WhitePaper

Giovanni Giorgi
29/10/2017 V.1.0

Introduzione

La tecnologia blockchain è sicuramente una delle più grandi innovazioni degli ultimi anni.
Attualmente la sua efficacia e sicurezza sono già state ampiamente dimostrate ma il successo e una più ampia distribuzione hanno portato alla luce importanti problematiche di scalabilità che hanno portato ad una limitata possibilità di utilizzo e ad un costante aumento delle fee.
Le problematiche non sono limitate all'utilizzo da parte degli utenti ma sono presenti anche nel sistema di controllo della sicurezza; l'attuale sistema di mining oltre a produrre un eccessivo e inutile spreco di energia, concede anche un forte potere decisionale ai miners, che di fatto hanno la possibilità di impedire qualsiasi tipo di aggiornamento che limiti il loro guadagno.

Molti di questi problemi sono risolvibili sostituendo la struttura lineare della blockchain con un DAG (Directed Acyclic Graph), che però ha lo svantaggio di avere un overhead maggiore che comporta spreco di memoria e se non adeguatamente controllato porterebbe ad un grafo divergente, che ne limita l'efficacia

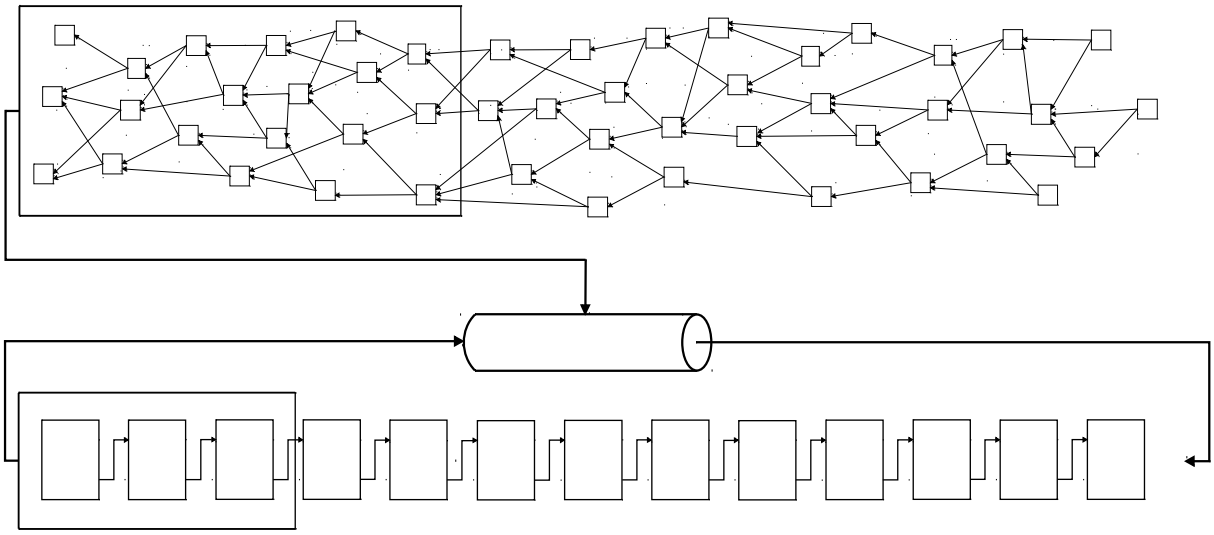
La soluzione è unire le due tecnologie; combinando la scalabilità, assenza di mining e fee tipica del DAG con la sicurezza ed efficienza di memorizzazione della blockchain per la memorizzazione sul lungo periodo.
Questo tipo di implementazione permette anche di modificare il funzionamento della blockchain, rielaborando il concetto di inalterabilità, rendendo possibile un'ulteriore diminuzione nell'utilizzo di memoria.

Utilizzi e vantaggi

Questa struttura fornisce un ledger totalmente decentralizzato, altamente scalabile, efficiente nella memorizzazione, senza costi di utilizzo e senza la possibilità che un sottogruppo di utenti possano esercitare potere sul resto della rete.

La struttura è pensata oltre che per lo scambio di valuta anche per il salvataggio di dati e risorse di varia tipologia, in modo da permettere un buon supporto per l'implementazione di smart contracts e in modo da garantire supporto come backend per web 3.0

Caratteristiche



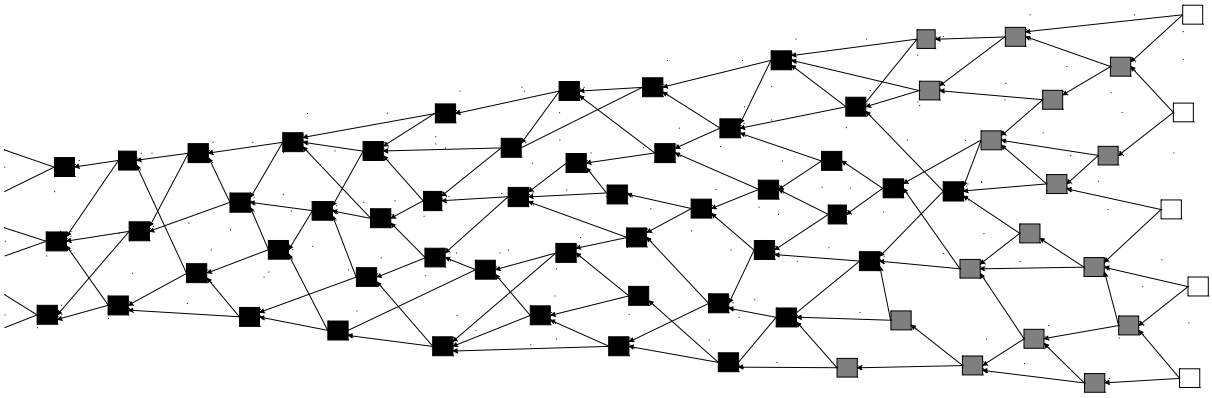
La struttura ibrida prevede un buffer di memorizzazione delle transizioni basato su DAG.
Questo permette a chiunque di aggiungere istantaneamente le transizioni, senza pagamento di fee ai miners e senza tempi di attesa.
Questo componente gestisce anche l'approvazione delle transizioni e la sicurezza.
Le tempistiche di approvazione delle transizioni dipenderanno dall'utilizzo della rete e diminuiranno linearmente con l'aumentare delle transazioni eseguite in quel momento (al contrario della blockchain, dove le tempistiche aumentano).
Con l'aumento dell'utilizzo aumenterà anche la sicurezza perché il peso della transizione (concetto spiegato di seguito) aumenterà più velocemente, rendendo più efficiente la gestione di double spending e rendendo più difficili da manipolare i dati aggiunti.

Per garantire un salvataggio in memoria efficiente e sicuro sul lungo periodo, a intervalli regolari, le transizioni più vecchie del DAG, verranno prelevate, salvate sulla Shifting BlockChain ed in seguito eliminate dal DAG.

Sulla blockchain sono presenti due tipologie di blocco differenti: la prima tipologia contiene un database di coppie chiave-valore, che può contenere come record i balance di coin e token appartenuti ad uno specifico address strutturati come (token, address, value); oppure dati generici strutturati come (macrogruppo, key, value).
La seconda tipologia, nella sezione dei dati, contiene un unico asset da salvare senza alterazioni, contraddistinto da un identificativo e firmato digitalmente dall'utente che lo pubblica.

DAG (Directed Acyclic Graph)

Il DAG è un grafo orientato formato da blocchi, che a differenza della blockchain non seguono un ordine sequenziale.
Ogni blocco è collegato a 2 blocchi precedenti, in modo da poter essere aggiunto in parallelo agli altri, senza conoscere l'intero grafo.
Per ogni blocco è possibile individuare una profondità (depth) che rappresenta il numero di blocchi presenti nel percorso più lungo per raggiungere un blocco senza conferme (tip).



Per aggiungere un nuovo blocco, l'utente deve selezionare due blocchi precedenti (ancora non confermati) per convalidarli.
il processo di convalida consiste nel certificare la validità della firma, che il conto non sia in conflitto con le transizioni precedenti e che sia stato eseguito il pow (per proteggere la rete dallo spam).
se i blocchi selezionati sono legittimi possono essere usati per agganciare il nuovo blocco.

Ad ogni blocco viene assegnato un peso(weight), che ha un certo valore iniziale basato sul PoW, a cui vengono sommati i pesi dei blocchi collegati di seguito e un punteggio(score) rappresentato dal peso iniziale del blocco sommato agli score dei blocchi che conferma.
Con l'aggiunta di un blocco, si conferma solo la sezione di grafo sequenzialmente precedente ai blocchi direttamente selezionati, questo comporta un aumento del peso dei blocchi in quella sezione.
Un blocco viene considerato completamente confermato quando tutte le sezioni di grafo seguenti lo confermano, ovvero tutti i nuovi blocchi ne aumentano il peso.
Tutti i blocchi che hanno una adeguata profondità sono completamente confermati.

Per selezionare i 2 blocchi da approvare viene data maggiore priorità ai blocchi con un punteggio maggiore. Può capitare che transizioni propagate con lentezza si aggancino in una posizione che non aumenta il peso di alcuni blocchi già confermati; in quel caso i blocchi continuano ad essere considerati confermati anche se il consenso non è più 100%.

in caso di double spending può capitare che entrambe le transizioni siano in un primo momento approvate in sezioni differenti del DAG ma è impossibile che una singola transizione approvi una sezione di grafo che le conferma entrambe contemporaneamente.
anche se il double spending non viene individuato immediatamente, con il passare del tempo, la sezione di grafo con la transizione maligna con il punteggio minore verrà abbandonata.
Come effetto collaterale tutte le transizioni che si sono agganciate di seguito non verranno mai confermate, ma è possibile agganciarle nuovamente in una posizione differente senza modifiche, a parte eseguire nuovamente il pow.

È possibile continuare ad eseguire transizioni anche se si perde la connessione degli altri nodi ma con il rischio che il nuovo tratto non sia conforme al resto della rete.
Nel caso ci siano problemi di approvazione, è necessario collegare i blocchi nuovamente in una differente posizione.

Shifting BlockChain:

Per il salvataggio nel lungo periodo viene utilizzata un'implementazione custom della blockchain.

La struttura del blocco è quella classica; contenente oltre alla sezione dedicata ai dati, un numero identificativo sequenziale e l'hash del blocco precedente.
In aggiunta ogni blocco ha un identificativo che ne delinea la tipologia del contenuto.
Manca la sezione dedicata al PoW perché la sicurezza viene gestita separatamente, in modo che l'aggiunta di nuovi blocchi non sia vincolata da tempistiche prestabilite.
Il blocco non ha limiti pratici di dimensione, questo è possibile perché in fase di aggiunta, tutti i dati da inserire sono già presenti nel nodo e non bisogna tener conto dei problemi di propagazione del contenuto tra i nodi.

A differenza delle classiche blockchain viene introdotto il concetto di aggiornamento dello stato dei dati.
A intervalli regolari (fase di Add & Update) vengono prelevati i blocchi in coda e eliminati dalla blockchain; i dati prelevati vengono riorganizzati, integrati con i nuovi dati da inserire e vengono eliminati i record ridondanti.
In seguito il tutto viene aggiunto in testa.

La sicurezza viene garantita salvando l'hash dell'ultimo blocco nel DAG per garantire l'inalterabilità e per propagare l'hash tra i nodi, in modo da garantire la consistenza dei dati sulla rete.
Questa operazione viene eseguita solo da una certa percentuale di nodi; la percentuale viene decisa in base al numero di agganci eseguiti in precedenza e calcolata in modo da garantire una buona sicurezza, senza eccedere con lo spam sulla rete.
Per garantire che la percentuale venga rispettata ogni nodo esegue autonomamente un algoritmo basato sul random per decidere se eseguire questo compito o meno.

Nel caso in cui un nodo si rende conto di avere uno stato differente dagli altri, inizia un colloquio con i nodi vicini per recuperare il giusto stato.
Durante questa fase vengono scambiati gli hash dei vari blocchi per ricostruire la giusta sequenza dei dati e nel caso sia necessario vengono recuperati i blocchi mancanti, in modo da ottenere uno stato conforme con quello del resto della rete.

La perdita di dati dalla coda della blockchain viene impedita dall’impossibilità di ricostruire i nuovi blocchi, senza conoscere il contenuto degli ultimi

Add & Update:

Ogni nodo in autonomia, a intervalli regolari, vincola la sezione più vecchia del DAG.
la giusta sezione viene individuata ogni volta che un blocco supera un certo valore di depth e viene selezionata tutta la sezione di blocchi il cui depth rientra in un certo range di valori.
Il valore di depth che innesca la fase di add and update varia dinamicamente in modo che l'operazione venga eseguita con la giusta frequenza e il range varia in modo che il DAG non assumi dimensioni troppo grandi (che ne rendano difficile la gestione) o troppo piccole (che ne limiti sicurezza e affidabilità).

Eventuali problemi nella propagazione dei blocchi non influenzano l'individuazione della sezione, perchè nel caso venga aggiunto un nuovo blocco, la profondità di tutti i blocchi confermati aumenta dello stesso valore, pertanto la differenza con il blocco con profondità più alta rimane costante.
l'unica cosa che varia da un nodo all'altro è l'istante in cui si inizia il processo.

sui blocchi di questa sezione vengono estratte e ordinate in base all'hash le transizioni, le coppie chiave-valore e gli assets

In contemporanea vengono prelevati dalla coda della blockchain tutti i blocchi fino a raggiungere un blocco dedicato ai balance e coppie chiave-valore.
I blocchi contenenti assets, se non sono presenti versioni aggiornate, vengono spostati in testa .

Per ultimo viene prelevato il blocco dedicato ai balance e coppie chiave-valore dalla blockchain e viene aggiornato; integrando il contenuto con i nuovi record ed eliminando i dati già presenti, in versione aggiornata, in punti differente della blockchain.
In questo caso se si supera il limite di dimensione prestabilito, il contenuto viene spezzato in due blocchi, di cui quello contenente dati più vecchi viene aggiunto in mezzo tra i vecchi assets (proveniente dalla blockchain) e i nuovi assets (provenienti dal DAG) mentre il nuovo blocco, contenente i balance aggiornati più di recente, viene aggiunto in testa alla blockchain.
Questo garantisce che con l'aumentare della dimensione della catena aumentino anche le fasi di add & update necessarie per scorrerla completamente, limitando la potenza di calcolo necessaria per eseguire l'operazione.

References:

1. Sergio Demian Lerner (2015) DagCoin: a cryptocurrency without blocks. https://bitslog.wordpress.com/2015/09/11/dagcoin/

2. Iota: a cryptocurrency for Internet-of-Things. See http://www.iota.org/, and https://bitcointalk.org/index.php?topic=1216479.0