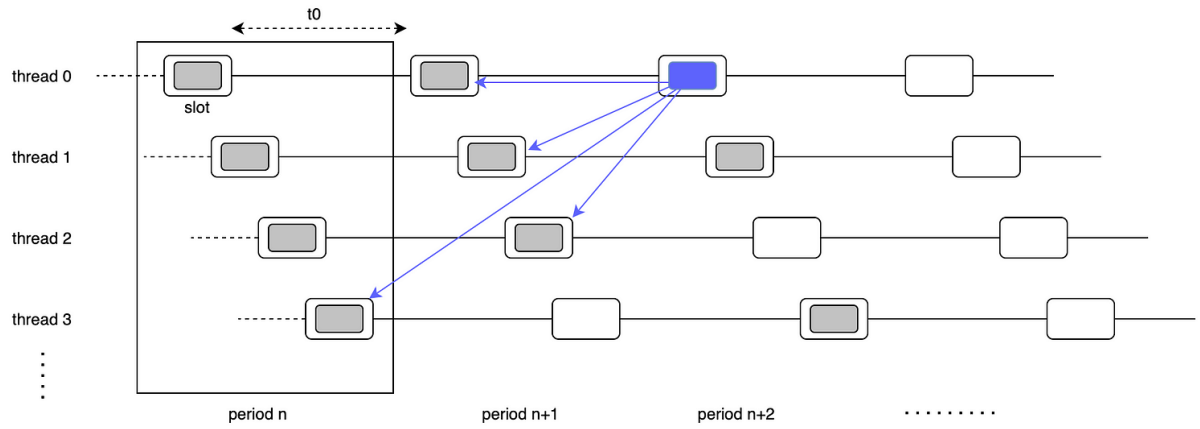
MASSA CONCETTI DI BASE

Immergiamoci nelle definizioni e nei concetti di base della blockchain di Massa.

l'obiettivo della rete Massa è costruire un consenso tra i nodi per raccogliere e ordinare blocchi che contengono elenchi ordinati di operazioni. Lo scopo ultimo di un'operazione, una volta eseguita, è quello di fungere da transizione per lo stato della rete globale, chiamato registro.

Le operazioni sono prodotte da client esterni e inviate alla rete di Massa tramite un nodo. Alcune operazioni contengono codici da eseguire come contratti intelligenti, consentendo complesse modifiche programmatiche del registro. I nodi raccolgono le operazioni in sospeso e le raggruppano in blocchi. Ogni blocco ha uno spazio limitato per memorizzare le operazioni. Le blockchain tradizionali in genere collegano i blocchi in sequenza, includendo un hash del blocco precedente nell'intestazione del blocco per l'ordinamento temporale. Al contrario, i blocchi di Massa sono organizzati in una struttura spazio-temporale complessa, consentendo la parallelizzazione e le migliori prestazioni di creazione dei blocchi.Invece di una catena, ci sono esattamente 32 thread di catene che corrono in parallelo, con blocchi equamente distribuiti su ciascun thread nel tempo e archiviati all'interno di slot distanziati a intervalli di tempo fissi:Il tempo che intercorre tra due slot posti sullo stesso thread è chiamato periodo e dura 16s (convenzionalmente chiamato t0 t 0). Gli slot corrispondenti nei threads sono leggermente spostati nel tempo l'uno rispetto all'altro, di un periodo diviso per il numero di threads, che è 16s/32=0.5s16 s /32=0.5 s , in modo che un periodo contenga esattamente 32 slot equidistanti nei 32 threads.

Un ciclo è definito come la successione di 128 periodi e quindi dura poco più di 34 minuti. I periodi sono numerati con incrementi di uno, quindi possono essere utilizzati insieme a un numero di thread per identificare in modo univoco uno slot di blocco. Il periodo 0 è la genesi e contiene blocchi di genesi senza genitori.Il compito della rete dei nodi di Massa è essenzialmente quello di riempire collettivamente gli slot con blocchi validi. Per fare ciò, ad ogni intervallo di 0,5 s, viene scelto un nodo specifico nella rete per poter creare un blocco (maggiori informazioni sul processo di selezione e sul meccanismo di proof_of_stake si trovano nel relativo documento), e sarà ricompensato se crea un blocco temporale valido. È anche possibile che un nodo perda l'opportunità di creare il blocco, nel qual caso lo slot rimarrà vuoto (questo si chiama blocco mancato).Nelle blockchain tradizionali, i blocchi fanno semplicemente riferimento al loro genitore univoco, formando una catena. Nel caso di Massa, ogni blocco fa riferimento a un blocco genitore in ogni thread (quindi, 32 genitori). Ecco un esempio illustrato con un blocco particolare:



Introduciamo alcune definizioni e concetti rilevanti che sono necessari per comprendere come opera la rete di Massa. Spiegheremo poi l'architettura del nodo e come funzionerà l'intero sistema .

Registro

Il registro o registro è una mappa che memorizza una mappatura globale tra indirizzi e informazioni relative a questi indirizzi. Viene replicato in ogni nodo. Il meccanismo di costruzione del consenso garantisce che venga raggiunto un accordo su quali operazioni sono state finalizzate (e in quale ordine) su tutta la rete. Il registro è lo stato della rete di Massa e le operazioni (vedi sotto) sono richieste per modificare il registro.

Le informazioni memorizzate nel registro con ciascun indirizzo sono le seguenti:

Informazioni sul registro associate a ciascun indirizzo

`Balance` La quantità di monete Massa possedute dall'indirizzo.

`Bytecode` Quando l'indirizzo fa riferimento a uno smart contract, questo è il codice compilato corrispondente allo smart contract (in genere contiene diverse funzioni che fungono da punti di ingresso API).

`Datastore` Una mappa chiave/valore in grado di memorizzare qualsiasi dato persistente relativo a uno smart contract, alle sue variabili, ecc.

Per promuovere un'adozione diffusa e facilitare il funzionamento dei nodi con tariffe di ingresso ridotte, la dimensione del registro a Massa è stata limitata a un massimo di 1 TB. Questa decisione distingue Massa dagli altri registri blockchain di riferimento e lo rende più accessibile agli utenti.

Per ottenere dimensioni del registro così ridotte, sono state prese diverse decisioni tecniche. In primo luogo, i cambiamenti di stato che sono stati finalizzati e si trovano nei Blocchi finali non richiedono più la tenuta dei registri nella memoria del Ledger. Questa ottimizzazione aiuta a ridurre al minimo i requisiti di archiviazione per i dati storici, consentendo al registro di funzionare in modo efficiente entro il limite di dimensione specificata.

Oltre a ciò, Massa ha introdotto i costi di archiviazione come un nuovo approccio per migliorare l'efficienza di archiviazione.

Gli utenti sono ora tenuti a bloccare una certa quantità di monete quando richiedono spazio di archiviazione. Questa innovativa combinazione tra archiviazione e monete circolanti garantisce un utilizzo equilibrato delle risorse.

Implementando questo meccanismo, Massa ha ottimizzato l'utilizzo dello spazio di archiviazione mantenendo l'integrità e la sicurezza del registro

Queste decisioni tecniche, inclusa l'esclusione dei cambiamenti di stato finalizzati dalla memoria del registro e l'introduzione dei costi di archiviazione, svolgono un ruolo cruciale nel consentire la dimensione compatta del registro e, in definitiva, nel facilitare un ecosistema blockchain più efficiente e accessibile.

Indirizzi

Un indirizzo sulla blockchain di Massa funge da identità univoca, garantendoti la possibilità di intraprendere varie operazioni, archiviare informazioni e scambiare dati con altri partecipanti. Con un indirizzo, ottieni accesso a un'ampia gamma di funzionalità all'interno dell'ecosistema blockchain.

Utilizzando il tuo indirizzo, puoi avviare operazioni che interagiscono con la blockchain. Ciò include l'esecuzione di transazioni, l'invio di chiamate di contratti intelligenti e l'impegno in altre attività blockchain. Il tuo indirizzo funge da chiave per sbloccare queste funzionalità, permettendoti di partecipare pienamente alla rete decentralizzata.

Inoltre, il tuo indirizzo ti consente di archiviare e recuperare informazioni sulla blockchain. Che si tratti di dati personali, documenti finanziari o qualsiasi altra forma di informazione digitale, puoi archiviarli in modo sicuro utilizzando il tuo indirizzo come riferimento. Ciò fornisce una soluzione di archiviazione affidabile e immutabile all'interno dell'ambiente blockchain.

È importante sottolineare che il tuo indirizzo facilita anche la comunicazione e lo scambio di dati con altri partecipanti alla blockchain. Condividendo il tuo indirizzo con altri, puoi interagire, effettuare transazioni e collaborare con diversi individui ed entità all'interno della rete blockchain. Questo scambio continuo di dati e valore promuove un ecosistema decentralizzato e interconnesso.

Ad ogni indirizzo utente su Massa è associata una chiave pubblica e una privata. Questo è il modo in cui i messaggi possono essere firmati e l'identità può essere applicata. L'indirizzo di un account è semplicemente l'hash della sua chiave pubblica.Gli indirizzi vengono generati utilizzando un formato specifico che include un prefisso `A`e una codifica base58. Il prefisso distingue tra indirizzi utente, collegati a una KeyPair, e indirizzi smart-contract, indicati rispettivamente dai prefissi `uos` .

Per gli indirizzi utente (AU), il calcolo dell'hash implica prendere l'hash Blake3 della rappresentazione in byte della chiave pubblica dell'utente. Questo processo garantisce un'identificazione univoca e sicura per ciascun indirizzo utente all'interno del sistema.

Contratto intelligente

I contratti intelligenti sono un pezzo di codice che può essere eseguito all'interno della macchina virtuale Massa, che può modificare il registro e accettare richieste in arrivo attraverso un'interfaccia pubblica (tramite operazioni di contratto intelligente).I contratti intelligenti sono attualmente scritti in AssemblyScript, una derivazione da TypeScript, che è esso stesso una versione indipendente dai tipi di JavaScript. AssemblyScript viene compilato nel bytecode WebAssembly (wasm). Il modulo di esecuzione dei nodi Massa esegue tale bytecode. I contratti intelligenti hanno accesso al proprio archivio dati, quindi possono modificare il registro.I contratti intelligenti seguono un calcolo dell'hash diverso rispetto agli indirizzi degli utenti. Inizia costruendo un array di byte comprendente vari elementi.

Questo array è costituito dallo slot rappresentato in 5 byte, con 4 byte allocati per il periodo (codificato come u64 in formato big endian), 1 byte per il thread e un indice che incrementa per ogni indirizzo creato all'interno dello stesso slot. Il valore dell'indice è rappresentato come u64 in formato big endian e viene reimpostato all'inizio di ogni nuovo slot. Inoltre, viene aggiunto un singolo byte per indicare se l'indirizzo è per l'esecuzione reale (1) o per l'esecuzione di sola lettura (0). L'array di byte risultante è quindi soggetto alla funzione hash Blake3, generando un valore hash univoco che funge da indirizzo SC.

Esecuzione autonoma di contratti intelligenti

Una particolarità degli smart contract Massa rispetto ad altri smart contract blockchain è la loro capacità di attivarsi da soli indipendentemente da una richiesta esterna sulla loro interfaccia. Li chiamiamo Autonomous Smart Contracts (ASC), poiché consentono maggiore autonomia e minore dipendenza da servizi centralizzati esterni. Gli ASC offrono una vasta gamma di casi d'uso che sfruttano la funzionalità di autoattivazione. Nel campo della finanza decentralizzata (DeFi), questi contratti possono automatizzare liquidazioni, strategie di yield farming e ribilanciamento del portafoglio. La gestione della catena di fornitura trae vantaggio da contratti autonomi attraverso la gestione automatizzata dell'inventario e processi di controllo della qualità. Nel settore assicurativo, la liquidazione dei sinistri può essere accelerata con pagamenti istantanei e assicurazioni parametriche. Le piattaforme di gioco e NFT possono fornire esperienze dinamiche e interattive con NFT in evoluzione e aste automatizzate. Inoltre, le transazioni immobiliari possono essere semplificate con l'automazione del deposito a garanzia e contratti di affitto semplificati. Questi casi d'uso esemplificano il potenziale di trasformazione degli Smart Contract autonomi nel consentire processi automatizzati ed efficienti in vari settori.

I costi di archiviazione

In Massa ogni nodo della rete conserva una copia completa del registro. Avere un registro di dimensioni enormi (centinaia di terabyte), porrebbe elevare barriere all'ingresso per i potenziali gestori dei nodi. Per garantire un funzionamento regolare e consentire l'hosting dei nodi a casa, è essenziale stabilire un limite di dimensioni ragionevoli ed eliminare la necessità di una capacità di archiviazione eccessiva. Dopo un'attenta considerazione, abbiamo stabilito che un limite di dimensione di archiviazione di 1 TB rappresenta il giusto equilibrio. Ciò significa che ciascun partecipante può archiviare i dati sul registro fino al raggiungimento della soglia di 1 TB. Implementando questo limite, miriamo a promuovere un'adozione diffusa ea consentire alle persone di gestire i nodi senza sforzo. Per rispettare questo limite, gli utenti sono tenuti a bloccare una quantità corrispondente di monete per ogni byte di spazio di archiviazione richiesto. Questo vale per vari elementi di dati come indirizzo, saldo, chiavi nel tuo datastore, bytecode e altro. Bloccando le monete, stabilisci un impegno che garantisce un utilizzo corretto delle risorse di archiviazione. Una volta rilasciato lo spazio assegnato nel deposito, anche le monete bloccate verranno successivamente rilasciate. Questo meccanismo garantisce un approccio equilibrato e responsabile alla gestione dello storage all'interno della rete.

Gas

In Massa non esiste il prezzo del gas. Ogni operazione dichiara una quantità massima di gas che può utilizzare e prevede una commissione che viene aggiunta ai premi del blocco in cui viene eseguita l'operazione. I generatori di blocchi scelgono quindi quali operazioni includere nei loro blocchi per soddisfare i vincoli relativi al gas massimo del blocco e alla dimensione massima del blocco, massimizzando al tempo stesso la tariffa totale.

Blocco

Un blocco è una struttura dati costruita da nodi e la sua funzione è quella di aggregare più operazioni. Come spiegato sopra, per ogni nuovo slot che diventa attivo, viene eletto in modo deterministico un particolare nodo della rete con il compito di creare il blocco che verrà memorizzato in quello slot. Un blocco di un dato thread può contenere solo operazioni originate da

un creator_public_key i cui primi cinque bit dell'hash designano il thread corrispondente, evitando così implicitamente collisioni nelle operazioni integrate nei thread paralleli. La dimensione del blocco è limitata a 1 MB.

Il contenuto di un blocco è il seguente:

Intestazione del blocco

`Slot` Una descrizione dello slot del blocco, definita da una coppia (periodo, thread) che lo identifica in modo univoco

`creator_public_key` La chiave pubblica del creatore del blocco (32 byte) `parents`Un elenco dei 32 genitori del blocco, un genitore per thread (i blocchi genitori sono identificati dall'hash del blocco)

`endorsements` Un elenco delle 16 approvazioni per il blocco (maggiori informazioni sulle approvazioni di seguito)

`operations_hash` Un hash di tutte le operazioni incluse nel blocco (=hash del corpo del blocco di seguito)

`signature` Firma di tutto quanto sopra con la chiave privata del creatore del blocco

Corpo del blocco

`Operations` L'elenco di tutte le operazioni incluse nel blocco

Operazione

Fondamentalmente, la rete di Massa ruota attorno all'aggregazione, al sequenziamento e all'esecuzione delle operazioni. Le operazioni vengono registrate all'interno dei blocchi che si trovano negli slot.

Le operazioni sono indicate da una stringa con il prefisso "O" che incapsula le informazioni cruciali all'interno di un array di byte. L'array di byte comprende la versione in formato varint u64, l'hash Blake3 del contenuto completamente serializzato dell'operazione e la chiave pubblica del creatore. Organizzando e registrando meticolosamente le operazioni all'interno dei blocchi che risiedono in slot specifici, la rete di Massa garantisce l'integrità e l'efficienza delle proprie operazioni.

Tipi di operazioni

Esistono tre tipi di operazioni: transazioni, operazioni roll ed esecuzione del codice del contratto intelligente. La struttura generale di un'operazione è la seguente ed i diversi tipi di operazioni differiscono per il loro payload o carico.

Rappresentazione binaria delle transazioni

Campo	Descrizione	Tipo
`creator_public_key`	La chiave pubblica dell'autore dell'operazione	32 byte
`expiration_period`	Periodo dopo il quale l'operazione scade	u64 varint
`fee`	L'importo delle commissioni che il creatore è disposto a pagare	u64 varint
`type`	Il tipo di operazione (da 0 a 4: transazione, acquisto roll, vendita roll, esecuzione, sc chiamata sc)	u64 varint
`payload`	Il contenuto dell'operazione	Vedi ogni operazione
`Signature`	Firma di tutto quanto sopra con la chiave privata dell'autore dell'operazione	64 byte

Operazioni di transazione

Le transazioni sono operazioni che spostano le monete Massa native tra indirizzi. Ecco il payload corrispondente:

Rappresentazione binaria del payload delle transazioni

Campo	Descrizione	Tipo
`amount`	La quantità di monete da trasferire	u64 varint
`destination_address`	L'indirizzo del destinatario	32 byte

Operazioni di acquisto/vendita dei “Rolls”

I rolls sono dei token che permettono di fare lo staking. Chiunque può acquistare o vendere i Rolls utilizzando le monete native di Massa. Possedendo i Rolls, gli indirizzi possono partecipare alla creazione di blocchi. Ciò avviene tramite operazioni speciali, con un semplice payload:

Rappresentazione binaria del payload dei rolls di acquisto/vendita

Campo	Descrizione	Tipo
`Nb_of_rolls`	Il numero di rolls da acquistare o vendere	u64 varint

Operazioni di smart contract

Gli Smart Contracts sono pezzi di codice che possono essere eseguiti all'interno della macchina virtuale Massa. Esistono due modi per richiedere l'esecuzione del codice; tramite l'esecuzione diretta del bytecode e tramite una chiamata di funzione smart-contract. Il primo viene eseguito utilizzando l'operazione Esegui SC, il secondo con l'operazione Chiama SC.

1. Eseguire l'operazione SC

   L'operazione ExecuteSC fornisce una potente funzionalità all'interno della rete Massa consentendo l'esecuzione diretta di smart contract invece di archiviarli. Invece di memorizzare il bytecode, il codice stesso viene inserito nell'operazione come smart contract. Quando viene eseguita l'operazione ExecuteSC, la blockchain attiva l'esecuzione della funzione principale all'interno del codice dello smart contract. Dopo che il codice è stato eseguito, la blockchain procede ad altre attività conservando e riflettendo le modifiche apportate al registro e ad altri dati rilevanti. Questo approccio garantisce che le modifiche eseguite vengano registrate e mantenute nel registro, anziché conservare il bytecode stesso. Eseguendo gli smart contract in questo modo, la rete Massa offre flessibilità ed efficienza nella gestione ed esecuzione del codice all'interno del suo ecosistema blockchain.

Rappresentazione binaria del payload degli Smart Contract

Campo	Descrizione	Tipo
max_gas	Il gas massimo spendibile per questa operazione	u64 varint
bytecode_len	La lunghezza del campo bytecode	u64 varint
bytecode	Il bytecode da eseguire (nel contesto dell'indirizzo del chiamante)	u64 varint
datastore_len	Il numero delle chiavi del datastore (u64 varint), ogni record viene quindi memorizzato uno dopo l'altro	u64 varint
Elenco dei record del datastore	Concatenazione di `key_len`(u8), `key`, `value_len`(u64 varint),`value`	

2. Chiamare l'operazione SC

In questo caso il codice viene richiamato tramite la chiamata a una funzione di smart contract esistente, insieme ai parametri richiesti:

Rappresentazione binaria del payload degli Smart Contract

Campo	Descrizione	Tipo
`max_gas`	Il gas massimo spendibile per questa operazione	u64 varint
`coins`	Le monete trasferite nella chiamata	u64 varint
`target_address`	L'indirizzo dello smart contract da eseguire	32 byte
`function_name_length`	La lunghezza del nome della funzione chiamata	u8
`function_name`	Il nome della funzione che viene chiamata	utf8
`param_len`	Il numero di parametri della chiamata di funzione	u64 varint
`params`	I parametri della chiamata di funzione	

Approvazioni

Le approvazioni sono incluse facoltativamente nel blocco, ma la loro inclusione è incentivata per i creatori di blocchi. Sono conferme del fatto che il blocco genitore sul thread del blocco è il miglior genitore che avrebbe potuto essere scelto, fatto da altri nodi che sono stati anch'essi selezionati deterministicamente tramite la prova della distribuzione della probabilità di puntata. Una descrizione completa delle approvazioni può essere trovata nel documento relativo, quindi non entreremo ulteriormente nei dettagli nel contesto di questa introduzione.