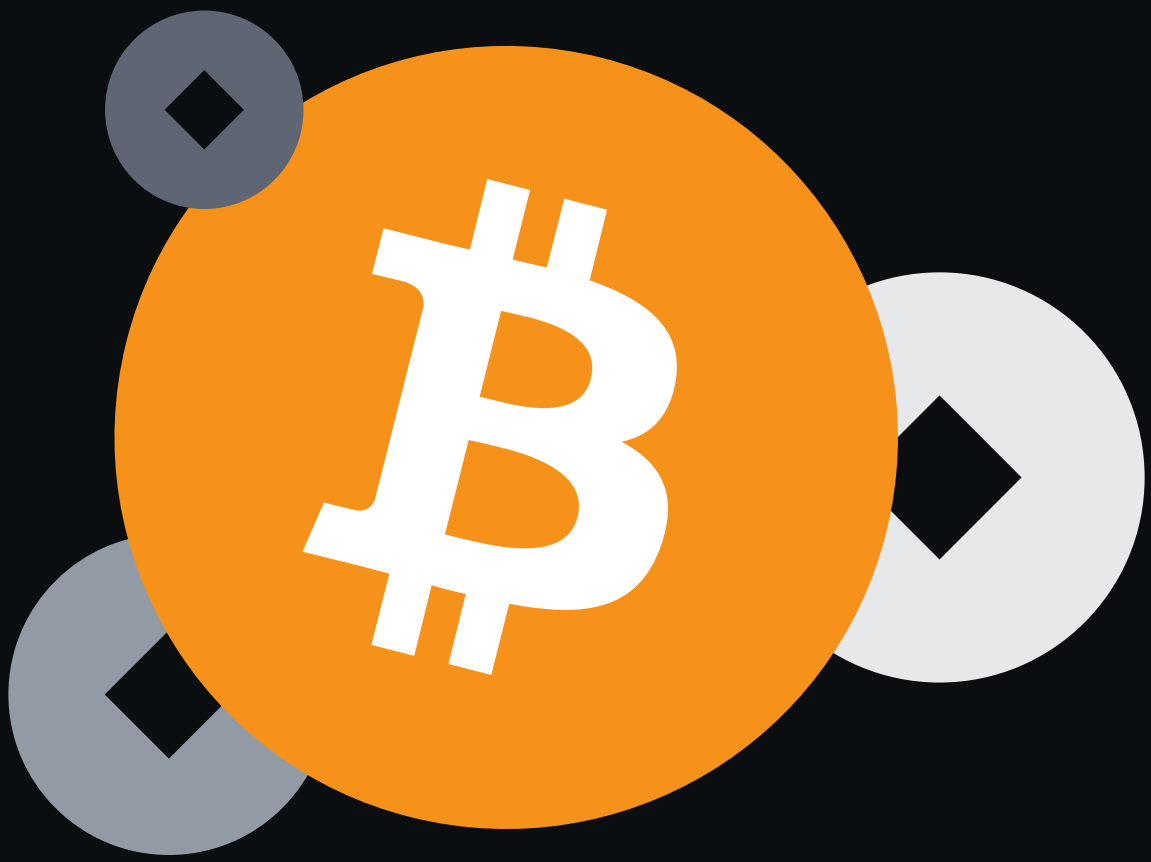
BINANCE RESEARCH

Il futuro di Bitcoin #2: i token

MAY 2024



Shivam Sharma

Indice

1 Punti chiave

- L'avvento degli Ordinals e delle Inscription ha segnato un punto di svolta nella storia di Bitcoin, inaugurando una nuova era per la prima criptovaluta. Abbiamo assistito a ogni tipo di NFT Bitcoin e la comunità è riuscita anche a trovare un modo per implementare token fungibili sopra gli Ordinals con i token BRC-20.
- Più di recente, il creatore degli Ordinals (Casey Rodarmor) ha lanciato un nuovo e più efficiente modo per portare i token fungibili su Bitcoin: il protocollo Runes.
- Il protocollo Runes utilizza l'esclusivo modello UTXO di Bitcoin per portare i token fungibili sulla chain. Gli UTXO Bitcoin, che contengono pile di Satoshi (sat), sono stati estesi per contenere anche saldi di token fungibili arbitrari, denominati Rune.
- Non vengono apportate modifiche al software di Bitcoin o alle regole di consenso. Quello che occorre per la ricostruzione delle Rune è già esistente all'interno della chain Bitcoin, senza componenti di terze parti o off-chain.
- Le Rune non hanno alcun legame con Ordinals, Inscription e token BRC-20 e sono direttamente in competizione con i BRC-20. Sono infatti molto più efficienti nell'utilizzo del blockspace rispetto ai BRC-20 (e contribuiscono meno allo state bloat della chain). Potrebbero anche essere più compatibili con i protocolli Bitcoin (wallet, bridge e soluzioni di scalabilità), poiché esistono semplicemente sugli UTXO (come Bitcoin). Al contrario, i BRC-20 richiedono solitamente un'infrastruttura che supporta Ordinals per poter interagire.
- Al momento del lancio, sono disponibili solo nomi Rune da 13 a 26 caratteri. Ogni quattro mesi e fino al prossimo halving, verrà sbloccato un limite di caratteri più breve. Tutti i nomi di 12 caratteri saranno sbloccati entro agosto 2024. Il culmine del processo è lo sblocco di nomi Rune a un solo carattere che avverrà nel 2028, creando un ciclo di hype naturale per Runes nei prossimi quattro anni.
- Le Rune hanno avuto un impatto visibile sulle commissioni e sul numero delle transazioni Bitcoin dato che, dal loro lancio, hanno portato a oltre 145 milioni di dollari in commissioni e circa il 45% di tutte le transazioni Bitcoin.
- Le Rune hanno meccaniche interne di airdrop (come la creazione posticipata) e altre funzionalità in fase di sviluppo. Negli ultimi mesi anche le proposte di soft fork Bitcoin hanno guadagnato maggiore popolarità. Il miglioramento

dell'infrastruttura Runes sarà fondamentale, soprattutto se mira a detronizzare lo standard BRC-20.

2 Introduzione

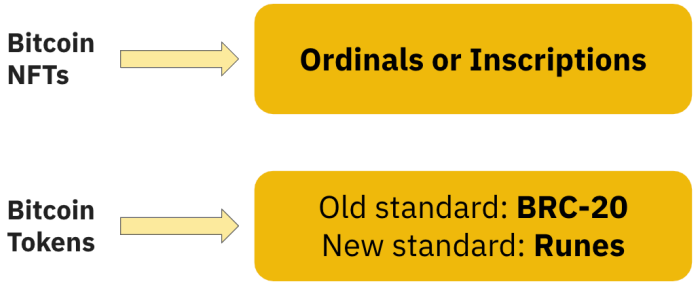
Come abbiamo sottolineato nel nostro report, **Una nuova era per Bitcoin?**, l'avvento degli Ordinals e delle Inscription ha segnato una svolta nella storia di Bitcoin. Sebbene Bitcoin mantenga le sue classiche caratteristiche di "oro digitale", ora c'è anche un gruppo completamente diverso di costruttori e utenti che stanno sperimentando altre funzionalità su Bitcoin.

La **Teoria degli Ordinals** di Casey Rodarmor ci ha fornito una prospettiva speciale attraverso cui vedere Bitcoin. Da qui, sono nate le **Inscription, artefatti digitali su Bitcoin, o NFT Bitcoin**. Abbiamo assistito a ogni tipo di ispirazione, dai classici "JPEG su Bitcoin" alle collezioni di satoshi "rari" e "leggendari". La comunità ha creato un modo per inserire token fungibili sugli Ordinals, lanciando così i **BRC-20**, che hanno conquistato i titoli dei giornali e portato l'attenzione sulle commissioni per tutto il 2023.

Ora, mentre ci troviamo nella nuova era Bitcoin, grazie alle nuove possibilità create tramite Ordinals e al recente halving, arriva un nuovo protocollo di token fungibili. Creato anch'esso da Casey, **il protocollo Runes è un altro tentativo di implementare i token fungibili sui protocolli in un modo diverso e probabilmente più efficiente rispetto allo standard BRC-20**.

In questo report, vogliamo aggiornare gli utenti sugli Ordinals, le Inscription e i token BRC-20 prima di dare un'occhiata da vicino al nuovo protocollo Runes. Parleremo delle caratteristiche principali di Runes e degli utilizzi che possono farne gli utenti. Daremo quindi un'occhiata alla tecnologia alla base del protocollo e alle prossime stagioni di Runes. Analizzeremo inoltre gli effetti che Runes ha avuto finora sulle metriche chiave di Bitcoin, oltre a fornire una prospettiva per i prossimi mesi.

Grafico 1: Un breve ripasso dei termini



Fonte: Binance Research

Questo report fa parte della nostra nuova serie ***Il futuro di Bitcoin*** , in cui analizzeremo le principali aree in cui Bitcoin sta crescendo attraverso una serie di report mirati. In questa edizione parleremo dei token su Bitcoin, tra cui i BRC-20, e del nuovo protocollo Runes.

Nota: quando ci riferiamo a Bitcoin, a volte potremmo utilizzare il suo ticker, BTC. Dal punto di vista tecnico, Bitcoin (BTC) è il token nativo della blockchain di Bitcoin.

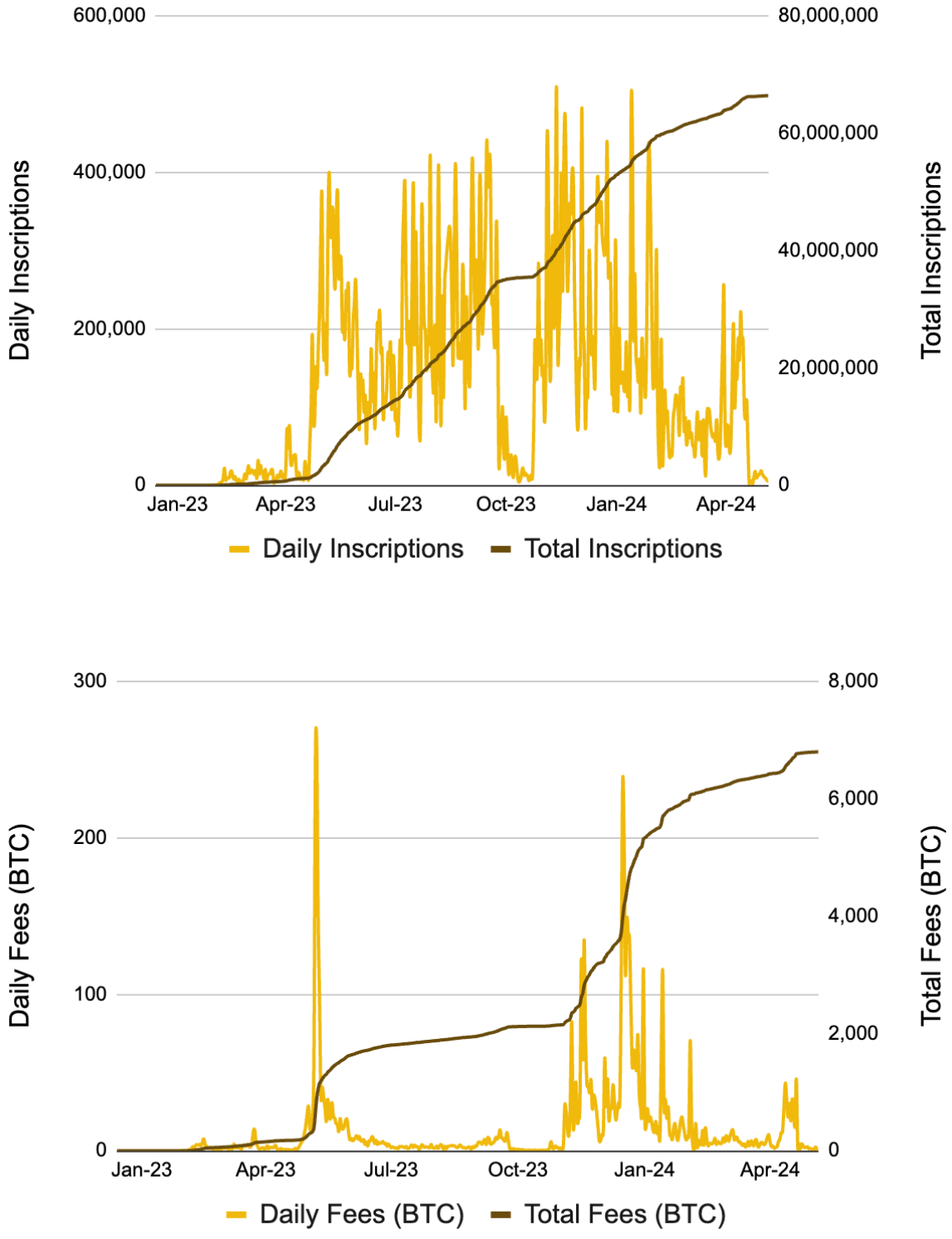
3 Ripasso sugli Ordinals e sui token BRC-20

Come funzionano gli Ordinals e le Inscription?

Ord, un software open-source che può essere eseguito su qualsiasi full node di Bitcoin, consente di monitorare i singoli Satoshi in base a quella che il fondatore Casey Rodarmor ha definito "Teoria degli Ordinals". I satoshi ("sat") sono l'unità più piccola della rete Bitcoin, con 1 Bitcoin = 100.000.000 sat. **La Teoria degli Ordinals attribuisce un identificatore univoco a ogni singolo sat su Bitcoin**. Inoltre, questi singoli sat possono essere "inscritti" con contenuti di ogni tipo, come testo, immagine, video, ecc., per creare una "Inscription", ovvero un artefatto digitale nativo di Bitcoin[1], chiamato anche NFT. I membri della comunità usano spesso i termini Ordinals e Inscription in modo intercambiabile (come può avvenire anche di seguito).

"...i singoli sat possono essere "inscritti" con contenuti di ogni tipo, come testo, immagine, video, ecc., per creare una "Inscription", ovvero un artefatto digitale nativo di Bitcoin, chiamato anche NFT."

Grafico 2: Dalla prima Inscription a dicembre 2022, sono state create oltre 66 milioni di Inscription su Bitcoin, generando oltre 6.800 BTC (~US$430M) in commissioni



Fonte: Dune (@dgtl_assets), Binance Research, al 7 maggio 2024

Per saperne di più sugli Ordinals e sulle Inscription, tra cui la loro storia, il background tecnico, le specifiche rispetto ad altri NFT e i loro effetti sul mercato, consulta il nostro precedente report: **Una nuova era per Bitcoin?**

I token BRC-20

Pochi mesi dopo il lancio degli Ordinals (NFT su Bitcoin), la domanda naturale che ha fatto seguito è stata: "E i token fungibili?". A marzo, un utente di Crypto X con lo pseudonimo di domo ha avviato un thread che teorizzava un metodo chiamato BRC-20 per creare uno standard di token fungibili sul protocollo Ordinals. **L'idea prevedeva la registrazione di dati JSON[2] sui singoli sat tramite gli Ordinals per distribuire, creare e trasferire token BRC-20 fungibili.** JSON è un formato di dati basato su testo, quindi, in sostanza, il metodo consisteva essenzialmente nell'inscrivere testo nei sat per creare token fungibili.

Nei mesi successivi, i token BRC-20, ovvero le Inscription testuali, sono diventati il tipo dominante di Inscription e lo standard predefinito per i token fungibili su Bitcoin. I token BRC-20 hanno raggiunto una capitalizzazione di mercato combinata di oltre 1 miliardo di dollari durante i periodi più attivi dell'anno scorso e, attualmente, mantengono una capitalizzazione di mercato di circa 650 milioni di dollari[3]. Alcuni dei principali progetti di token BRC-20 sono stati listati anche sui principali exchange centralizzati, tra cui $ordi e $sats.

Grafico 3: L'inizio dei token BRC-20 (il primo thread di domo sull'argomento)

Fonte: Twitter (@domodata)

Perché Runes?

Prima di passare a Runes, consideriamo un elemento importante sui token BRC-20. **Lo standard di token BRC-20 ha creato un protocollo per token fungibili sopra un protocollo per token non fungibili (il protocollo Ordinals).** Ricorda che gli Ordinals sono un meta-protocollo sopra Bitcoin, quindi i BRC-20 sono essenzialmente un meta-protocollo sopra un meta-protocollo. Sebbene sia una soluzione intelligente, dovrebbe essere facile intuire che i BRC-20 siano relativamente complicati e poco efficienti.

Il protocollo Runes cerca di risolvere questi problemi creando un metodo **dedicato ai token fungibili su Bitcoin**. Il protocollo Runes non è correlato agli Ordinals o alle Inscription e quindi non eredita quindi la loro complessità, come avviene invece per i BRC-20. Il protocollo Runes è una concettualizzazione molto semplice, che si concentra esclusivamente sui token fungibili su Bitcoin e nient'altro.

"Il protocollo Runes non è correlato agli Ordinals o alle Inscription e non eredita quindi la loro complessità, come avviene invece per i BRC-20."

4 Runes

Gli UTXO Bitcoin

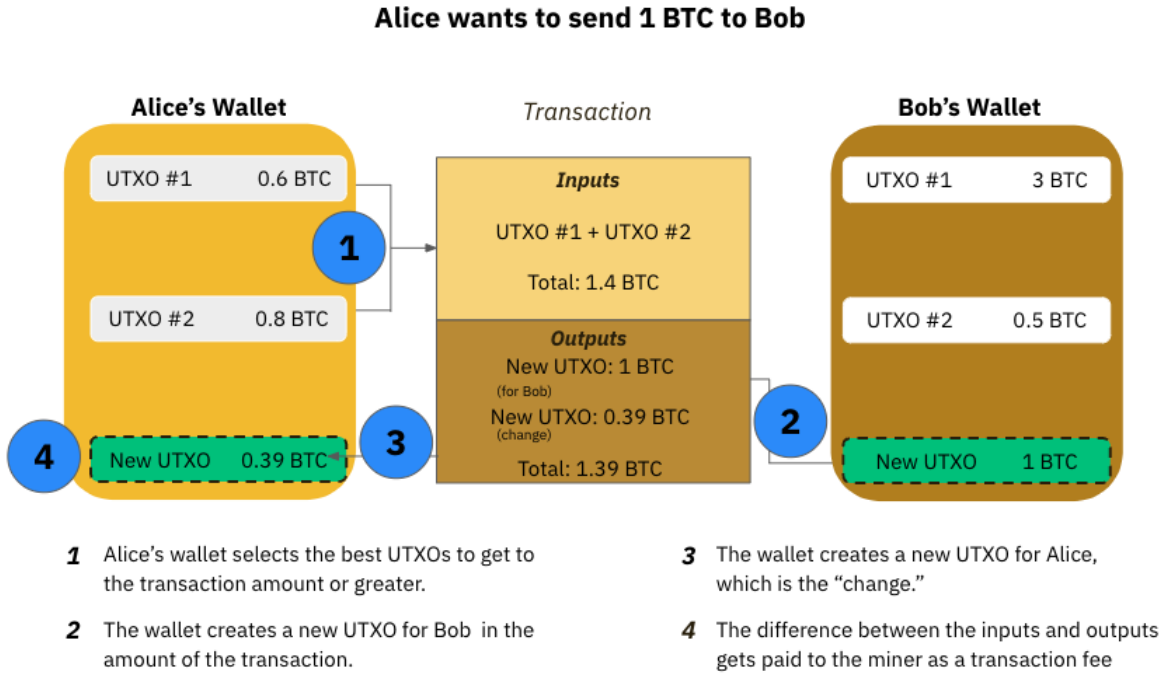
Prima di esplorare Runes, dobbiamo parlare dell'unicità del **modello UTXO di Bitcoin**. UTXO sta per "output di transazione non speso" ("UTXO") e può essere considerato come una pila di Bitcoin (o più specificamente, una pila di satoshi o sat). Tutti i sat, ovvero tutti i Bitcoin, nel mondo sono suddivisi tra vari UTXO. **Alcuni UTXO hanno molti sat, mentre altri ne hanno meno. Un UTXO non ha un'assegnazione predefinita di sat; tutti i tipi di UTXO possono contenere diverse quantità di sat.**

Il modello UTXO di Bitcoin significa questo: **quando hai un wallet Bitcoin, non hai un semplice saldo di Bitcoin, ma un serie di sat su vari UTXO.** Il tuo wallet può spendere uno o più di questi UTXO, e riceverai un UTXO come resto.

Considera un semplice esempio in cui Alice vuole trasferire 1 BTC a Bob. Supponiamo che Alice abbia due UTXO nel suo wallet Bitcoin, del valore di 0,6 BTC e 0,8 BTC. Quando Alice invia 1 BTC a Bob, il protocollo Bitcoin prende entrambi gli UXTO di Alice (del valore totale di 1,4 BTC) e li divide in tre output separati. Uno di questi diventa la commissione di

transazione (che va ai miner); Bob ottiene un UTXO del valore di 1 BTC, mentre Alice riceve il resto.

Grafico 4: Il modello UTXO di Bitcoin



Fonte: Binance Research

Questo meccanismo è **distinto dal modello basato su account utilizzato dalla maggior parte degli altri token Layer 1 ("L1"), tra cui Ethereum**. Sebbene non sia del tutto preciso, un **modello teorico a cui possiamo pensare è quello dei contanti rispetto alla carta di debito.** Ad esempio, se Alice vuole inviare 1 ETH a Bob, dato che non esiste il concetto di UTXO su Ethereum, non c'è bisogno di dividere gli UTXO in diversi output. Il protocollo Ethereum può semplicemente prendere 1 ETH dal saldo di Alice e inviarlo a Bob dopo aver pagato una commissione di transazione separata. È più simile a una transazione con carta rispetto agli UTXO di Bitcoin, che possono essere invece paragonati ai contanti.

Cos'è Runes

Il protocollo Runes

Il protocollo Runes[4] è un protocollo di token fungibili su Bitcoin. Il protocollo **estende il modello UTXO di Bitcoin in un modello in cui gli UTXO possono contenere saldi di token fungibili arbitrari (chiamati Rune)** insieme ai loro sat.

Ord, lo stesso software che consente anche il monitoraggio dei sat per gli Ordinals **fornisce un'implementazione del protocollo Runes**. Ord è anche un wallet e un block explorer. L'esecuzione di Ord insieme a un nodo core Bitcoin ti consente quindi di visualizzare quali UTXO contengono anche Rune.

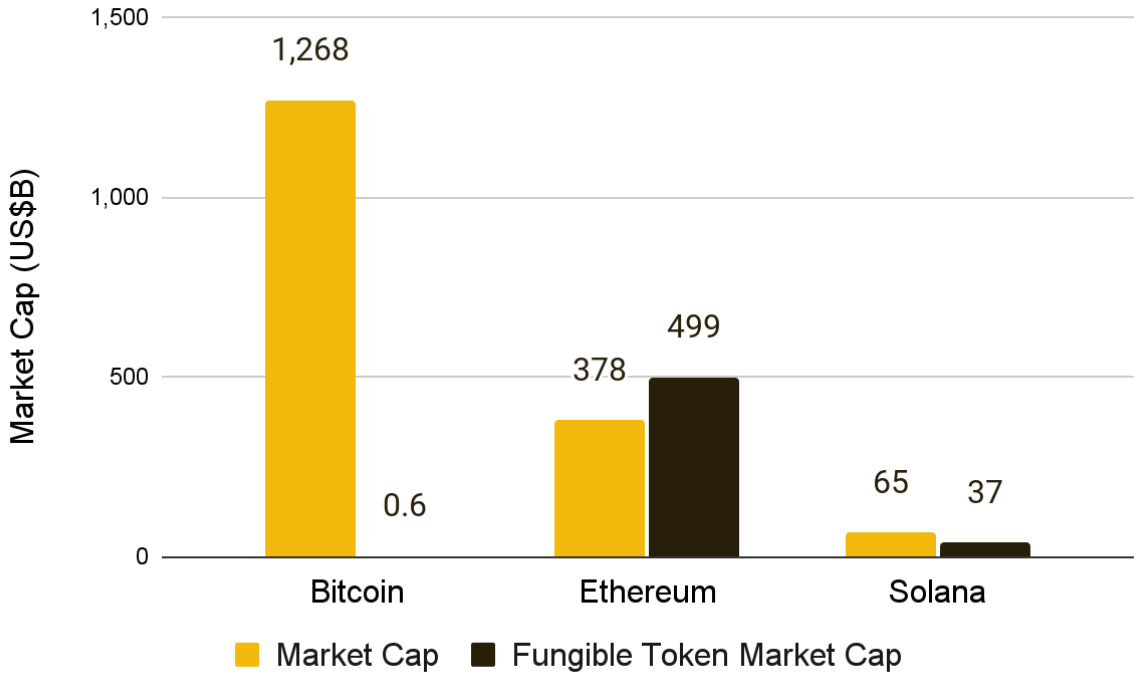
Un fatto importante da notare è che **né gli Ordinals né le Rune richiedono modifiche al software Bitcoin o alle regole di consenso.** La creazione di questi token è possibile semplicemente osservando le stesse transazioni Bitcoin con una lente speciale. Il software ord è la lente speciale e dà un significato aggiuntivo alle transazioni standard di Bitcoin.

Infatti, **tutto ciò che serve per ricostruire gli Ordinals, le Inscription e le Rune esiste già all'interno della blockchain di Bitcoin**. Non c'è **nessun affidamento su terze parti o componenti off-chain, ed è un punto di forza notevole di questi token**. Un'altra caratteristica positiva che ne deriva è che tutti potrebbero teoricamente interrompere l'esecuzione del proprio software ord, riprendere dopo un mese e tutto sarà aggiornato. Ogni aspetto all'interno dell'universo Ordinals e Runes è retro-compatibile con Bitcoin, senza dipendenze esterne.

Dobbiamo anche notare che si tratta di un **meta-protocollo costruito su Bitcoin, ma Bitcoin non ne è a conoscenza, e non ha bisogno di esserlo**. Gli utenti e i validatori interessati possono scegliere di visualizzare questo universo aggiuntivo eseguendo un software in più insieme al proprio nodo. Ma possono anche scegliere di ignorarlo completamente.

"...tutto il necessario per ricostruire gli Ordinals, le Inscription e le Rune esiste all'interno della blockchain di Bitcoin. Non occorre fare affidamento su terze parti o componenti off-chain"

Grafico 5: Il mercato dei token fungibili su Bitcoin ha un grande potenziale di crescita



Fonte: Franklin Templeton, Binance Research, al 15 aprile 2024

OP_RETURN

Su ogni UTXO può esistere un numero casuale di Rune, insieme alla quantità di sat che contiene. In particolare, i dati per le **Rune sono memorizzati all'interno del campo OP_RETURN di una transazione Bitcoin**. OP_RETURN[5] è un codice operativo ("opcode") del linguaggio di scripting Bitcoin che **consente agli utenti di salvare dati arbitrari sulla blockchain**. Il limite ufficiale per i dati in un campo OP_RETURN è di 80 byte. La documentazione ufficiale di Runes offre ulteriori dettagli sull'utilizzo degli output di OP_RETURN.

Gli obiettivi di Runes

Come abbiamo già anticipato sopra, una delle motivazioni principali alla base di Runes è quella di creare uno standard di token fungibili dedicato per Bitcoin, senza ereditare la complessità degli Ordinals.

Tuttavia, questo non è l'unico obiettivo. Il fondatore Casey Rodarmor ha indicato che l**e memecoin e la speculazione continuano a guadagnare terreno nel mondo crypto, ma per lo più al di fuori di Bitcoin.** Ha inoltre notato che dopo aver speculato su altri L1 come Ethereum, Solana o BNB Chain, spesso gli utenti usano parte dei loro profitti per acquistare L1 di base. Ad esempio, se un utente guadagna all'interno dell'ecosistema Solana, potrebbe essere più propenso ad acquistare $SOL con quei fondi.

Casey vuole che questo ciclo avvenga anche su Bitcoin ed è estremamente onesto e diretto su cosa siano le Rune:

"Le Rune sono una forma di gioco d'azzardo degenerato... Non è il futuro della finanza... Runes è un protocollo di token fungibili, in modo che le persone possano scambiare meme..."

Fonte: Casey Rodarmor, sul podcast Hell Money

Questo aspetto è molto importante da notare perché alcuni creatori di Rune potrebbero promettere un certo livello di utilità e valore dall'acquisto di Runes. Nel medio termine, l'evoluzione potrebbe anche essere in questo senso, e l'utilità potrebbe iniziare a svilupparsi nelle prossime settimane e mesi, soprattutto se ci dirigiamo verso i Layer Bitcoin ("L2"). Tuttavia, non dobbiamo perdere di vista che **parte della motivazione iniziale di Runes è la capacità di creare memecoin in modo efficiente ed efficace e di speculare su Bitcoin.**

Proprietà di Runes

Il processo di creazione di una nuova Rune viene chiamato **incisione**. Quando si incide una nuova Rune, si riserva un nome e si impostano le sue proprietà.

- **Nome:** Il nome di una Rune è **unico** e può essere composto da qualsiasi combinazione di lettere dalla A alla Z maiuscola.
  - Al momento del lancio, i nomi possono essere **tra 13 e 26 caratteri**, anche se questo cambierà tra le varie stagioni Runes.
  - Il nome può anche contenere un "**distanziatore**", che è essenzialmente un punto elenco nel nome, per migliorare la leggibilità. Ad esempio, il primo Rune, Rune #0, è chiamato UNCOMMON•GOODS.
  - L'**unicità di un nome è indipendente dai distanziatori.** Ad esempio, non puoi nominare un'altra Rune UNCOMMONG•OODS. I distanziatori possono essere inseriti solo tra due lettere e non contano per il numero dei caratteri di un nome.

- **Simbolo:** Questo è un singolo punto Unicode per illustrare la "valuta" di una Rune. Può essere un'emoji, purché sia un singolo punto Unicode[6]. Il simbolo non deve essere necessariamente unico.

- **Divisibilità:** Definisce in quante sottounità può essere suddivisa una Rune. Ad esempio, una divisibilità pari a 1 significherebbe che ogni Rune può essere ulteriormente suddivisa in dieci sottounità.

- **Pre-mining:** L'emittente, o etcher, può scegliere di allocare preventivamente le unità di una nuova Rune.

- **Termini:** Una Rune può avere un mint aperto, che consente a qualsiasi utente di mintare e allocare unità di quella Rune, purché paghi le commissioni di transazione. Questa possibilità può essere soggetta a un numero limitato di termini.
  - **Limite**: Il numero di volte in cui una Rune può essere creata.
  - **Importo per mint**: La quantità di Rune create con ogni mint.
  - **Altezza del blocco iniziale/finale**: Tra quali blocchi è aperto il mint? Questa caratteristica può essere personalizzata in modo che il mint si apra subito o dopo diversi blocchi successivi all'incisione. Le implicazioni sono interessanti, e ne parleremo nella sezione Prospettive.

Il processo di riscatto di una nuova Rune viene chiamato **mint,**, in modo simile a quando viene creato un NFT.

La fase finale del processo è il **trasferimento** della Rune. Quando gli input delle transazioni, ad esempio gli UTXO Bitcoin, contengono Rune, queste vengono trasferite agli output delle transazioni quando trasferisci l'UTXO.

In particolare, se trasferisci un numero di UTXO con quantità differenti di Rune diverse, tutte le Rune andranno al primo output non OP_RETURN di quella transazione. Per modificare e gestire come e quali Rune di input vengono trasferite a quali output, l'utente può utilizzare una **Runestone**, un messaggio del protocollo Runes (che vedremo in dettaglio di seguito).

- **Editti:** Sono le istruzioni di trasferimento all'interno di una Runestone, che consentono agli utenti di personalizzare l'output a cui una Rune viene trasferita e l'importo. Le Rune possono anche essere sottoposte a burn.

In sintesi, un creatore incide una Rune e ne imposta le proprietà. Gli utenti possono quindi creare e trasferire. È stato volontariamente creato come un sistema molto semplice.

Rune #0

- La prima Rune, Rune #0, è stata **incisa dal fondatore del protocollo Runes, Casey Rodarmor**. Il nome della Rune è **UNCOMMON•GOODS**.
  - Il mint per questa Rune è iniziato nel blocco dell'halving e continuerà fino al prossimo halving.
  - Gli utenti possono creare la Rune tutte le volte che vogliono, ma ogni mint può riscattare solo una Rune UNCOMMON•GOODS alla volta.
  - La divisibilità di UNCOMMON•GOODS è 0, ovvero non può essere ulteriormente suddivisa.

Runestone

- Una **Runestone è un insieme codificato di istruzioni, memorizzate nel campo OP_RETURN, che definisce cosa vorresti fare con le Rune in una transazione Bitcoin.**
  - ➢ Ad esempio, la Runestone può dichiarare "Voglio creare questa Rune", o "Voglio incidere una nuova Rune" o "Voglio trasferire queste Rune".

- Come accennato in precedenza, **in assenza di una Runestone, per impostazione predefinita tutte le Rune negli input vanno al primo output non OP_RETURN.** Quindi, se vuoi un risultato diverso, includi una Runestone e aggiungi un editto (che fornirà le istruzioni specifiche su quali rune dovrebbero essere inviate).

- Bitcoin attualmente consente solo un **massimo di 80 byte di dati nel campo OP_RETURN.** Sebbene le Runestone normali si adattino facilmente a quelle dimensioni, a **una transazione di grandi dimensioni potrebbe richiedere una Runestone più grande**. Questo potrebbe essere dovuto al fatto che l'utente sta cercando una distribuzione arbitraria di un numero di Rune diverse su un numero di output differenti (un **airdrop** per esempio). Pertanto, se le Rune si dimostreranno sufficientemente popolari, la discussione sull'aumento del limite di dimensione OP_RETURN di 80 byte di Bitcoin potrebbe diventare più importante.

"...se le Rune si dimostreranno sufficientemente popolari, la discussione sull'aumento del limite di dimensione OP_RETURN di 80 byte di Bitcoin potrebbe diventare più importante."

- Dobbiamo anche notare che è improbabile che gli utenti si occupino direttamente di Runestone, ed è probabile che questo processo venga astratto dai fornitori di front-end.

Confronto con i token BRC-20

Vogliamo sottolineare ancora una volta che **le Rune sono completamente estranee agli Ordinals, alle Inscription e ai token BRC-20 ed entrano infatti direttamente in competizione con i BRC-20.**

Nella nostra tabella di seguito abbiamo riportato alcune differenze. Due punti che vorremmo evidenziare in particolare sono **l'efficienza** e **la compatibilità**. Le Rune rappresentano un uso molto più efficiente del blockspace, perché i token BRC-20 richiedono due transazioni on-chain per ogni trasferimento, rispetto a una sola prevista invece per Runes. Questo comporta, in concreto, che **possiamo aspettarci molto meno blockchain bloat da Runes, rispetto ai token BRC-20**. Di conseguenza possiamo pensare a una mempool meno affollata e una minore probabilità che le commissioni aumentino per Runes, rispetto ai BRC-20.

Per quanto riguarda la compatibilità, considera il fatto che **le Rune vengono trasferite attraverso UTXO, ovvero nel modo tipico con cui avvengono i trasferimenti Bitcoin.** Qualsiasi protocollo che funzioni con Bitcoin, che si tratti di un wallet, un bridge, Lightning Network o altri L2, dovrebbe (molto probabilmente) funzionare anche con le Rune. Questo non è necessariamente vero per i token BRC-20, che richiedono un'infrastruttura aggiuntiva per supportare gli Ordinals, prima di poter supportare i BRC-20.

Grafico 6: Alcune differenze chiave tra i BRC-20 e le Rune

Caratteristica	BRC-20	Runes
Design	BRC-20 è un meta-protocollo su Ordinals, ovvero un protocollo di token fungibili che opera su un protocollo di token non fungibili. Aggiunge complessità.	Le Rune sono appositamente studiate per i token fungibili e intenzionalmente molto semplice. Non ereditano la complessità degli Ordinals.
Tech	BRC-20 è stato rilasciato come specifica sperimentale da un membro della comunità. L'implementazione è stata lasciata alla comunità.	Runes è stato rilasciato con una specifica dettagliata e un'implementazione di riferimento.
Archiviazione dei dati	L'uso di dati witness (fino a 4 MB) porta a un maggiore ingombro on-chain.	L'uso del campo OP_RETURN (80 byte) è più efficiente.
Efficienza	Richiede due transazioni on-chain per ogni trasferimento.	Gli utenti possono trasferire Rune tramite normali transazioni Bitcoin, con una sola transazione per trasferimento.
Distribuzione	Mint aperto: una volta completata la prima creazione, chiunque può creare.	Maggiore flessibilità in quanto supporta varie forme di distribuzione, tra cui mint aperto, pre-mining, mint posticipato, ecc.
Compatibilità	Solo wallet che supportano Ordinals.	Il design UTXO offre a Runes una maggiore compatibilità con wallet (ad es., Lightning), L2, bridge e app DeFi.

Fonte: Ordinals / documentazione BRC-20, Binance Research

Stagioni Runes

Una delle caratteristiche interessanti di Rune è la loro **convenzione di denominazione**. Come accennato in precedenza, il nome di una Rune è unico e può essere composto da qualsiasi combinazione di lettere A-Z in maiuscolo. **Al momento del lancio, i nomi possono avere una lunghezza compresa tra 13 e 26 caratteri**. Tuttavia, nel tempo, gli utenti potranno incidere Rune con nomi più brevi.

- In particolare, ogni quattro mesi dal lancio verrà sbloccata una nuova lunghezza più breve di possibili nomi Rune.

- **Ad esempio, entro agosto 2024 (quattro mesi dal lancio di Runes), verranno sbloccati tutti i nomi Rune a 12 caratteri. Quattro mesi dopo si sbloccheranno i nomi a 11 caratteri e così via.**

- Questo meccanismo è destinato a continuare fino al prossimo halving Bitcoin nel 2028, quando negli ultimi quattro mesi si sbloccheranno le Rune a carattere singolo.

- Dobbiamo notare che **gli sblocchi avvengono per blocco**, e non in un cliff release di quattro mesi. Ogni blocco vedrà più nomi Rune disponibili, in cui tutti i possibili nomi per un determinato numero di caratteri verranno sbloccati alla fine di ogni periodo di quattro mesi.

- Questo aiuta a innescare un **ciclo di hype naturale per Runes nei prossimi quattro anni**, dando vita alle stagioni Runes.

- Ci sono anche alcune implicazioni interessanti dal punto di vista della performance di mercato. Ad esempio, se le Rune di 3-6 caratteri si sbloccano durante un ciclo bear, potrebbe esserci l'opportunità, per gli utenti, di incidere e creare nomi Rune più brevi e più allettanti in un momento in cui il prezzo di Bitcoin e le commissioni sono relativamente bassi.

"Ad esempio, se le Rune di 3-6 caratteri si sbloccano durante un ciclo bear, potrebbe esserci l'opportunità, per gli utenti, di incidere e creare nomi Rune più brevi e più allettanti in un momento in cui il prezzo di Bitcoin e le commissioni sono relativamente bassi."

4 Effetti sul mercato

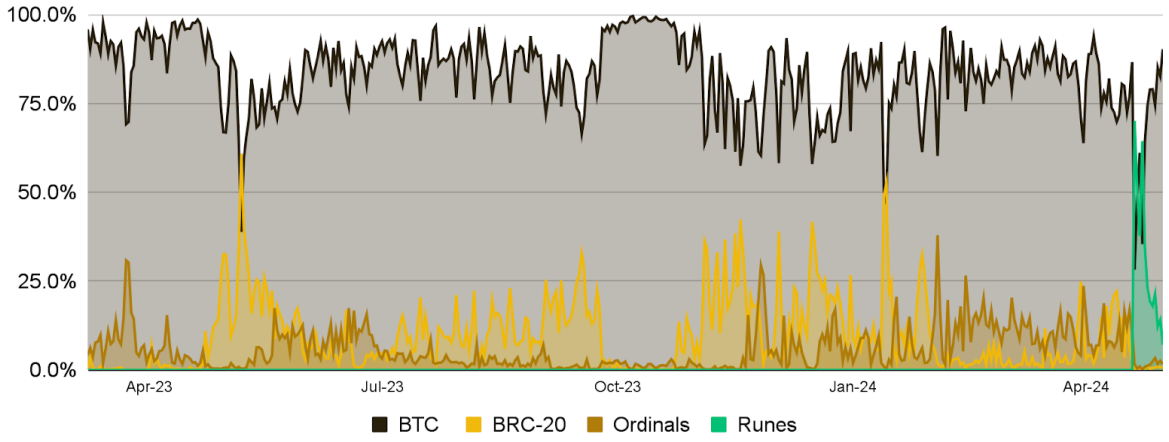
Il protocollo Runes è stato lanciato durante l'halving di Bitcoin del 2024 ed è stato ben commercializzato in anticipo, con diversi progetti Ordinals che offrivano airdrop pre-Rune e molte discussioni sull'argomento su Crypto X. Come previsto, il lancio iniziale è stato molto entusiasmante, con effetti evidenti sulle metriche di Bitcoin.

Commissioni

- Dal lancio, le Rune hanno generato oltre 2.200 BTC in commissioni, equivalenti a circa 145 milioni di dollari al momento della stesura.
  - Questo rappresenta il **~30% di tutte le commissioni sulla rete Bitcoin dal 20 aprile.**

- Tuttavia, sia la proporzione delle commissioni rispetto agli altri tipi di transazioni, sia le commissioni nominali **sono lentamente diminuite nei giorni successivi al lancio**.
  - La quota di commissioni Runes è scesa da una media del ~43% nella prima settimana dopo il lancio al ~21% negli ultimi sette giorni.

Grafico 7: Quota delle commissioni Bitcoin (per tipo di transazione)



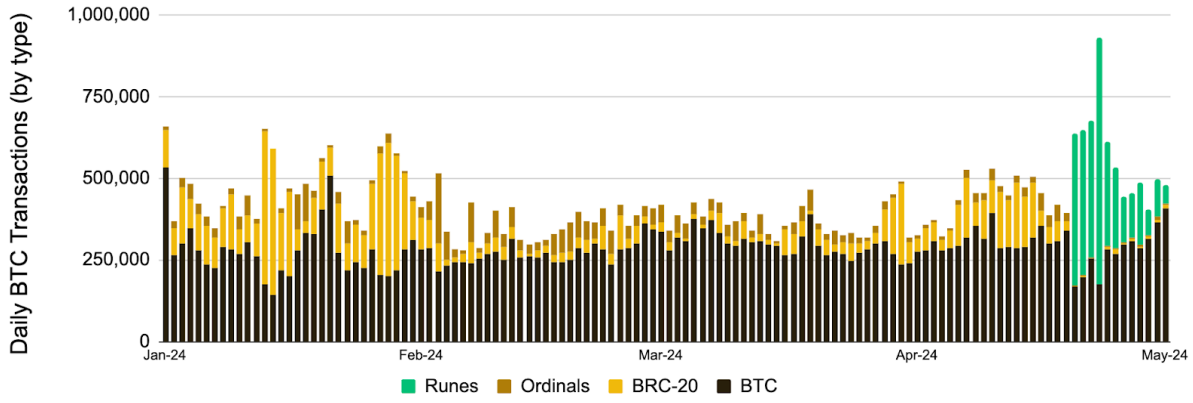
Fonte: Dune (@cryptokoryo), Binance Research, al 7 maggio 2024

Numero di transazioni

- Dal lancio, si sono verificat**e oltre 4,8 milioni di transazioni che hanno coinvolto Rune** sulla rete Bitcoin.
  - ➢ Questo rappresenta il **~45% di tutte le transazioni Bitcoin dal 20 aprile.**

- Tuttavia, il valore **è in seguito diminuito**, passando da una media di ~400.000 transazioni nella prima settimana dopo il lancio, a una media di ~208.000 negli ultimi sette giorni.

Grafico 8: Transazioni Bitcoin (per tipo)



Fonte: Dune (@cryptokoryo), Binance Research, al 7 maggio 2024

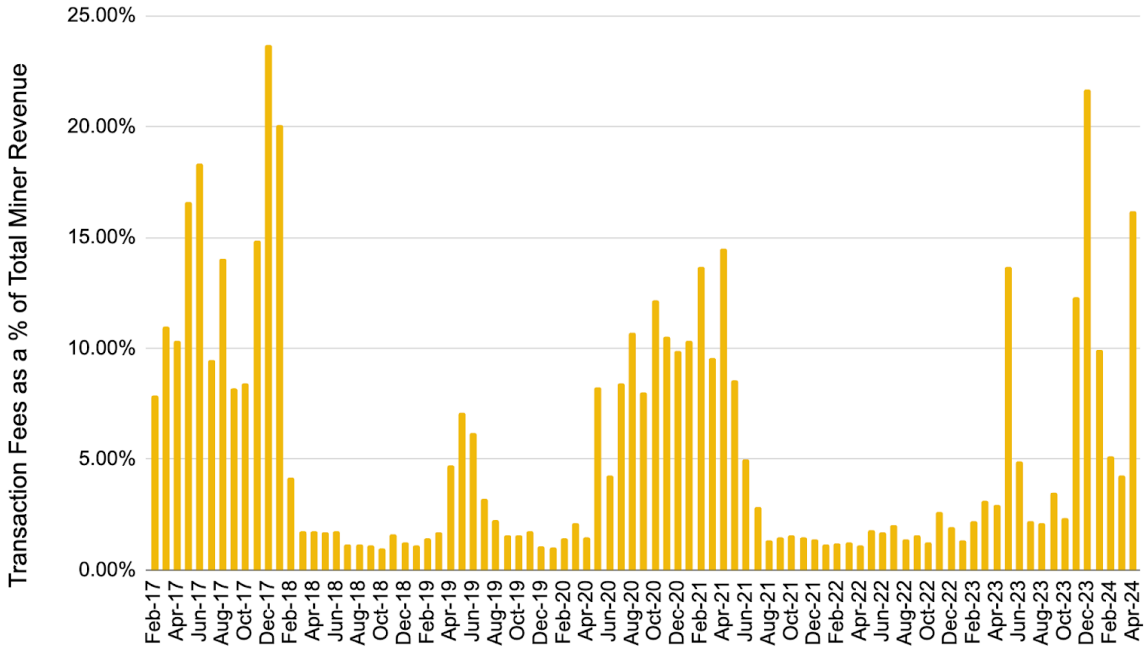
Commissioni di transazione e miner

Una cosa che dovremmo tenere a mente è che, **mentre l'aumento delle commissioni di transazione** non è uno scenario ideale per gli utenti che vogliono effettuare transazioni su Bitcoin L1, è invece **fondamentale per la sopravvivenza a lungo termine dei miner Bitcoin** e, di conseguenza, per la sostenibilità del modello di sicurezza di Bitcoin.

Abbiamo affrontato questo problema in modo più dettagliato nel nostro recente report, Il futuro di Bitcoin #1: L'halving e i prossimi passi. In sintesi, le entrate dei miner sono costituite dalla sovvenzione per blocco e dalle commissioni di transazione. **Storicamente, le commissioni di transazione hanno rappresentato una percentuale relativamente limitata dei loro ricavi complessivi, anche se la situazione è cambiata con l'avvento degli Ordinals, delle Inscription, e dei token BRC-20 l'anno scorso.**

Tuttavia, come mostra il grafico 9, da gennaio 2017 le commissioni di transazione mensili di Bitcoin, in misura percentuale rispetto alle entrate totali dei miner, sono spesso inferiori al 5%. In particolare, le commissioni di transazione mensili di Bitcoin hanno raggiunto una media del 4,5% delle entrate totali dei miner dall'inizio del 2022, anche se questo numero è in crescita e si attesta all'8,5% dall'inizio dell'anno.

Grafico 9: Le commissioni di transazione mensili di Bitcoin in % rispetto alle entrate totali dei miner erano in media dell'1,6% nel 2022, del 6% nel 2023 e dell'8,5% nel 2024 finora



Fonte: The Block Data, Binance Research, al 30 aprile 2024

Con la sovvenzione per blocco che si dimezza ogni quattro anni (l'ultimo è diminuito da 6,25 BTC a 3,125 BTC), **le commissioni di transazione Bitcoin devono aumentare e compensare le mancate entrate dei miner. Se questo non avviene, la sostenibilità a lungo termine del modello di sicurezza di Bitcoin viene messa in discussione**, poiché l'halving rappresenta un drastico calo delle entrate (fino al 50% in meno per alcuni miner).

Se non vengono sufficientemente ricompensati, sempre più miner abbandoneranno il mercato, rendendo la rete Bitcoin meno sicura e più facile da attaccare. Pertanto, le commissioni DEVONO aumentare nel medio termine. Sebbene le commissioni abbiano ancora molta strada da fare prima di diventare un ingrediente assolutamente necessario per la sicurezza di Bitcoin, i progressi compiuti attraverso Ordinals, Inscription, BRC-20 e ora Runes sono positivi e incoraggianti.

5 Prospettive

Funzionalità future

- Gli emittenti possono impostare una "**turbo flag**"[7] sul loro token Rune, che **attiva le funzionalità future per le loro Rune**. Se questa bandiera non è impostata, il token Rune non verrà aggiornato con le modifiche future.

- Una delle idee che Casey ha discusso in precedenza è una **Runes Lottery**.
  - L'idea è che, ad ogni adeguamento della difficoltà su Bitcoin (all'incirca ogni 14 giorni), ogni Rune eseguirà la propria lotteria.
  - Gli utenti possono scambiare le loro Rune per biglietti della lotteria ogni due settimane e il vincitore alla fine di quel periodo riceverà tutte le Rune raccolte.
  - Dobbiamo notare che questa è semplicemente un'idea che Casey ha proposto e non un'idea scolpita nella pietra.

- Dato che la stessa implementazione software, ord, ci consente di vedere sia **gli Ordinals che le Rune su Bitcoin, c'è il potenziale per un certo livello di integrazione tra le due primitive.** Anche se questo aspetto non è stato discusso, dato che entrambi sono fondati da Casey e collegati tramite il software ord, c'è una certa probabilità di integrazioni interessanti tra i due.

- Ricorda, anche se può essere un ottimo slogan di marketing dire che il tuo **token Rune ha le stesse proprietà di sicurezza di Bitcoin (il che è tecnicamente vero)**, questo **non significa che le Rune abbiano un'utilità** o un caso d'uso reali.
  - Sebbene alla fine possa svilupparsi una vera utilità, ribadiamo che parte della motivazione alla base di Rune è quella di fornire uno strumento efficiente per creare memecoin e consentire la speculazione all'interno dell'ecosistema Bitcoin.

Meccanismi airdrop

- Come accennato in precedenza, il protocollo Runes consente agli emittenti di incidere la propria Rune e scegliere quando iniziare e terminare il mint del proprio token. Il potenziale per un **mint posticipato** può introdurre alcune proprietà interessanti.
  - Ad esempio, un emittente potrebbe voler **incidere la propria Rune in un momento importante** (magari durante un regolamento della difficoltà di Bitcoin o un evento macro globale), ma **posticipare il mint fino a quando le**

commissioni saranno più convenienti o dopo aver promosso e pubblicizzato la Rune per qualche settimana.

- Anche le Runestone forniscono **un supporto esplicito per la suddivisione equa delle Rune di input in un numero di output**.
  - Ad esempio, se un emittente vuole eseguire un airdrop per 1.000 persone di 1.000 Rune ciascuno, c'è un modo nativo per strutturare una Runestone chiedendogli di dividere equamente gli input tra gli output.

Le proposte soft fork riaccendono l'attenzione

- Gli aggiornamenti tecnici più recenti di Bitcoin, o soft fork, sono stati Segregated Witness ("SegWit") nel 2017 e Taproot nel 2021. L'implementazione dei soft fork in Bitcoin è storicamente lenta, ed è stata vista come una caratteristica sia positiva che negativa della rete. Tuttavia, negli ultimi mesi, le proposte di soft fork di Bitcoin hanno attirato attenzione e slancio in seguito alla crescita di Ordinals, Inscription e BRC-20.
  - **OP_CAT:** Si tratta di un codice operativo disponibile nelle prime versioni di Bitcoin, ma rimosso molto presto dallo stesso Satoshi Nakamoto. "CAT" è l'abbreviazione di "concatenate", dato che **OP_CAT consiste nell'unire due diversi elementi nello script Bitcoin.**
  - Anche se non entreremo nei dettagli tecnici, **le implicazioni di OP_CAT possono essere significative, soprattutto nello sviluppo di L2 Bitcoin e delle capacità e funzioni smart contract**. Puoi trovare maggiori dettagli tecnici qui.

  - **OP_CTV:** Questo codice operativo è l'abbreviazione di "CHECKTEMPLATEVERIFY" e, se abilitato, **consentirebbe agli utenti di specificare esattamente quanti Bitcoin possono essere spesi in una transazione e verso quale direzione possono andare quei Bitcoin.**
  - OP_CTV può essere fondamentale per l'abilitazione di **patti** (regole specifiche che limitano il modo in cui gli UTXO possono essere spesi e che hanno **implicazioni positive per la sicurezza e la scalabilità**. OP_CTV può anche avere altri vantaggi di scalabilità e contribuire ad abilitare le pool di pagamento. Puoi trovare un articolo utile con varie implicazioni qui.

- La cosa più interessante è che, **siccome le Rune si mappano su Bitcoin in modo estremamente nativo** (muovendosi con gli UTXO di Bitcoin), **qualsiasi aggiornamento tecnico implementato tramite soft fork può essere utilizzato per aggiungere funzionalità interessanti alle Rune.**

- ➢ Di conseguenza, **un nuovo gruppo di utenti Bitcoin**, che si tratti di entusiasti degli Ordinals, trader o semplicemente degen, improvvisamente hanno un **incentivo per fare pressione per proposte soft fork di Bitcoin.**
- ➢ Questo crea un nuovo livello di supporto per le proposte soft fork di Bitcoin, un supporto che finora è mancato.

Il miglioramento dell'infrastruttura è fondamentale

- ❖ L'infrastruttura Runes, simile a quella dei BRC-20, **non è molto intuitiva e può essere difficile da capire**, soprattutto per gli utenti non nativi crypto.
  - ➢ Questo è un **punto critico da migliorare** se le Rune vogliono diventare relativamente mainstream in tempi brevi.
  - ➢ Da un punto di vista informale, questo è sicuramente qualcosa che ha frenato i BRC-20, e sarà importante monitorare se Runes può fare meglio.

- ❖ Entità native di Bitcoin come Unisat e Xverse stanno guidando la carica, e altri CEX sono coinvolti. Tuttavia, il processo rimane relativamente complicato rispetto all'esperienza su Ethereum, Solana o BNB Chain.

La domanda finale: Runes riuscirà a detronizzare i BRC-20?

- ❖ Allo stato attuale delle cose, **BRC-20 ha chiaramente un vantaggio** e alcuni effetti di rete che Runes dovrà superare. Ricordiamo che i BRC-20 detengono ancora una capitalizzazione di mercato di oltre 640 milioni di dollari.

- ❖ Tuttavia, come abbiamo sottolineato sopra, **Runes è lo standard di token più efficiente, meno complesso rispetto ai BRC-20 e ha anche maggiori probabilità di essere nativamente compatibile con le soluzioni dell'ecosistema Bitcoin**, compresi L2 e bridge. Il loro successo finale dipenderà dalla capacità di Runes di capitalizzare i suoi vantaggi competitivi e di concludere le giuste **integrazioni e partnership**, insieme allo sviluppo dell'infrastruttura.

- ❖ Dovremmo anche notare che **circolano voci sul rilascio di un aggiornamento da parte di BRC-20** per risolvere alcuni dei suoi problemi di progettazione. Questo potrebbe rivelarsi uno sviluppo interessante nei prossimi mesi.

6 In sintesi

Il protocollo Runes è un'aggiunta interessante al crescente ecosistema Bitcoin in questa nuova era per la principale criptovaluta. In ultima analisi, ci sono due fattori principali:

1. Ordinals, Inscription, BRC-20 e Runes stanno tutti **avendo degli effetti sulle commissioni di Bitcoin e stanno lavorando per risolvere il problema del budget di sicurezza a lungo termine di Bitcoin**. Stanno creando ulteriori tipi di comportamenti transazionali su Bitcoin, rendendo il blockspace sempre più dinamico dal punto di vista delle commissioni. È difficile negare che questa sia un'ottima cosa, soprattutto in seguito al più recente halving di Bitcoin, riflettendo sulla rapida diminuzione della sovvenzione per blocco e sulla crescente importanza delle commissioni di transazione per la sostenibilità di Bitcoin.

2. Tutte queste diverse primitive continuano a **incentivare l'attività di sviluppo di Bitcoin** e contribuiscono a cambiare il livello sociale e la cultura Bitcoin, rendendo interessante costruire sul protocollo. Senza escludere il fatto che fungono anche da gateway per comprare Bitcoin e renderlo più popolare tra un gruppo completamente nuovo di utenti e costruttori.

Se le Rune raggiungeranno le vette dei BRC-20 e la mania Ordinals, o addirittura li supereranno, è ancora da vedere. Quello che il loro successo (o insuccesso) potrebbe significare per Bitcoin nei prossimi mesi sarà molto importante e interessante da seguire. Rimaniamo cautamente ottimisti, continuando a monitorare attentamente l'evoluzione delle cose.

"Stanno creando ulteriori tipi di comportamenti transazionali su Bitcoin, rendendo il blockspace sempre più dinamico dal punto di vista delle commissioni."

Questa è la seconda parte della nostra nuova serie Il futuro di Bitcoin. Tieni d'occhio la prossima puntata, dove tratteremo un altro aspetto importante di Bitcoin: la scalabilità.

Fonti

1. https://docs.ordinals.com/digital-artifacts.html
2. https://en.wikipedia.org/wiki/JSON
3. https://ordspace.org/brc20
4. https://docs.ordinals.com/runes.html
5. https://arxiv.org/pdf/1702.01024
6. https://www.unicode.org/standard/WhatIsUnicode.html
7. https://x.com/rodarmor/status/1778521190623215862

Nuovi report di Binance Research

Approfondimenti mensili sul mercato - Maggio 2024

Una sintesi degli sviluppi più importanti del mercato, grafici interessanti ed eventi in arrivo

Q1 State of Crypto: Market Pulse

Una raccolta dei principali grafici e approfondimenti sul mercato

Il futuro di Bitcoin #1: L'halving e il suo impatto

Uno sguardo all'halving di Bitcoin del 2024, ai potenziali impatti sulle metriche chiave di Bitcoin, sul settore di mining e altro ancora

Perché dovrebbe interessarti la disponibilità dei dati

Un'analisi tecnica approfondita del mercato della disponibilità dei dati ("DA")

Informazioni su Binance Research

Binance Research è il braccio di ricerca di Binance, il principale exchange crypto al mondo. Il team si impegna a fornire analisi obiettive, indipendenti e complete e mira a diventare il leader di pensiero nello spazio delle criptovalute. I nostri analisti pubblicano regolarmente articoli di approfondimento su argomenti relativi, tra gli altri, all'ecosistema delle crypto, alle tecnologie blockchain e agli ultimi temi del mercato.

Shivam Sharma

Macro Researcher

Shivam lavora attualmente per Binance come Macro Researcher. Prima di entrare in Binance, ha lavorato come Investment Banking Associate / Analyst presso Bank of America nel desk Debt Capital Markets, specializzato in istituzioni finanziarie europee. Shivam ha conseguito una laurea in Economia presso la London School of Economics & Political Science ("LSE") ed è impegnato nello spazio delle criptovalute dal 2017. Seguilo su X: @ **Sh_ivam**.

Fonti

Scopri di più qui

Condividi il tuo feedback qui