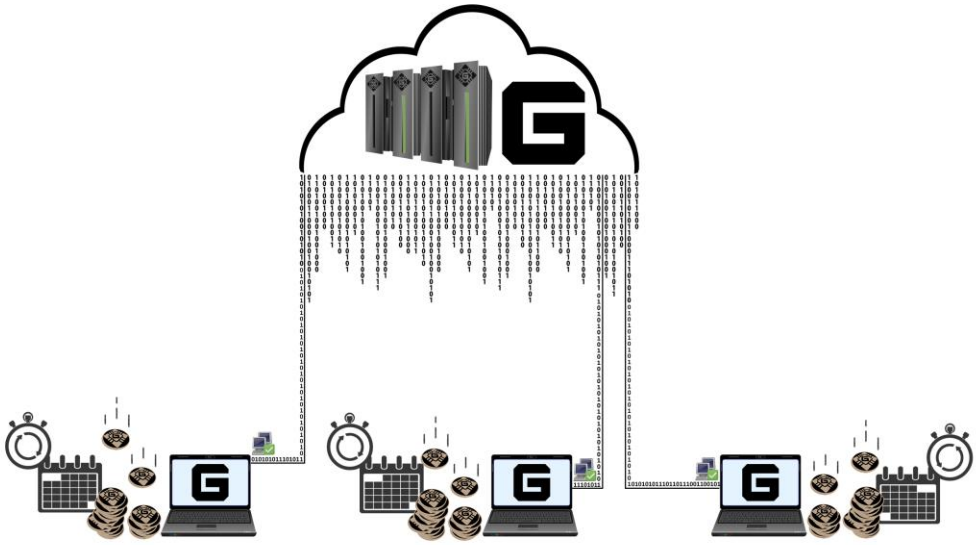

Figure 4. Term Deposits basato su calendario in un portafoglio offline.

La quantità minima richiesta di monete per utilizzare Galilel Term Deposit (gTD) è di **cinquemila [5.000]** GALI. Il periodo di vincolo è di **un [1]** anno. La ricompensa del blocco è di **dieci [10]** percento e le monete vincolate dei diversi portafogli vengono ponderate. Con un nuovo blocco nei wallets aventi le monete vincolate, si ottiene l'importo in base al loro peso. Fino alla fine del periodo del deposito a termine, questo premio è vincolato. Una volta vincolato, spostare o spendere monete per gli acquisti non è possibile, la cancellazione del deposito a termine prima della scadenza non è consentita. Ciò ridurrà efficacemente la fornitura di monete durante il periodo del vincolo.

Money Supply Control (gMSC)

Il controllo dell'inflazione è la parte più difficile per il denaro digitale per essere riconosciuto ed accettato come alternativa alla moneta legale. Senza alcun meccanismo di controllo, il valore di qualsiasi moneta digitale è imprevedibile. Ciò porta a una situazione in cui gli investitori iniziano a scommettere sul valore e questo può seriamente danneggiare il mercato in poche ore e eliminare immediatamente la possibilità di mettere il denaro digitale sul mercato come opzione di pagamento accettata. Con il controllo dell'inflazione, riteniamo che le persone al di fuori della sfera del denaro digitale siano attratte a usarlo, poiché non è necessario guardare ogni giorno il proprio portafoglio. A differenza delle banche centrali e delle valute fiat, non ci sarà un luogo centrale per osservare e gestire l'emissione di moneta. In Galilel, implementiamo un approccio decentralizzato per distruggere moneta, il cosiddetto meccanismo *Proof-of-Burn*[10] per monete private e pubbliche. Sebbene questo sia un passo necessario per controllare la circolazione del denaro, i proprietari dei masternode hanno la possibilità di votare per la riduzione della ricompensa o la distruzione completa per un periodo specifico, per ridurre la generazione di nuova moneta.

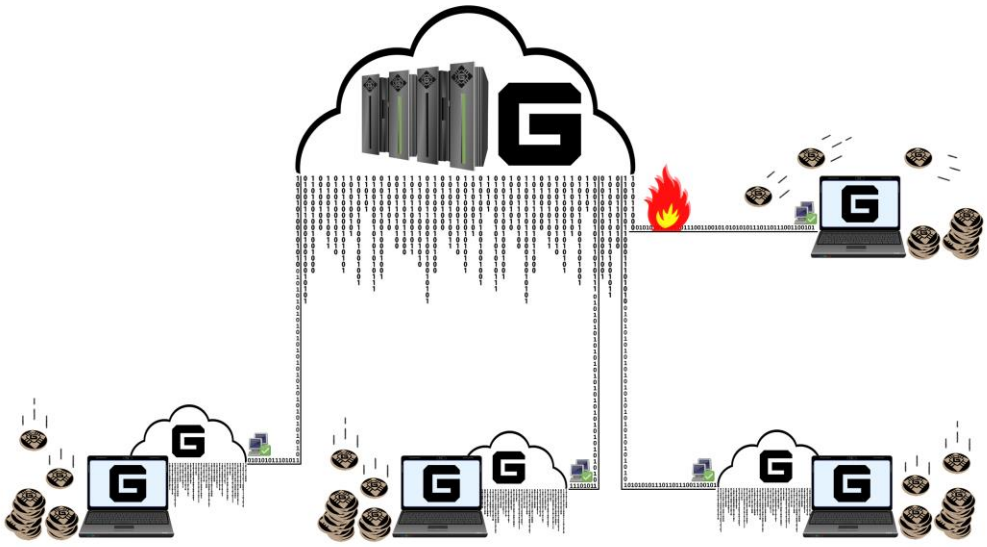

Figure 5. Votazione Masternode per ridurre la generazione delle ricompense.

Lo chiamiamo Galilel Money Supply Control (gMSC), effettivamente Proof-of-Burn v2. Questo sistema distrugge solo ricompense, non il *Term Deposit* e il budget di sviluppo. Il periodo per la distruzione delle monete sarà di un [1] mese, in fasi descritte nella tabella delle strutture che distruggono i premi diminuendo l'offerta annuale. I possessori di Masternode sono autorizzati a votare ogni mese. La proposta può essere presentata

una volta al mese, iniziando una [1] settimana prima della fine del periodo di distruzione. La blockchain accetta qualsiasi proposta a partire da mille [1000] GALI. Una volta che la proposta è stata distribuita nella blockchain, i detentori di Masternode possono votare spendendo un ulteriore [1] o più GALI. La proposta con il maggior numero di monete e con oltre il cinquanta [50] percento di voti masternode al termine del periodo della proposta, vincerà. Se il periodo di proposta termina ed è accettato, le monete bloccate nelle proposte vengono distrutte e il periodo di ricompense per la distruzione inizia dal prossimo blocco di distruzione. Se non vengono raggiunti i requisiti minimi per l'accettazione della proposta, le monete bloccate saranno sbloccate.

Sistema delle Ricompense di Distruzione	
Percentuale di Distruzione	Quantità di Distruzione per mese[1]
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

[1] Calcoli basati su ricompensa di 5 GALI > blocco 430000

Instant On Masternodes (gIOMN)

I Masternodes hanno già attirato molte attenzioni nella sfera del denaro digitale. Molte nuove cryptovalute digitali cercano di creare monete ridicole con un alto return of investment (ROI) e falliscono quando subentra l'inflazione, inoltre hanno una distribuzione sbilanciata della ricompensa tra i masternodes e i wallets; e questo non è lo scopo principale per l'esecuzione di un masternode. In Galilel, il principale scopo dei masternodes è quello di proteggere la rete, avendo l'opportunità di votare sugli aspetti futuri dello sviluppo e di mantenere la circolazione delle monete. Tuttavia, il principale punto debole per le implementazioni dei masternode disponibili è il requisito di avere la blockchain sincronizzata e indicizzata su ogni macchina che opera da masternode.

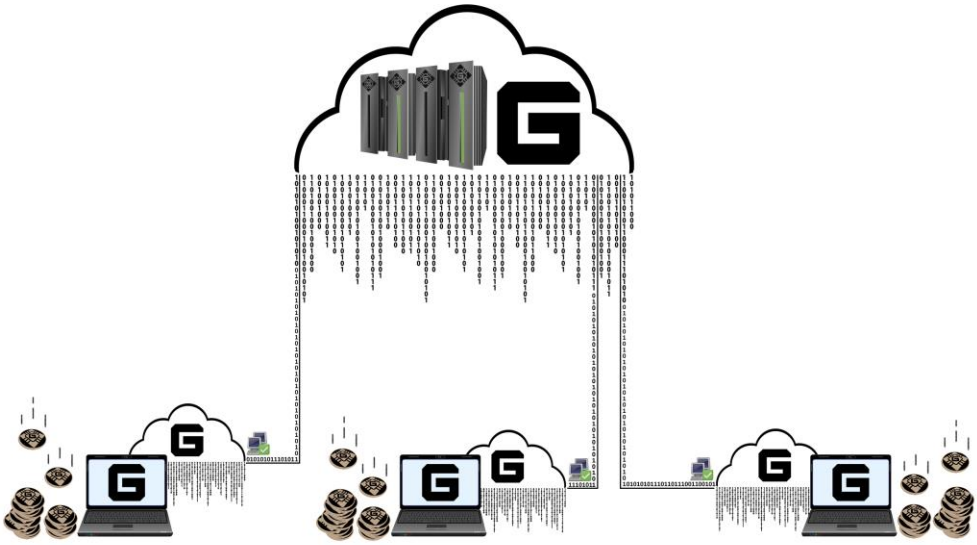

Figura 6. Alcuni masternodes connessi a una singola blockchain nel Cloud.

Galilel Instant On Masternode (gIOMN) risolve questo problema implementando una blockchain condivisa per eseguire i deamons wallet *one-to-many*[11] in un modello client-to-server. É paragonabile al modello “Instant On” disponibile nel client *Electrum*[12].

Caratteristiche e Specifiche

Caratteristiche della Moneta	
Nome della Moneta	Galilel
Ticker della Moneta	GALI
Algoritmo di Hash	Quark
Algoritmo di Consenso	PoS + zPoS Hybrid
Dimensione del Blocco	2 MB
Tempo del Blocco	60 Secondi (Re-targeting di ogni blocco)
Porta RPC	36002
Porta P2P	36001
Tipo	PoW / PoS / zPoS / MN
Tempo minimo pre-staking	2 Ore
Tempo di maturazione	120 conferme
Invio Idoneità	6 conferme
Ricompense (fino al blocco 1500)	MN 60%, PoW 40%
Ricompense (fino al blocco 205000)	MN 60%, PoS 40%
Ricompense (dal blocco 205001)	MN 70%, PoS 30%
Ultimo Blocco PoW	1,500
Masternode Collateral	15,000
Fornitura Massima (Gennaio 2020)	19,035,999 GALI
Fornitura Massima (Gennaio 2030)	45,315,999 GALI
Fornitura Massima (Gennaio 2040)	71,595,999 GALI
Fornitura Massima (Gennaio 2050)	97,875,999 GALI
Fornitura di moneta dinamica	Commissioni di transazione & commissioni di conio di zGALI vengono distrutte
Indirizzo delle donazioni	UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX
Dev Budget (dal blocco 250001)	10% in superblocchi mensili

Caratteristiche della Zerocoin	
Attivazione Zerocoin v1	blocco 245,000
Attivazione Zerocoin v2	blocco 245,000
zGALI Autoconiati	10%
zGALI Ricompense (dal blocco 245,001)	1 zGALI
zGALI Ricompense (dal blocco 340,001)	MN 40%, zPoS 60%
zGALI Ricompense (dal blocco 430,001)	MN 40%, zPoS 60%
zGALI Denominatori	1, 5, 10, 50, 100, 500, 1000, 5000
Modulo di accumulo	RSA-2048
Maturazione	240 conferme
Invio Idoneità	20 conferme
Commissioni (conio)	0.01 GALI per denominazione zGALI coniata
Commissioni (spesa)	Nessuna Commissione

Ripartizione delle Ricompense da Proof-of-Work						
Altezza del Blocco	Ricompensa	MN	PoW	Fornitura	Periodo	Fase Fine
Blocco 1	220,000	60%	40%	220,000	0 giorni	2018-05-25
Blocco 2 – 1,500	1	60%	40%	221,499	1 giorni	2018-05-26

Ripartizione da Proof-of-Stake							
Fasi	Altezza del Blocco	Ric...	MN	PoS	Fornitura	Periodo	Fase Fine
Fase 1	1,501-12,000	100	60%	40%	1,271,399	7 giorni	2018-06-02
Fase 2	12,001-22,000	90	60%	40%	2,171,309	7 giorni	2018-06-09
Fase 3	22,001-42,000	80	60%	40%	3,771,229	14 giorni	2018-06-23
Fase 4	42,001-100,000	70	60%	40%	7,831,159	40 giorni	2018-08-02
Fase 5	100,001-160,000	60	60%	40%	11,431,099	42 giorni	2018-09-13
Fase 6	160,001-205,000	50	60%	40%	13,681,049	31 giorni	2018-10-14
Fase 7	205,001-250,000	25	70%	30%	14,806,024	31 giorni	2018-11-14
Fase 8	250,001-340,000	13.5	70%	30%	16,156,009	62 giorni	2019-01-15
Fase 9	340,001-430,000	10	70%	30%	17,055,999	62 giorni	2019-03-18
Fase X	430,001-in corso	5	70%	30%	in corso	in corso	in corso

Analisi Competitiva

Ogni giorno nascono nuovi progetti di criptovaluta digitale, per lo più valute di servizio per uno scopo specifico. Sebbene sia uno scenario valido, ciò limita l'utilizzo della moneta a un particolare mercato e dimensione. Questo alla fine, limita il valore della valuta. Il mercato delle cryptovalute con simili caratteristiche e diverse quantità di moneta e ricompense a blocchi è sovrasaturato. In passato sono nati alcuni progetti con idee uniche e un futuro brillante. Galilel continuerà questa tendenza e migliorerà la blockchain utilizzata per il denaro digitale mentre genererà una criptovaluta di uso generale e di facile utilizzo per l'adozione di massa nel mercato.

Caratteristica	Galilel	Dash	PIVX	ROI Coin
Staking Pubblico	✓	✗	✓	✗
Staking Privato	✓	✗	✓	✗
Instant Send	✓	✓	✓	✗
Private Send	✓	✓	✓	✗
Masternodes	✓	✓	✓	✗
Votazione Governance Decentralizzata	✓	✓	✓	✗
Distribuzione Variabile delle Ricompense[1]	✗	✗	✓	✗
Dynamic Zerocoin Proof-of-Stake	✓	✗	✗	✗
Proof-of-Transaction	✓	✗	✗	✗
Distruzione Variabile delle Ricompense	✓	✗	✗	✗
Blockchain Disconnessa	✓	✗	✗	✗
Mobile Proof-of-Stake[2]	✓	✗	✗	✗
Term Deposits	✓	✗	✗	✓

[1] Possibile implementare in Galilel usando l'algoritmo Seesaw

Roadmap dello Sviluppo

Lo sviluppo di Galilel Coin è fondamentale per la blockchain del futuro. Alcuni codici sono già stati scritti e sono in test interni. La funzione Galilel Instant On Masternode (gIOMN) è quasi completa mentre la Galilel Hybrid Proof-of-Stake (ghPoS) richiede ulteriori cicli di sviluppo e test dopo l'attivazione programmata di Zerocoin v2 al blocco 245.000. La nostra roadmap include principalmente solo elementi di sviluppo; crediamo

che sia necessario definire obiettivi, aspettative e risultati accettabili piuttosto che mettere elementi di marketing ben accordati.

- Q2 2018 – fork dal codebase di PivX e avvio della MAINNET. Creazione del canale Discord[13] per il voto della community e pre-annuncio nel forum BitcoinTalk[14].
- Q3 2018 – Iscrizione al primo exchange e ai siti di ranking. Implementazione dei risultati dalla votazione della comunità relativa alla distribuzione delle ricompense, alla modifica della struttura delle stesse e al collateral masternode nella v2.0. Il Team di progettazione crea il marchio e il sito Web Galilel con colori, loghi e guide del marchio per gli sviluppatori di applicazioni. Oltre allo sviluppo e alla progettazione, passeremo alla verifica pubblica Know Your Developer (KYD).
- Q4 2018 – Abilitazione e rilascio della TESTNET, dando agli sviluppatori la possibilità di testare il nuovo codice blockchain e agli utenti di testare funzionalità all'avanguardia. Refactoring del codebase al sorgente PIVX 3.1.1 e rilascio della v3.0 con Zerocoin v1 e v2 attivazione al blocco 245.000 e votazione della Decentralized Autonomous Organization (DAO) per la blockchain mantenendo la stessa e la rete scalabili a ritroso. Abilitazione Zerocoin Proof-of-Stake (zPoS) per stake privato e rilascio della v3.1. Creazione e pubblicazione di white paper per Galilel Coin con un nuovo annuncio nel forum BitcoinTalk.
- Q1 2019 – Completare l'implementazione della funzione Galilel Instant On Masternode (gIOMN) e procedere con General Availability (GA) della v4.0. Questo aggiornamento causerà un hard-fork ed è obbligatorio. Sviluppo del Mobile Wallet a partire dalla fine del primo trimestre dopo il rilascio di Galilel Core.
- Q2 2019 – Completare l'implementazione di Galilel Hybrid Proof-of-Stake (ghPoS) per staking pubblico e privato. Pubblicheremo il blocco di attivazione non appena prossimi alla data di rilascio della v5.0. Questo aggiornamento causerà un hard-fork della catena ed è obbligatorio. Versione Mobile Wallet v1.0. Alla fine del secondo trimestre, iniziamo lo sviluppo del portafoglio mobile di prossima generazione e includiamo Galilel Hybrid Proof-of-Stake (ghPoS).
- Q3 2019 – La funzionalità Galilel Term Deposit (gTD) sarà disponibile al pubblico con wallet v5.1. Questa funzione dipende da Galilel Hybrid Proof-of-Stake (ghPoS) e verrà sviluppata successivamente. Questo aggiornamento causerà un

hard-fork della catena ed è obbligatorio. Pubblicheremo il blocco di attivazione non appena prossimi alla data di rilascio.

- Q4 2019 – Galilel Money Supply Control (gMSC) è pronto per la produzione e procediamo con General Availability (GA) della **v6.0**. Questo aggiornamento causerà un hard-fork della catena ed è obbligatorio. Pubblicheremo il blocco di attivazione non appena prossimi alla data di rilascio. Alla fine del quarto trimestre pubblichiamo il mobile wallet **v2.0** con la funzione Galilel Term Deposit (gTD).
- Q1 2020 – Versione completa del Mobile Wallet **v3.0** con Galilel Money Supply Control (gMSC).

Mentre la roadmap sopra è nitida e focalizzata sulla blockchain, il Team ha in mente diverse altre idee per ulteriori miglioramenti tecnologici per semplificare l'utilizzo del wallet. Una di queste aree deboli è il Qt Wallet integrato. Per una migliore interoperabilità della piattaforma, è necessario sostituirlo con un leggero webserver integrato utilizzando un framework di frontend che offra la migliore esperienza possibile all' utente.

Aiuto

Anche se ci impegniamo per i nostri obiettivi di sviluppo a lungo termine, chiunque può aiutare o aiutare gli obiettivi del progetto. Mentre lo sviluppo è una parte molto importante, chiunque possa aiutare con il marketing, scrivere articoli, spiegare le caratteristiche a persone non tecniche è il benvenuto.

Links Importanti

Website

https://galilel.cloud

Block Explorer (MAINNET)

https://explorer.galilel.cloud

Block Explorer (TESTNET)

https://explorer.testnet.galilel.cloud

Wallet

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

Discord

https://discord.galilel.cloud

Twitter

https://twitter.com/GalilelEN

Facebook

https://facebook.com/GalilelEN

YouTube

https://youtube.com/channel/UC26rKBciicXp33dK8NkALmg

BitcoinTalk Announcement

https://bitcointalk.galilel.cloud

Brand Guide

https://galilel.cloud/downloads/guides/Galilel_Brand_Guide_v2.pdf

Tor Masternode Guide

https://galilel.cloud/downloads/guides/Galilel_TOR_Masternode_Guide.pdf

Appendix

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/

www.galilel.cloud