I VADEMECUM DI TERRABITCOIN CLUB

Chainlink

Decentralized Oracle Network

Il ponte tra on-chain e off-chain

I Vademecum di TerraBitcoin Club

Chainlink

Decentralized Oracle Network

Il ponte tra off-chain e on-chain

a cura di Alessandro Benedetti di Yield Hunters

Sommario

Introduzione

Chainlink è quello che si dice un protocollo *primitive* e cioè un protocollo storico della finanza decentralizzata.
È stata, infatti, la prima rete di nodi oracolo completamente decentralizzata e dotata di un proprio protocollo di consenso.
Nata, dunque, con l'idea di offrire feed di prezzo per gli assets sulla chain Ethereum, negli anni Chainlink si è evoluta diventando un vero e proprio ecosistema che eroga una quantità significativa di servizi.
Questo Vademecum, pensato a corredo delle puntate video di Yield Hunters - il servizio di TerraBitcoin Club dedicato alla Finanza Decentralizzata (DeFi) -, analizzerà nel dettaglio questo nuovo ecosistema.
Consigliamo, comunque, la visione delle puntate di Yield Hunters dedicate al tema.

1. Cos'è Chainlink

Chainlink è una rete decentralizzata di oracoli che consente agli smart contracts di interagire in modo sicuro con dati e servizi del mondo tradizionale (off-chain), non disponibili nel mondo della blockchain (on-chain).
Nata con l'idea di offrire feed di prezzo per gli assets sulla chain Ethereum, negli si è evoluta diventando un vero e proprio ecosistema che eroga una quantità significativa di servizi.
Ma cosa sono gli oracoli? Li possiamo considerare alla stregua di veri e propri «ponti» (middleware) che mettono in connessione qualsiasi dato del mondo tradizionale alle blockchain.
Immaginiamo di voler far eseguire a uno Smart Contract il trasferimento di un token quando l'Euro dovesse raggiungere la parità con il Dollaro. Quest'ultimo dato non è reperibile on-chain, ma off-chain e cioè nel mondo tradizionale. Senza un collegamento (Link) tra la rete (Chain) e il mondo reale, ciò non sarebbe possibile. Ed è proprio questo collegamento che Chainlink rende possibile, da qui il suo nome.
La funzione svolta dai DON (Decentralized Oracle Networks) di Chainlink e dagli altri oracle providers è essenziale.

Facendo un parallelo con il web, se la chain può considerarsi il computer che ci consente di navigare in internet, gli oracoli possiamo considerarli alla stregua di un modem, e cioè ciò che fa da “ponte” tra il nostro PC e il web.
Chainlink consente sia il trasferimento di dati, che la loro verifica e autenticazione, impedendo qualsiasi manomissione dei dati medesimi (tamper proof data), una volta pubblicati su blockchain.

Chainlink Labs viene fondato nel 2017 e lanciato ufficialmente su Mainnet Ethereum nel 2019, allo scopo di fornire all'ecosistema degli smart contract l'accesso a dati tamper proof (price feeds) provenienti dal mercato finanziario.
Original team: Ari Juels (Chief scientist), Sergey Nazarov (CEO of Chainlink Labs), Steve Ellis (CTO), Benedict Chan (Vice president of Engineering);
Individuals: Eric Schmidt (advisor and ex Google CEO), Kemal el Moujahid (CPO, ex Google and Messenger), Dahlia Malkhi (Chief Research Officer, ex CTO Diem);
Investors: Fundamental Labs, Nirvana Capital, Framework Ventures.

1.1 Il token LINK

Il token LINK è stato lanciato nel settembre 2017 al prezzo di 0.09 $ per unità; la successiva presale è stata, invece, fissata a 0.11 $.

Quanto alla sua distribuzione, è avvenuta come segue:

- il 35% è stato assegnato agli investitori nei seed e presale investing rounds;
- il 35% è stato riservato ai node operators e alle rewards per l'ecosistema, da distribuirsi per incentivare i partecipanti alla rete;
- il 30% è stato assegnato alla società madre di LINK, SmartContract.com (di proprietà del fondatore Sergey Nazarov).

Tutta la supply di 1B è stata mintata, benché non sia ancora tutta circolante (perché vested o riservata a scopi specifici).
Il token LINK svolge essenzialmente 3 funzioni all'interno dell'ecosistema:

1. Payment: viene utilizzato per remunerare gli operatori di nodi Chainlink a fronte del servizio oracle reso;

2. Work: viene messo in staking dai nodi validatori per garantire la corretta fornitura di servizi oracle;

3. Security and revenues sharing (coming soon): introduzione dello staking per aumentare il livello di sicurezza del network e, al contempo, consentire alla community di beneficiare delle revenues generate dall'infrastruttura.

1.2 Market data

1h	24h	7 g.	14 g	30 g.	1 a
-1.5%	-2.1%	6.9%	6.8%	13.6%	-69.6%

LINK Statistiche prezzi

Chainlink Prezzo	7,32 USD
Minimo in 24 ore / Massimo in 24 ore	7,27 USD / 7,57 USD
Minimo in 7 giorni / Massimo in 7 giorni	6,84 USD / 8,17 USD
Volume trading	413.901.112 USD
Classifica cap. di mercato	#26
Cap. di mercato	3.414.959.468 USD
Dominanza cap. di mercato	0,308%
Volume / Capitalizzazione di mercato	0.1219
Massimo storico (ATH)	52,70 USD -86.1% May 10, 2021 (circa un anno)
Minimo storico	0,148183 USD 4833.0% Nov 29, 2017 (oltre 4 anni)

Cap. di mercato	3.414.959.468 USD	Offerta in circolazione	467.099.986
Volume scambi 24 h	413.901.112 USD	Offerta totale	1.000.000.000
Valutazione completamente diluita	7.310.981.730 USD	Offerta massima	1.000.000.000

2. Come funziona Chainlink

Chainlink è un oracle network decentralizzato, sviluppato sulla blockchain Ethereum. La sua funzione principale è quella di trasferire dati dal mondo tradizionale agli smart contract e viceversa.
Ma Chainlink non si occupa solo del trasferimento di dati, ma anche della loro verifica e autenticazione; garantisce, inoltre, l'impossibilità di manomissione del dato (tamper proof data) una volta pubblicato su blockchain.
I dati oggetto degli oracle reports possono essere di qualsiasi tipo, le limitazioni sono quelle specifiche di ciascuno smart contract.
Chainlink risolve i problemi derivanti dalla mancanza di un ponte tra i mondi off-chain e on-chain e dall'esigenza di comunicare con diversi network.
Interagendo con più blockchain in modo simultaneo, Chainlink inoltrerà i dati, quali che siano, su tutti gli smart contract interessati contemporaneamente.

2.1 Il funzionamento di base

Il network è decisamente complesso. Però, il funzionamento di base può essere suddiviso in alcuni passaggi, risultando di più agevole comprensione. Vediamoli qui di seguito.

1. Uno sviluppatore/team/progetto che necessita di ottenere determinati dati su uno smart contract, magari aggiornati a cadenze regolari, si rivolge a Chainlink.

2. Chainlink analizza le esigenze di questa entità e le incrocia con gli oracoli a disposizione, selezionando quelli adatti al caso. Ad esempio, se lo smart contract dovesse ricevere i risultati delle partite di calcio del campionato italiano, Chainlink assocerà dei provider che si occupano proprio di questo tema.
3. In seguito, il dev (team/founder/ CEO, ecc.) sarà tenuto a depositare dei LINK nel contratto che andrà a stipulare. Questa somma servirà per ripagare gli oracoli, purché le informazioni siano di qualità e in linea con quanto stabilito.
4. Per garantire che tutto proceda secondo i piani, gli utenti devono utilizzare il Service Level Agreement (SLA). Trattasi di un software in cui indicare ciò di cui si ha bisogno, in modo tale da non creare alcun tipo di incomprensione.
5. Nella seconda fase, gli oracoli designati possono ricercare le info e immetterle nel network. In seguito, Chainlink aggrega i dati, li incrocia, verifica e ne elimina le incongruenze.
6. Infine, il pacchetto di informazioni si sposta sulla blockchain del cliente.
   Grazie al procedimento descritto, quanto ricevuto sarà esatto e affidabile, evitando perdite di tempo dovute a ulteriori verifiche.

9. A questo punto, il flusso può proseguire a tempo indeterminato. Questa soluzione è perfetta per realtà che necessitino di aggiornamenti continui, come, ad esempio, un exchange che ha bisogno dei prezzi delle principali crypto o del mercato azionario.

YIELDHUNTERS

3. Le nuove funzionalità

Il 15 aprile 2021 è stato pubblicato il Whitepaper di Chainlink 2.0, che ridefinisce in modo ambizioso gli obiettivi di lungo termine del progetto e traccia una roadmap per i futuri upgrades.
Prevedendo un ruolo sempre più ampio per le reti di oracoli, gli sviluppatori hanno posto a fondamento del progetto ciò che hanno chiamato Decentralize Oracle Network (DON) e cioè una rete gestita da un comitato di nodi Chainlink. Radicata in un protocollo di consenso, essa supporta una gamma illimitata di funzioni di oracolo scelte dal comitato stesso.
Un DON agisce quindi come un livello di astrazione della blockchain, fornendo interfacce a risorse esterne alla catena, sia per gli Smart Contract che per altri sistemi. Fornisce, inoltre, l'accesso a risorse informatiche off-chain altamente efficienti e decentralizzate.

3.1 Chainlink 2.0

Come dichiarato nel Whitepaper, a partire dai DON, Chainlink intende concentrarsi su sette aree chiave:

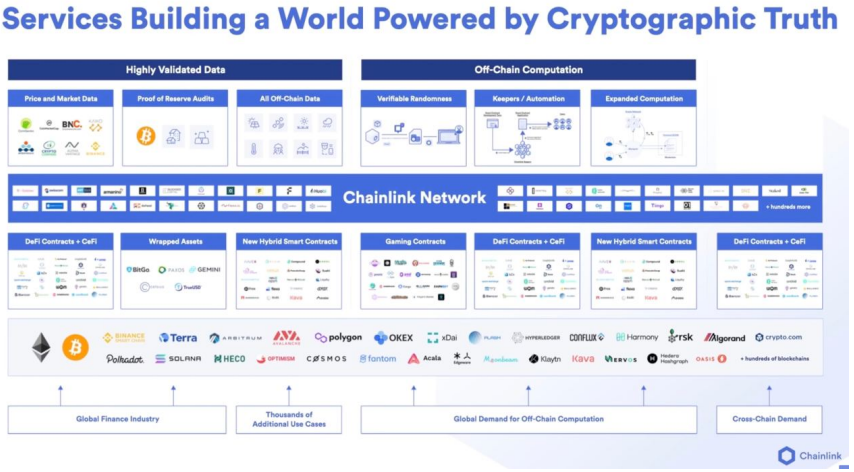
- **Smart Contract ibridi**: lo scopo è migliorare le funzionalità degli smart contract esistenti, per far dialogare dati off-chain e on-chain in modo sicuro

Box 1
Le novità più rilevanti

1. Modifiche al DON volte alla creazione di un metalayer decentralizzato (Transaction Execution Framework; Hybrid SCs);
2. Proof of Reserve
3. Fair Sequencing Service
4. Verifiable Random Function
5. CCIP
6. Staking e Implicit Incentive Framework (node reputation)
7. Off Chain Reporting
8. DECO (e Town Crier), il «Transaction Layer Security» - in fase di sviluppo
9. Decentralized Identity
10. Priority Channels
11. Defi Confidentiality Preserving / Mixicles
12. Keepers

• **Astracting away complexity**: prevedere funzionalità semplici per evitare agli utenti di avere a che fare con i complessi protocolli sottostanti
• **Scaling**: garantire che i servizi di oracolo raggiungano le latenze e i throughput richiesti dai sistemi decentralizzati ad alte prestazioni.
• **Confidentiality**: prevedere sistemi di nuova generazione che combinino l'innata trasparenza delle blockchain con nuove e forti misure di riservatezza per i dati sensibili.
• **Order-fairness for transactions**: supportare la sequenza delle transazioni in modo equo per gli utenti finali e prevenire il front-running e altri attacchi da parte di bot e minatori malevoli.

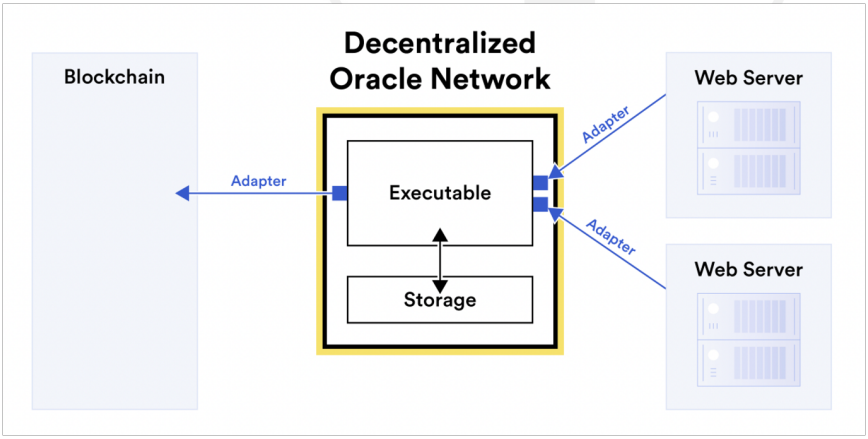
- **Trust-minimization**: creare un livello di supporto altamente affidabile per gli smart contract e altri sistemi dipendenti dagli oracoli mediante la decentralizzazione, un solido ancoraggio a blockchain ad alta sicurezza, tecniche crittografiche e garanzie criptoeconomiche.
- **Incentive-based (cryptoeconomic) security:** Progettare in modo rigoroso e distribuire in modo sicuro meccanismi che assicurino che i nodi nei DON abbiano forti incentivi economici a comportarsi in modo affidabile e corretto.



3.2 Il DON

Prima di analizzare nel dettaglio le principali novità di Chainlink 2.0, soffermiamoci per prima cosa su uno degli elementi che contraddistingue questo progetto dalle altre

soluzioni oracle centralizzate: il Decentralized Oracle Network, più noto come DON.
Il DON consente a Chainlink di operare come un network pienamente decentralizzato ed è stato progettato per migliorare ed estendere le capacità degli smart contracts, aggiungendo funzioni che non sarebbero disponibili on-chain.
Mettendo a disposizione delle blockchain le tre risorse presenti nei sistemi informatici (network, storage e computation), il DON garantisce riservatezza e integrità dei dati trasmessi e ricevuti.
Nell'immagine che segue, è mostrato come un DON possa assolvere alle funzionalità base di un oracolo, ossia trasmettere dati off-chain a un contratto on-chain. In particolare un executable utilizza degli adapters per recuperare i dati off-chain, sui quali esegue i propri calcoli, inviando poi l'output attraverso un altro adapters a una



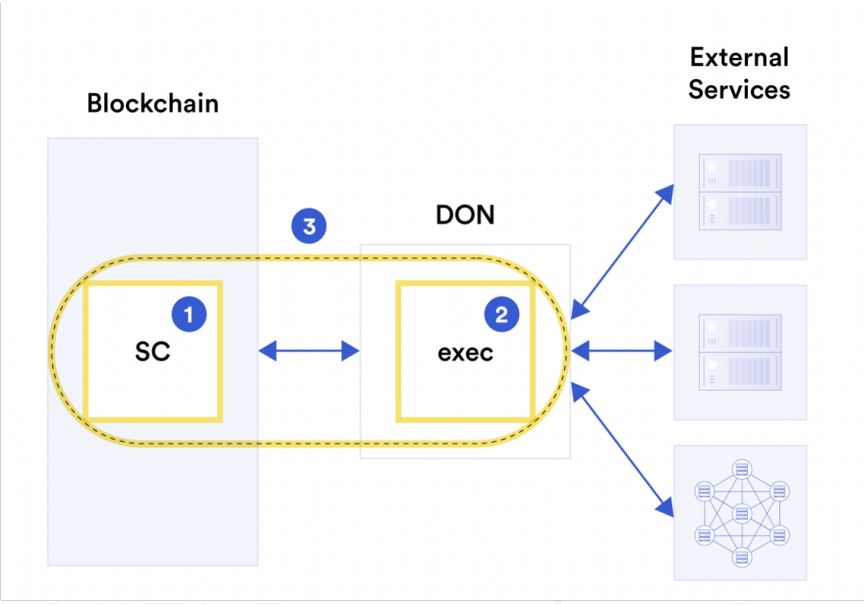
blockchain di destinazione (le frecce mostrano la direzione del flusso di dati).

Due tipi di funzionalità realizzano le caratteristiche di un DON:

- gli **executables**, programmi che vengono eseguiti in modo continuo e decentralizzato sul DON (simili a SC). Sebbene non memorizzino direttamente le risorse della chain principale, presentano importanti vantaggi, tra cui prestazioni elevate e la possibilità di eseguire computazioni riservate. Vengono runnati (eseguiti in modo continuo) autonomamente su un DON ed eseguono operazioni deterministiche. Lavorano in collaborazione con gli adapters.
  Possono, inoltre, leggere e scrivere sullo storage locale del DON per mantenere lo stato e/o comunicare con altri executables. La rete, il calcolo e l'archiviazione flessibile nei DON consentono una serie di applicazioni innovative, ad esempio gli Smart Contract ibridi (Hybrid Smart Contracts).
- gli **adapters** che collegano il DON a risorse esterne e possono essere richiamati dagli executables. Sono interfacce attraverso le quali gli executables possono inviare e ricevere dati da sistemi esterni al DON.

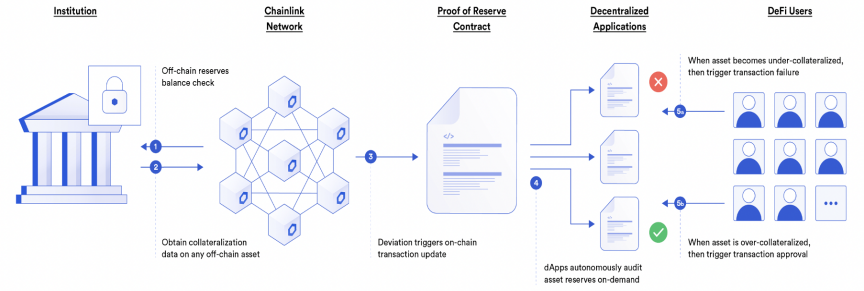
Uno **Smart Contract ibrido** (vedi punto 3, nell'immagine che segue) è costituito da due elementi complementari: una componente on-chain "SC (1)" - che risiede appunto su blockchain - e una componente off-chain "exec (2)", che

viene eseguito su un DON.
Il DON funge da ponte tra le due componenti e connette il Contract ibrido con risorse off-chain come servizi web, altre blockchain, storage decentralizzati, ecc.



3.3 Proof of reserve

Il Chainlink Proof of Reserve è un servizio che fornisce agli smart contract i dati necessari per calcolare la reale collateralizzazione di qualsiasi asset on-chain (anche RWAs), coperto da riserve off-chain o cross-chain. Consente la verifica indipendente del collaterale in tempo reale, contribuendo a garantire che i fondi degli utenti siano protetti da pratiche di riserva frazionaria impreviste e da altre attività fraudolente da parte di custodians off-chain. Armanino, BigGo, Paxos, Celsius, Nexo sono solo alcune delle piattaforme che hanno scelto di fruire del servizio erogato da Chainlink.



3.4 Fair Sequencing Service - FSS

L'FSS è un servizio di order fairness delle transazioni nei blocchi che rispetta il criterio temporale (CT). In altri

termini, sono strumenti forniti dal DON per decentralizzare l'ordine delle transazioni e attuarlo in base ad una politica specificata da un creatore di relying contracts, idealmente una politica equa e che non avvantaggi gli attori che desiderano manipolare l'ordine delle transazioni (MEV, front runners, ecc).

> I relying contract sono smart contact sviluppati da color che necessitano dei servizi di Chainlink.

L'FSS si compone di tre fasi:

1. **Monitoraggio delle transazioni**. In FSS, i nodi oracolo monitorano il mempool della MAINCHAIN e permettono l'invio di transazioni off-chain attraverso un canale specializzato.
2. **Sequenziamento delle transazioni**. I nodi ordinano le transazioni per un relying contract, secondo la politica definita per quel contratto o sulla base del criterio temporale, di default.
3. **Invio delle transazioni**. Dopo che le transazioni sono state ordinate, i nodi oracle inviano congiuntamente le transazioni alla chain principale.

Potential benefits

Un'altra peculiarità dell'FFS è quella di mettere a disposizione dei benefit che le blockchain tradizionali non possono offrire. In altri termini, l'Order Fairness (e cioè il FSS) include strumenti per aiutare gli sviluppatori a

garantire che le transazioni di un particolare contratto siano ordinate in modo tale da non dare un vantaggio iniquo agli utenti dotati di maggiori risorse e/o tecnicamente esperti.
Tali strumenti sono:

- **Riduzione o eliminazione delle info leaks**, assicurando che i partecipanti alla rete non possano sfruttare la conoscenza delle transazioni imminenti. Il sistema FSS può ridurre o eliminare attacchi come il front-running, che si basano su informazioni disponibili in rete prima che le transazioni siano committed on chain.
- **Riduzione dei costi di transazione**, eliminando l'esigenza di velocità dei players nell'inviare le loro transazioni ad uno SC. L'FSS può ridurre notevolmente il costo dell'elaborazione delle transazioni stesse.
- **Ordine di priorità**: L'FSS può assegnare automaticamente alle txns critiche un ordine prioritario. Ad es, per prevenire i front-running attacks vs i reports di oracolo, l'FSS può inserire un report di oracolo in un flusso di transazioni in modo retroattivo.

3.5 Verifiable Random Functions - VRF

Il VRF è un servizio erogabile dai DON di Chainlink che viene generato per i protocolli interessati delle funzioni casuali verificabili on chain. In questo modo, la prova della correttezza del dato casuale è pubblica ed eseguibile da chiunque.

Diversi tipi di DApp richiedono una fonte di casualità verificabile, per consentire la prova del loro funzionamento corretto.
Gli NFT ne sono un esempio: perché attraverso la VRF l'assegnazione di attributi per i PFP (PortFolio Picuteres) e la generazione di NFTs vengono eseguiti in modo randomico e cioè casuale.

4. Lo staking

L'introduzione dello staking è un momento cruciale che segna l'evoluzione verso Chainlink Economics 2.0; una nuova era nella sicurezza a lungo termine di Chainlink e nell'economia della rete.
Mentre l'implementazione iniziale dello staking di Chainlink è stata progettata per minimizzare il rischio per i partecipanti e creare una solida base, gli obiettivi a lungo termine ruotano intorno alla scaling di Chainlink in uno standard globale con una base di utenti crescente e sostenibile. Essa, a sua volta, offre maggiori opportunità di ricompensa per gli staker che aumentano la sicurezza criptoeconomica della rete e le garanzie per gli utenti.

4.1 La versione iniziale

La versione iniziale v0.1 di Chainlink staking si concentra sull'introduzione di un quadro di reputazione (reputation framework) e di un sistema di allerta (alerting system); requisiti fondamentali, questi, per lo slashing e per altre funzionalità previste e che verranno introdotte nelle versioni successive.
Per garantire la robustezza in un ambiente “in production” (cioè durante la sua operatività), questi sistemi saranno utilizzati per monitorare le prestazioni dei feed del prezzo ETH/USD sulla mainnet di Ethereum.

Gli staker avranno la possibilità di monitorare il feed, lanciare un allarme e ricevere una ricompensa se riusciranno a rilevare tempestivamente che il feed ETH/USD non ha rispettato le condizioni del Service Level Agreement (SLA).
Nella versione 0.1, le condizioni di allerta si concentreranno sul tempo di attività del feed, ma la portata si amplierà nelle versioni successive.
Una volta emesso un avviso, uno smart contract di aggiudicazione verificherà automaticamente che le condizioni dello SLA dello smart contract siano state violate e che l'avviso sia valido. Al termine di questo processo, l'autore della segnalazione riceverà una ricompensa in un secondo momento.
I risultati di una segnalazione valida confluiranno in un sistema di reputazione che aggiornerà la reputazione individuale degli operatori del nodo colpevole.
Nella v1, si prevede che il sistema di reputazione si espanda per tenere traccia di un maggior numero di metriche chiave relative alle prestazioni degli operatori dei nodi e svolga un ruolo sempre più importante, man mano che la rete Chainlink si espande.

In definitiva, la v0.1 del sistema di staking di Chainlink rappresenta il nucleo del sistema di reputazione e di allerta, che si evolverà per fornire garanzie di sicurezza lineari e, successivamente, scalare per supportare garanzie di sicurezza super-lineari.

4.2 Come partecipare allo staking

Il pool iniziale di staking nella versione 0.1 sarà di dimensioni limitate, offrendo assegnazioni distinte agli operatori dei nodi, ai membri della comunità e al coordinatore delle reti oracolo.
Il pool inizierà con una dimensione aggregata di 25 milioni di token LINK, con l'obiettivo previsto di scalare a una dimensione di 75 milioni nei mesi successivi al lancio, in base alla domanda. Per i rilasci futuri è prevista un'ulteriore espansione delle dimensioni del pool e il supporto di ulteriori Data Feed e servizi oracolo (in termini di commissioni che verranno riversate nella pool nper i servizi oracle offerti).
Per riempire inizialmente l'assegnazione (allontment) della comunità, verrà utilizzato un meccanismo di ingresso equo per garantire la partecipazione di un'ampia gamma di membri della comunità.
Questo meccanismo di ingresso avrà lo scopo di dare priorità ai possessori di token a lungo termine, che hanno maggiori probabilità di partecipare attivamente al meccanismo di alerting.
Gli operatori di nodi che forniscono attivamente servizi ai feed di dati di Chainlink riceveranno i propri allotment distinti da riempire. È in fase di studio un sistema di delega dei nodi da parte di terzi, che attualmente dovrebbe essere supportato nella versione v1.

Gli staker che partecipano alla versione v0.1 avranno i loro LINK bloccati almeno fino al rilascio della versione v1, dove potranno scegliere periodi di locking di varia durata.

4.3 Ricompense per lo staking

Nella versione 0.1, si prevede che le emissioni native di token dirette agli staker potranno garantire un APY (Annual percentuale yield) fino al 5%. Dopo il rilascio della v1, le ricompense annualizzate varieranno in base alle fees degli utenti e alla durata del periodo di locking (i long term stakers avranno l'opportunità di ricevere una quota maggiore delle ricompense).
Inoltre, gli staker della v0.1 potranno ottenere ulteriori vantaggi dal Partner Growth Program (PGP).

Questo programma è un'iniziativa prevista per il lancio insieme allo staking di Chainlink, in cui i progetti Chainlink forniscono vari benefici per accelerare la loro crescita e allineare i loro incentivi economici con la community di Chainlink. Questo allineamento crea incentivi per gli staker di Chainlink a diventare partecipanti attivi nell'ecosistema di un progetto, fornendo una via per un'adozione accelerata.
Una prima versione del PGP è prevista per la v0.1, mentre una versione più completa è prevista per la v1.
Con la transizione dello staking alla v1, si prevede che una parte delle fees degli users dei servizi oracle inizierà a essere assegnata agli staker, in concomitanza con la

sicurezza criptoeconomica fornita dalla riduzione dello staking LINK.
Inoltre, le fees associate alla protezione dalle perdite, in fase di studio per la v2, potrebbero diventare una fonte di ricompense in aggiunta alle emissioni, alle fees per gli utenti dei servizi oracle e ai benefici del PGP.
Ulteriori dettagli e specifiche su ciascuna versione saranno resi noti nel corso del tempo.

4.4 Incentivi e comportamenti malevoli

Chainlink utilizza incentivi economici impliciti ed espliciti, per garantire che i nodi oracolo non si comportino in modo malevolo. In modo esplicito, Chainlink richiede due "depositi":

- uno che può essere soggetto a slashing per aver segnalato un valore errato non concordato dalla rete aggregata
- e un altro che può essere soggetto a slashing per aver falsamente segnalato che una rete di nodi ha collettivamente indicato un valore falso a un adjudicator noto come "second tier".

Implicitamente, Chainlink presuppone che gli attori economici razionali (i nodi) invieranno valori corretti agli oracoli perché è nel loro interesse farlo (cioè c'è un costo opportunità di ricompensa che un nodo perde se si comporta in modo malevolo).
Gli incentivi impliciti sono noti come "future fee opportunity" (FFO) e Chainlink mira a misurarli con il suo

"Implicit-Incentive Framework", un tentativo rivoluzionario di quantificare il costo opportunità dei nodi che include:

- la storia delle prestazioni di un nodo,
- l'accesso ai dati,
- la partecipazione all'oracolo,
- e l'attività multipiattaforma (ad esempio, i nodi che potrebbero essere su altre reti come Chorus One e il modo in cui si comportano su di esse per quanto riguarda i tempi di inattività (downtime), gli slashing, ecc.).

Di fatto, Chainlink è arrivato a creare un'equazione per trovare gli incentivi impliciti dei nodi, che si può vedere nella seguente formula.

$$\$S \approx \$D + \$F + \$FS + \$R,$$

where:

- $\$D$ is the aggregate of all explicitly deposited stake across all networks in which the operator participates;
- $\$F$ is the net present value of the aggregate of all FFO across all networks in which the operator participates;
- $\$FS$ is the net present value of the speculative FFO of the operator; and
- $\$R$ is the reputational equity of the operator outside the Chainlink ecosystem that might be jeopardized by identified misbehavior in its oracle nodes.

Questa formula definisce il motivo per cui un nodo di Chainlink continuerebbe implicitamente a riportare i valori corretti agli oracoli, perché se non lo fa rischia di perdere la

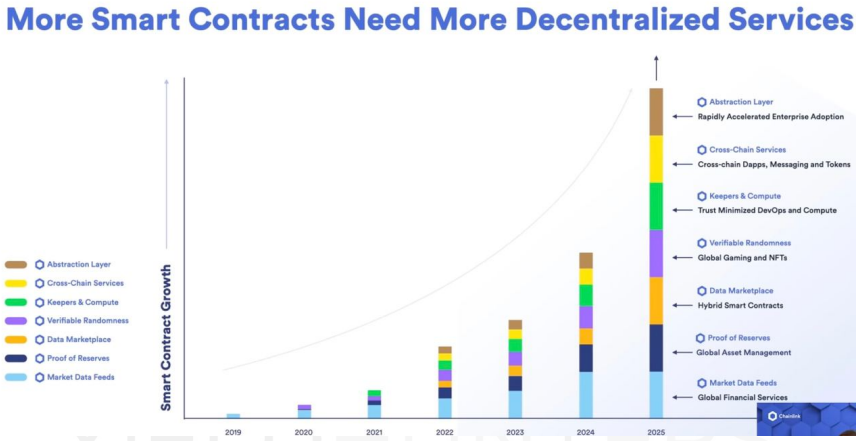
sua futura opportunità di compenso (che si trova nell'equazione precedente).

4.5 Incentivi implici e FFO speculativo

Un punto interessante da notare sugli incentivi impliciti, tratto dal Whitepaper di Chainlink, è quello del “Future Fee Opportunity speculativo” (FFO).
I nuovi nodi che entrano in funzione su Chainlink scommettono che le loro spese saranno superate dalle future opportunità di guadagno. In sostanza, coloro che gestiscono un nodo su Chainlink nelle fasi iniziali stanno facendo una scommessa speculativa sul fatto che guadagneranno commissioni considerevoli in futuro.
L'aspetto "speculativo" dell'FFO (cioè la scommessa sul futuro successo di Chainlink) moltiplica l'incentivo implicito per i nodi ad assicurarsi di comportarsi correttamente, perché hanno un interesse nel buon andamento della rete.
L'FFO speculativo è un'interessante interpretazione del valore reale di questo incentivo implicito.

È ragionevole pensare che il valore di questo incentivo implicito sia stato compreso solo ora dalle reti. Questo incentivo implicito può essere ulteriormente rafforzato dando agli operatori dei nodi una maggiore "partecipazione al gioco” (skin in the game).
Un incentivo implicito ancora maggiore potrebbe essere quello di offrire ricompense maggiorate agli operatori dei

nodi che hanno una maggiore reputazione; il che costituirebbe un'esternalità positiva per l'intero ecosistema delle cripto, dato che i nodi vogliono aumentare la loro reputazione in tutte le reti.
Quanto prima un validatore è coinvolto nel gioco e quanto più grande è la sua partecipazione, tanto più è probabile che presti attenzione al futuro successo e alla sicurezza della rete.



In un prossimo corso di Yield Hunters (il servizio di TerraBitcoin Club dedicato alla finanza decentralizzata), discuteremo più approfonditamente dell'importanza degli incentivi impliciti ed espliciti per gli operatori dei nodi su altre reti.

4.6 Aumentare gli incentivi espliciti per i nodi a comportarsi correttamente attraverso il super-linear staking

Chainlink 2.0 introduce il concetto di super-linear staking (o quadratic staking), per garantire che i nodi siano incentivati a riportare sempre valori corretti (come concordato dagli altri nodi).
In questo modo, Chainlink ha essenzialmente creato un secondo layer (noto come tier nel whitepaper), che verrà utilizzato come backstop se un watchdog ritiene che un valore aggregato riportato da una rete di nodi sia falso.
Un watchdog è un qualsiasi nodo del primo layer che avvisa il secondo layer superiore, quando ritiene che un valore riportato sia errato. Si può pensare a questo sistema come a un sistema "dibber-dobber".
Un watchdog è come uno studente di una classe (livello 1), rispetto al quale l'insegnante (livello 2) confida nel fatto che costui gli riferisca sempre se il resto della classe si comporta male. Per continuare con questa analogia, supponiamo che un insegnante se ne vada per 10 minuti e offra una ricompensa in caramelle a tutti gli studenti se non si comportano male quando lui non c'è (questo è come un deposito di incentivi espliciti per tutti gli studenti); poi ne offre una seconda per la segnalazione nel caso in cui più del 50% della classe si comporta male (la ricompensa viene data togliendo il deposito di incentivi espliciti agli studenti che si comportano male).

Quando l'insegnante se ne va, più della metà della classe inizia a comportarsi male, il che significa che chi si comporta bene non può lavorare perché distratti dagli altri. Inoltre, i compagni che si comportano male vogliono il meglio dei due mondi; vogliono cioè comportarsi male e guadagnare la ricompensa (mantenere il deposito) offerta dall'insegnante.

Ora, immaginiamo che chiunque possa dire all'insegnante quando più della metà della classe si comporta male per guadagnare una ricompensa, ma l'insegnante ha già una priorità randomizzata su come distribuire le ricompense dall'incentivo esplicito degli studenti che si comportano male a un sistema "chi vince prende tutto" (cioè un solo studente riceve tutte le ricompense “slashed" dagli studenti che si comportano male per aver fatto la spia ai loro compagni).

Immaginiamo ora che gli studenti che si comportano male cerchino di convincere quelli che si comportano bene a non segnalare il comportamento scorretto. Se solo uno studente segnala un comportamento scorretto, guadagnerà tutte le ricompense (depositi) degli studenti che si comportano male. Pertanto, gli studenti che si comportano male devono pagare più della ricompensa massima che uno studente che si comporta bene potrebbe ricevere, per tutti gli studenti che si comportano bene. Tenendo presente la priorità, le ricompense non sono paritarie poiché tutte le ricompense per una segnalazione corretta di comportamento scorretto andranno ad un solo studente.

Questo è l'effetto quadratico super-lineare del sistema Chainlink 2.0.
In altri termini, diventa molto più costoso corrompere gli studenti che si comportano bene (nodi) in classe, perché l'importo massimo richiesto per corrompere un singolo studente è la massima ricompensa che uno studente potrebbe ricevere dal taglio complessivo degli studenti che si comportano male.

Il minimo che gli avversari devono pagare per garantire la scorrettezza è la massima ricompensa per ogni studente che si comporta bene, perché se solo uno studente lo dice all'insegnante, può ricevere tutte le ricompense degli studenti che si comportano male (si tratta di un sacco di caramelle).
Se le ricompense degli studenti inadempienti fossero distribuite equamente, sarebbe molto più conveniente convincere (corrompere) gli studenti che si comportano bene a riferire dati falsi all'insegnante. In questo senso, il sistema a tier (con un secondo tier che ha l'ultima parola) e la priorità del "cane da guardia" o watchdog - con un nodo con una certa priorità che si guadagna tutte le ricompense dei nodi che si comportano male per aver segnalato correttamente che stanno agendo in modo malevolo - assicurano l'integrità dei dati dei valori riportati in Chainlink.

YIELDHUNTERS

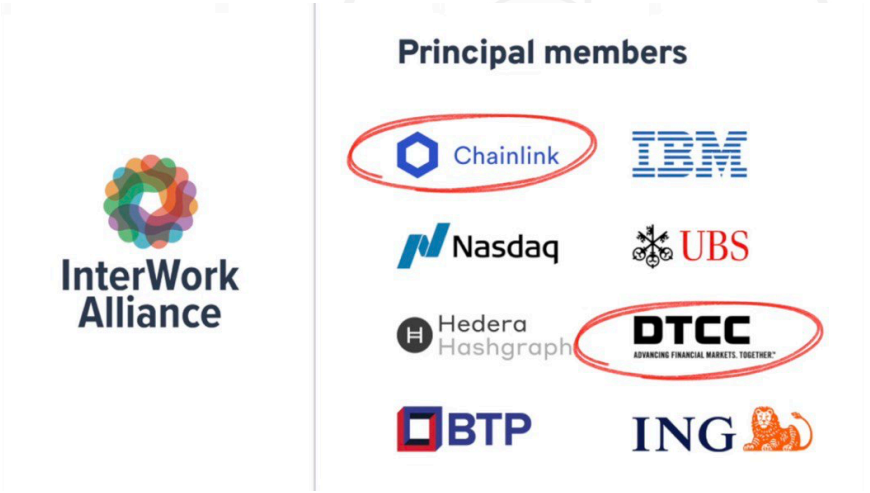
IL COMMENTO FINANZIARIO

Per dare un'idea di quali sono le potenzialità di Chainlink, ci limitiamo a citare tre iniziative volte a potenziare l'interoperabilità tra il mondo blockchain e i sistemi legacy:

- il rilascio imminente di un compliance oracle che monitora in tempo reale il possesso dei requisiti di reddito, capitale, merito creditizio, ecc., in capo ai soggetti che intendono accreditarsi per poter acquistare particolari asset finanziari, prodotti esotici (ad es certificati, hedge funds, ecc.) o partecipare a determinati eventi (es IPOs). Questo potrebbe ridurre i costi burocratici, amministrativi e legali delle procedure di accreditamento fino al 90%;
- la collaborazione con DTCC (Depository Trust & Clearing Corporation), una società di servizi finanziari che agisce da trust negli Stati Uniti e che ha in programma di sviluppare una propria blockchain per fornire servizi di tokenizzazione di securities, emissione e pagamento di dividendi on-chain, aumento di capitale on-chain e consimili;
- la collaborazione attiva con SWIFT, il circuito internazionale di pagamento più utilizzato al mondo e che - da quest'anno, attraverso ISO20022 - connetterà più di 11mila banche agli Smart Contracts su blockchain ETH, favorendo i pagamenti in-ramp e off-ramp (rampe di acceso e uscita) da e tra moneta cripto e FIAT.

Inoltre, le collaborazioni e interconnessioni tra Chainlink e gli attori della finanza tradizionali si vanno facendo sempre più fitti. Basti pensare che Chainlink collabora attivamente

con il World Economic Forum (WEF). Lo stesso Sergey Nazarov, cofounder del progetto, ha partecipato ai forum come speaker.
Inoltre, Chainlink fa parte dell'InterWork Allaince (IWA), un'iniziativa del Global Blockchain Business Council (GBBC), nata per aiutare le imprese ad adottare e utilizzare servizi distribuiti basati su token per le loro attività commerciali.
Date queste premesse, è facile supporre che chi richiederà i servizi di Chainlink li dovrà pagare con il token LINK. Dunque, il token, avrà, presumibilmente, una sempre più reale e significativa utilità.



Se è pur vero che ci sono competitor (BAND, APIFREE, ecc.), è anche vero che le recenti implementazioni hanno

fatto fare a Chainlink un discreto numero di passi rispetto ai suoi diretti concorrenti.
Ad oggi (agosto 2022), consideriamo il prezzo di LINK un ottimo prezzo per accumulare, in una visione di lungo periodo. Questo, naturalmente, al netto di eventi macroeconomici imprevisti e dirompenti.

Ogni analisi presentata rispecchia esclusivamente il punto di vista degli autori e non rappresenta un suggerimento operativo o un consiglio o un segnale di trading e non deve essere presa come supporto previsionale sull'andamento futuro dei mercati e degli strumenti finanziari analizzati.

YIELDHUNTERS

TerraBitcoin è un paese immaginario e reale al tempo stesso. Un Paese che ospita tutti gli asset finanziari ed economici ad oggi presenti nel mondo finanziario che già conosciamo e anche, e soprattutto, quelli che si stanno facendo strada nel mondo delle criptovalute e della blockchain.
Terrabitcoin Ltd ha creato un proprio club privato: il Terrabitcoin Club. Per diventare un membro del Terrabitcoin Club è necessario essere invitati, essere investitori accreditati, essere una persona libera e pagare una fee annuale di ingresso. UNISCITI AL TERRABITCOIN CLUB QUI.

YIELDHUNTERS

Yield Hunters è il servizio di TerraBitcoin Club dedicato alla Finanza Decentralizzata (DeFi). Per accedere al servzio UNISCITI AL TERRABITCOIN CLUB QUI.