



Technical White Paper

Liracoin V. 3.0



Queste note tecniche hanno lo scopo di documentare e descrivere in maniera ufficiale le caratteristiche e i concetti alla base di Liracoin. Questo documento specifico spiegherà dettagliatamente le caratteristiche tecniche e i vantaggi del sistema di ricompense Seesaw.

INTRODUZIONE

La maggior parte delle criptovalute utilizza i masternode, dividendo equamente le ricompense per i blocchi tra il mining e i masternode. Questo tipo di distribuzione equa di ricompense può essere indebolita dalla imponente crescita dei masternode detenuti da grandi investitori, portando a una potenziale centralizzazione del sistema di budgeting, proprio come nel caso di un azionista di maggioranza in una società. I vantaggi aggiuntivi dei masternode possono portare a un minor numero di utenti che svolgono attività di mining Proof of Stake (PoS) e quindi alla riduzione della sicurezza della rete PoS.

I masternode rappresentano un servizio prezioso e vanno quindi ricompensati, ma il nostro scopo non è quello di assegnare ricompense superiori all'effettivo valore aggiunto che forniscono. Crediamo infatti che ricompense sproporzionate assegnate ai proprietari di masternode, rispetto agli altri utenti, porterebbero a un ulteriore livello di centralizzazione



Per risolvere il problema, descritto in questo documento è stato sviluppato e implementato il protocollo PoS con l'unico scopo di garantire la sicurezza della rete. Ciò si ottiene creando un incentivo alla partecipazione, che promuove la liquidità negli exchange e controlla il tasso di crescita e il numero di masternode nella rete

Liracoin OVERVIEW

Liracoin è una criptovaluta open source, decentralizzata e incentrata sulla privacy, lanciata a novembre 2017 e che ha in seguito assunto il marchio LIT. La fase di distribuzione iniziale Proof of Work (PoW) si è conclusa nel mese di Maggio 2019, quando Liracoin è passata alla attuale fase Proof of Stake (PoS). LIT funziona con il protocollo Blackcoin PoS 2.0 ed è basato sul codice Bitcoin core 0.14.x.

A partire da agosto 2019 verrà e stata rilasciata la versione 3 ed avviata la rete di masternode per una governance decentralizzata e visibile e per una maggiore privacy delle transazioni. L'obiettivo principale di LIT è ottenere transazioni private quasi istantanee e creare una governance che aiuti a sostenere la rete a vantaggio di tutti gli utenti coinvolti.

Siamo sulla buona strada per raggiungere questo obiettivo, tuttavia alcune delle funzionalità sono in fase di sviluppo e saranno lanciate prossimamente.

L'ambiente di lavoro LIT è open task, gestito da un team di sviluppo sempre disponibile, che utilizza vari canali di networking, compresi i social media. Il team di sviluppo è sempre pronto ad accogliere nuovi utenti che vogliano supportare la causa, indipendentemente dalla loro esperienza tecnica. Incoraggiamo le persone ad agire, piuttosto che avere una serie di gatekeeper organizzati con una struttura gerarchica e la necessità di ottenere autorizzazioni per procedere.

Per informazioni più dettagliate su Liracoin, visita la pagina liracoin.it.

PROOF OF STAKE 2.0

INFORMAZIONI GENERALI

Per raggiungere il consenso, il Proof of Stake 2.0 (PoS) necessita che i nodi mantengano un wallet attivo, dimostrando di avere monete nella blockchain per verificare un blocco di transazioni. I nodi attivi ricevono una quantità di blocchi, ottenendo una ricompensa proporzionale allo staking per un determinato periodo di tempo.

Ciò significa che con un numero elevato di nodi partecipanti (e una pari quantità di monete) la rete diventa molto sicura, poiché diventa più difficile possedere la maggioranza di monete disponibili nella rete.

MASTERNODE

INFORMAZIONI GENERALI

I masternode sono nodi che eseguono lo stesso software di un wallet sulla stessa blockchain, per fornire servizi aggiuntivi alla rete. Questi servizi comprendono il mixing per una maggiore privacy delle transazioni, transazioni istantanee e una governance che fornisce un sistema di spesa decentralizzato, con un sistema di proposte e di voto invariabili.

I masternode ricevono una ricompensa per ogni blocco anche per fornire tali servizi. Ciò può rappresentare un introito passivo per i proprietari dei masternode, escludendo il costo di gestione.



CARATTERISTICHE PRINCIPALI

Per promuovere un rapporto bilanciato tra i nodi di staking e i nodi master nella rete, il team LiraCoin ha sviluppato un sistema variabile di ricompense (Seesaw Reward Balance System), che bilancia dinamicamente le ricompense tra nodi staking e master.

Ogni ricompensa per un blocco LIT PoS viene così suddivisa: il 10% va al sistema di spesa e il 90% viene utilizzato per le ricompense ai masternode e al mining. La parte di ricompensa viene ulteriormente suddivisa dinamicamente tramite il sistema Seesaw, tra nodi master e staking.

La logica di base è semplice. Più alto è il numero di masternode, minore è la ricompensa di ciascun blocco PoS che verrà distribuita ai masternode, e maggiore sarà la ricompensa per i nodi di staking. Al contrario, quando diminuisce il numero di masternode, aumenta la ricompensa per i masternode stessi e di conseguenza cala la ricompensa per i nodi di staking.

La ricompensa del blocco PoS inizia con un rapporto di 9 a 1 verso i masternode, quando la quantità di monete bloccate sui masternode è inferiore all'1% della quantità totale di monete. Tuttavia, quando il numero di monete bloccate sui masternode supera il 41,5% della quantità totale di coin LIT, l'importo della ricompensa del blocco si sposterà sui nodi di staking, con oltre il 50% di ricompensa.

Ciò ha l'effetto di rendere meno attraente la fornitura di più masternode in quanto ha il potenziale per ridurre significativamente la sua redditività rispetto alla punta che ha meno costi di manutenzione.

Di conseguenza, l'obiettivo non è quello di aumentare il numero di masternode, poiché ciò potenzialmente diminuirebbe la loro redditività rispetto allo staking, che ha meno costi di gestione.

Si è scelto di stabilire questa soglia poiché promuove lo sviluppo di una solida rete di masternode redditizi, creando al contempo incentivi per circa il 60% delle monete totali, che diventerebbe disponibile per lo staking per rendere la rete più sicura e mantenere la liquidità.

Un altro vantaggio e obiettivo del sistema Seesaw è quello di garantire che la gestione di un masternode sia più redditizia per gli utenti rispetto allo staking, seppur in pari numero di coin, nelle condizioni sotto la soglia stabilita. Mantenere i masternode, infatti, rappresenta maggiori costi, rischi e tempo dedicato alla gestione, rispetto allo staking.

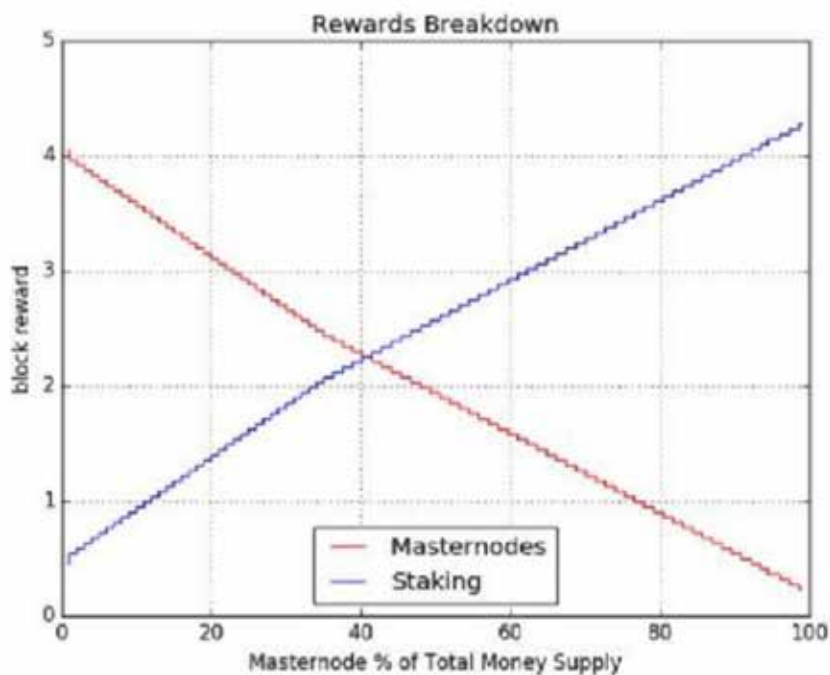


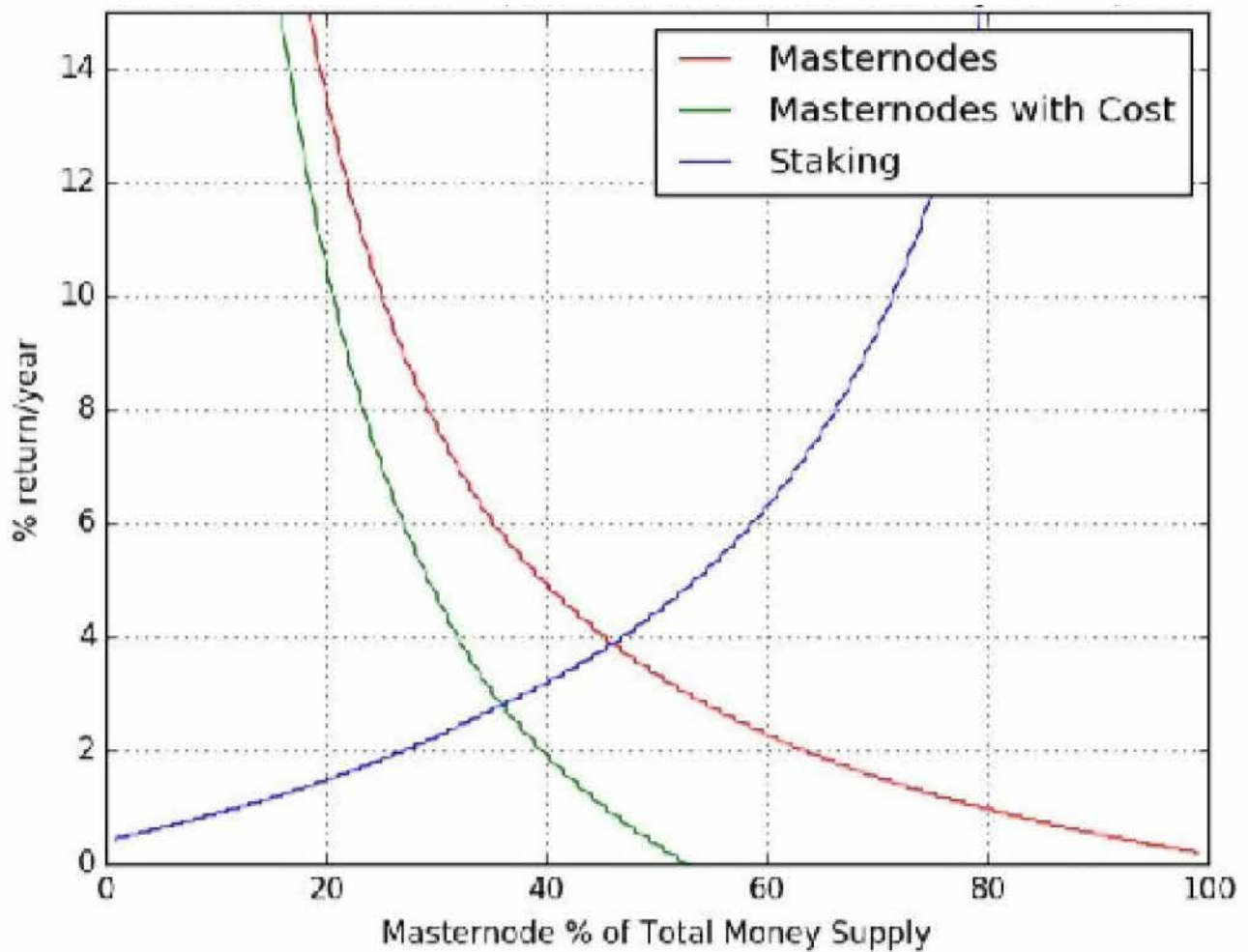
EFFETTO SEESAW

Il grafico mostra l'importo della ricompensa per blocco (asse Y) per i masternode (ROSSO) e per lo staking (BLU), rispetto alla percentuale delle monete totali bloccate dai masternode (asse X) a partire dal blocco 148.000 (metà maggio 2017) in cui ogni ricompensa per blocco era fissata a 5 LIT.

Il grafico mostra la percentuale di profitto annuale teorica, a partire dal blocco 148.000 dove ogni blocco è fissato a 5 LIT con un intervallo di 60 secondi.

(1.440 blocchi al giorno)





La linea ROSSA rappresenta il reddito dei masternode quando il costo di gestione dei masternode è zero, e la linea VERDE è la curva di reddito dei masternode su uno scenario ipotetico in cui il costo di gestione annuale per masternode è pari a 300 Euro, con un valore LIT a 1 Euro.



LOGICA DEL CODICE NEL DETTAGLIO

La logica è efficace, pur rimanendo il più semplice possibile. Questo per garantirne la stabilità e per essere in grado di determinarne facilmente i risultati e migliorarne eventualmente la logica.

```
if (mNodeCoins <= (nMoneySupply *.01) && mNodeCoins > 0) { ret = blockValue *.90;}
```

Il valore del blocco è il numero totale di monete per blocco. Questo valore viene moltiplicato per il rapporto variabile, determinato dalla percentuale di monete masternode (mNodeCoins) in relazione alla quantità totale di monete (nMoneySupply). Il risultante valore ret è il numero di monete per la ricompensa ai masternode.

L'esempio sopra mostra la logica di base utilizzata per determinare l'importo più alto destinato alle ricompense dei masternode. Si può vedere che se mNodecoins è minore o uguale all'1% della quantità di monete (nMoneySupply) e anche maggiore di 0, il valore di ricompensa del blocco per il masternode corrisponderà al 90% del blocco PoS (ret = blockValue *.90).

Questa logica è valida per ogni aumento delle percentuali impostate fino a quando mNodeCoins è inferiore o uguale al 99% della quantità di moneta.

```
else if (mNodeCoins <= (nMoneySupply *.99) && mNodeCoins > (nMoneySupply *.987)) { ret = blockValue *.05;}
```

Qualsiasi valore mNodeCoins superiore al 99% della quantità totale di monete restituirà un valore fisso pari all'1% del valore del blocco. La previsione è che non si arrivi mai a questo punto, ma la logica vuole coprire tutti i risultati possibili.

```
else { ret = blockValue *}
```

il ciclo del sistema di ricompense Seesaw all'inizio aveva solo 16 passaggi percentuali. Da allora è stato migliorato e attualmente implementa un totale di 105 passaggi percentuali nell'algoritmo variabile, cosa che permette di ottenere importi molto più dettagliati



SINTESI

Il Seesaw Reward Balance System utilizzato da LIT offre numerosi vantaggi rispetto ai metodi di divisione delle ricompense utilizzati dalla maggior parte dei masternode con criptovalute Proof of Stake.

1. Può influenzare indirettamente il numero totale di masternode nella rete variando l'importo della ricompensa per alterarne la redditività rispetto allo staking.
2. Incentiva lo staking aumentandone la ricompensa quando il numero di masternode è elevato, mantenendo così un alto livello di sicurezza della rete.
3. La redditività del masternode è mantenuta superiore rispetto allo staking, purché il numero di masternode rimanga al di sotto della soglia predefinita (circa il 40% della quantità di monete).
4. Non solo i proprietari di masternode, ma tutti gli utenti che possiedono monete saranno ricompensati; il sistema risulta quindi più equo e meno centralizzato.

PROGETTI FUTURI

Poiché il Seesaw Reward Balance System è ancora relativamente nuovo (lanciato da 5 mesi, al momento della stesura di questo documento), saranno necessari ulteriori sviluppi qualora la rete continuasse a crescere e se verranno individuate delle soglie che risultino maggiormente efficaci.

CODICE SORGENTE

GITHUB

<https://github.com/gammatecnology/litacoin-italia>

Sito ufficiale

<https://www.liracoin.it>

RIFERIMENTI

- [1] Whitepaper PoS 2.0 <http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper-cn.pdf>
- [2] Masternode DASH <https://dashpay.atlassian.net/wiki/display/DOC/Masternode>

AUTORi:

Claudio Rossini
Andrea Vitiani

Versione 1.0 del 20 Agosto 2019
(c) tutti i diritti riservati TECNOINFO - Svizzera

Il software di riferimento di questo documento è tuttora oggetto di sviluppo e di miglioramenti tecnici e tecnologici.

Gli autori non si assumono responsabilità circa eventuali differenze tra i contenuti di questo documento ed eventuali modifiche al software avvenute succesivamente.



www.liracoin.it