Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Informatica per il management

Ethereum alla prova dei fatti: Analisi sull'utilizzo degli smart contracts per l'implementazione di opzioni nei mercati finanziari

Relatore:
Chiar.mo Prof.
Gabriele D'Angelo

Presentata da:
Andrea Gurioli

Correlatore:
Chiar.mo Prof.
Stefano Ferretti
Dr. Mirko Zichichi

III Sessione
2018/2019

Ringrazio il Professor Stefano Ferretti e il Dr. Mirko Zichichi per avermi aiutato durante lo sviluppo di questo progetto, rendendolo stimolante e attinente ai miei interessi.
Desidero ringraziare i miei genitori, i quali mi hanno appoggiato durante tutti questi anni.
Ringrazio inoltre i miei coinquilini Enrico, Roberto, Riccardo, Vincenzo, Marco, Matteo e Giovanni che mi hanno accompagnato rendendo fantastica questa esperienza.
Infine, desidero ringraziare chi mi ha aiutato durante tutto questo percorso dandomi un enorme supporto morale, in particolare Sofia, Luca, Matteo, Giovanni, Michele, Federico, Francesco, Andrea, Mirco, Onico, Martina, Chris, Chiara, Alberto, Thomas, Antonio, Lorenzo e Matilda.

Abstract

Spesso, quando si parla di mercati finanziari, si visualizza subito un'entità centralizzata parte del paradigma monolitico creatosi. E' dunque difficile discostarsi col pensiero da una metodologia così radicata nella struttura sociale qual è la centralizzazione dei mercati, così difficile che la mente evita di abbozzarne una versione differente.
Lo sviluppo informatico, fautore di innovazione, è stato, attraverso l'avvento della piattaforma decentralizzata Ethereum, in grado di ristrutturare questo paradigma rompendo lo stigma (solo all'apparenza immutabile) della centralizzazione.
Scopo principale di questo lavoro di tesi è dato da un confronto sotto vari aspetti tra il modello attualmente in uso (centralizzato), ed una alternativa proposta da Vishakh immessa nel sistema Ethereum; confronto che è stato attuato prendendo in analisi l'acquisto e la vendita di opzioni finanziarie.

Indice

Elenco delle figure

Introduzione

Spesso, quando si parla di mercati finanziari, si visualizza subito un'entità centralizzata parte del paradigma monolitico creatosi. E' dunque difficile discostarsi col pensiero da una metodologia così radicata nella struttura sociale qual è la centralizzazione dei mercati, così difficile che la mente evita di abbozzarne una versione differente.
Lo sviluppo informatico, fautore di innovazione, è stato, attraverso l'avvento della piattaforma decentralizzata Ethereum, in grado di ristrutturare questo paradigma rompendo lo stigma (solo all'apparenza immutabile) della centralizzazione.
Scopo principale di questo lavoro di tesi è dato da un confronto sotto vari aspetti tra il modello attualmente in uso (centralizzato), ed una alternativa proposta da Vishakh(da Vishakh, 2016) immessa nel sistema Ethereum; confronto che è stato attuato prendendo in analisi l'acquisto e la vendita di opzioni finanziarie.
Al fine di strutturare questa analisi dando giustizia al retaggio tecnologico utilizzato, come primo capitolo si potrà trovare lo stato dell'arte, sezione che partirà con uno sguardo verso le blockchain ed ethereum, senza trascurare però il lato finanziario. Successivamente, all'interno del secondo capitolo si è passati ad un iniziale confronto astratto tra i due modelli, prendendo come supporto il paper di Massimo Morini(da Morini, 2017); analisi che inizierà ad avere consistenza nel capitolo tre, attraverso lo studio del modello creato da Vishakh. Al termine del lavoro, rispettivamente nel quarto capitolo, si applicherà il modello strutturato nel capitolo precedentemente descritto e si effettueranno una serie di rilevazioni per valutare la bontà del modello, per andare poi a confrontarlo col modello proposto dal sistema Fineco.

Capitolo 1

Stato dell'arte

In questa sezione sono descritte le principali tecnologie usate a supporto del progetto, a partire dalla struttura della blockchain fino ad arrivare al funzionamento della piattaforma Ethereum con annessi smart contracts. Infine, vengono descritti i contratti di opzione e la strategia Bull call spread che verrà poi implementata nei capitoli successivi.

1.1 Blockchain

La continua necessità di una maggiore sicurezza informatica e i costi legati alla centralizzazione, ormai paradigma dello sviluppo di qualsiasi modello, che sia informatico o meno, ha spinto verso la creazione di una tecnologia completamente decentralizzata basata su una rete peer to peer: La Blockchain.
Le sue origini prendono forma grazie a Satoshi Nakamoto, pseudonimo per una entità ancora sconosciuta, nel 2008.
Satoshi è stato infatti il creatore della prima Blockchain, seppur sia il connubio di tecnologie precedentemente utilizzate separatemente, ed ha dato di conseguenza luce alla ormai più famosa criptovaluta esistente al mondo, il Bitcoin.
Seppur il nome del creatore della blockchain sia ormai legato a Satoshi, 'l'idea dietro alla tecnologia blockchain viene descritta già nel 1991, quando i ricercatori Stuart Haber e W. Scott Stornetta introducono una soluzione computazionalmente pratica per la marcatura temporale di documenti digitali per fare in modo che non possano essere retrodatati o alterati', e, successivamente, nel 2004, l'esperto informatico e attivista crittografico Hal Finney (Harold Thomas Finney II) introduce un sistema chiamato RPoW, Reusable Proof Of Work(da BinanceAcademy, 2017).
Satoshi Nakamoto colse quindi successivamente, nel 2008, i frutti di tali soluzioni e li racchiuse nel whitepaper del Bitcoin. Il sistema bitcoin risulta essere quindi una

piattaforma per pagamenti elettronici attraverso lo scambio di criptovaluta, il tutto basato su di una tecnologia a Blockchain.

1.1.1 Principali punti di forza del sistema

Un sistema decentralizzato quale la blockchain risulta essere molto vantaggioso secondo vari aspetti, a seconda anche dello scopo di utilizzo della stessa; Il sistema ha quindi come principale punto di forza l'assenza di una unità centrale grazie alla tecnologia peer to peer.
Tra le fondamenta che vanno a modellare la resistenza al passaggio verso questa tecnologia, si fa spazio il dubbio dato dalla sicurezza di tale approccio; tale dubbio, non solo risulta essere infondato, ma la sicurezza del sistema è un punto chiave del sistema stesso in quanto tutti i nodi terranno traccia delle transazioni avvenute all'interno del sistema, rendendo il controllo, precedentemente unilaterale e centralizzato, plurilaterale. Risulterà quindi essere un registro più sicuro rispetto ad una classica struttura a server.

1.1.2 Struttura del sistema

La struttura dati implementata nella blockchain è di tipo immutabile e condiviso; tali condizioni sono date dal fatto che ogni blocco è costituito da un hash generato dal blocco precedente, e ogni nodo principale possieda l'intera copia della blockchain contenente quindi il registro delle transazioni.
Ogni nodo andrà quindi ad occuparsi della validazione di nuovi blocchi, inoltre si occuperà della costruzione di essi attraverso la risoluzione di un algoritmo; algoritmo che potrà essere diverso a seconda della piattaforma.
Andando ad analizzare le parti principali di ogni blocco, notiamo subito che, oltre alla presenza di un codice hash relativo al blocco precedente, è presente un blocco di dati inerente alle transazioni ultimate all'interno della blockchain, queste transazioni avranno quindi effetto solo dopo la creazione di un blocco che le contenga, mantenendo inalterata la struttura dati della blockchain sino all'inserimento del blocco contenente la transazione stessa.
I blocchi verranno generati volta per volta dai nodi della rete. La difficoltà dello scoprire i nodi (detto anche 'mining') è data dalla Proof of work, algoritmo a crescente difficoltà che risulta essere complesso da risolvere ma al contempo facile da verificarne la veridicità attraverso un sistema decentralizzato di consenso.
Avremo quindi come risultato che, ogni blocco, prima di essere iscritto alla blockchain sarà controllato da tutti i nodi del sistema, il sistema di consenso è basato su

di una politica maggioritaria, non sarà quindi necessario che tutti i nodi presenti abbiamo approvato il nodo entrante.
Ogniqualvolta che un nodo riesce a scoprire un blocco nuovo, verrà ricompensato con un quantitativo di denaro nella criptovaluta in uso nel sistema, questo risulta essere il principale incentivo per stimolare l'utenza verso l'utilizzo della blockchain attraverso un full node.
I nodi del sistema gestiranno le transazioni e avranno accesso ai propri fondi attraverso l'utilizzo dei wallets: applicazioni esterne poste come intermediario tra l'utente e la blockchain, in grado di gestire chiavi pubbliche e private dell'utilizzatore.
I wallet risulteranno essere quindi parte fondamentale del sistema, sia per la sicurezza, che per tener traccia dei trasferimenti, in quanto ogni utente sarà identificato attraverso una chiave pubblica, a sua volta generata da una chiave privata (unica chiave in grado di firmare e rendere valida la transazione) visibile solo dal proprietario della stessa. Sarà poi il wallet a porre la firma sulla transazione, rendendola quindi valida per il sistema.
Risulta inoltre possibile accedere alla piattaforma senza una copia dell'intera blockchain, sarà però necessario appoggiarsi ad un nodo centrale, il che comporterà una riduzione in termini di sicurezza andando ad utilizzare un nodo come proxy per l'utilizzo del servizio, ed un indebolimento del sistema, in quanto i nodi non partecipanti al processo di proof of work, non avranno un registro della blockchain e non prenderanno parte alla validazione dei nuovi blocchi.

1.1.3 Principali utilizzi

Il sistema risulta quindi essere estremamente affidabile in termini di sicurezza, negli anni infatti ha visto la sua implementazione per i più svariati ambiti e risulta essere un valido sostituto alla classica memorizzazione su server.
Oltre all'utilizzo per un sistema di scambi elettronici su criptovaluta, uno sviluppo fondamentale è l'utilizzo della Blockchain come piattaforma che offre servizi di implementazione per codice iscritto all'interno della stessa creando nuovi paradigmi di programmazione; più specificatamente andremo a vedere nelle sezioni successive la piattaforma Ethereum e gli smart contracts.

1.2 Ethereum

La piattaforma Ethereum è un sistema decentralizzato basato su di una general purpose Blockchain. Possiamo definirla come una "state machine" distribuita ma che, al posto di tener traccia del solo possesso della valuta come faceva la Bitcoin

blockchain, traccia le transizioni di stato di un archivio di dati; archivio che sarà in grado di memorizzare un qualsiasi dato esprimibile sotto la forma di tupla chiave-valore.(da Dr. Gavin Wood, 2019a)

1.2.1 Ethereum come interprete globale

La piattaforma Ethereum si avvale dell'Ethereum Virual Machine, ovvero un runtime enviroment per smart contracts la cui copia sarà presente in ogni nodo del sistema dando la possibilità alla piattaforma di eseguire il codice (denominato 'smart contract'), comportandosi quindi come un computer mondiale decentralizzato a singola istanza; sarà grazie alla blockchain base della piattaforma che si registreranno i cambiamenti di stato del "computer globale" e si processeranno transazioni e smart contracts.

1.2.2 I client Ethereum

I nodi che operano all'interno della rete sono i client della piattaforma Ethereum, essi si distinguono in due tipologie principali:

- Remote client.

- Client full node.

I due si differenziano dal possesso o meno dell'intera copia della blockchain e dall'ethereum virtual machine; I client full node avranno l'intera copia sia della blockchain che dell'ethereum virual machine; saranno in grado di generare blocchi, prenderanno parte al meccanismo di consenso decentralizzato e potranno effettuare transazioni; I remote client non avranno un copia locale della blockchain, non valideranno blocchi e transazioni, ma offriranno la possibilità di avere un wallet e di creare transazioni; I remote client, per funzionare daranno fiducia ad un full client, andando quindi a perdere in sicurezza ed anonimità.

1.2.3 Wallets

Parlando di nodi, sia remote client che client full node, non si possono tralasciare i wallets, applicazioni utilizzate come interfaccia utente per l'archiviazione e gestione di chiavi, facilitando quindi l'utente nell'esecuzione di operazioni nel sistema. L'applicazione avrà accesso agli ether(valuta utilizzata all'interno di Ethereum) relativi alla chiave privata posseduta, terrà traccia del bilancio, creerà e firmerà le transazioni e, inoltre, potrà interagire con i contratti. Bisogna quindi specificare che un wallet non contiene dati riguardanti i quantitativi di ether che il client possiede o bytecode dei contratti, in quanto questi dati saranno contenuti esclusivamente nella blockchain; chiunque potrà quindi vedere qualsiasi bilancio presente all'interno della blockchain, anche se probabilmente non riuscirà a risalire al proprietario. I wallets si dividono principalmente in due tipologie:

- Wallets non deterministici.
- Wallets deterministici.

I wallets non deterministici sono stati la prima tipologia di wallet utilizzata nella piattaforma ethereum, sono basati sul concetto di massimizzazione della privacy, andando a cambiare le chiavi private e pubbliche per ogni transazione generata. Ogni chiave, in questa tipologia di wallet, viene generata in modo indipendente rispetto alle altre chiavi, caratteristica che rende irrecuperabile una chiave una volta smarrita. Il wallet non deterministico risulta quindi essere molto difficile da gestire. Questa pratica, considerata obsoleta, è stata superata con l'avvento dei wallets deterministici. La principale differenza tra le due tipologie di wallets risiede proprio nella modalità in cui le chiavi vengono generate. Nei wallets di tipo deterministico avremo quindi che le chiavi generate deriveranno tutte da una master key, detta anche "seed". In questa tipologia, sarà molto più facile ripristinare le chiavi perse in quanto sarà necessario semplicemente essere in possesso della master key. Il wallet utilizzato come base per i test dei contratti è "Metamask", wallet di tipo deterministico sviluppato per interfacciarsi con la piattaforma Ethereum.

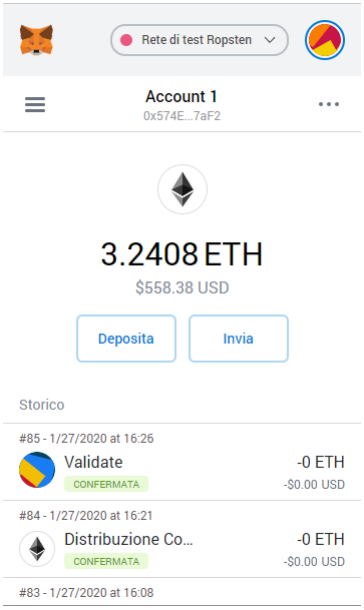

Figura 1.1: Esempio dell'interfaccia grafica di MetaMask

1.2.4 Transazioni e Gas

Ruolo cruciale all'interno della piattaforma è svolto dalle transazioni, in quanto ogni movimento all'interno della blockchain viene schedato come transazione, partendo da un semplice invio di denaro fino a passare ad una chiamata di funzione di uno smart contract, una particolarità è appunto che la piattaforma Ethereum non funziona in maniera autonoma. Le transazioni sono dei messaggi serializzati firmati, inviati da un external owned account, trasmessi sul network ethereum e poi iscritti alla blockchain all'interno del primo blocco disponibile. Una transazione è rispettivamente composta da:

- Nonce, ovvero un valore scalare utilizzato per evitare la replicazione della transazione.
- Gas price, ovvero la quantità di ether per unità di gas che l'utente è disposto a pagare.
- Gas limit, ovvero l'ammontare massimo di gas che l'utente è disposto a pagare per la transazione.
- Value, ovvero la quantità di ether da mandare al destinatario.
- Data, ovvero la variabile contenente i dati per la transazione.
- V,R,S, ovvero i tre componenti per la firma digitale.

Tra questi componenti, ci soffermeremo particolarmente sul gas price e lo scopo della gas tax all'interno della piattaforma, in quanto fondamentali ai fini del calcolo dei costi di sviluppo e mantenimento dei contratti testati. Al fine di far iscrivere una transazione all'interno della blockchain, viene pagata una tassa, la cui valuta

è espressa in 'gas'. La scelta di utilizzare una valuta differente dagli ether per il pagamento delle tasse di transazione è basata sulla problematica data dalla valuta 'ether', soffrente di una enorme volatilità di prezzo, andando a rendere troppo incostanti i prezzi delle tassazioni.

Figura 1.2: Variazione della valuta Ether nel corso dei mesi

La quantità di gas da pagare risulta essere direttamente proporzionale alla lunghezza e complessità computazionale del codice da eseguire, sarà inoltre possibile stabilire il valore 'gas price', ovvero la quantità di ether per unità di gas che si vogliono pagare; Andando a modificare questa variabile, andremo ad incidere sulla priorità che questa transazione avrà nella iscrizione sulla blockchain, infatti, con un gas price maggiore, la transazione sarà registrata in una quantità di tempo inferiore rispetto ad una transazione effettuata con gas price di valore inferiore. Avremo quindi un incremento sulla velocità di iscrizione della transazione, andando a subire come effetto collaterale un prezzo maggiore.
Valori molto elevati di gas price sono consigliati solo nel caso in cui la tempistica della transazione abbia una criticità elevata.

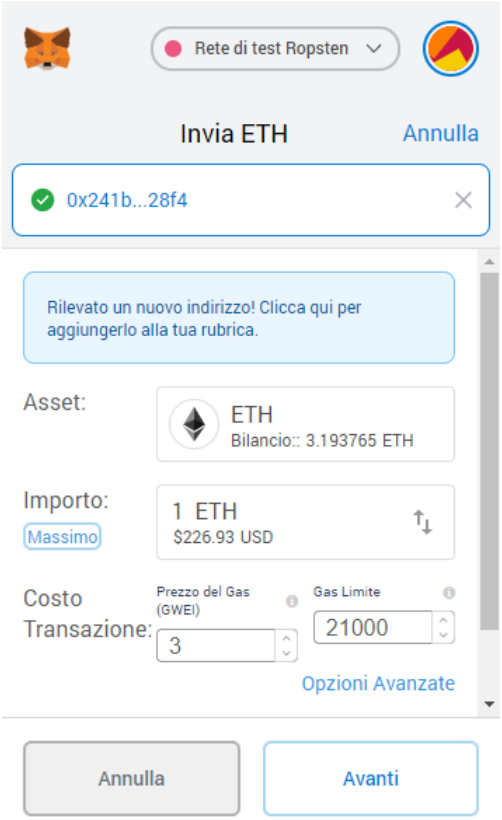

Figura 1.3: Esempio schermata transazione su MetaMask

Il quantitativo di gas price può equivalere a zero, trasformando la tassa di transazione a nulla ma rendendo improbabile la registrazione della transazione. Si potrà inoltre impostare un valore di 'gas limit' che andrà a porre un massimo, al quantitativo di ether che il sistema utilizzerà per l'iscrizione della transazione.

1.2.5 Smart contracts e Solidity

Alla base della differenziazione tra una comune piattaforma basata su blockchain ed Ethereum, prendono spazio gli Smart contracts, cornerstone della piattaforma sviluppata da Vitalik Buterin e Joseph Lubin agli inizi del 2013. Con il termine smart contract si va ad indicare un immutabile programma che gira deterministicamente nel contesto della Ethereum virtual machine come parte del network protocol di Ethereum' (da Dr. Gavin Wood, 2019b). Quando ci riferiamo ad uno smart contract è importante sottolineare la distanza da un'entità con valore legale in quanto si basa su di un utilizzo general purpose. Caratteristica fondamentale degli smart contracts risiede nella loro immutabilità, infatti, una volta completata l'iscrizione del contratto alla blockchain di ethereum attraverso una specifica transazione che andrà ad inserire il bytecode del contratto nel blocco, non sarà più possibile andare a modificarne il contenuto, ma sarà possibile solamente interagire con esso andando a chiamare le funzioni precedentemente determinate, tramite l'utilizzo delle transazioni. L'iscrizione dello smart contract all'interno della blockchain andrà a definire un address specifico per le interazioni con esso; questo address, potrà ricevere Ether, ma non potrà mai risultare l'originante di una transazione seppur sia in grado di interagire con altri contratti. La principale differenza tra un address di un EOA (Externally owned account) e un address di uno smart contract risiede nell'univoca possibilità di creazione di transazioni native, attuabili solo attraverso un account Externally owned.

Il linguaggio di programmazione principalmente utilizzato per la scrittura degli smart contracts è 'solidity', linguaggio di tipo procedurale creato dal Dr Gavin Wood, attualmente sviluppato e mantenuto come progetto indipendente su GitHub, pensato esplicitamente per la scrittura di smart contracts; Il prodotto principale del progetto Solidity è il compilatore 'solc', in grado di convertire programmi scritti in Solidity in Ethereum virtual machine Bytecode.(da Dr. Gavin Wood, 2019b).

1.3 Opzioni nel mercato finanziario

Il sistema che andremo ad analizzare nei successivi capitoli ha come scopo principale quello di modificare la classica gestione del trading di opzioni finanziare andando ad applicare questa tipologia di contratti alla piattaforma Ethereum, rendendo quindi il sistema completamente decentralizzato.

1.3.1 Opzioni

Quando si parla di opzioni, si parla di una tipologia di contratto derivato, dove per 'derivato' intendiamo un titolo che derivi il suo valore da un asset sottostante, in grado di conferire all'acquirente un diritto di acquisto su di un determinato bene, ad una determinata data, detta data di maturity, ad un determinato prezzo, detto strike price. Il principale vantaggio delle opzioni rispetto ai più classici strumenti derivati come le futures, risiede nella possibilità di recesso dall'acquisto, quindi il contratto non determina un obbligo ma appunto un diritto sul bene, o sul guadagno derivato da esso in caso di cash settlement. Il diritto d'acquisto verrà conferito dopo il pagamento di un premio dal valore inversamente proporzionale alla distanza dello strike price rispetto al prezzo del sottostante al momento della sottoscrizione al contratto. Questa tipologia di contratto viene usata per scopi sia speculativi, sia di hedging aziendale, dove per hedging aziendale intendiamo una copertura dai rischi al solo costo del premio opzionario. Le opzioni si suddividono in due tipologie principali:

- Opzioni di call

- Opzioni di put

Le opzioni di call sono di stampo rialzista, ovvero coprono il rischio in caso di un eventuale rialzo del bene sottostante mantenendo i benefici in caso di ribasso, al prezzo del premio. Nel caso di acquisto di una opzione put, copro il rischio in caso di ribasso del bene sottostante mantenendo i benefici in caso di risalita, al prezzo del premio. All'interno del sistema implementato, tratteremo direttamente la gestione delle opzioni, ma senza lo scambio del bene sottostante, in quando i contratti vengono terminati con un cash settlement.

1.3.2 Hedging aziendale

L'utilizzo dei contratti di opzione include tra i suoi principali scopi quello di coprire un eventuale rischio, sia di salita, che di discesa relativo al prezzo del bene sottostante. Quando occorrerà quindi fare hedging?

• In caso di elevata volatilità del bene, ovvero quando i prezzi del bene sono soggetti a estreme fluttuazioni, sarà necessario coprirsi dal rischio sviluppatosi.

• In caso di alta esposizione, ovvero nel caso in cui i prezzi non possano essere spalmati sugli acquirenti.

• In caso di alta incidenza sul costo del prodotto finito, ovvero nel caso in cui la fluttuazione del bene incida eccessivamente sul prezzo del prodotto.

1.3.3 Strategia di Bull Call Spread

La strategia finanziaria implementata da Vishakh(da Vishakh, 2016) nel sistema analizzato nel successivo capitolo, è la 'Bull Call Spread' strategy. Strategia basata sull'acquisto di un'opzione call ad uno strike price in concomitanza con la vendita di una opzione call ad uno strike price superiore rispetto alla opzione precedente, ma con la stessa data scadenza. Questa tipologia di strategia porta ad attutire i costi di premio in quanto ci sarà il pagamento del premio nell'acquisto della prima call, e l'incasso di un premio nella vendita della seconda call. Punto di forza sarà quindi il costo limitato, ma a discapito dei possibili benefici, in quanto anche il guadagno sarà limitato da un range prestabilito dallo spread tra le due opzioni.

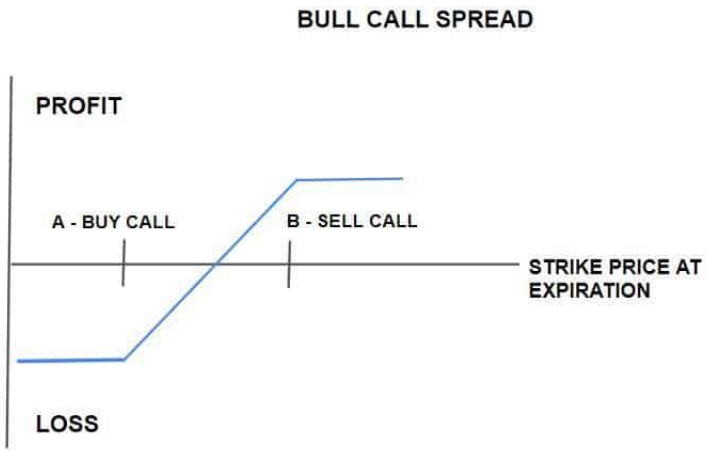

Figura 1.4: Funzionamento della strategia di Bull call spread

Con l'utilizzo di questa strategia si renderà necessario l'appoggiarsi ad una struttura di marginazione, necessità che prenderà luogo a causa della vendita dell'opzione call secondaria, rendendo possibili perdite controllate.
La marginazione andrà quindi gestita partendo dal calcolo dello spread tra i due strike price precedentemente sottoscritti e andrà poi aggiornata controllando periodicamente il prezzo degli asset sottostanti.

1.4 Differenza tra opzione fisica e cash settlement

Nel modello implementato, i contratti utilizzati terminano con un cash settlement, senza quindi la necessità da parte del venditore di detenere il bene fisico sottostante. Partendo dal presupposto che il modello risulti modificabile per l'implementazione dell'acquisto di opzioni fisiche, seppur sia necessaria la gestione di dati da terze parti, un acquisto di una opzione fisica comporta la facoltà, all'esecuzione del contratto, di ricevere il bene sottostante nella quantità precedentemente indicata.
La gestione di un contratto di call option fisico, implica dunque la necessità da parte del venditore di avere fisicamente il bene sottostante contrattato, sia che siano share, sia che sia un bene tangibile come può essere il petrolio. Tuttavia, la gestione relativa a questa tipologia di opzioni non risulta essere sempre applicabile, e, a meno che l'utente non sia interessato direttamente al bene sottostante, andando ad applicare una strategia di copertura del rischio come precedentemente descritto, risulta essere più complesso da gestire appunto per la necessità di possesso del bene sottostante. Quando si tratta di contratti con terminazione a cash settlement, non è più necessario da parte dell'esercente il possesso del bene sottostante, seppur si tratti di un vero e proprio contratto di opzione, raggiunto il tempo di maturity e eseguito il contratto, l'unico scambio che prende luogo è quello di un flusso di cassa a seconda dei risultati del contratto stesso.

Capitolo 2

Principali vantaggi della decentralizzazione sui mercati finanziari

In questo capitolo si svolgerà un'analisi teorica sui principali vantaggi di una decentralizzazione sui mercati finanziari attraverso l'utilizzo della piattaforma Ethereum, senza tralasciare svantaggi e vantaggi della metodologia attualmente utilizzata, focalizzandosi principalmente sul mercato dei derivati. Tra le principali asserzioni che saltano all'occhio, "Blockchain won't works if banks don't change" (da Rizzo, 2016) è quella di maggior rilevanza, poiché va a delineare il principale limite di questa tecnologia che risiede nella volontà di effettuare il passaggio dal vecchio standard centralizzato, al nuovo standard decentralizzato. A favore della tecnologia decentralizzata, le transazioni con criptovalute sono già ampiamente utilizzate e risultano essere una garanzia a fronte di un possibile futuro sviluppo ed utilizzo di queste piattaforme. A dare credito ad un possibile passaggio al sistema decentralizzato, abbiamo una gestione del rischio che non risulta essere sempre efficace, ad esso, si vanno a sommare una serie di problematiche date da una mancanza di automatizzazione delle procedure che, andranno a generare dei processi lenti ed imprecisi, andando ad aumentare i rischi.

2.1 La problematica dei collateral

Il principale fattore incriminato per l'aumento del rischio quando si parla di contratti di tipo derivato, è dato dalla possibilità di default da parte dell'acquirente. Il default, comporterebbe una massima perdita di un valore dato dal valore massimo del contratto derivato; nei mercati odierni, la forma base di protezione(collateral) da questa possibile perdita è data dal margine di variazione, infatti, quando la controparte acquista il derivato, dovrà provvedere a far avere al venditore un margine trattenuto solo come garanzia. In caso di successo dei processi legato all'opzione,

quindi in mancanza di default, il margine verrà restituito all'acquirente alla terminazione dell'opzione stessa. Questa forma di collateral a livello teorico riesce a coprire interamente il rischio generato dalla possibilità di default, tuttavia, si può incorrere in sei principali problematiche:

• Problematica dei ritardi: Uno dei punti cardine della transazione da sistemi centralizzati a sistemi decentralizzati risiede negli scambi di collateral da parte delle banche; Gli scambi di collateral sono tipicamente gestiti giornalmente da parte dei sistemi bancari andando a generare ulteriori ritardi, generalmente di due giorni, sull'aggiornamento dei collateral della controparte. Questa problematica può risultare particolarmente difficile da gestire in caso di rilevanti salti di cash flow.

• Salti di cash flow: Come discusso nel punto precedente, un salto di consistenti dimensioni di cash flow, porterà ad un rapido aumento del rischio non gestito, in quanto l'intero ammontare del cash flow risulta essere completamente scoperto dal collateral prima del successivo aggiornamento giornaliero.

• Differenze computazionali: Partendo dall'algoritmo per il calcolo del margine di variazione fino ad arrivare ai data sources, si può notare subito una discrepanza informativa tra le due parti; Il contratto firmato dalle due parti non andrà a specificare come e quando i dati vengono aggiornati ed elaborati. Avremo quindi una discrepanza tra le parti basata su differenti fonti di dati, differenti modelli ed implementazioni. Queste caratteristiche andranno a causare un ulteriore spread tra i calcoli dei collateral, andando a interferire con l'esposizione di una delle due parti, obbligata ad accettare un compromesso.

• Incertezza di default ed ulteriori ritardi: Caratteristica logorante nei riguardi della sicurezza dei processi è l'utilizzo del default closeout process, infatti, una volta dichiaratosi il default, l'esposizione e il collateral non vengono direttamente calcolati ma prenderà luogo una complessa procedura di valutazione causa di ulteriori ritardi. Il tempo di ritardo dal default viene definito come MPOR(Margin period of risk) e viene stimato di una durata dai 5 ai 40 giorni.

• Problematiche di automazione: Il processo sopra citato per il ricalcolo dei collateral in caso di default richiede processi sofisticati con possibilità di trasferire liquidità facilmente, una capacità di gestione degli input market data elevata, un utilizzo di complessi modelli di ricalcolo del rischio ed infine la possibilità di aver accesso a specifici account gestiti da intermediari. Questa serie di caratteristiche crea un

enorme deficit delle controparti, portando ad accordi con aggiornamenti mensili dei collateral; il risultato finale è un'enorme incertezza e consistenti ritardi per le parti.

• Il margine iniziale e la problematica della liquidità: Le imperfezioni date dal margine di variazione creavano un enorme lack espositivo per quanto riguarda il rischio di default e l'aggiornamento dei collateral; Il più efficace tentativo di rimediare a questi aumenti di rischio è stato fatto dalle istituzioni finanziare attraverso l'introduzione del margine iniziale. Il margine iniziale, è un collateral che va a sommarsi al margine di variazione, viene aggiornato regolarmente e risulta essere una stima del massimo disallineamento tra l'esposizione al rischio e il collateral adottato. Questa tipologia di margine viene utilizzato solamente nel caso in cui il margine di variazione non riuscisse a coprire completamente il default; risulta quindi essere a sua volta una stima di MPOR, in quanto questa variabile rappresenta il ritardo in caso di default. La principale problematica relativa al margine iniziale è data dal fatto che, essendo MPOR solitamente un tempo dilatato, viene richiesta una grande quantità di liquidità per far fronte al costo del margine iniziale. (da Morini, 2017)

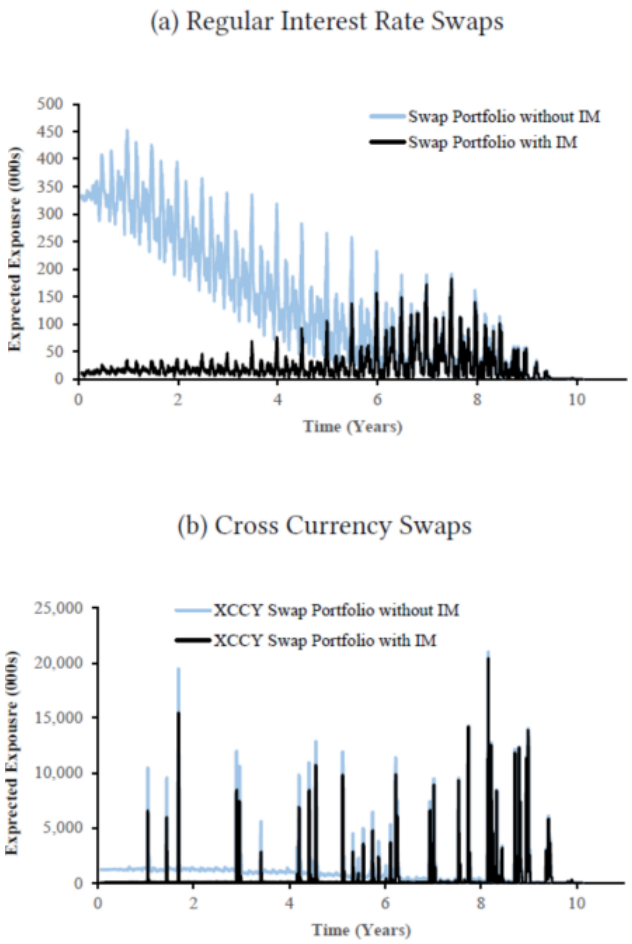

Figura 2.1: Esempio di variazione dell'esposizione a seconda della marginazione

2.2 Migliorare la gestione del rischio con gli smart collateral contracts

I primi quesiti che ci si può porre sono quindi:

'E' possibile migliorare questa tipologia di copertura dei rischi?'

'La struttura centralizzata può essere essa stessa un limite per i mercati finanziari?'

Il tentativo di risposta a questi interrogativi è stato fatto prendendo in analisi un modello basato sull'utilizzo della piattaforma Ethereum e degli smart contracts per evitare le maggiori problematiche date dall'utilizzo delle tecnologie centralizzate.
L'utilizzo della tecnologia a blockchain riesce ad eliminare i vantaggi delle banche, precedentemente utilizzate come parte centrale, nella gestione delle liquidità. In quanto tutti i nodi della blockchain hanno lo stesso valore e gli stessi effetti sulla blockchain stessa, non sarà più necessario l'ausilio di parti intermediarie. Inoltre, essendo questi contratti scritti su carta, con la digitalizzazione sarà possibile includere nei contratti stessi le tecnologie di calcolo dell'esposizione al rischio e di trasferimento dei collateral, rendendo tutte le parti consapevoli della modalità di gestione del rischio; gestione del rischio che, a differenza del sistema centralizzato, risulterà essere unica, eliminando quindi asimmetrie tra i calcoli dei collateral. Questa serie di peculiarità andranno a ridurre drasticamente i giorni di ritardo nell'applicazione di aggiornamento dei collateral.
Essendo un sistema di tipo digitale, gli smart contracts potranno incorporare azioni automatiche eseguite dal network nel momento in cui una controparte ritarda nel pagamento, eliminando quindi le problematiche tempistiche date dalla burocrazia. (da Morini, 2017)

2.2.1 Le problematiche della credibilità

Le caratteristiche di applicabilità di un contratto su di uno smart contract andranno a modificare radicalmente la struttura base di un contratto finanziario, alla base di ciò, abbiamo una impossibilità di identificazione delle parti aderenti al contratto che andrà ridefinire uno standard in materia di sicurezza.
Non sarà quindi più possibile accettare un contratto facendo esclusivamente affidamento sulla credibilità e sulle possibili ripercussioni legali della controparte, ma, il contraente dovrà immettersi nel mercato facendo affidamento solo sulla stabilità e sicurezza del sistema.
Il punto preso in considerazione risulta essere uno scoglio fondamentale in un'ottica di innovazione, la parte contraente si troverà di fronte ad una barriera psicologica al giorno d'oggi difficile da sormontare, in quanto la struttura sociale odierna è fondata sull'identificazione, e, il passaggio a tecnologie decentralizzate avrà luogo solo con la distruzione di questo costrutto.
La necessità di una struttura perfetta in grado di andare a colmare il vuoto dato dall'impossibilità di identificazione delle parti porta quindi all'elisione della classica forma di default conosciuta dal mercato finanziario classico, dove al suo posto prenderà parte una versione a rischio decisamente inferiore di gestione dei collateral e dell'esposizione. (da Morini, 2017)

2.3 Struttura funzionale di uno smart derivative

Alla base dell'applicazione decentralizzata degli smart derivative abbiamo una pluralità di smart contracts che dovranno adempiere a tutte le funzionalità precedentemente gestite dall'unità centrale; lo smart contract dovrà quindi essere in grado di computare il margine di variazione e il margine iniziale, anche se il calcolo del margine iniziale può risultare facoltativo in quanto il valore di MPOR all'interno di un costrutto decentralizzato come quello di Ethereum, risulta essere quasi irrilevante; inoltre, compito dello smart contract sarà quello di gestire i cashflow associati ai payoff.
Entrambe le parti dovranno quindi accettare un contratto in grado di svolgere le seguenti funzioni; A caratterizzare la struttura del contratto, abbiamo principalmente il tempo di validità, valore che andrà ad indicare il tempo massimo in cui la controparte potrà accettare ed in seguito inizializzare il contratto. Scaduta tale tempistica, il contratto risulterà invalido, andando ad autodistruggere se stesso e riportando i fondi presenti al creatore dello smart contract.
Nel caso in cui il contratto sia stato inizializzato con successo, si arriva ad uno dei

principali scogli della decentralizzazione su base Ethereum, il costo di aggiornamento dei collateral. In quanto ogniqualvolta si voglia aggiornare la struttura dati presente nella blockchain sarà necessario creare una transazione, avremo quindi un costo legato ad essa, il quale varierà a seconda del gas price scelto.
Quali sono le tempistiche giuste per aggiornare il collateral?
Le tempistiche minime per l'aggiornamento del collateral si aggirano intorno ai venti secondi, a seconda della latenza del network utilizzato. Una tempistica di aggiornamento troppo frequente porterà però a costi troppo elevati, mentre una tempistica di aggiornamento lenta condurrà ad un amento del rischio; si stima che una tempistica di aggiornamento adeguata si possa aggirare intorno ai dieci minuti. Sempre nel mondo della ottimizzazione dei costi, prende luogo la scelta di un gas price adeguato, in quanto gas price troppo bassi possono portare a latenze nell'esecuzione della transazione molto alte, mentre gas price troppo alti causeranno a loro volta costi troppo elevati.
Un ruolo fondamentale compiuto dallo smart contract è dato dal calcolo del periodo di grazia, ovvero il contratto dovrà stimare quanti pagamenti mancanti potrà accettare prima di chiudere automaticamente la trattazione.

2.4 Smart contract come Controparte centrale

Il ruolo degli smart contracts risulta quindi essere simile a quello precedentemente svolto dalla banca, vestita da controparte centrale. Lo smart contract si muove di conseguenza come agente calcolatore dei margini, e si prende carico del compito di trasferimento dei collateral. Pur se in maniera diversa, lo smart contract si mette in gioco nella risoluzione di eventuali dispute in caso di non adempienza del pagamento. Quale potrà essere quindi l'interazione tra CCP o controparte centrale e il modello a blockchain?
I principali scenari possibili risultano essere tre:

• Il modello di business descritto precedentemente non necessita di una controparte centrale al fine di rendere la pratica del collateral più trasparente ed effettiva, da questo punto di vista, il modello di smart derivative può essere un perfetto sostituto del modello classico centralizzato.

• Ulteriore possibilità potrebbe essere quella della riorganizzazione da parte della controparte centrale, andando a vestire i ruoli di parte decentralizzata, riorganizzando quindi completamente la sua struttura.

• La controparte centrale può infine adottare forme private di strutture a blockchain, mantenendo il modello di business precedentemente adottato ma, sfruttando la blockchain per il calcolo e l'aggiornamento dei collateral oltre che per la gestione dei fondi, appoggiandosi quindi alla crittografia finanziaria adottata dalle tecnologie decentralizzate per aumentare i livelli di sicurezza interni.

(da Morini, 2017)

Capitolo 3

Opzioni derivate applicate ad Ethereum

In questo capitolo si mostrerà un modello di applicazione per opzioni derivate all'interno della piattaforma ethereum che verrà poi analizzato successivamente; la base di tale modello è stata sviluppata da Vishakh, interamente appoggiandosi al linguaggio figlio del Dr. Gavin Wood, Solidity.(da Vishakh, 2016)

3.1 Componenti del modello

La struttura dell'applicativo è sviluppata su sei smart contract fondamentali per il raggiungimento di una struttura contrattuale basata sulla strategia di Bull Call Spread trattata nel capitolo uno. La struttura, risulta essere applicabile anche su di un singolo contratto di opzione andando a modificare le funzionalità del contratto di "Call option" successivamente descritto.
Alla base di tale modello si è istituita una gestione dei fondi attraverso l'utilizzo di uno smart contract per parte aderente in grado di comportarsi in maniera simile ad un portafoglio, l'effetto ottenutosi risulta essere simile a quello di un proxy, quindi un intermediario tra il contratto di opzione e la gestione dei fondi degli aderenti. La principale motivazione di questa scelta è scaturita dal contratto di Call Spread, il quale sarà poi responsabile della gestione dei fondi e dovrà dunque aver accesso a funzionalità dei contratti non possibili con il semplice appoggio di un wallet.
Questa tipologia di gestione dei fondi genera la problematica di mantenimento del bilancio dello smart contract, difatti, essendo il modello di bull call spread basato su di una marginazione aggiornata periodicamente, al fine di non suscitare un default del sistema, sarà necessario controllare costantemente i fondi sul bilancio dello smart contract. Lo smart contract relativo all'account di trading necessiterà quindi di autorizzazione per muoversi all'interno del modello; una volta adempita questa

richiesta, tutta la gestione di marginazione e gestione fondi sarà interamente gestita degli smart contract stessi.

3.1.1 Smart derivative semplice

Il cuore della struttura, nel caso in cui essa sia nella sua versione semplificata, ovvero attraverso il contratto di opzione semplice, sarà quindi la Call option.
Questo smart contract è stato sviluppato in modo da risultare modulare, sarà quindi possibile utilizzare questa tipologia di smart contract sia per una call option semplice, sia nella più complessa strategia di Bull Call Spread. Nel secondo caso, il contratto sarà utilizzato come gamba per la struttura, facendo da appoggio allo smart contract di Call Spread.
Nella forma semplificata, le due parti interagiranno direttamente con il contratto di call option avvalendosi della facoltà di inizializzarlo, validarlo e infine, raggiunto il tempo di maturità, eseguirlo. I dati all'interno del contratto relativi alle quotazioni aggiornate saranno dati in input da parte del contratto di Data Feed, contratto che può essere aggiornato manualmente, o avvalendosi della figura dell'oracolo, funzionalità in grado di ricevere dati esterni alla blockchain. In questa tipologia di struttura, i dati sono inseriti manualmente.

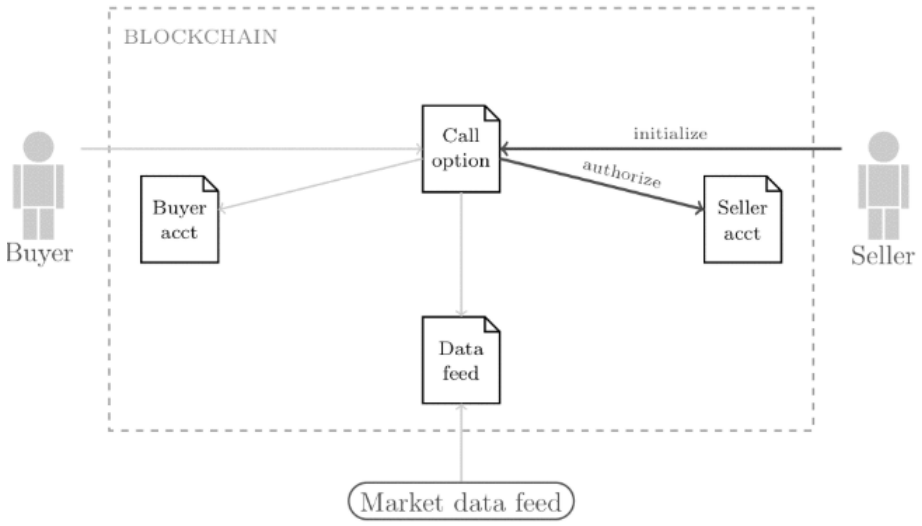

Figura 3.1: Fase di inizializzazione dello smart contract Call option

Come mostrato in figura 3.1, la prima fase per la gestione del sistema è quella di inizializzazione del Call option contract. In tale fase, bisognerà specificare l'indirizzo dei contratti di account e di Data feed per poi entrare nella fase di specifica dell'opzione vera e propria, andando ad inserire il sottostante, lo Strike price, il notional

e il tempo di maturità del contratto. Sarà poi compito del call option l'esecuzione della funzione di autorizzazione dello smart contract col ruolo di trading account della parte inizializzante.
Il contratto di Call option potrà essere inizializzato da entrambe le parti, con la limitazione di 'owner' per l'autorizzazione del trading account al fine di prevenire accessi ai fondi da parte di utenti malevoli. Solo gli utenti stessi potranno quindi autorizzare il Call option contract all'accesso sui contratti gestori dei fondi.

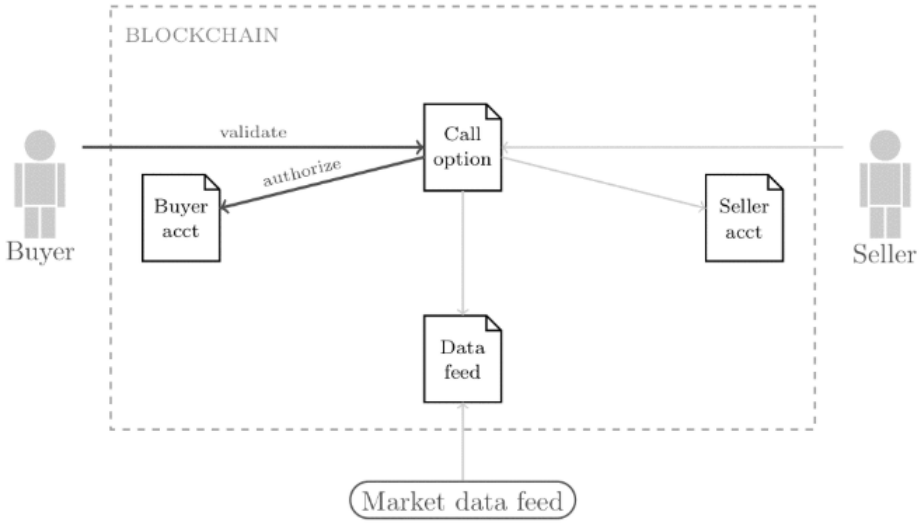

Figura 3.2: Fase di validazione dello smart contract Call option

La fase immediatamente successiva a quella di inizializzazione della call option è la fase mostrata in figura 3.2, ovvero la validazione del contratto da parte del contraente, resa possibile grazie alla trasmissione dell'address relativo alla call option su di un canale esterno alla piattaforma. Solo dopo la validazione sarà quindi possibile per il call option contract, andare a gestire i fondi rispettivamente dei due account. Durante la validazione, il contratto di call option autorizzerà lo smart contract dell'account contraente alla partecipazione sul contratto in atto. Di conseguenza, il sistema sarà pronto per gestire l'opzione in quanto avrà accesso a tutte le parti modulari fondamentali per il funzionamento.
L'ultima fase, la quale risulta essere facoltativa, è data dall'esercitare l'opzione; funzione disponibile solo una volta che il tempo di maturity sia stato raggiunto. Il contraente potrà quindi scegliere di esercitare il contratto generando un cash settlement attraverso l'utilizzo delle funzioni di cash flow.

In caso di esercizio del contratto, avverrà quindi un cashflow per entrambe le parti, dove rispettivamente l'agente venditore dovrà pagare il prezzo del sottostante moltiplicato per il notional, mentre l'acquirente dovrà pagare il prezzo dello strike price precedentemente concordato moltiplicato a suo volta per il notional. Il sistema procederà poi per l'esecuzione del cash settlement, andando a distribuire gli ether ai due contratti gestori del balance.
Nella figura 3.3 viene rappresentata la fase di esecuzione inizializzata dall'acquirente, che andrà poi a generare un cash flow su entrambi i contratti di balance.

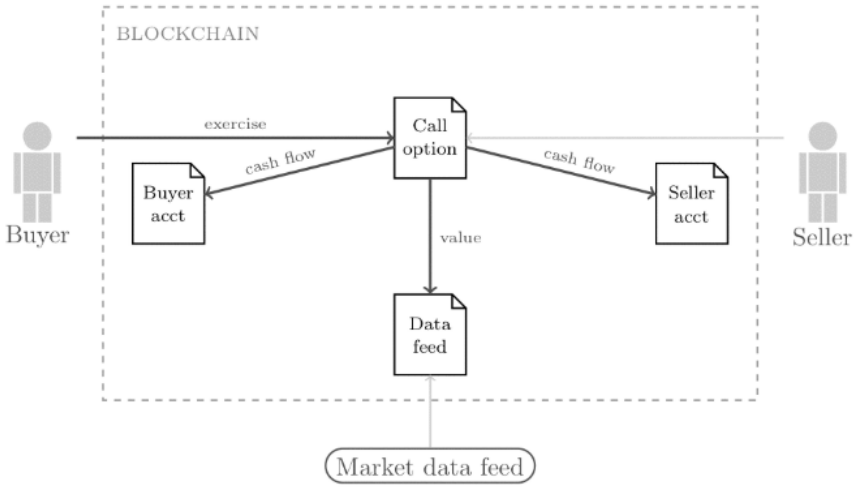

Figura 3.3: Fase di esecuzione dello smart contract Call option

3.1.2 Smart derivative Bull Call Spread

Alla base della differenziazione tra la struttura semplificata e quella per la strategia del bull call spread, abbiamo un contratto, chiamato a sua volta 'Call Spread', in grado di gestire le transazioni tra i contratti sottostanti. In questo caso, il contratto di call spread sarà quello inizializzato, prendendo il posto della precedente call option che ne uscirà semplificata essendo un contratto usato solamente come 'gamba' per il call spread. La fase di inizializzazione viene mostrata in figura 3.4 con le conseguenti autorizzazioni caratteristiche, autorizzazioni presenti anche nella versione semplificata del contratto.

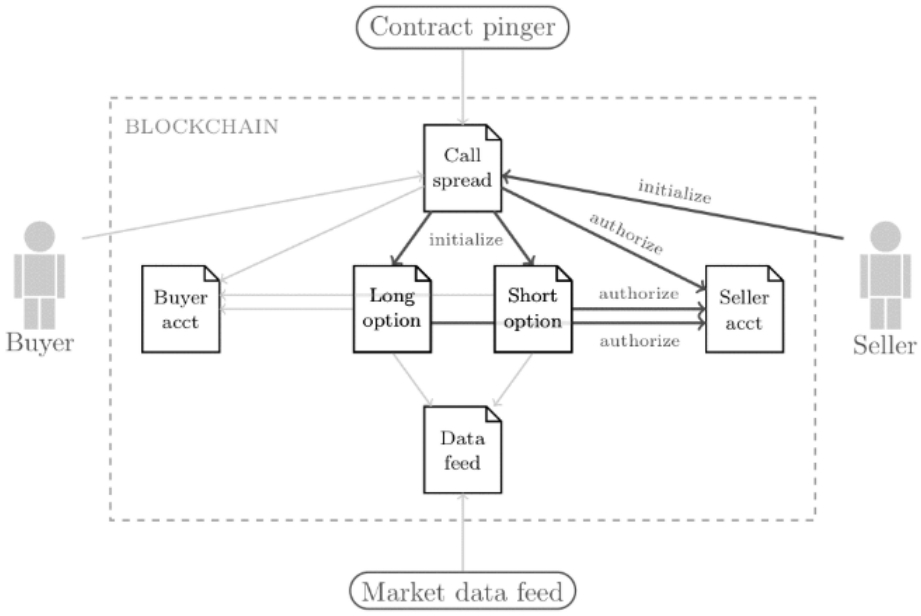

Figura 3.4: Fase di inizializzazione dello smart contract Call spread

Rispetto alla versione iniziale, avremo quindi un sistema arricchito di due contracts, un call spread, e un altra call option, in quanto la strategia è basata su di un acquisto ed una vendita di opzioni call. Il completamento delle richieste di autorizzazione avverrà solamente previa fase di inizializzazione, mostrata in figura 3.4 e validazione, mostrata in figura 3.5; entrambe le fasi saranno gestite passando del contratto principale di Call Spread.

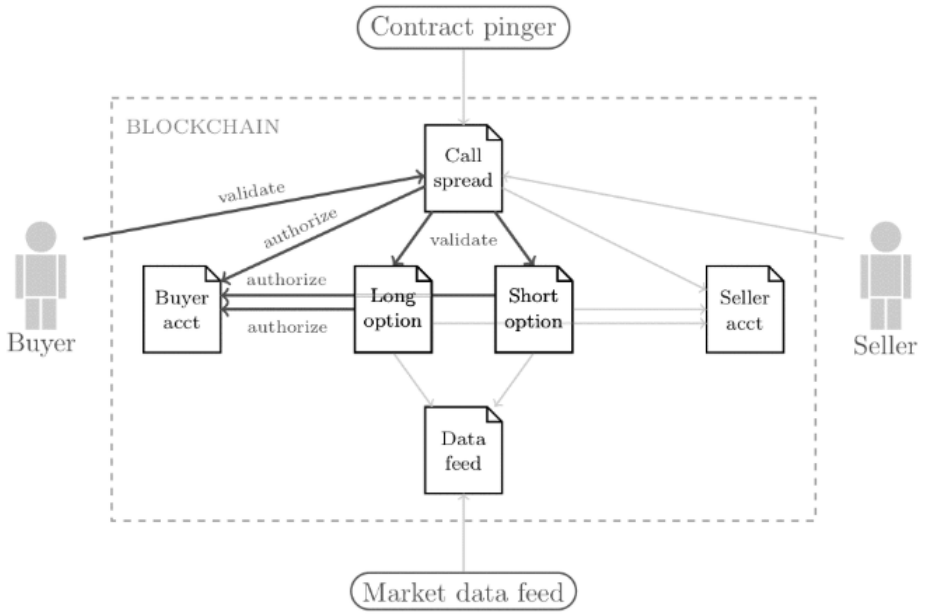

Figura 3.5: Fase di validazione dello smart contract Call spread

La principale differenza rispetto al modello semplificato risiede nella possibilità di gestione del margine sull'operazione, margine che sarà necessario in quanto l'utente non sarà più solo compratore di un'opzione call, ma anche venditore. L'utente che inizializzerà il contratto, potrà quindi richiedere una determinata percentuale di margine. Margine che sarà calcolato partendo dal valore dell'opzione, dato dalla differenza tra lo Spot price, ovvero il prezzo del sottostante, e lo strike price precedentemente concordato, il tutto moltiplicato per il quantitativo di opzioni acquistate.

```
function getSpotPrice() returns (uint) {
    return _underlier.getPrice(_feedName);
}
function getValue() returns (int) {
    return (int(getSpotPrice()) - int(_strikePrice)) * int(_notional);
}
```

Una volta acquisiti i valori delle due opzioni, sarà calcolato il margine richiesto prendendo la differenza tra i due valori delle opzioni, moltiplicandole poi per il margine percentuale precedentemente inizializzato dall'utente esercente. Si passerà infine ad una fase di scambi di cash flow basato sul valore del margine aggiornato.

```
function rebalanceMargin() returns (bool) {
    int buyerValue = _buyerLeg.getValue();
    int sellerValue = _sellerLeg.getValue();
    uint difference = uint(buyerValue - sellerValue);
    uint marginAmount = difference * _marginPct / 100;

    if (marginAmount > this.balance) {
        CashFlow(address(_sellerAcct), address(this),
        marginAmount - this.balance);
        _sellerAcct.withdraw(marginAmount - this.balance);
    } else if (marginAmount < this.balance) {
        CashFlow(address(this), address(_sellerAcct),
        this.balance - marginAmount);
        _sellerAcct.transfer(this.balance - marginAmount);
    }
    infoMargin(marginAmount);
    return this.balance == marginAmount;
}
```

Una problematica insorta con l'introduzione dei margini per la prevenzione del rischio è data dall'obbligo di un costante aggiornamento degli stessi. Forza di questo sistema è la possibilità, nei contratti che utilizzano un sistema di marginazione, di aggiornare i propri dati con frequenza notevolmente superiore rispetto alla più classica metodologia per contratto cartaceo. Il risultato ottenuto è quello di un MPOR quasi nullo, con un conseguente rischio notevolmente ridotto.
La funzione di aggiornamento del margine, mostrata in figura 3.6 e presente all'interno del contratto di call spread, andrà a modificare i valori interni della blockchain. Questa peculiarità rende impossibile la registrazione della funzione sotto forma di "view" [1].

```
function ping() returns (bool) {
    return rebalanceMargin();
    // timestamp del block
    infoTime(block.timestamp);
}
```

Essendo quindi la funzione di ping una transazione classica, ogni qual volta che si voglia aggiornare il valore del margine, avremo una tassa commissionabile che andrà a gravare sull'acquirente.

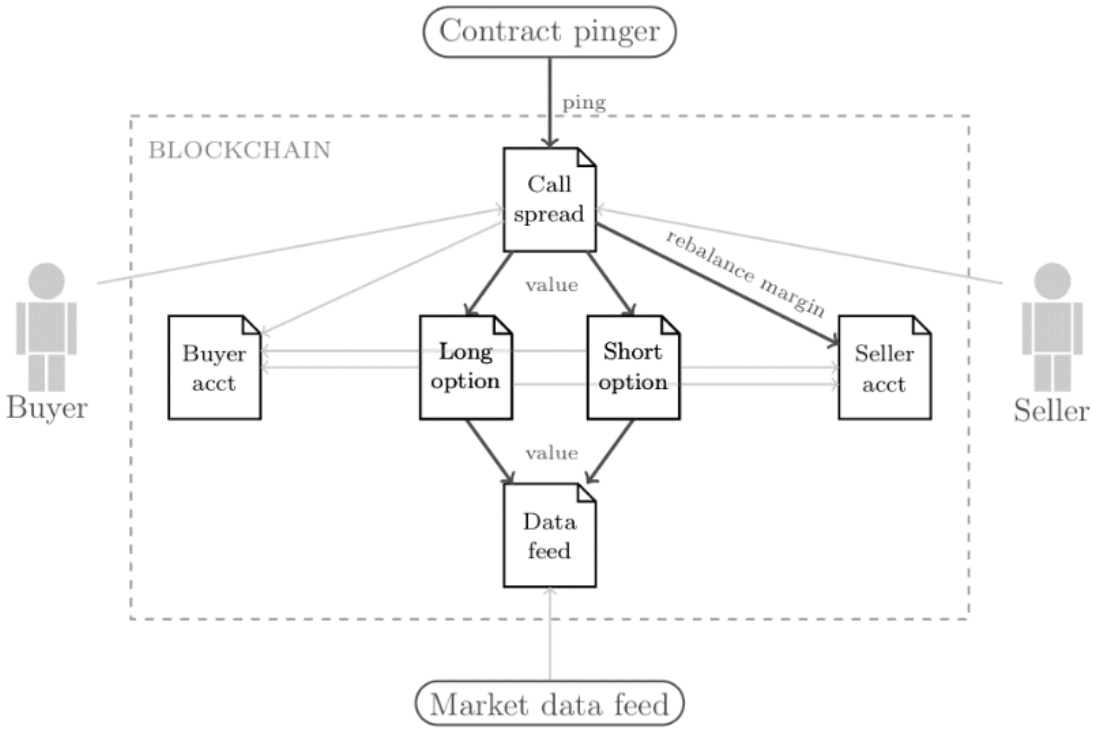

Figura 3.6: Fase di aggiornamento dei margini

[1]View: tipologia di funzione che non modificherà la struttura dati interna alla blockchain. Questa caratteristica la rende esente dal pagamento della tassa di transazione.

Ennesima variazione rispetto alla struttura semplice di call option prende atto nell'esecuzione del contratto, fase mostrata in figura 3.7; durante la fase di esecuzione, partendo dall'acquirente e previa maturità del contratto, verrà effettuato un return sul margine destinato all'esercente. L'esercizio del compratore sarà relativo solo al contratto di long call option.

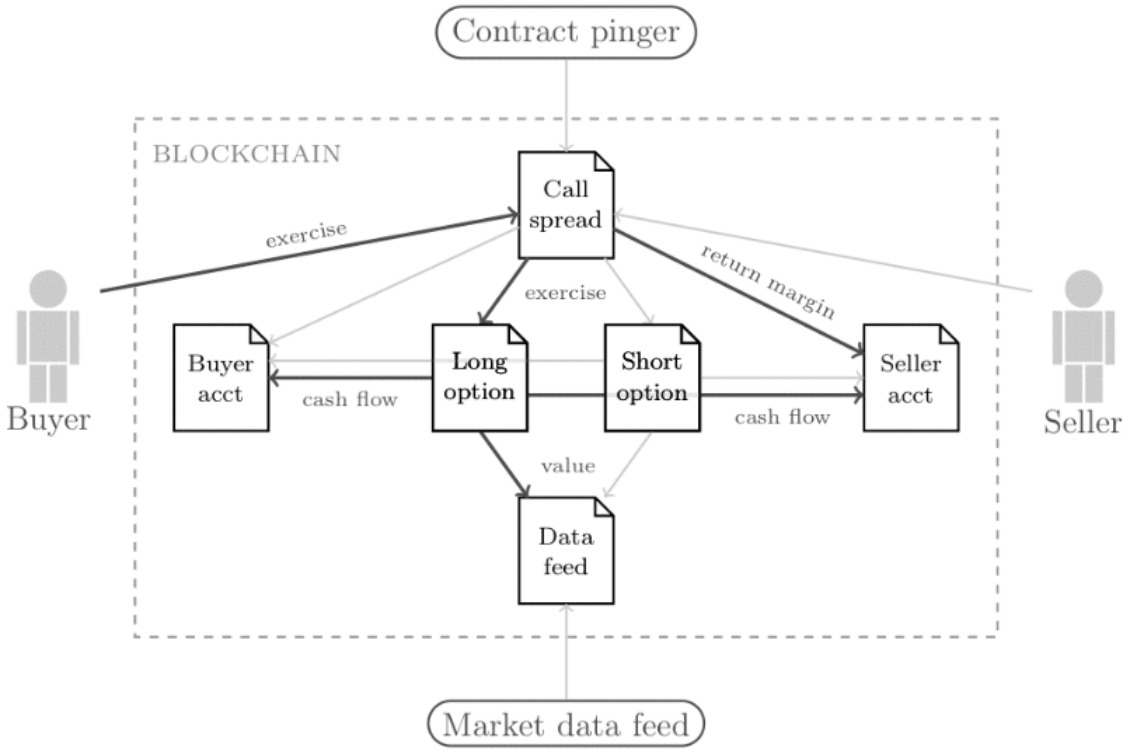

Figura 3.7: Fase di esercizio dell'opzione a maturity da parte dell'acquirente

L'esecuzione, oltre al ritorno del margine verso il venditore, darà luogo ad un cash flow destinato a compiere il cash settlement.
Essendo il venditore a sua volta acquirente in quanto questa strategia è basata su di un acquisto e su di una vendita di call option, raggiunta la maturity, anche il seller stesso potrà eseguire il contratto andando a generare un altro flusso di cassa.
Nella pagina successiva è presente un esempio della funzione di exercize() attuabile sia dal seller che dal buyer con la rispettiva rappresentazione grafica in figura 3.8 della fase di esecuzione da parte del seller.

```
function exercise() returns (bool) {
    bool buyerExercised = true;
    bool sellerExercised = true;
    if (initiatedBy(_buyer)) {
        returnMargin();
        buyerExercised = _buyerLeg.exercise();
        Exercise(address(_buyerLeg),
        toText(buyerExercised));
    }
    if (initiatedBy(_seller)) {
        sellerExercised = _sellerLeg.exercise();
        Exercise(address(_sellerLeg), toText(sellerExercised));
    }
    if (_sellerLeg._isComplete() && _buyerLeg._isComplete()) {
        _isActive = false;
        _isComplete = true;
        Exercise(address(this),
                 toText(true));
    }
    return (buyerExercised && sellerExercised);
}
```

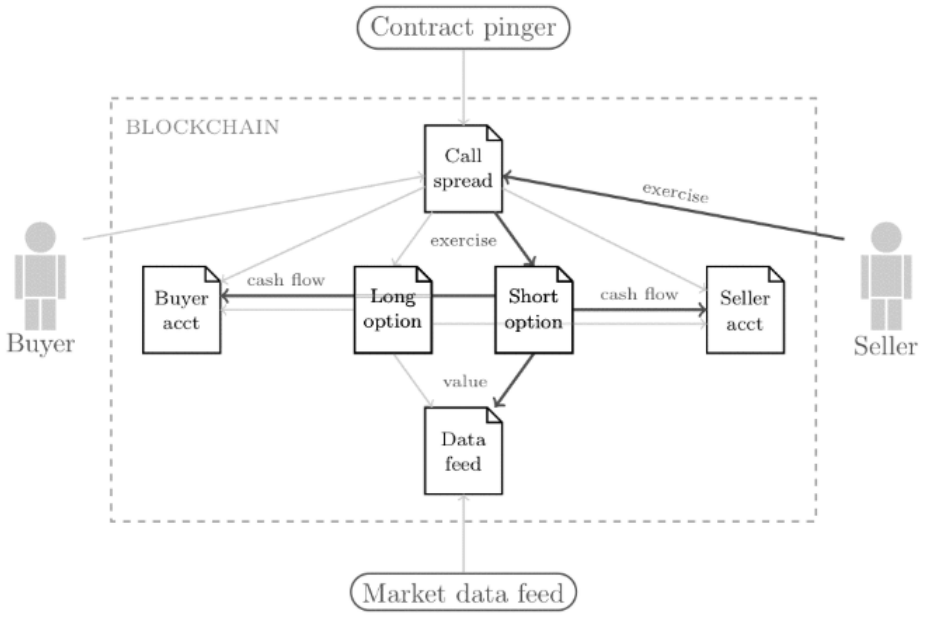

Figura 3.8: Fase di esercizio dell'opzione a maturity da parte del seller

3.2 Critiche sul modello implementato

Il modello studiato, basato sulla struttura ideata da Vishakh(da Vishakh, 2016), risulta essere di sua natura incompleto.
Tra le principali mancanze del modello abbiamo una completa assenza della gestione dell'out of money, ovvero una gestione in caso di default.
Inoltre, è assente la gestione dei premi di opzione, sia nel modello semplificato, che nel modello a bull call spread. Il sistema risulta essere dunque incompleto in quanto il calcolo del premio in un mercato reale viene eseguito a stipulazione del contratto.
Altro difetto riscontratosi nel modello è risultato a fronte dell'utilizzo della marginazione come forma di collateral; è stato utilizzato un calcolo privo dei valori al di sotto della virgola muovendosi verso una computazione del margine semplificata causata da un limitato supporto dei floating point da parte della piattaforma.

Capitolo 4

Analisi sulla decentralizzazione dei mercati finanziari

In questo capitolo si procederà verso un'analisi dei benefici e deficit nell'applicazione del paradigma decentralizzato su piattaforma ethereum prendendo come base il modello sviluppato da Vishakh(da Vishakh, 2016). Paradigma che, nell'analisi si trova come sostituto del modello classico centralizzato, solitamente gestito da un sistema bancario.

4.1 Costi di aggiornamento margini e costi di commissione

Il modello trattato nel capitolo 3, ha come costo fondamentale, escludendo le spese relative all'opzione stessa e le tasse di immissione dei contratti all'interno della blockchain, la tassa relativa alla transazione di aggiornamento margine. La riduzione dei tempi di aggiornamento di marginazione risulta essere uno dei punti di forza del sistema, ma, a seconda di come venga sviluppata la gestione dei costi transazionali, potremo trovarci in svantaggio o vantaggio rispetto ad un tradizionale sistema centralizzato o comunque privo di costi relativi all'aggiornamento margine.
Per strutturare la gestione dei costi di marginazione è possibile far leva su due variabili:

- Tempistica di aggiornamento.

- Gas price per operazione.

4.1.1 Tempistica aggiornamento margini

Riguardo alla prima variabile, ovvero la tempistica di aggiornamento, prendiamo come valore dieci minuti, valore suggerito da Massimo Morini(da Morini, 2017) per l'abbattimento del rischio; la tempistica di aggiornamento può essere qualsiasi al di sopra della frequenza di aggiornamento del network, frequenza che oscilla dai dieci ai trenta secondi; una frequenza troppo elevata andrà però ad impattare notevolmente sui costi. L'obiettivo fondamentale di un aggiornamento con frequenza maggiore rispetto alla versione centralizzata è l'abbattimento del rischio dato da default della controparte, a seconda della volatilità del valore riguardante il bene sottostante, sarà possibile aumentare o diminuire il tempo di frequenza.

4.1.2 Gas price per operazione

L'effetto della modifica del gas price sull'iscrizione della transazione alla blockchain è relativo alla priorità transazionale voluta. Inserendo nel sistema un valore molto basso di gas price, si pagherà un tassa di immissione relativamente bassa che andrà ad incidere sulla priorità e, di conseguenza sulla velocità di iscrizione. Il nodo scopritore dell'ultimo blocco andrà ad inserire le transazioni all'interno del blocco stesso dando priorità quindi a quelle con un valore di gas price maggiore.
Al fine di ottenere una risposta il più consistente possibile da parte del sistema mantenendo i costi bassi, è stato fatto un test con cinque valori diversi di gas price:

- 0,1
- 0,5
- 1
- 2
- 5

L'esecuzione del test è stata svolta all'interno della rete Ropsten, utilizzando due timestamp, il primo, generato da una funzione javascript grazie all'utilizzo dell'interfaccia truffle, il secondo, generato dal timestamp del blocco di iscrizione relativo alla transazione di aggiornamento margini; è stata poi calcolata la differenza tra i due timestamp per ottenere il tempo necessario all'iscrizione della transazione sulla blockchain. Sono stati svolti un totale di venti test per gasprice, successivamente è stato fatto il calcolo di media e deviazione standard sul tempo totale per gasprice.
Le medie dei risultati sono riportate nella tabella alla pagina successiva.

Gas price (GWEI)	media ping time (SEC)	Eth usati (ETH)	costo (€)
0.1	21.55	0.000005	0.00086
0.5	19.35	0.000027	0.00460
1	6.20	0.000054	0.00930
2	6.95	0.000109	0.01900
5	7.25	0.000272	0.04700

Dopo una prima analisi dei risultati si può notare una differenza notevole di ping time medio(tempo di aggiornamento margine) nell'incremento di gasprice sullo step da 0.5 a 1 GWEI, avremo quindi una risposta completamente diversa da parte del sistema. Si può evincere che il quantitativo di gas price in grado di ottimizzare sia i costi che le tempistiche, sia dato da un'unità in termini di GWEI per ether, con un costo in ether di 0.000054 per un valore di 0.0093 €con cambio valuta aggiornata al 01/02/2020. Il risultato di questa ottimizzazione consiste in una risposta media molto più veloce da parte del sistema, con una diminuzione complessiva del rischio sul modello utilizzato.

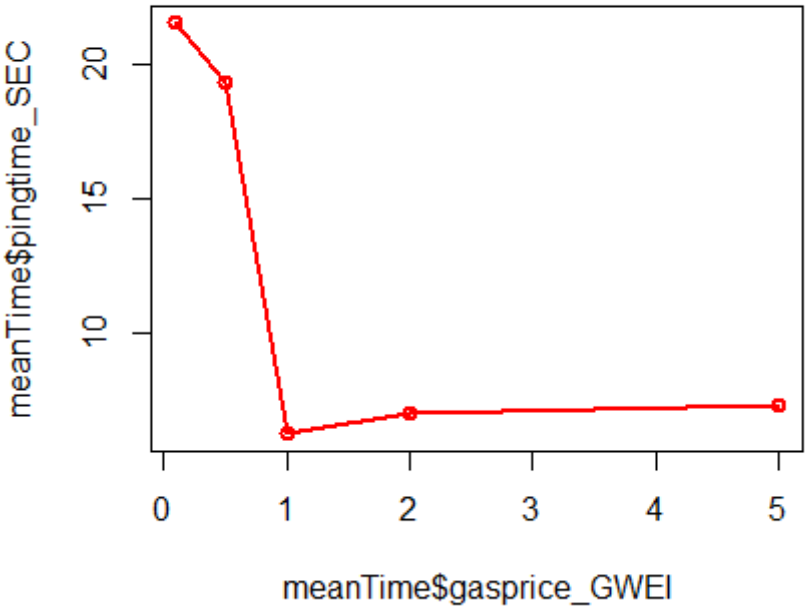

Figura 4.1: Plot rispetto alle tempistiche medie del ping time

Caratteristica fondamentale notatasi durante la fase di testing è data dall'estrema volatilità dei risultati, volatilità che varia a seconda del gas price utilizzatosi; al fine di valutare la stabilità del sistema, è stato eseguito a seguito della valutazione dei ping time medi, un calcolo della deviazione standard per gas price sul ping time di aggiornamento margine.

Gas price (GWEI)	deviazione standard ping time (SEC)
0.1	18.771
0.5	20.013
1	5.277
2	7.287
5	4.733

Dai risultati ottenuti si può notare una deviazione standard notevole quando la scelta è portata verso una riduzione dei costi. Il sistema genera un alto livello di incertezza sulle tempistiche di iscrizione alla blockchain in casi di gas price ridotti al minimo. Come precedentemente affermato, esiste la possibilità di utilizzare un cambio valuta per gas price pari a zero, ma ciò non dà la certezza di immissione sulla blockchain della transazione, inoltre i tempi potrebbero essere dilatati estremamente.

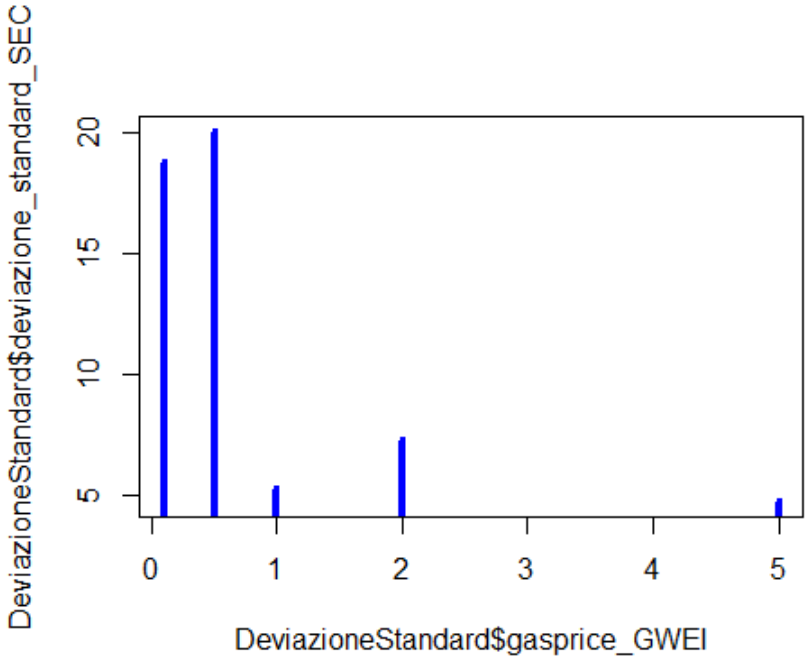

Figura 4.2: Plot rispetto alle deviazioni standard del ping time medio

Con l'aumento del gas price, oltre a tempi di risposta medi rapidamente ridotti, si può notare una notevole riduzione della deviazione standard, anche in questa casistica, una singola unità di gas price, sempre espressa in GWEI, risulta essere la scelta ottimale, essendo in grado di minimizzare tempistiche medie e volatilità dei risultati.

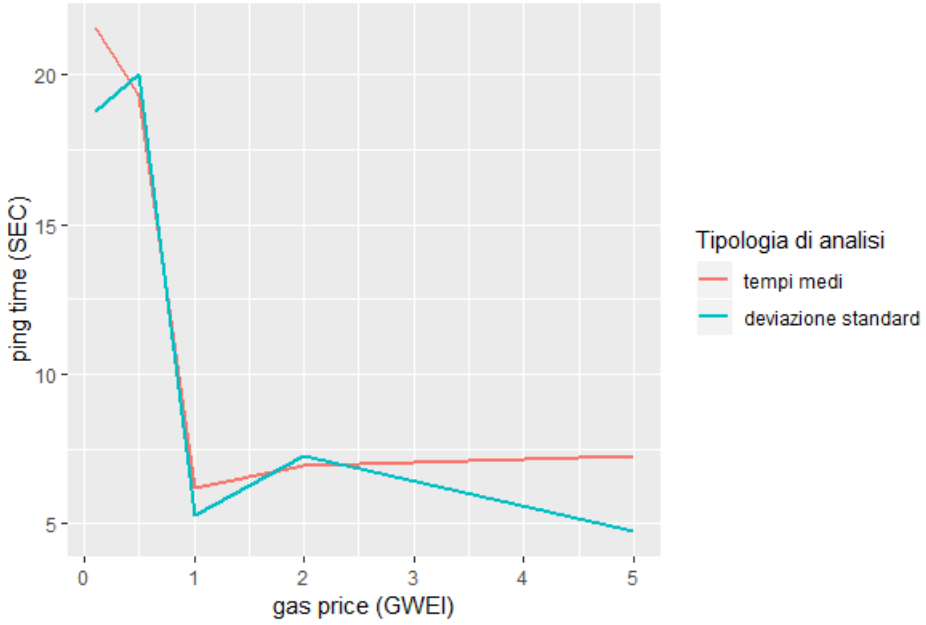

Figura 4.3: Confronto tra le tempistiche medie e le rispettive deviazioni standard

Aggiornando quindi il valore del margine ogni dieci minuti come suggerito da Massimo Morini(da Morini, 2017) e prendendo come valore di gas price 1 GWEI, avremo un costo complessivo per il mantenimento del contratto di 1.34€ al giorno.

Può quindi convenire sfruttare un mercato decentralizzato su base ethereum rispetto ad una classica soluzione centralizzata?

Oltre alle problematiche legate al valore di MPOR elevato, dato dal rischio di default, e ai ritardi di aggiornamento margine, l'appoggiarsi ad una struttura centralizzata ha come principale problematica l'applicazione di tasse di commissione. Al fine di porre un confronto tra i costi derivati dall'utilizzo di una piattaforma decentralizzata come ethereum e una piattaforma centralizzata, sono stati presi come tasse di commissione quelle di Finekobank.
L'utilizzo della piattaforma gestita da Fineco applica una tassa di commissione per lotto di 6.95€(da Fineco, 2019) , dove per lotto si intendono le unità del bene sottostante controllate da un unico contratto.(da borsaitaliana.it, 2017)
Ne risulterà quindi un vantaggio in termini di costi per la struttura decentralizzata

se il contratto avrà una scadenza breve relativamente ai costi di commissione impiegati dalla piattaforma centralizzata presa in analisi.
Nel caso in cui i tempi di maturity siano molto dilatati, relativamente al fattore di costo e non a quello di rischio avremo un'ottimizzazione attraverso l'utilizzo di una piattaforma centralizzata. Sotto questo punto di vista occorre differenziare il tipo di opzione presa in considerazione in quanto avremo:
• Opzioni europee, che prevedono l'esercizio del diritto soltanto ad una precisa data, coincidente con la data di maturity.
• Opzioni americane, che consentono l'esercizio del diritto in qualsiasi giorno compreso tra la conclusione del contratto e la data di scadenza dell'opzione. (da Stellato, 2019)
Prendendo tempi di maturity dilatati sarà quindi possibile trarre vantaggio dai costi legati alla decentralizzazione, ma solo nel caso in cui le opzioni trattate siano presenti nel mercato americano. Prendendo come caso d'esempio un acquisto di un lotto da 100 opzioni, il costo relativo ad un mercato centralizzato come quello posto dalla Fineco bank sarà dato da una tassa di commissione di 6.95€, mentre, prendendo il costo dato dalla piattaforma ethereum attraverso il sistema per acquistare opzioni via smart contract precedentemente descritto, utilizzando un gas price di 1 GWEI per ether, avremo un costo di 1.34€ al giorno. Ne risulterà che fino al quarto giorno, sul livello dei costi, avremo un netto vantaggio da parte del sistema decentralizzato, successivamente risulterà più conveniente il modello standard della Fineco. Da non trascurare il fattore rischio sull'esposizione che risulta essere invece sempre notevolmente ridotto nel modello decentralizzato per via delle sue caratteristiche descritte precedentemente.

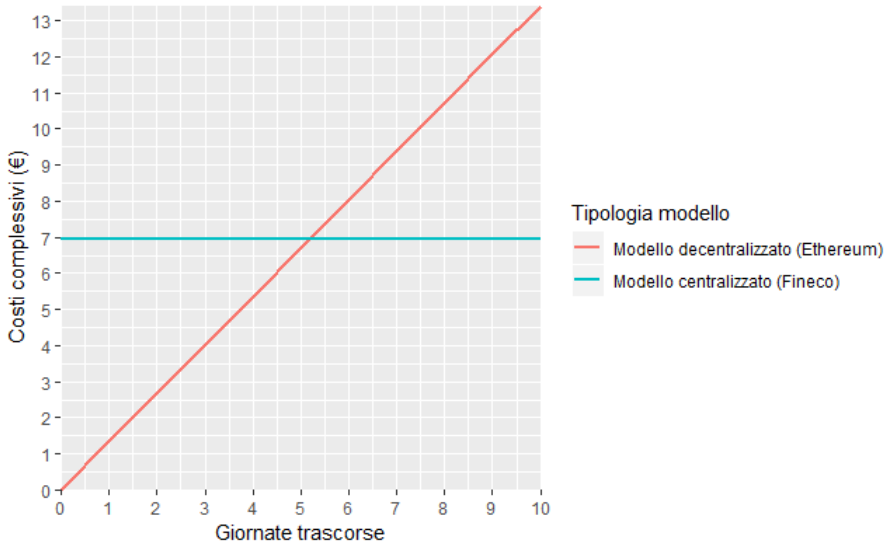

Figura 4.4: Comparazione tra modello su sistema ethereum e su sistema Fineco

Conclusioni

L'abbattimento del paradigma di centralizzazione, attualmente risulta essere la principale barriera in grado di impedire lo sviluppo verso un approccio come quello testatosi basato sul sistema decentralizzato Ethereum.

L'approccio decentralizzato è effettivamente più efficace rispetto a quello centralizzato?

Principale punto di snodo tra i due modelli è dato dalla piena trasparenza del modello decentralizzato, l'utente avrà quindi una completa e trasparente visuale su quello che andrà a firmare. Applicando questo modello si darà però spazio alla problematica gestionale da parte degli utenti non esperti, utenti che si troveranno a gestire contratti senza le competenze per farlo e quindi senza trarre benefici dalla trasparenza degli stessi.
Durante la fase di analisi, si è dato spazio ai costi, partendo dal modello decentralizzato si è trovata un serie di valori di setup per la gestione dei margini andando a modificare la periodicità degli aggiornamenti del margine stesso, per poi alterare il quantitativo di Gas price pagato per transazione. Per quanto riguarda il modello standard centralizzato, si è preso in esame il costo relativo all'acquisto di un lotto opzionario attraverso la piattaforma di Fineco.
Quel che ne risulta è un chiara potenzialità dal punto di vista economico da parte del modello decentralizzato per utilizzi a breve termine; potenzialità che si mantiene anche a lungo termine, ma dalla prospettiva della trasparenza, mentre andrà sfocandosi sotto l'aspetto economico. I modelli centralizzati hanno tuttavia una forte competitività economica per gli utilizzi sul lungo termine non avendo costi aggiuntivi oltre a quelli di commissione.
Analizzando le marginazioni, si otterrà inoltre un enorme vantaggio sotto il punto di vista della computazione dei margini. Le due parti non si appoggeranno più a fonti di dati diverse come accadeva nella metodologia centralizzata, ma si accorderanno su di una unica fonte, ed un unico sistema di marginazione, eliminando i compromessi necessari con il precedente sistema centralizzato.

Da questa comparazione non ne risulta un vero e proprio vincitore o un vero e proprio sconfitto, entrambi i modelli hanno pregi e difetti sotto vari punti di vista, il nuovo modello basato sulla piattaforma ethereum si è però dimostrato un valido competitore, lasciando le porte aperte a possibili sviluppi e integrazioni future.

Appendice

Dati relativi a rilevazioni tempi di aggiornamento margini.

Gas price (GWEI)	Ping time (SEC)	Costo (Eth)	Costo (€)
0.1	8	0.000005	0.00086
0.1	6	0.000005	0.00086
0.1	14	0.000005	0.00086
0.1	37	0.000005	0.00086
0.1	46	0.000005	0.00086
0.1	40	0.000005	0.00086
0.1	46	0.000005	0.00086
0.1	8	0.000005	0.00086
0.1	1	0.000005	0.00086
0.1	75	0.000005	0.00086
0.1	7	0.000005	0.00086
0.1	11	0.000005	0.00086
0.1	11	0.000005	0.00086
0.1	30	0.000005	0.00086
0.1	12	0.000005	0.00086
0.1	14	0.000005	0.00086
0.1	21	0.000005	0.00086
0.1	4	0.000005	0.00086
0.1	22	0.000005	0.00086
0.1	18	0.000005	0.00086
0.5	8	0.000027	0.00460
0.5	16	0.000027	0.00460
0.5	16	0.000027	0.00460
0.5	12	0.000027	0.00460
0.5	20	0.000027	0.00460
0.5	1	0.000027	0.00460

Gas price (GWEI)	Ping time (SEC)	Costo (Eth)	Costo (€)
0.5	28	0.000027	0.00460
0.5	10	0.000027	0.00460
0.5	1	0.000027	0.00460
0.5	26	0.000027	0.00460
0.5	15	0.000027	0.00460
0.5	7	0.000027	0.00460
0.5	3	0.000027	0.00460
0.5	20	0.000027	0.00460
0.5	10	0.000027	0.00460
0.5	3	0.000027	0.00460
0.5	74	0.000027	0.00460
0.5	15	0.000027	0.00460
0.5	70	0.000027	0.00460
0.5	32	0.000027	0.00460
1	5	0.000054	0.00930
1	3	0.000054	0.00930
1	6	0.000054	0.00930
1	13	0.000054	0.00930
1	7	0.000054	0.00930
1	1	0.000054	0.00930
1	1	0.000054	0.00930
1	6	0.000054	0.00930
1	10	0.000054	0.00930
1	6	0.000054	0.00930
1	9	0.000054	0.00930
1	20	0.000054	0.00930
1	8	0.000054	0.00930
1	2	0.000054	0.00930
1	3	0.000054	0.00930
1	16	0.000054	0.00930
1	4	0.000054	0.00930
1	1	0.000054	0.00930
1	2	0.000054	0.00930
1	1	0.000054	0.00930

Gas price (GWEI)	Ping time (SEC)	Costo (Eth)	Costo (€)
2	11	0.000109	0.01900
2	2	0.000109	0.01900
2	1	0.000109	0.01900
2	3	0.000109	0.01900
2	5	0.000109	0.01900
2	16	0.000109	0.01900
2	10	0.000109	0.01900
2	1	0.000109	0.01900
2	4	0.000109	0.01900
2	5	0.000109	0.01900
2	1	0.000109	0.01900
2	2	0.000109	0.01900
2	13	0.000109	0.01900
2	5	0.000109	0.01900
2	2	0.000109	0.01900
2	29	0.000109	0.01900
2	18	0.000109	0.01900
2	3	0.000109	0.01900
2	6	0.000109	0.01900
2	2	0.000109	0.01900
5	15	0.000272	0.04700
5	8	0.000272	0.04700
5	5	0.000272	0.04700
5	8	0.000272	0.04700
5	5	0.000272	0.04700
5	9	0.000272	0.04700
5	10	0.000272	0.04700
5	9	0.000272	0.04700
5	2	0.000272	0.04700
5	9	0.000272	0.04700
5	4	0.000272	0.04700
5	7	0.000272	0.04700
5	8	0.000272	0.04700
5	2	0.000272	0.04700
5	8	0.000272	0.04700

Gas price (GWEI)	Ping time (SEC)	Costo (Eth)	Costo (€)
5	1	0.000272	0.04700
5	20	0.000272	0.04700
5	2	0.000272	0.04700
5	11	0.000272	0.04700
5	2	0.000272	0.04700

*Il tasso di conversione Ether/Euro è aggiornato al 1/02/2020.

Bibliografia

BinanceAcademy 2017, *Storia della blockchain*

Dr. Gavin Wood A. M., 2019a, *Mastering Ethereum, A general purpose Blockchain*

Dr. Gavin Wood A. M., 2019b, *Mastering Ethereum, Smart contracts and solidity*

Fineco 2019, *Mercati e trading opzioni*

Morini M., 2017, *Managing Derivatives on a Blockchain. A Financial Market Professional Implementation*

Rizzo P., 2016, *Coindesk, Banca IMI researcher: Blockchain Won't Work if Banks Don't Change*

Stellato L., 2019, *Fare trading con le opzioni*

Vishakh 2016, *A deeper look into a financial derivative on the Ethereum blockchain*

borsaitaliana.it 2017, *Dimensioni del contratto*