Loopring:
Un Protocollo di Scambio Token Decentralizzato

Daniel Wang
daniel@loopring.org

Jay Zhou
jay@loopring.org

Alex Wang
alex@loopring.org

Matthew Finestone
matt.finestone@gmail.com

https://loopring.org

May 9, 2018

Abstract

Loopring é un protocollo aperto per l'implementazione di Exchange decentralizzati. Loopring opera mediante un set pubblico di smart contracts responsabili di scambio e liquidazione, contando inoltre su di un insieme di attori off-chain responsabili dell'aggregazione e comunicazione degli ordini. Il protocollo é gratuito, espandibile, e funge da elemento standard portante per la costruzione di applicazioni decentralizzate (dApps) che incorporano la funzionalitá di Exchange. I suoi standard interoperabili permettono di effettuare trading in modo anonimo e trustless. Un importante miglioramento rispetto agli attuali protocolli di Exchange decentralizzati é rappresentato dal fatto che gli ordini qui possono anche essere combinati ed abbinati ad altri ordini dissimili, ovviando al vincolo rappresentato dalla necessitá di costituire delle coppie di scambio tra due tokens e aumentando drasticamente la liquiditá. Loopring implementa inoltre una robusta soluzione per la prevenzione del front-running: il tentativo scorretto che consiste nell'invio ad un block di una richiesta di processamento di transazioni in modo piú rapido della stessa soluzione originaria. Loopring é agnostico riguardo alla Blockchain d'implementazione, permettendo di fatto un'implementazione su qualsiasi Blockchain che supporti la funzionalitá di smart contracts. Al momento attuale, risulta operativo su Ethereum [1] [2] e Qtum [3], con NEO [4] in corso d'implementazione.

1 Introduzione

Con la proliferazione dei beni basati sulla blockchain, il bisogno di scambiare tali beni tra controparti é incrementato significativamente. L'introduzione di migliaia di nuovi tokens - che comprende anche la tokenizzazione dei beni tradizionali - ha fatto sí che questo bisogno si amplificasse. Sia che si scambino tokens per motivazioni di trading speculativo, o che vengano convertiti in token d'utilizzo per accedere a networks specifici, la capacitá di scambiare un bene crypto per un altro costituisce le fondamenta di un ecosistema piú grande. Difatti, questi beni possiedono una potenziale energia [5], tuttavia liberare questa energia - sbloccare capitali - richiede non solo di determinare la proprietá, cosa che la blockchain ha immutabilmente consentito di fare, ma anche l'abilitá di trasferire e trasformare liberamente questi beni.

In questo modo, lo scambio di tokens che non richiedono un rapporto di fiducia, é un caso d'uso convincente per la tecnologia blockchain. Tuttavia, fino ad ora, gli appassionati di cripto-beni si sono in larga parte accontentati di scambiare tokens in exchanges centralizzati tradizionali. Il protocollo di Loopring é necessario perché, cosí come coscienziosamente Bitcoin [6] ha enfatizzato, a proposito di denaro elettronico peer-to-peer, "i maggiori benefici sono persi se una terza parte fidata é ancora necessaria per prevenire la doppia spesa", allo stesso modo, i principali benefici delle risorse decentralizzate sono perduti se devono passare attraverso exchanges fidati, chiusi e centralizzati.

Scambiare tokens decentralizzati su exchanges centralizzati perde di significato dal punto di vista filosofico, considerando che fallisce nel supportare i valori che questi progetti decentralizzati sposano. Vi sono numerosi rischi pratici e limitazioni nell'uso di exchanges che saranno descritti in seguito. Gli exchanges Decentralizzati (DEXs) [7] [8] [9] hanno cercato di affrontare questi problemi, e in molti casi sono riusciti a mitigare i rischi per la sicurezza usando la blockchain per trattative dirette. Tuttavia, mentre le competenze di DEX stanno diventando infrastrutture cruciali per la new economy, vi é un significativo spazio di manovra per migliorarne le prestazioni. Loopring ha lo scopo di fornire strumenti modulari per la suddetta infrastruttura con il suo protocollo dApp aperto e agnostico.

2 L'Attuale Panorama degli Exchange

2.1 Inadeguatezze degli Exchanges Centralizzati

I tre rischi primari degli exchange centralizzati sono; 1) Mancanza di sicurezza, 2) Mancanza di trasparenza, 3) Mancanza di liquiditá.

La mancanza di Sicurezza sorge generalmente da utenti che consegnano il controllo delle loro chiavi private (quindi dei fondi) ad un'entitá centralizzata. Ció, espone gli utenti alla possibilitá che gli exchange centralizzati cadano preda di hackers. I rischi sulla sicurezza e di attacco informatico di cui soffrono gli exchanges sono ben noti[10] [11], nonostante ció sono spesso accettati come fattori indispensabili nello scambio di token. Gli exchanges centralizzati continuano ad essere attraenti per gli hackers, che seguitano negli attacchi ai server i quali custodiscono milioni di dollari di fondi di utenti. Inoltre, gli sviluppatori di exchange possono anche commettere errori accidentali, in buonafede, con i fondi degli utenti. Semplicemente, gli utenti non sono in controllo dei loro tokens quando li depositano in un exchange centralizzato.

La mancanza di Trasparenza espone gli utenti al rischio che exchanges disonesti si comportino in maniera scorretta. La distinzione sta nelle intenzioni malevole degli operatori degli exchanges, dato che gli utenti non scambiano realmente i loro beni negli exchange centralizzati, bensí un IOU. Quando i tokens sono spediti al wallet dell'exchange, l'exchange li prende in custodia e offre un IOU al loro posto. Tutti gli scambi sono quindi effettuati con IOUs tra utenti. Per prelevare, gli utenti riscattano i loro IOU dall'exchange e ricevono in cambio i tokens sull'indirizzo del loro wallet esterno. In questo processo vi é una carenza di trasparenza e l'exchange puó chiudere, congelare il tuo account, dichiarare bancarotta etc. Sussiste anche la possibilitá che utilizzino i beni degli utenti per altri scopi mentre li tengono in custodia, come ad esempio prestarli a terze parti. La mancanza di trasparenza puó costare agli utenti a prescindere dalla totale perdita di fondi, ad esempio si puó concretizzare in piú alte commissioni di scambio, ritardi nei momenti di picco di domanda, rischi legati a regolamentazioni e che gli ordini siano oggetto di front running

Mancanza di Liquiditá. Dal punto di vista degli operatori degli exchange, la liquiditá frammentata impedisce l'ingresso di nuovi exchanges dovuta alla presenza di due scenari in cui il vincitore prende tutto . Nel primo, l'exchange con il piú alto numero di coppie di scambio vince, perché gli utenti trovano piú vantaggioso effettuare tutti gli scambi su un unico exchange. Nel secondo, l'exchange con il piú grande registro delle commesse vince, ció é dovuto allo spread denaro-lettera favorevole per ognuna delle coppie di scambio. Questo, scoraggia la competizione dei nuovi arrivati perché diventa difficile per loro accumulare la liquiditá iniziale necessaria. Il risultato é che molti exchange controllano una grande porzione di mercato nonostante le lamentele degli utenti e sostanziali incidenti di attacchi informatici da parte di hackers. É importante sottolineare che piú gli exchange centralizzati si accaparrano porzioni di mercato, piú sono esposti ad attacchi di hackers.

Dal punto di vista degli utenti, la liquiditá frammentata riduce sostanzialmente l'esperienza del fruitore. In un exchange centralizzato, gli utenti possono solo scambiare all'interno della disponibilitá dell'exchange stesso contro il suo stesso registro delle commesse e tra le coppie di tokens supportati. Per scambiare il token `A` per il token `B`, gli utenti devono andare in un exchange che supporta entrambi i token o registrarsi in exchange diversi, divulgando informazioni personali. Gli utenti spesso hanno bisogno di eseguire scambi preliminari o intermedi, generalmente tra BTC o ETH, pagando uno spread denaro-lettera nel processo. Infine, il registro delle commesse potrebbe non avere sufficiente disponibilitá per completare lo scambio senza un materiale rallentamento. Anche se l'exchange afferma di processare grandi volumi non c'é garanzia che questo volume e questa liquiditá non siano dei falsi [12].

Il risultato é un disconnesso silos di liquiditá e un ecosistema frammentato che assomiglia al vecchio sistema finanziario, con un significativo volume di scambio centralizzato su pochi exchange. La liquiditá globale promessa dalla blockchain non ha nessun valore all'interno degli exchange centralizzati.

2.2 Inadeguatezze degli Exchange Decentralizzati

Gli exchange decentralizzati differiscono dagli exchange centralizzati in parte perché gli utenti mantengono il controllo delle loro chiavi private (dei loro beni) attraverso l'esecuzione diretta degli scambi sulla blockchain sottostante. Facendo leva sulla stessa tecnologia trustless delle criptovalute, sono riusciti a mitigare con successo molti dei sopracitati problemi di sicurezza. Tuttavia, i problemi persistono riguardo alla prestazione e alle limitazioni strutturali.

La liquiditá spesso resta un problema, dato che gli utenti devono ricercare controparti all'interno di riserve di liquiditá e standard eterogenei. Gli effetti della liquiditá frammentata si palesano se DEXs o dApps non utilizzano standard consistenti di interoperabilitá, o se gli ordini non sono condivisi/propagati all'interno di un ampio network. La liquiditá di un registro di commesse (order books) su scambi a prezzo limitato, e specificatamente la sua capacitá di recupero - quanto velocemente gli ordini eseguiti vengono sostituiti da nuovi ordini - puó avere un impatto considerevole sulle strategie di scambio ottimali [13]. L'assenza di questi standard ha avuto il risultato non solo di ridurre la liquiditá, ma anche di esporre gli utenti a smart contracts proprietari con potenziali falle di sicurezza.

Inoltre, visto che gli scambi sono effettuati on-chain, i DEXs ereditano le limitazioni della blockchain su cui sono

costruiti, nominalmente: scalabilitá, ritardi in esecuzione (mining), e costose modifiche agli ordini. Quindi il registro delle commesse della blockchain non scala particolarmente bene, in quanto eseguire codice sulla blockchain causa un costo (gas), rendendo cancellazioni multiple di ordini proibitivamente costoso. .

Infine, dato che i registri delle commesse della blockchain sono pubbliche, la transazione per collocare un ordine é visibile ai minatori nel frattempo che aspetta di essere minato nel prossimo blocco e piazzato in un registro di commissioni. Questo ritardo espone gli utenti al rischio di front running e di ritrovarsi il prezzo o l'esecuzione rivolto contro di lui.

2.3 Soluzioni Ibride

Per le ragioni sopracitate, gli exchange basati puramente sulla blockchain presentano delle limitazioni che li rende non competitivi rispetto agli exchange centralizzati. Esiste un trade-off tra la proprietá di assenza di fiducia caratteristica delle soluzioni on-chain e la velocitá e flessibilitá degli ordini propri degli exchange centralizzati. Protocolli come Loopring e 0x [14] propongono una soluzione di regolamento degli scambi on-chain con il management degli ordini off-chain. Queste soluzioni ruotano intorno agli open smart contracts ma superano le limitazioni di scalabilitá compiendo molte funzioni off-chain e lasciando ai nodi molta flessibilitá nei diversi ruoli critici per il network. Tuttavia, i svantaggi rimangono anche per i modelli ibridi [15]. Il protocollo di Loopring propone differenze significative, il nostro approccio ad una soluzione ibrida viene presentata attraverso questo articolo.

3 Il Protocollo Loopring

Loopring non é un DEX, ma un protocollo modulare per costruire DEX su multiple blockchains. Abbiamo disassemblato i componenti principali di un exchange tradizionale e offerto al loro posto un insieme di smart contacts pubblici e attori decentralizzati. I ruoli nel network includono i wallet (portafogli), i relé (relays), la blockchain del consorzio di condivisione di liquiditá, i browser dei registri di commesse, i minatori di anelli, e i servizi di tokenizzazione di asset. Prima di definire ognuno di questi elementi, dovremmo prima comprendere cosa sono gli ordini in Loopring.

3.1 Anelli di Ordini

Gli ordini in Loopring sono espressi in ció che chiamiamo Modello di Ordine Unidirezionale (UDOM)[16]. L'UDOM esprime gli ordini come richieste di scambio di token, `amountS`/`amountB`, (quantitá da vendere/comprare) invece che in denaro e lettera. Dato che ogni ordine é solamente un tasso di scambio tra due token, una caratteristica importante del protocollo é quella di combinare ed abbinare ordini multipli in uno scambio circolare. Utilizzando fino a 16 ordini contemporaneamente invece di una singola coppia di scambio, viene generato un drastico aumento di liquiditá e il potenziale per un miglioramento del prezzo.

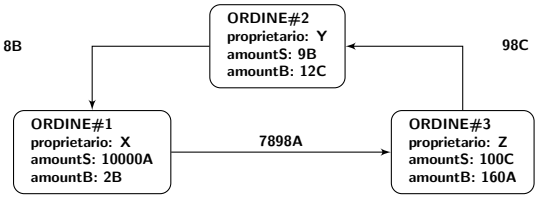

Figure 1: Un anello composto da 3 ordini

La figura 1 mostra un anello di ordini composto tra 3 ordini. Ogni token in un ordine di vendita (`tokenS`) é anche un token in un altro ordine d'acquisto (`tokenB`). Viene cosí creato un loop che permette ad ogni ordine di scambiare i token desiderati senza la necessitá di un ordine opposto per quella coppia. Gli ordini tradizionali di scambio di coppie possono, ovviamente, essere ancora essere eseguiti, in quello che é essenzialmente un caso speciale di anello di ordini.

Definition 3.1 (anello di ordini) *Siano* C_0, C_1, $\cdots$, C_{n-1} *n differenti token, e siano* $O_{0\to1}$, $\cdots$, $O_{i\to i\oplus1}$, $\cdots$, $O_{n-1\to0}$ *n differenti ordini. Questi ordini possono formare un anello di ordini per lo scambio:*

$$O_{0\to1} \to \cdots \to O_{i\to i\oplus1} \to \cdots \to O_{n-1\to0},$$

dove n é la lunghezza dell'anello di ordini, e $i \oplus 1 \equiv i + 1 \mod n$.

Un anello di ordini é valido quando tutte le transazioni che lo compongono possono essere eseguite ad un tasso di scambio uguale o migliore del tasso originale specificato implicitamente dall'utente. Per verificare la validitá dell'anello di ordini, gli smart contracts del protocollo Loopring devono ricevere gli anelli di ordini dai minatori e controllare che il prodotto dei tassi di scambio originali di tutti gli ordini é maggiore o uguale a 1.

Assumiamo che Alice e Bob vogliono scambiare i loro token `A` e `B` . Alice possiede 15 token `A` vuole scambiarli con 4 token `B`; Bob possiede 10 token `B` vuole scambiarli con 30 token `A`.

Chi sta comprando e chi sta vendendo? Ció dipende esclusivamente dal bene che scegliamo di fissare per dare un prezzo alle quotazioni. Se il token `A` é preso come riferimento, allora Alice sta comprando un token `B` al prezzo di $\frac{15}{4} = 3.75$`A`, mentre Bob sta vendendo 10 token `B` al prezzo di $\frac{30}{10} = 3.00$`A`. Nel caso in cui fissassimo il token `B` as reference, we say that Alice is selling 15 token `A` for the price of $\frac{4}{15} = 0.26666667$`B` and Bob is buying 10 token `A` for the price of $\frac{10}{30} = 0.33333334$`B`. Hence, who's the buyer or seller is arbitrary.

Nella prima situazione Alice é disposta a pagare un prezzo piú alto (3.75`A`) rispetto al prezzo che Bob chiede per vendere i suoi token (3.00`A`), mentre nella seconda situazione Bob é disposto a pagare un prezzo piú alto (0.33333334`B`) rispetto al prezzo a cui Alice sta vendendo i suoi token (0.26666667`B`). É chiaro che uno scambio é possibile quando

il compratore é disposto a pagare un prezzo uguale o maggiore di quello richiesto dal venditore.

$$\frac{\frac{15}{4}}{\frac{30}{10}} = \frac{\frac{10}{30}}{\frac{4}{15}} = \frac{15}{4} \cdot \frac{10}{30} = 1.25 > 1 \quad (1)$$

Pertanto, perché un insieme di n ordini possano essere completati, integralmente o parzialmente, dobbiamo sapere se il prodotto tra ogni singolo tasso di scambio degli ordini d'acquisto é maggiore o uguale a 1. Se ció avviene, tutti gli n ordini possono essere completati, parzialmente o totalmente [17].

Se aggiungiamo un terzo soggetto, Charlie, per cui Alice vuole cedere x_1 token `A` e ricevere y_1 token `B`, Bob vuole cedere x_2 token `B` e ricevere y_2 token `C`, e Charlie vuole cedere x_3 token `C` e ricevere y_3 token `A`. I token necessari sono presenti, e lo scambio é possibile se:

$$\frac{x_1 \cdot x_2 \cdot x_3}{y_1 \cdot y_2 \cdot y_3} \geq 1 \quad (2)$$

Vedere la sezione 7.1 per maggiori dettagli sugli ordini di Loopring.

4 Partecipanti dell'Ecosistema

I seguenti partecipanti dell'ecosistema forniscono congiuntamente tutte le funzionalitá che un exchange centralizzato puó offrire.

- **Wallets**: Un comune servizio di portafoglio o un'interfaccia che permette agli utenti di accedere ai propri token ed un modo per inviare ordini al network Loopring. I Wallets saranno incentivati a produrre ordini condividendo commissioni con i minatori di anelli (vedere sezione 8). Con la credenza che il futuro degli scambi avrá luogo al sicuro all'interno dei wallets degli utenti, connettere queste riserve di liquiditá attraverso il nostro protocollo é fondamentale.

- **Blockchain del Consorzio di Condivisione di Liquiditá/Mesh di Relé**: Un network di mesh di relé per la condivisione di ordini e liquiditá. I nodi che eseguono il software Loopring per relé, hanno la possibilitá di unirsi ad un network giá esistente e condividere liquiditá con altri relé attraverso un consorzio. Il consorzio che stiamo costruendo in una prima implementazione ha un capacitá di condivisione ordini quasi in tempo reale (1-2 secondi per blocco), ed elimina lo storico degli ordini molto antico per permettere ai nuovi nodi di scaricare la blockchain piú velocemente. Si tenga in considerazione che i relé non devono necessariamente unirsi a questo consorzio; possono agire in modo indipendente e non condividere la liquiditá con altri, o possono creare e gestire un loro network di condivisione di liquiditá.

- **Relé/Minatori di Anelli**:I Relé sono nodi che ricevono ordini dai wallet o dal mesh di relé, mantengono un registro di commesse ed uno storico degli scambi pubblici, ed eventualmente trasmettono ordini ad altri relé (attraverso un qualunque strumento oltre alla blockchain) e/o a nodi di mesh di relé. L'operazione di minare anelli é una caratteristica aggiuntiva - non un requisito - dei relé. Questa é infatti computazionalmente molto intensiva ed é svolta completamente fuori dalla blockchain. Chiamiamo i relé che minano "Ring-Miners", in quanto producono anelli di ordini combinando insieme ordini diversi. I relé sono liberi di (1) scegliere di comunicare tra di loro, (2) decidere come costruire il loro registro di commesse, e (3) scegliere quale algoritmo utilizzare per minare gli anelli di ordini.

- **Smart Contracts del Protocollo Loopring (LPSC)**: Un insieme di smart contracts pubblici e gratuiti che controllano gli anelli di ordini ricevuti dai minatori di ordini, trasferiscono i token per conto degli utenti in modo sicuro, incentivano le operazioni dei wallets e dei minatori di anelli attraverso la creazione di commissioni, e creano eventi. I browsers di ordini/Relé utilizzano questi eventi per mantenere aggiornati i propri registri ed il proprio storico di scambi. Vedere l'appendice **??** per i dettagli.

- **Servizi di Tokenizzazione Asset (ATS)**: Un ponte tra assets che non possono essere scambiati direttamenti con Loopring. Sono servizi gestiti in modo centralizzato da imprese ed organizzazioni rispettabili. Gli utenti depositano assets (beni reali, fiat o token di altre blockchains) ed ottengono in cambio token che in futuro potranno essere nuovamente convertiti per i loro depositi. Loopring non é un protocollo che permette scambi tra blockchains differenti (fino a quando non verrá individuata una soluzione idonea), ma l'ATS permette lo scambio tra tokens ERC20 [18] e beni fisici, cosí come con beni presenti su altre blockchains.

5 Processo di Scambio

1. **Autorizzazione del Protocollo**: In figura 2, l'utente `Y` che vuole scambiare tokens autorizza gli LPSC a gestire `amountS` del token `B` the user wants to sell. che l'utente vuole vendere. Questa operazione non blocca i tokens dell'utente, che rimane libero di trasferirli mentre l'ordine viene processato.

2. **Creazione dell'Ordine**: Il tasso di cambio corrente ed il registro delle commesse per il token `B` da scambiare per il token `C`, sono offerti dai relé o da altri agenti connessi al network, come i browsers di ordini. L'utente `Y` piazza un ordine (ordine con limite di prezzo) specificando `amountS` e `amountB` e altri parametri attraverso le interfacce dei wallet che

integrano il protocollo. Un certo ammontare di LRx puó essere aggiunto all'ordine come commissione per i minatori d'anelli; piú é alta la commissione di LRx piú é alta la probabilitá che un minatore processi rapidamente l'ordine. L'hash dell'ordine é firmato con la chiave privata dell'utente `Y`.

3. **Trasmissione dell'Ordine**: Il wallet invia l'ordine e la sua firma digitale ad uno o piú relé che quindi aggiornano i propri registri pubblici delle commesse. Il protocollo non richiede che il registro sia costruito in un modo specifico, ad esempio con il metodo primo-arrivato-primo-servito. I relé hanno il potere di crearlo come meglio preferiscono.

4. **Condivisione della Liquiditá**: I relé trasmettono l'ordine agli altri relé attraverso il metodo che ritengono piú idoneo. Ancora una volta, c'é flessibilitá sul come/se i nodi interagiscono. Per facilitare il raggiungimento di un certo livello di connettivitá, é stato implementato un meccanismo di condivisione della liquiditá tra mesh di relé utilizzando un consorzio. Come menzionato nella sezione precedente, questo mesh di relay é ottimizzato per velocitá ed inclusivitá.

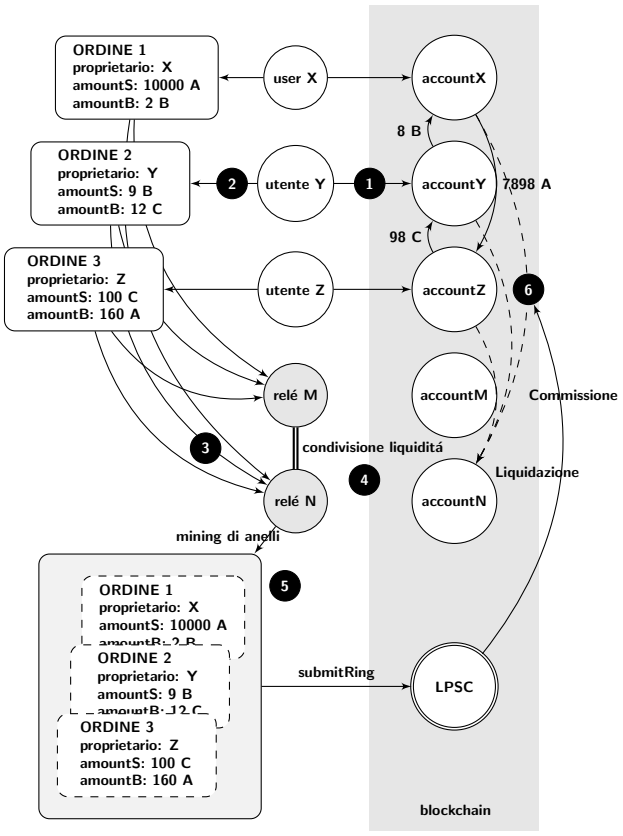

Figure 2: Processo di Scambio Loopring

5. **Mining di Anelli (Abbinamento di Ordini)**: I minatori di anelli provano ad eseguire l'ordine interamente o parzialmente ad un dato tasso di scambio o ad un tasso migliore, abbinandolo a diversi altri ordini. Il mining di Anelli é il motivo principale per cui il protocollo é in grado di offrire un'alta liquiditá per qualunque coppia di ordini. Se il tasso a cui l'ordine é eseguito é migliore di quello specificato dall'utente `Y`, il margine é condiviso tra tutti gli ordini che compongono l'anello. Come premio, il minatore puó scegliere tra la riscossione di una parte del margine (Divisione del Margine, e ritornare agli utenti gli LRx), o semplicemente trattenere la commissione in LRx.

6. **Verifica & Transazione**: L'anello di ordini é ricevuto dagli LPSC. Sono necessari diversi controlli per verificare i dati forniti dal minatore e determinare se l'anello di ordini puó essere completato integralmente o parzialmente (ció dipende dal tasso di completamento degli ordini nell'anello e dai token presenti nei wallet degli utenti). Se tutti i controlli hanno esito positivo, il contratto trasferisce i token agli utenti e paga i minatori e le commissioni ai wallet contemporaneamente. Se gli LPSC rilevano una mancanza di fondi necessari allo scambio nel wallet dell'utente `Y`, l'ordine verrá ridimensionato: un ordine ridimensionato torna automaticamente alla sua dimensione originaria se un quantitativo sufficiente di fondi viene depositato all'indirizzo dell'utente, diversamente da una cancellazione, che é una operazione manuale a senso unico che non puó essere annullata.

6 Flessibilitá Operativa

É importante notare che gli open standard di Loopring permettono ai partecipanti di operare con una significativa flessibilitá. Gli attori sono liberi di implementare nuovi modelli di business e generare valore per gli utenti, guadagnando commissioni in LRx sui volumi di scambio o su altre metriche definite nel processo (se lo decidono). L'ecosistema é modulare e pensato per incoraggiare la partecipazione di una moltitudine di applicazioni.

6.1 Il Registro delle Commesse

I relé possono progettare i loro registri in svariati modi per combinare ed abbinare e gli ordini degli utenti. Una prima implementazione del nostro registro delle commesse segue un modello OTC, dove gli ordini a prezzo limitato sono posizionati basandosi soltanto sul prezzo. Il momento in cui sono stati generati gli ordini, in altri termini, non ha un impatto sulla formazione del registro.Tuttavia, un relé é libero di progettare il proprio registro in modo da emulare il funzionamento tipico di exchange centralizzati, dove gli ordini sono classificati per prezzo ma rispettando anche il momento temporale di creazione dell'ordine. Se un relé é piú incline ad offrire questo tipo di meccanismo, puó creare/integrarsi con un wallet, e avere che gli ordini che partono da quel wallet vengano inviati a questo singolo relé,

che sará poi in grado di smistarli basandosi sul tempo. Ogni tipo di configurazione é possibile.

Mentre altri protocolli DEX richiedono a volte che i relé possiedano delle risorse - una riserva di token iniziali per piazzare gli ordini dell'acquirente - i relé Loopring devono soltanto trovare ordini abbinabili per far eseguire lo scambio, e possono farlo senza risorse iniziali.

6.2 Condivisione della Liquiditá

I relé sono liberi di progettare come condividere la liquiditá (ordini) tra di loro. Il nostro consorzio é solo una delle soluzioni per raggiungere questo scopo, e l'ecosistema é libero di interagire e comunicare come desidera. Oltre ad unirsi al consorzio blockchain, é possibile creare e gestire nuovi consorzi, creando le regole/incentivi che si ritengono piú opportuni. I relé possono anche lavorare in autonomia, come visto nel caso dell'implementazione che tiene conto del tempo. Sicuramente ci sono chiari vantaggi nel comunicare con gli altri come ad esempio la ricerca dell'effetto rete, tuttavia, differenti modelli di business possono avere necessitá di tipologie particolari di condivisioni e di divisioni delle commissioni.

7 Specifiche del Protocollo

7.1 Anatomia di un Ordine

Un ordine é un pacchetto di dati che descrive l'intento dell'utente allo scambio. Un ordine Loopring é definito utilizzando il Modello di Ordine Unidirezionale, o UDOM, come segue:

```
message Order {
  address protocol;
  address owner;
  address tokenS;
  address tokenB;
  uint256 amountS;
  uint256 amountB;
  unit256 lrcFee
  unit256 validSince; // Seconds since epoch
  unit256 validUntil; // Seconds since epoch
  uint8   marginSplitPercentage;  // [1-100]
  bool    buyNoMoreThanAmountB;
  uint256 walletId;
  // Dual-Authoring address
  address authAddr;
  // v, r, s are parts of the signature
  uint8   v;
  bytes32 r;
  bytes32 s;
  // Dual-Authoring private-key,
  // not used for calculating order's hash,
  // thus it is NOT signed.
  string  authKey;
  uint256 nonce;
}
```

Per assicurare l'origine dell'ordine, questo viene firmato contro l'hash dei suoi parametri con la chiave privata dell'utente, escludendo `authAddr`. Il parametro `authAddr` viene usato per firmare gli anelli d'ordine di cui lo stesso ordine é parte, in modo da prevenire il front-running. Si veda la sezione 9.1 per ulteriori dettagli. La firma é rappresentata dai campi `v`, `r`, ed `s` , e viene trasmessa sulla rete insieme ai parametri d'ordine. Ció assicura che l'ordine rimanga invariato durante la sua intera esistenza. Nonostante l'ordine rimanga invariato, il protocollo é comunque in grado di calcolarne lo stato attuale sulla base dell'ammontare del suo indirizzo e di altre variabili.

UDOM non include alcun prezzo (che per natura deve essere un numero a virgola mobile), ma utilizza piuttosto il termine `rate` o r, che viene espresso come `amountS/amountB`. Il rate non é un numero a virgola mobile, ma un'espressione che verrá solamente valutata a richiesta con altri interi non oggetto di firma, cosí da mantenere tutti i risultati intermedi come interi non firmati ed aumentarne l'accuratezza di calcolo.

7.1.1 Importi d'acquisto

Quando un minatore d'anelli crea un anello abbinando degli ordini, é possibile che risulti perseguibile un rate migliore, che permetterá agli utenti di ottenere piú `tokenB` del numero `amountB` che hanno specificato. Ad ogni modo se il parametro `buyNoMoreThanAmountB` é impostata a `True`, il protocollo assicura che gli utenti ricevano un numero di `amountB` non maggiore di `tokenB`. Il parametro di UDOM `buyNoMoreThantokenB` determina quindi quando un ordine sia da considerarsi completamente evaso. `buyNoMoreThantokenB` applica un valore massimo ad `amountS` o `amountB`, e permette agli utenti di esprimere le proprie intenzioni di scambio in modo piú granulare rispetto ai tradizionali ordini.

Per esempio: con `amountS` = 10 w `amountB` = 2, il rate $r = 10/2 = 5$. L'utente é quindi intenzionato a vendere 5 `tokenS` per ciascun `tokenB`. Il minatore trova e fa ottenere all'utente un rate di 4, permettendogli di ricevere 2.5 `tokenB` al posto di 2. Ad ogni modo, se l'utente vuole soltanto 2 `tokenB` ed imposta il parametro `buyNoMoreThanAmountB` a `True`, gli LPSC effettuano la transazione ad un rate di 4, e l'utente vende 4 `tokenS` per ogni `tokenB`, con un risparmio effettivo di 2 `tokenS`. Da considerare che non sono qui prese in esame le commissioni. (cf. sezione 8.1).

Quindi utilizzando

```
Order(amountS,tokenS,
      amountB,tokenB,
      buyNoMoreThantokenB)
```

per rappresentare un ordine in modo semplificato, per i mercati ETH/USD di un exchange tradizionale, una nor-

male modellazione di compravendita puó gestire il 1 ed il 3 ordine riportato sotto, ma non i due rimanenti:

1. Vendi 10 ETH ad un prezzo di 300 USD/ETH. Questo pu esprimersi come: `Order(10, ETH, 3000, USD, False)`.
2. Vendi ETH ad un prezzo di 300 USD/ETH per ottenere 3000 USD. Questo puó esprimersi come: `Order(10, ETH, 3000, USD, True)`.
3. Compra 10 ETH ad un prezzo di 300 USD/ETH, Questo puó esprimersi come: `Order(3000, USD, 10, ETH, True)`.
4. Spendi 3000 USD per comprare quanti piú ETH possibile ad un prezzo di 300 USD/ETH, Questo puó esprimersi come: `Order(3000, USD, 10, ETH, False)`.

7.2 Verifica dell'anello

Gli Smart Contracts del protocollo Loopring non calcolano il rate di scambio o gli importi, ma devono ricevere e verificare cosa i minatori forniscono come tali valori. Queste computazioni vengo effettuate dai minatori essenzialmente per due motivazioni principali: (1) il linguaggio di programmazione degli smart contracts, come solidity[19] nel caso di Ethereum, non supporta il calcolo a virgola mobile, specialmente pow(x, 1/n) (calcolare la radice n-esima di un numero a virgola mobile), (2) é auspicabile che tale calcolo avvenga off-chain cosí da ridurre le operazioni ed il costo di utilizzo della blockchain.

7.2.1 Verifica del Sub-Ring

Questo passaggio inibisce agli arbitraggisti la possibilitá di ottenere in modo scorretto l'intero margine di un anello d'ordine, mediante la creazione di nuovi ordini al suo interno. Sostanzialmente, una volta che un minatore identifica un anello d'ordine valido, potrebbe cadere nella tentazione di aggiungere ulteriori ordini allo stesso anello, cosí da assorbire il margine dell'utente (tasso di sconto). Come illustrato nella sottostante figura 3, calcolando opportunamente x1, y1, x2 e y2 sará possibile rendere il prodotto di tutti i rate d'ordine pari ad 1, cosí da annullare qualsiasi tasso di scambio.

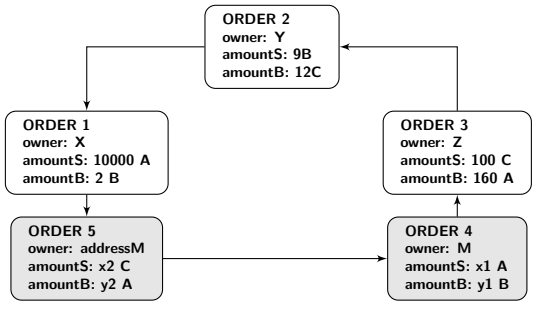

Figure 3: Un anello d'ordine con un sotto-anello

Ció comporta zero rischi, non apporta alcun valore aggiunto al network, ed é da considerarsi pertanto un comportamento scorretto da parte del minatore. Per prevenire questa possibilitá, Loopring impone che un loop valido non possa contenere alcun sotto-anello. Per verificare questa condizione, gli LPSC fanno in modo che ogni token non possa comparire piú di una volta in posizione di acquisto o vendita. Nel diagramma sopra, possiamo vedere come il token `A` compaia due volte come token d'acquisto e altrettante come token di vendita, questo non sarebbe pertanto permesso.

7.2.2 Verifica del Tasso di Completamento

Il calcolo del tasso di scambio nell'anello d'ordine é svolto dai minatori per le motivazioni sopra esposte. Gli LPSC devono verificarne la correttezza. Innanzitutto verificano che il tasso d'acquisto eseguibile dal minatore per ciascun ordine sia minore o uguale al tasso d'acquisto imposto dall'utente. Questo assicura che l'utente ottenga nella transazione almeno il tasso di scambio richiesto, se non migliore. A seguito della conferma dei tassi di scambio, gli LPSC assicurano che ciascun ordine che compone l'anello benefici dello stesso sconto. Ad esempio, se il tasso di sconto é γ, allora il prezzo per ogni ordine sará:

$r_{0\to1}\cdot(1-\gamma)$, $r_{1\to2}\cdot(1-\gamma)$, $r_{2\to0}\cdot(1-\gamma)$, e soddisferá:

$$r_{0\to1}\cdot(1-\gamma)\cdot r_{1\to2}\cdot(1-\gamma)\cdot r_{2\to0}\cdot(1-\gamma)=1 \qquad (3)$$

da cui:

$$\gamma = 1-\frac{1}{\sqrt[3]{r_{0\to1}\cdot r_{1\to2}\cdot r_{2\to0}}}. \qquad (4)$$

Se la transazione aggrega n ordini, allora lo sconto `discount` é:

$$\gamma = 1-\frac{1}{\sqrt[n]{\prod_{i=0}^{n-1} r^i}}, \qquad (5)$$

dove r^i rappresenta il tasso di scambio dell'ordine i-esimo. Ovviamente, solamente quando lo sconto é $\gamma \geq 0$, questi ordini possono esser soddisfatti; ed il tasso di scambio dell'ordine i-esimo (O^i) é $\hat{r^i} = r^i\cdot(1-\gamma)$, $\hat{r^i} \leq r^i$.

Ricordiamo il nostro esempio precedente in cui Alice ha 15 token `A` e vuole scambiarli con `B`, e Bob ha 10 token `B` e vuole scambiarli con 20 token `A`. Se il token `A` é preso come riferimento, allora Alice sta comprando token `B` per $\frac{15}{4} = 3.75$`A`, mentre Bob sta vendendo token `B` per $\frac{30}{10} = 3.00$`A`. Per calcolare lo sconto: $\frac{150}{120} = 1.25$ da cui $\frac{1}{1.25} = 0.8 = (1-\gamma)^2$. Da qui, il tasso di scambio che rende equa la transazione per entrambe le parti é $\sqrt{0.8}\cdot 3.75 \approx 3.3541$ token `A` per ogni token `B`.

Bob ha 4 token `B` e riceve 13.4164 token `A`, piú dei 12 che si aspettava di ottenere. Alice riceve i 4 token `B` che si aspettava ma li paga solo 13.4164 token `A`, meno dei 15 che era disposta a pagare. Si noti che una frazione di questo margine verrá utilizzata per pagare le commissioni che servono ad incentivare i minatori (e i wallet). (Vedere la sezione 8.1).

7.2.3 Tracciamento del completamento & cancellazione

Un utente puó cancellare parzialmente o completamente un ordine mediante l'invio di una specifica transazione agli LPSC, contenente i dettagli dell'ordine e l'importo da cancellare. Gli LPSC ne prendono atto, registrano l'importo da cancellare ed emettono al network un evento `OrderCancelled` Gli LPSC tengono e traccia di importi eseguiti e cancellati tramite un registro che utilizza l'hash dell'ordine come identificativo. Questi dati sono accessibili pubblicamente e gli eventi di `OrderCancelled` ed `OrderFilled` vengono emessi ad ogni variazione. Il tracciamento di questi valori rappresenta qualcosa di critico per gli LPSC nel processo di evasione dell'anello d'ordine.

Gli LPSC supportano inoltre la cancellazione di un ordine per qualsiasi coppia di scambio attraverso l'evento `OrdersCancelled` e la cancellazione di tutti gli ordini relativi ad un indirizzo tramite l'evento `AllOrdersCancelled`.

7.2.4 Scaling degli ordini

Gli ordini vengono riscalati in base all'esistenza di precedenti importi storici transati o cancellati, nonché sulla base del saldo degli account emittenti. Il processo identifica sulla base di queste caratteristiche l'ordine da eseguire con l'importo minore e lo utilizza come riferimento per ordinare tutte le transazioni dell'anello d'ordine. L'identificazione dell'ordine caratterizzato dal minor valore agevola la stima del volume d'esecuzione di ogni ordine. Ad esempio, supponendo che l'ordine i-esimo sia quello caratterizzato dal minor valore, il numero di token venduti per ogni ordine $\hat{s}$ ed il numero di token acquistati $\hat{b}$ per ogni ordine puó essere calcolato come:

$$\hat{s}^i = \overline{s}_i,\ \hat{b}^i = \hat{s}^i/\hat{r}^i,\ ;$$
$$\hat{s}^{i\oplus 1} = \hat{b}^i,\ \hat{b}^{i\oplus 1} = \hat{s}^{i\oplus 1}/\hat{r}^{i\oplus 1};$$
$$\hat{s}^{i\oplus 2} = \hat{b}^{i\oplus 1},\ \hat{b}^{i\oplus 2} = \hat{s}^{i\oplus 2}/\hat{r}^{i\oplus 2};$$
$$...$$

dove $\overline{s}_i$ é il saldo rimanente dopo che gli ordini sono stati parzialmente eseguiti.

In fase d'implementazione, possiamo tranquillamente assumere che qualunque ordine dell'anello abbia il minor valore, e quindi iterare nell'anello al massimo due volte per calcolare il volume d'esecuzione di ciascun ordine.

Esempio: Se il minor importo da soddisfare rappresenta il 5%, dell'ordine originale, tutte le transazioni dell'anello saranno ridotte del 5%. Una volta che le transazioni sono completate, l'ordine che si considerava avesse l'importo minore ancora da soddisfare dovrá risultare completamente eseguito.

7.3 Liquidazione dell'anello

Se l'anello d'ordine soddisfa tutti i punti precedenti, lo stesso puó essere chiuso cosí da permettere l'esecuzione delle transazioni. Ció significa che tutti gli n ordini formeranno un anello chiuso, connesso come in figura 4:

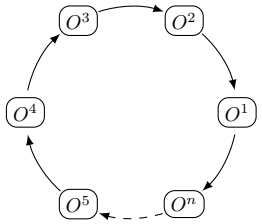

Figure 4: Liquidazione dell'anello

Per effettuare le transazioni, gli LPSC utilizzano lo smart contract `TokenTransferDelegate` .L'introduzione di tale preposto rende piú semplice l'upgrade di qualsiasi smart contract del protocollo, in quanto tutti gli ordini dovranno soltanto autorizzare quest'ultimo anziché gestire le differenti versioni del protocollo. Per ogni ordine dell'anello, il pagamento di `tokenS` viene effettuato con il successivo od il precedente ordine, a seconda dell'implementazione. Quindi la commissione del minatore viene versata in funzione del modello di commissioni scelto dal minatore stesso. Infine, una volta che tutte le transazioni sono effettuate, viene emesso l'evento `RingMined`.

7.3.1 Eventi emessi

Il protocollo emette eventi che permettono ai relé, ai gestori d'ordine e ad altri attori coinvolti di ricevere aggiornamenti sul registro delle commesse in modo piú efficiente possibile. Questi eventi sono:

- **OrderCancelled**: Un ordine specifico é stato cancellato.
- **OrdersCancelled**: Tutti gli ordini provenienti da un singolo indirizzo per una specifica coppia di scambio sono stati cancellati.
- **AllOrdersCancelled**: Tutti gli ordini provenienti da un singolo indirizzo sono stati cancellati.
- **RingMined**: Un anello d'ordine é stato correttamente liquidato. Questo evento contiene i dati relativi ad ogni singolo trasferimento di token all'interno dell'anello.

8 LRx Token

LRx é la nostra notazione generica di token. LRC é il token Loopring su Ethereum, LRQ su Qtum, LRN su NEO, etc. Altre tipologie di LRx saranno introdotte in futuro, man mano che Loopring verrá esteso ad altre blockchain pubbliche.

8.1 Modello di Commissioni

Quando gli utenti creano un ordine, specificano un importo di LRx da versare al minatore come commissione, oppure una percentuale del margine ottenuto tramite l'ordine (`marginSplitPercentage`) che il minatore puó richiedere, definito margin split. Spetta al minatore la decisione su quale opzione applicare tra commissione o margin split.

Qui una rappresentazione del margin split:

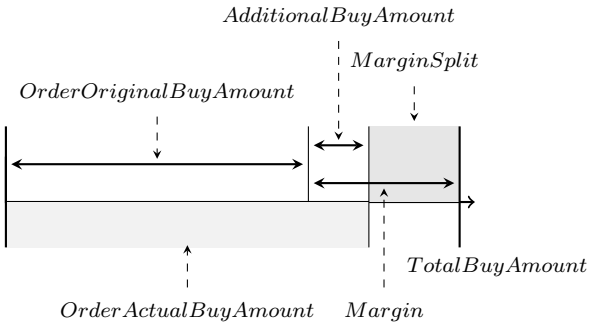

Figure 5: A 60% Margin Split

Se il margine sull'anello di ordini é troppo contenuto, il minatore propenderá per la commissione in LRx. Se, al contrario, il margine é tale da rendere conveniente il margin-split rispetto alla commissione in LRx, il minatore propenderá per il margin split. Si applica per un'ulteriore condizione: quando il minatore propende per il margin split, questo dovrá versare all'utente che ha creato l'ordine una commissione almeno pari al numero di LRx che l'utente avrebbe dovuto versare come commissione al minatore. Ció eleva di fatto la soglia a partire da cui il minatore potrá considerare l'adozione del margin split a due volte la commissione in LRx, aumentando di fatto la propensione verso l'adozione della commissione in LRx. Questo permette ai minatore di ottenere un compenso fisso su anelli di ordini a margine ridotto, ottenendo allo stesso tempo un compenso inferiore su anelli di ordini con margine piú alto. Il nostro modello di commissione si basa sull'aspettativa che, con la crescita e maturazione del mercato, ci sará un numero sempre inferiore di anelli di ordini con alto margine, da cui la necessitá di incentivare una commissione fissa in LRx. Otteniamo pertanto il seguente grafico:

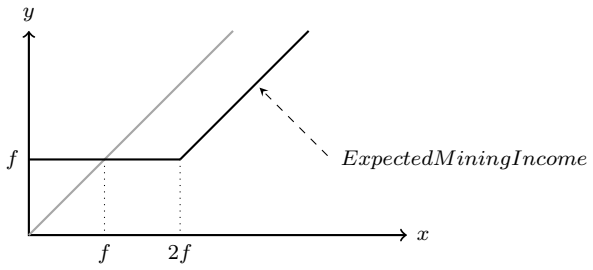

Figure 6: Modello di commissioni di Loopring

dove f é la commissione in LRx, x é il margin split, y é il compenso del minatore. $y = max(f, x - f)$ come indicato dalla linea continua; se la commissione in LRx per l'ordine é 0, l'equazione diviene $y = max(0, x - 0)$ che si semplifica in $y = x$ come indicato dalla linea in grigio. Queste le conseguenze:

1. Se il margin split é 0, i minatori propenderanno per la commissione fissa in LRx, traendone comunque incentivo.
2. Se la commissione in LRx é 0, il risultato é un modello generico lineare come rappresentato dalla linea in grigio.
3. Quando il guadagno da il margin split é maggiore di 2x(LRx fee), i minatori sceglieranno il margin split, versando la commissione in LRx all'utente.

Da notare che se la commissione in LRx é diversa da zero, a prescindere dall'opzione adottata dal minatore, vi sará comunque un trasferimento di LRx tra il minatore ed il creatore dell'ordine. In un caso il minatore guadagna la commissione in LRx, nell'altro versa la stessa commissione in LRx al creatore d'ordine, propendendo per il margin split. I minatori condivideranno una certa percentuale del compenso con i gestori di wallet. Quando un utente piazza un ordine attraverso un wallet e questo viene eseguito, il gestore di wallet viene compensato con una porzione della commissione o del margin split.

Nonostante questo approccio sia modulare, e sia possibile implementare il proprio modello a riguardo, consideriamo che la percentuale di commissioni da condividere con i wallet sia approssimativamente del 20%-25%. I wallet rappresentano infatti un target chiave per l'implementazione del protocollo Loopring, avendo una propria base utenti, e potendo al momento contare su limitate fonti di guadagno.

8.2 Governance decentralizzata

Il protocollo Loopring é nel suo fondamento un protocollo social, nel senso che si affida sulla coordinazione di diversi attori per permettere loro di collaborare in modo efficiente verso un goal comune. Ció non é dissimile da altri protocolli che caratterizzano la Cryptoeconomia in senso lato, la cui utilitá é ampiamente regolata dagli stessi meccanismi dei problemi di coordinamento [20], equilibrio d'attivazione e razionalitá limitata. A questo fine, i token LRx non sono solamente intesi per il pagamento di commissioni, ma bensí per allineare gli incentivi finanziari dei diversi partecipanti del network. Questo allineamento é una condizione fondamentale per l'adozione di qualsiasi protocollo, ma ancor di piú per i protocolli di scambio, considerando che il successo di quest'ultimi é determinato dalla capacitá di migliorare la liquiditá di un ecosistema decentralizzato.

I token LRx saranno utilizzati per permettere di gestire i futuri aggiornamenti del protocollo tramite governance decentralizzata. Gli aggiornamenti degli smart contracts saranno governati dai possessori di token cosí da assicurarne continuitá e sicurezza, mitigando i rischi di eccessiva liquiditá, non compatibile. L'immutabilitá degli smart

contracts una volta rilasciati, costituisce un rischio che le dApps o gli utenti finali continuino ad interagire con version deprecate, e ne precludano l'aggiornamento. La possibilitá di aggiornamento é chiave per il successo di un protocollo, che deve potersi adattare dinamicamente alla richiesta del mercato e sottostanti blockchain. Una governance decentralizzata da parte dei possessori di LRx permetterá l'aggiornamento degli smart contracts del protocollo senza compromettere dApps o utenti finali, o senza affidarsi eccessivamente all'astrazione degli smart contracts. I token LRx esistono in quantitá limitate, e nel caso degli LRC, una percentuale di questi sono tenuti bloccati dalla Fondazione Loopring ed allocati in fondi speciali diretti alla comunitá [21].

Tuttavia, i possessori dei token LRx non sono i soli portatori di interessi da considerare nell'evoluzione da imprimere al protocollo: relé/minatori, wallet, sviluppatori ed altri sono parte integrante dell'ecosistema e la loro voce deve essere ascoltata. Infatti, dato che questi agenti non hanno la necessitá di possedere alcun LRx per svolgere il loro rispettivo lavoro (dato che i market makers e i makers/takers tradizioni non esistono, le riserve iniziali non sono obbligatorie) dobbiamo mettere in atto metodi alternativi per rispettare i loro interessi. Inoltre, il semplice voto basato sui token, sia on-chain che off-chain, é una soluzione imperfetta, perché la concentrazione della proprietá ed un basso turnout di voto pongono dei rischi. Da ció, l'obiettivo é quello di implementare un modello di governance che é costruito su diversi livelli, e che poggia sulla consapevolezza che un certo insieme di processi decisionali sono la normalitá. Questo puó essere facilitato da istituti di coordinamento che offrono segnali da diversi insiemi di partecipanti, e forse, da punti focali stabiliti a priori. Man mano che il sistema diventerá operativo, la Fondazione Loopring evolverá inevitabilmente da un insieme di sviluppatori di protocollo ad assistenti di protocollo.

9 Protezione dagli Attacchi e dalle Frodi

9.1 Prevenzione del Front-running

Negli exchange decentralizzati, il front-running avviene quando qualcuno prova a copiare l'ordine di scambio di un altro nodo, e a farlo minare prima della transazione originale, che si trova in attesa nell'insieme delle transazioni (mempool). Questa azione puó essere attuata specificando una commissione di transazione piú alta (prezzo di gas). Il principale schema di front-running in Loopring (e in qualunque protocollo di abbinamento ordini) é il furto di ordini (order-flitch): quando un front-runner ruba uno o piú ordini di un anello da una transazione pendente; e specificatamente riguardo Loopring: quando un front-runner ruba un intero anello d'ordini da una transazione pendente. Quando una transazione submitRing non é stata confermata ed é ancora nell'insieme delle transazioni pendenti, chiunque puó facilmente individuare queste transazioni e sostituire `minerAddress` con il loro indirizzo (il `filcherAddress`), cosí facendo, possono firmare nuovamente il pacchetto dati con `filcherAddress` tper sostituire la firma dell'anello d'ordini. Il ladro puó fissare un prezzo di gas piú alto e inviare una nuova transazione sperando che i minatori prenderanno la sua nuova transazione all'interno del prossimo blocco invece della transazione submitRing originale. Le soluzioni precedentemente trovate a questo problema presentavano considerevoli aspetti negativi: richiedendo piú transazioni e quindi aumentando i costi di gas per i minatori; e prendendo almeno il doppio dei blocchi per fissare un anello. La nostra nuova soluzione, il Dual Authoring [22], implica l'adozione di un meccanismo che mette a punto due livelli di autorizzazione per gli ordini uno per il regolamento, ed uno per il mining dell'anello.

Il processo di Dual Authoring:

1. Per ogni ordine, il wallet genererá una coppia di chiave pubblica/chiave privata casuale, la coppia di chiavi verrá inserita nel JSON snippet dell'ordine. (Un'alternativa é quella di usare l'indirizzo derivato dalla chiave pubblica invece che la chiave pubblica di per sé per ridurre la dimensione in termini di byte. Utilizziamo `authAddr` per rappresentare questo indirizzo, e `authKey` per raffigurare la combaciante chiave privata `authAddr`).

2. Viene calcolato l'hash dell'ordine con tutti i campi all'interno dell'ordine (ad eccezione di `r`, `v`, `s`, e `authKey`),e viene firmato l'hash utilizzando la chiave privata del proprietario `owner` (non `authKey`).

3. Il wallet manderá l'ordine insieme a `authKey` ai relé per essere minato. I minatori verificheranno che `authKey` e `authAddr` sono abbinate correttamente e che la firma dell'ordine é valida rispetto all'indirizzo del proprietario.

4. Quando un anello é stato identificato, i minatori useranno `authKey` dell'ordine per firmare l'hash dell'anello, il `minerAddress`, e tutti i parametri del mining. Se un order-ring contiene n ordini, ci saranno conseguentemente, n firme da n `authKey`s. Abbiamo nominato queste firme come `authSignature`s. Il minatore potrebbe anche aver bisogno di firmare l'hash dell'anello insieme a tutti i parametri del mining utilizzando la chiave privata del `minerAddress`.

5. Il minatore richiama la funzione submitRing con tutti i parametri, e allo stesso tempo tutte le extra `authSignature`s. importante notare che `authKey`s NON é parte delle transazioni on-chain e quindi rimangono sconosciute ad altre parti ad eccezione del minatore.

6. Il protocollo di Loopring verificherá ognuna delle `authSignature` rispetto al corrispondente `authAddr` di ogni ordine, e rifiuterá l'order-ring se qualcuna delle `authSignature` é mancante o invalida.

Il risultato é che adesso:

- La firma dell'ordine (grazie alla chiave privata dell'indirizzo dell' `owner`) garantisce che l'ordine non possa essere modificato, incluso il `authAddr`.
- La firma del minatore (grazie alla chiave privata del `minerAddress`), se fornita garantisce che nessuno possa utilizzare la sua identitá per minare un anello d'ordini.
- La `authSignature`s garantisce che l'intero anello non possa essere modificato, incluso i `minerAddress`, e quindi nessun ordine puó essere rubato.

Il Dual Authoring previene il furto d'ordini ed il furto di anello e nel frattempo assicura che il regolamento dell'anello possa essere eseguito in un'unica transazione. Ulteriormente, la Dual Authoring apre le porte per la trasmissione di ordini condivisi in due modi: condivisioni che non combaciano e condivisioni che combaciano. Da condizione predefinita Loopring utilizza un modello OTC e supporta solamente ordini a prezzo limitato, ció vuol dire che le marche temporali (timestamps) degli ordini vengono ignorate. Questo implica che il front-running non ha nessun impatto sul prezzo reale di quello scambio, ma ha un impatto solo se viene eseguito o no.

10 Altri Attacchi

10.1 Attacchi Sybil o DOS

Utenti malintenzionati – operando in chiaro o sotto falsa identitá – potrebbero mandare un grande numero di piccoli ordini per attaccare i nodi di Loopring. Tuttavia, visto che i nodi hanno il potere di creare da sé le regole sulla base delle quali accettare o rifiutare gli ordini – informazioni che possono rendere pubbliche o mantenere private – la maggior parte di questi ordini sarebbe rigettata per via dell'incapacitá di produrre profitti soddisfacenti quando abbinati. Dando il potere ai relé di decidere le proprie modalitá di gestione degli ordini non riteniamo che un attacco con molti piccoli ordini possa essere una reale minaccia.

10.2 Saldo Insufficiente

Utenti in malafede potrebbero firmare e diffondere ordini il cui valore dell'ordine non é zero ma il cui indirizzo ha effettivamente un saldo pari a zero. I nodi potrebbero monitorare e notare che alcuni ordini hanno un saldo attuale di zero, aggiornare lo stato di questi ordini di conseguenza e quindi scartarli. I nodi spendono tempo per aggiornare lo stato di un ordine, ma possono anche scegliere di minimizzare lo sforzo attraverso, per esempio, una lista nera di indirizzi e interrompendo i relativi ordini.

11 Riepilogo

Il protocollo di Loopring vuole essere una base fondamentale per gli exchange decentralizzati. Cosí facendo, il protocollo ha delle profonde ripercussioni in come le persone scambiano valori e beni. Il denaro, come bene intermediario, facilita o sostituisce il baratto risolvendo la problematica comunione di necessitá [23], per cui due controparti devono desiderare i rispettivi beni o servizi. Similmente, il protocollo Loopring si pone l'obiettivo di liberarci da questa dinamica di necessitá di corrispondenza tra beni che si vogliono scambiare, utilizzando gli anelli come modo per facilitare gli scambi. Ció é significativo per il modo in cui la societá e i mercati scambiano tokens, beni tradizionali, e altro. Infatti, cosí come le criptovalute decentralizzate pongono una minaccia al controllo delle nazioni sulla moneta, un protocollo combinatorio che puó mettere insieme traders (consumatori/produttori) su ampia scala, é una minaccia teorica al concetto stesso di moneta. Tra i benefici del protocollo vi sono:

- La gestione degli ordini off-chain e regolamento degli scambi on-chain, questo significa nessun sacrificio in termini di prestazione per la sicurezza.
- Grande liquiditá dovuta al mining di anelli e alla condivisione degli ordini.
- La Dual Authoring risolve il dannoso problema del front running subito oggi da tutti i DEXs e dai loro utenti.
- Smart contracts aperti e pubblici consentono a qualunque dApp di costruire o interagire con il protocollo.
- La standardizzazione tra operatori consente effetti di rete e migliora l'esperienza dell'utente.
- Il network mantiene flessibilitá nella gestione del registro delle commesse e nella comunicazione.
- La riduzione delle barriere di entrata, ció si traduce in dire costi minori per i nodi che partecipano al network e per gli utilizzatori finali.
- Scambi anonimi effettuati direttamente dai portafogli degli utenti.

12 Ringraziamenti

Vorremmo esprimere la nostra gratitudine ai nostri mentori, consulenti e a tutte le persone nella community che sono state cosí disponibili e generosi a condividere la loro conoscenza. In particolare vorremmo ringraziare Shuo Bai

(di ChinaLedger); il Professore Haibin Kan; Alex Cheng, Hongfei Da; Yin Cao; Xiaochuan Wu; Zhen Wang, Wei Yu, Nian Duan, Jun Xiao, Jiang Qian, Jiangxu Xiang, Yipeng Guo, Dahai Li, Kelvin Long, Huaxia Xia, Jun Ma, and Encephalo Path per aver corretto e averci consigliato in merito a questo progetto.

References

[1] Vitalik Buterin. Ethereum: a next generation smart contract and decentralized application platform (2013). *URL {http://ethereum. org/ethereum. html}*, 2017.

[2] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151, 2014.

[3] Patrick Dai, Neil Mahi, Jordan Earls, and Alex Norta. Smart-contract value-transfer protocols on a distributed mobile application platform. *URL: https://qtum. org/uploads/files/ cf6d69348ca50dd985b60425ccf282f3. pdf*, 2017.

[4] Viktor Atterlönn. A distributed ledger for gamification of pro-bono time, 2018.

[5] Hernando de Soto. *The Mystery Of Capital*. Basic Books, 2000.

[6] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[7] Fabian Schuh and Daniel Larimer. Bitshares 2.0: Financial smart contract platform, 2015.

[8] Bancor protocol. *URL https://bancor.network/*, 2017.

[9] Yaron Velner Loi Luu. Kybernetwork: A trustless decentralized exchange and payment service. `https://kr.kyber.network/assets/KyberNetworkWhitepaper.pdf`, Accessed: 2018-03-05.

[10] Fortune. How to steal $500 million in cryptocurrency. `http://fortune.com/2018/01/31/coincheck-hack-how`, Accessed: 2018-03-30.

[11] Robert McMillan. The inside story of mt. gox, bitcoins 460 dollar million disaster. 2014.

[12] Sylvain Ribes. Chasing fake volume: a crypto-plague. `https://medium.com/@sylvainartplayribes/chasing-fake-volume-a-crypto-plague-ea1a3c1e0b5e`, Accessed: 2018-03-10.

[13] Rossella Agliardi and Ramazan Genay. Hedging through a limit order book with varying liquidity. 2014.

[14] Will Warren and Amir Bandeali. 0x: An open protocol for decentralized exchange on the ethereum blockchain, 2017.

[15] Iddo Bentov and Lorenz Breidenbach. The cost of decentralization. `http://hackingdistributed.com/2017/08/13/cost-of-decent/`, Accessed: 2018-03-05.

[16] Daniel Wang. Coinport's implemenation of udom. `https://github.com/dong77/backcore/blob/master/coinex/coinex-backend/src/main/scala/com/coinport/coinex/markets/MarketManager.scala`, Accessed: 2018-03-05.

[17] Supersymmetry. Remarks on loopring. `https://docs.loopring.org/pdf/supersimmetry-loopring-remark.pdf`, Accessed: 2018-03-05.

[18] Fabian Vogelsteller. Erc: Token standard. *URL https://github.com /ethereum /EIPs /issues /20*, 2015.

[19] Chris Dannen. *Introducing Ethereum and Solidity*. Springer, 2017.

[20] Vitalik Buterin. Notes on blockchain governance. `https://vitalik.ca/general/2017/12/17/voting.html`, Accessed: 2018-03-05.

[21] Loopring Foundation. Lrc token documents. `https://docs.loopring.org/English/token/`, Accessed: 2018-03-05.

[22] Daniel Wang. Dual authoring looprings solution to front-running. *URL https://medium.com/loopring-protocol/dual-authoring-looprings-solution-to-front-running-d0fc9c348ef1*, 2018.

[23] Nick Szabo. Menger on money: right and wrong. `http://unenumerated.blogspot.ca/2006/06/menger-on-money-right-and-wrong.html`, Accessed: 2018-03-05.