LUISS

CORSO DI LAUREA TRIENNALE
in
ECONOMI E MANAGEMENT

Economia dei Mercati e degli Intermediari Finanziari

FINANZA DECENTRALIZZATA
Protocolli e applicazioni

Laureando: Valerio Schettini

Relatore: Prof. Francesco Cerri

Anno accademico 2020-2021

INDICE

1. BREVE STORIA DELLA BLOCKCHAIN

1.1. La blockchain tra concetti preesistenti e contenuti innovativi

Sebbene nella comunità di esperti e appassionati di crittografia non manchino riferimenti alla blockchain come un protocollo alla base di un nuovo Internet, a differenza del numero contenuto di protocolli riconosciuti come standard nella trasmissione di dati tra dispositivi elettronici, esistono attualmente migliaia di diversi protocolli *blockchain*. Diversamente da quanto avvenuto per Internet, l'ideazione e l'implementazione di tali protocolli segue un approccio *bottom-up* e avviene secondo una logica *open source*, concedendo a chiunque la possibilità di proporre nuove soluzioni. Essendo elevato il numero di protocolli esistenti è ad oggi difficile stabilire, soprattutto in assenza di conoscenze tecniche approfondite, quali di questi rappresenteranno gli standard del settore. Inoltre, piuttosto che identificare la tecnologia con una singola *blockchain*, è bene riferirsi ad essa come un ecosistema composto da protocolli tra loro complementari. Tra i tanti protocolli *blockchain* ad oggi noti è possibile individuarne tre in grado di descrivere in maniera completa le caratteristiche essenziali che consentono la realizzazione delle applicazioni finanziarie oggetto dell'elaborato.

Prima di effettuare una ricostruzione storica del percorso che ha portato alla nascita della prima *blockchain* e le modifiche che hanno successivamente esteso i suoi ambiti di utilizzo, è bene fornire una prima approssimazione delle caratteristiche di questa nuova tecnologia. Essa va annoverata tra le scoperte frutto della combinazione di teorie appartenenti a diverse discipline scientifiche. Fa uso dei contributi della teoria dei giochi, del *network computing* e della crittografia per realizzare una nuova forma di consenso sociale, un nuovo sistema di interazioni socioeconomiche che non abbia bisogno di autorità di vigilanza, ma che sia in grado di arginare comportamenti disonesti attraverso la combinazione di protocolli crittografici e incentivi economici. Dal punto di vista della teoria dei giochi è come rendere un sistema sociale un gioco nel quale esista un'unica strategia dominante in grado di massimizzare contemporaneamente il benessere individuale e sociale attraverso il comportamento onesto di ogni giocatore. Considerando l'utilità di descrivere una qualunque innovazione tecnologica partendo dal problema che l'ha resa necessaria, pare opportuno strutturare la cronologia della blockchain partendo dalle novità che, attraverso essa, sono state introdotte: un sistema elettronico decentralizzato di pagamento contante, una piattaforma per la programmazione di contratti intelligenti e un protocollo di condivisione dati per realizzare l'interoperabilità tra blockchain e sistemi esterni.

1.2. Bitcoin: una nuova forma di contante elettronico

1.2.1 Ecash

Uno dei primi tentativi di realizzazione di una moneta digitale in grado di preservare l'anonimità degli utilizzatori si ebbe nel 1983 con la pubblicazione di un *paper* ad opera dell'informatico e crittografo David

Chaum. Nell'articolo accademico Chaum propone le *"blind signatures"*[1] come mezzo per assicurare l'anonimità del pagatore, mantenendo comunque il controllo del corretto funzionamento del sistema di pagamento. Nelle conclusioni, il professor Chaum scrive: "Un nuovo tipo di crittografia, le *blind signatures*, è stato introdotto. Questo consente la realizzazione di un sistema di pagamenti non tracciabile dotato di migliorate capacità di controllo e revisione rispetto ai sistemi attuali, offrendo allo stesso tempo una migliore protezione della privacy"[2]. La tecnologia fu implementata e brevettata nel 1990 da DigiCash, società fondata dallo stesso Chaum nel 1989, e concesso in uso alla Mark Twain Bank del Missouri, la quale fu però l'unica banca americana ad offrire un servizio di pagamento basato sulle *blind signatures*. A causa della scarsa attenzione degli utenti dell'epoca al tema della privacy digitale, il servizio raggiunse un bacino d'utenza limitato, costringendo la DigiCash a dichiarare fallimento nel 1998. Il contributo del professor Chaum alla realizzazione del primo protocollo blockchain è evidente per via dell'introduzione di alcuni concetti chiave che saranno, con alcune variazioni, ripresi da Ecash come l'utilizzo della crittografia simmetrica[3] per garantire la sicurezza del canale di pagamento. Nonostante ciò, il protocollo sviluppato da Chaum manca ancora di un'importante caratteristica della blockchain: la decentralizzazione. Nel protocollo Ecash la banca veniva preposta alla funzione di garanzia del protocollo in quanto l'emissione delle chiavi era ad essa delegata. In un articolo pubblicato sulla rivista *IEEE Spectrum* il 4 gennaio 1999[4], Chaum riconosce come l'utilizzo della crittografia asimmetrica offra caratteristiche in termini di sicurezza e di autenticazione superiori rispetto a quella simmetrica. Sarà infatti la prima ad essere implementata nel protocollo Bitcoin.

1.2.2. Bitgold e bmoney

Due ulteriori proposte per la realizzazione di un protocollo per lo scambio di una moneta virtuale che imitasse le caratteristiche di anonimità e portabilità del denaro contante con i vantaggi della decentralizzazione e dei pagamenti elettronici, furono 'bmoney', pubblicata da un utente internet noto con lo pseudonimo di Wei Dai, e 'Bitgold', avanzata dall'informatico, crittografo e dottore di legge Nick Szabo. Il termine 'bmoney' fa riferimento all'articolo ispirato all'ideologia sociale cripto-anarchica e coincide con il nome a dominio del sito web utilizzato per la pubblicazione dello stesso. La criptoanarchia, formalizzata alla fine degli anni Ottanta dall'ingegnere elettronico e scrittore politico Timothy C. May nel "Crypto Anarchist Manifesto"[5], è una forma di libertarismo che ritiene necessario l'utilizzo di sistemi di comunicazione basati sulla crittografia per garantire la privacy degli utenti, costantemente minacciata dai continui tentativi di violazione e controllo da parte dei Governi e dalle loro agenzie di intelligence. Nella società cripto anarchica ciascun membro è

[1] Si veda l'esempio proposto dal professor Chaum a pagina 200 dell'articolo di cui alla nota 2.
[2] Chaum, David; Blind Signatures for Untraceable Payments; Department of Computer Science, University of California Santa Barbara.
[3] Sistema crittografico consistente nel rendere un messaggio informatico leggibile solo ai possessori dello specifico parametro da inserire nell'algoritmo di cifratura.
[4] Brands, Stefan; Chaum, David; "Minting" elettronic-cash, 4 gennaio 1999.

[5] Cay, Timothy; The Crypto Anarchist Manifesto, 1988.

identificato attraverso uno pseudonimo che gli consente di mantenere segreta la sua vera identità e ogni interazione socioeconomica si svolge attraverso canali di comunicazione criptati. L'articolo di Dai esplora due possibili protocolli finalizzati alla realizzazione della visione di May attraverso una versione crittografica di due elementi essenziali della cooperazione sociale: la moneta e i contratti[3]. Nella sua esposizione, Dai affronta cinque questioni: la creazione di moneta, il suo trasferimento, la validità dei contratti, la loro conclusione e l'esecuzione. Sebbene la proposta descrivesse in buona parte la logica successivamente utilizzata nella progettazione del protocollo Bitcoin, alcuni problemi legati alla sua implementazione non vennero menzionati. Nonostante ciò, la citazione dell'articolo di Dai nel whitepaper di Bitcoin lascia intendere la sua rilevanza nell'implementazione del primo protocollo blockchain.

Il protocollo Bitgold fu proposto dal già citato Szabo nel 1998, anche se non venne mai effettivamente implementato. La sua idea rappresenta un ulteriore passo avanti nella realizzazione di un protocollo per lo scambio di moneta elettronica completamente decentralizzato. Tale decentralizzazione si sarebbe potuta ottenere richiedendo la soluzione di un problema crittografico a dimostrazione dell'impegno speso per la validazione delle transazioni. Un'ulteriore caratteristica che sarà riproposta in Bitcoin che accumuna le idee di Dai e Szabo è quella della scarsità monetaria. Entrambi i progetti, infatti, non delegando ad alcuna autorità monetaria la coniazione della moneta, stabiliscono una modalità di emissione che vede la quantità di moneta emessa diminuire nel tempo.

1.2.3. Hashcash

Per la comparsa di altre importanti componenti del protocollo bisogna attendere l'invenzione del Proof Of Work Algorithm. Ideato nel 1999 dal crittografo britannico Adam Back, la sua formalizzazione avvenne solo nel 2002[6]. L'algoritmo venne proposto come soluzione ai problemi di "spam" nei servizi di posta elettronica e, più in generale, come contromisura ai Denial of Service Attacks consistenti nel sovraccaricare di richieste l'host di un servizio internet al fine di rendere il servizio inutilizzabile dagli utenti. Con lo sviluppo di Hashcash si esauriscono le innovazioni tecnologiche in assenza delle quali non sarebbe stato possibile lo sviluppo di Bitcoin.

1.2.4. Bitcoin

Il 31 ottobre 2008, mentre i timori di una crisi finanziaria causata da una bolla nel settore immobiliare statunitense si intensificavano, alcuni appassionati di crittografia abbonati alla *mailing list* '*cryptography*' ricevettero un messaggio da parte di Satoshi Nakamoto in cui annunciava l'ideazione di un sistema di pagamento in contante elettronico completamente *peer-to-peer*[7] funzionante in assenza di ruoli di garanzia ricoperti da soggetti terzi. Il 3 gennaio 2009 il sistema divenne ufficialmente operativo, la prima transazione

[6] Back, Adam; Hashcash – A Denial of Service Counter-Measure, 1 Agosto 2002.

[7] Con il termine si fa riferimento allo scambio diretto tra due controparti in assenza di intermediari.

venne registrata nel blocco genesi della catena insieme ad una stringa di testo, un chiaro riferimento alle soluzioni che i governi dei paesi industrializzati stavano mettendo in atto per risolvere la famosa crisi dei mutui Subprime: *"The Times Jan/03/2009 Chancellor on brink of second bailout for banks."*[8]

Questa svolse la doppia funzione di documentare la data di formazione del primo blocco di transazioni e di sottolineare la fragilità del sistema finanziario e la sua inadeguatezza a risolvere le sue crisi interne, lasciando intendere come la nuova valuta digitale costituisse una via di fuga rispetto ad un sistema bancario fino a quel momento insostituibile.

Alla nascita di Bitcoin si sono succeduti dodici anni di intensi dibattiti di varia natura: riflessioni legali ed economiche in merito alla possibilità di definire bitcoin una valuta o paragonarlo ad un titolo azionario; fiorenti attività economiche aventi ad oggetto l'offerta di servizi legati a bitcoin; si è discussa l'approvazione di ETF aventi bitcoin come sottostante. Infine, le più recenti discussioni hanno riguardato l'adeguato inserimento nel quadro normativo di una nuova categoria di beni meritevoli di specifica attenzione: i cosiddetti *crypto-assets*[9].

1.3. Ethereum: la blockchain programmabile e gli smart contracts

1.3.1. Il Whitepaper di Ethereum

Il 27 novembre 2013 Vitalik Buterin, programmatore di origine russa e cofondatore della rivista Bitcoin Magazine, pubblicò il *whitepaper* di Ethereum contenente la proposta di una blockchain indipendente. L'obiettivo dichiarato fu di rendere possibile l'implementazione di soluzioni di larga scala non consentite dalla struttura del protocollo Bitcoin. Nel documento Buterin riconobbe la rivoluzione iniziata da Bitcoin, la cui realizzazione diede vita, secondo l'autore, "al primo bene digitale simultaneamente caratterizzato da assenza di valore intrinseco ed emissione o controllo da parte di autorità centrali"[10]. Un'altra importante caratteristica attribuita a Bitcoin fu la sua capacità di dare vita ad una forma di "consenso distribuito" attraverso l'utilizzo della tecnologia blockchain. Inoltre, egli sostenne che "[…] la rappresentazione digitale di valute personalizzate e contratti finanziari, di proprietà di dispositivi fisici sottostanti, di beni non fungibili come i nomi a dominio, ma anche complesse applicazioni comprendenti la gestione di beni digitali direttamente da parte di porzioni di codice che eseguono logiche arbitrarie" sono solo alcune delle ulteriori possibilità di utilizzo di Bitcoin. Nonostante ciò, la tesi del programmatore consistette nell'affermare l'impossibilità di apprezzare il potenziale impatto che la tecnologia avrebbe potuto avere a causa delle sue limitazioni. Dopo aver evidenziato i pregi di Bitcoin, Buterin arriva ad elencare le 4 principali limitazioni all'efficienza del protocollo (il cui significato specifico verrà approfondito nel secondo capitolo e che si intende ora soltanto menzionare): la mancanza della cosiddetta *Turing equivalenza*, l'utilizzo di un complesso meccanismo di gestione dei conti che rende difficile la realizzazione di applicazioni finanziarie come i derivati con sottostante

[8] Coinbase, Bitcoin Wiki: https://en.bitcoin.it/wiki/Genesis_block.

[9] Secondo il regolamento EU 265/2020, con il termine 'crypto-asset' si intende la "rappresentazione digitale di valore o diritti che può essere trasferita o mantenuta in formato elettronico, utilizzando la distributed ledger technology o technologie simili".

[10] Ethereum Whitepaper.

bitcoin, l'esistenza di due soli stati per una transazione (spesa o non spesa) che rende impossibile la rappresentazione di stadi intermedi in una logica di esecuzione automatica dei contratti, l'inesistenza di una fonte di casualità che limita gli impieghi nel vasto settore delle scommesse.

Il 1° aprile 2014, l'informatico e cofondatore di Ethereum Gavin Wood, pubblicò il cosiddetto *yellow paper*, un documento nel quale vennero descritte le caratteristiche tecniche del nuovo protocollo. Nello stesso anno, nei 42 giorni compresi tra il 22 luglio e il 2 settembre, è stato avviato un *round* di finanziamento per lo sviluppo della blockchain consistente nella possibilità di acquistare la valuta nativa di Ethereum, denominata ETH, ad un tasso di conversione fisso rispetto a bitcoin. L'operazione di finanziamento fruttò circa 31.591 BTC equivalenti circa a $18,4 milioni al tasso di cambio del 2 settembre 2014. Come avvenuto per Bitcoin, il progetto ha subito numerosi sviluppi resi possibili dalla partecipazione di una community che è attualmente costituita da decina di migliaia di ingegneri e sviluppatori dedicati a mantenere la tecnologia al passo con i tempi e con le esigenze dei suoi utilizzatori.

Nei sette anni successivi alla nascita di Ethereum, la piattaforma ha beneficiato di una vasta partecipazione da parte di ingegneri e programmatori con la conseguente nascita di numerose valute digitali con diverse logiche di utilizzo.[11] Nonostante i meriti di Ethereum nel rendere veramente possibile un nuovo ambiente di sviluppo di applicazioni decentralizzate, nei primi tre anni dal lancio della *mainnet*[12] le possibilità di utilizzo in contesti esterni alle logiche di scambio di *crypto token*[13] o contratti derivati da essi rimasero limitate. Questo per via di un ultimo tassello da inserire nell'ecosistema per mantenere le promesse di *trustlessness* e di *single point of failure resistance*.

1.4. Chainlink: un sistema di oracoli decentralizzato

Nel settembre dello stesso anno della pubblicazione del whitepaper di Ethereum, un gruppo di sviluppatori iniziò a lavorare ad una delle possibili applicazioni menzionate nel documento dallo stesso Buterin: gli oracoli. Con questo termine ci si riferisce ad uno *smart contract* che si occupi di assicurare la validità dei dati reperiti da fonti esterne. Nel paragrafo precedente si è menzionato il problema della *single point of failure*. È infatti evidente che un'applicazione decentralizzata che utilizzi dati forniti da un'unica fonte esterna espone gli utilizzatori a qualunque tipo di attacco, errore o malfunzionamento nei confronti di tale fonte. Per questo motivo l'imprenditore Seregey Nazarov con l'aiuto di Ari Juels, dottore in informatica e professore presso il Jacobs Technion-Cornell Institute, compose un gruppo di lavoro per lo sviluppo di un protocollo per la fornitura di dati esterni ai contratti di Ethereum. Nel settembre del 2017, dopo la pubblicazione del whitepaper,

[11] Fra tutte, le più interessanti ai fini di questa analisi sono le piattaforme di *peer-to-peer decentralized lending* come Aave, le piattaforme di *parametric insurance* come Arbol e i *Decentralized Exchange* come Uniswap, tutte applicazioni oggetto della trattazione nel capitolo 3.

[12] Con il termine si intende identificare la rete di calcolatori che si occupa di mantenere e aggiornare lo stato di un registro distribuito. Viene utilizzato per distinguerla dalla *testnet*, rete mantenuta al solo scopo di provare le applicazioni prima del "lancio" sulla rete principale.

[13] Un *asset* digitale il cui diritto di proprietà è garantito da una blockchain.

Chainlink raccolse circa $32 milioni attraverso un Initial Coin Offering[14], ottenendo i fondi necessari a rendere possibile il lancio sulla *mainnet* Ethereum nel giugno del 2019. Ad oggi Chianlink è arrivato a conquistare la posizione di leader di mercato nel settore degli oracoli, realizzando integrazioni con le maggiori blockchain programmabili nate negli ultimi quattro anni. Su piattaforme come Polkadot, Cosmos e Algorand, la squadra di Nazarov ha già implementato versioni analoghe del contratto inizialmente sviluppato su Ethereum.
Nei due anni successivi al lancio, gli sviluppatori di ChainLink hanno portato avanti il progetto iniziale, espandendo la gamma di servizi offerti e integrando nuove soluzioni tecnologiche. Il 15 aprile 2021 è stata pubblicata una nuova versione del Whitepaper contente le novità che hanno ulteriormente esteso i possibili utilizzi degli *smart contracts* nel mondo reale.

1.5. La tendenza DeFi

Come già accennato, con la comparsa di questo terzo ed ultimo protocollo si è avuta la rimozione dei limiti alla realizzazione del massimo potenziale dell'ecosistema blockchain. Tra il 2016 e il 2017 a San Francisco furono fondate diverse *start-up* con l'obiettivo di offrire le prime piattaforme decentralizzate di scambio di criptovalute. Tuttavia, nonostante la condivisione di visione ed obiettivi, il livello di cooperazione fu prossochè inesistente. La situazione rimase tale fino a che un gruppo di leader di queste *start-up* non avviò un *brainstorming* su un gruppo Telegram per dare un nome e un'identità comune all'obiettivo che essi cercavano di raggiungere. Nacque così il movimento della Decentralized Finance o "DeFi", inconsapevolmente destinato ad attrarre, da lì a pochi anni, l'attenzione delle più importanti testate giornalistiche e a stimolare l'organizzazione di convenzioni in tutto il mondo per riunire esperti e appassionati desiderosi di approfondire la proposta innovativa della DeFi. A testimoniarne l'impatto nel mondo finanziario è l'incremento esponenziale dai volumi totali di scambio totali realizzati sulle piattaforme DeFi. Da un valore stimato di circa $250 milioni nel maggio del 2019 si è arrivati ad un picco di $89 miliardi nell'aprile 2021.

[14] Una ICO è l'analogo di una IPO nel settore dei *crypto-assets*.

2. IL FUNZIONAMENTO DEI PRINCIPALI PROTOCOLLI BLOCKCHAIN

In questo capitolo sarà fornita una spiegazione più approfondita del funzionamento dei principali protocolli blockchain: Bitcoin, Ethereum e ChainLink. Al capitolo successivo è affidata l'analisi delle applicazioni finanziarie che essi rendono possibili.

2.1. La Blockchain di prima generazione: il protocollo Bitcoin

2.1.1. Il problema dei generali bizantini

Nel capitolo 1 è stata citata la caratteristica di Bitcoin di essere un protocollo per il raggiungimento del consenso distribuito in una rete di computer. La capacità del protocollo di assicurare il raggiungimento del consenso, nonostante la possibile presenza di un certo numero di nodi malevoli, è ciò che viene definita Byzantine Fault Tolerance. Con questo termine si vuole indicare la capacità di un protocollo di comunicazione tra nodi di una rete di mantenere fra i nodi stessi il consenso in merito al contenuto dei messaggi scambiati. Il termine Byzantine è un riferimento alla metafora utilizzata per descrivere un possibile fallimento del protocollo: il problema dei generali bizantini. Del problema esistono due versioni. La prima, più semplice nella formulazione, fu proposta nel 1975 per rappresentare la difficoltà di raggiungere uno stato consistente a riguardo dell'apertura di una connessione tra due terminali di rete[15]. La seconda fu utilizzata per descrivere la necessità, per un sistema computerizzato affidabile, di gestire informazioni contraddittorie provenienti da componenti malfunzionanti[16].

Nella prima versione si hanno solamente due generali, A e B. L'obiettivo di questi è di ideare un algoritmo in grado di rendere possibile il raggiungimento di una decisione: attaccare o meno il nemico C. Al momento della decisione, i due generali si trovano sui lati opposti del campo di battaglia e l'unico modo di comunicare è attraverso un messaggero che attraversi il campo nemico. Nessuno dei due singoli eserciti sarebbe da solo in grado di vincere la battaglia. I due generali devono dunque raggiungere la medesima conclusione: attaccare entrambi o ritirarsi. A complicare la decisione è il fatto che il messaggero potrebbe essere intercettato ed ogni messaggio perso prima di raggiungere il destinatario. Si potrebbe pensare di risolvere il problema utilizzando una versione riadattata del *three-way handshake*[17], modalità con cui il protocollo TCP instaura una connessione tra due terminali in Internet. Il generale A invia il primo messaggio a B: "Se rispondi a questo messaggio, attacco". Se il messaggio viene perso, nessun problema, poiché né A né B si sono impegnati ad attaccare. Se B riceve il messaggio, risponde con "Se rispondi, attacco", inviando ad A contemporaneamente la conferma del proprio attacco e un'ultima richiesta di conferma prima di attaccare. Ancora una volta, la perdita del messaggio non comporta l'attacco da parte dei due generali che non sono ancora arrivati ad un

[15] Akkoyunlu, E. A.; Ekanadham, K.; Huber, R.V. Some constraints and trade-offs in the design of network communications, ,1975.
[16] Lamport, Leslie; Shostak, Robert; Pease, Marshall. The Byzantine Generals Problem: https://lamport.azurewebsites.net/pubs/byz.pdf.
[17] Meccanismo attraverso cui il Transfer Control Protocol instaura una connessione tra due terminali di rete.

accordo. Dunque, A invia l'ultimo messaggio: "attacchiamo!". Ma a questo punto il problema non è risolto. Infatti, se quest'ultimo messaggio dovesse andare perso, A si sarebbe impegnato ad attaccare prima di avere la certezza che anche B abbia raggiunto la stessa conclusione. Inoltre, richiedere un'ulteriore conferma ad A significherebbe entrare in un circolo vizioso senza possibilità di uscita. Al problema dei due generali viene applicata una soluzione non perfetta, ma statisticamente valida. Per risolvere il problema del consenso tra i due nodi, è infatti possibile decidere di inviare un numero arbitrariamente elevato di messaggeri. In questo modo un fallimento nelle procedure del protocollo è ancora possibile, ma statisticamente meno probabile. Questa soluzione è sufficientemente soddisfacente nel protocollo di trasporto TCP. In questo caso, infatti, la perdita della connessione conseguente alla perdita del messaggio può essere ristabilita in un secondo tentativo tramite il riavvio del protocollo. Al contrario, un simile fallimento in un protocollo blockchain causerebbe un default del sistema. Mentre, nello standard di comunicazione Internet, un certo grado di incertezza può essere accettato per non rinunciare ai benefici che lo standard comporta, per ottenere un sistema veramente *trustless* tutta la fiducia dell'utilizzatore deve essere riposta nella completa infallibilità del protocollo.

La seconda versione si avvicina più propriamente al concetto di Byzantine Fault Tolerance necessaria alla corretta implementazione di un protocollo blockchain. Essa prevede un numero qualunque di generali, con la variante della presenza di un ordine gerarchico tra essi e della possibile presenza di traditori. Nel caso più semplice abbiamo tre generali. Un comandante al vertice incaricato di impartire l'ordine di attaccare o ritirarsi, due tenenti che devono arrivare ad un accordo in merito all'ordine impartito dal comandante. I due tenenti, dunque, ricevuto l'ordine, comunicheranno tra loro per confrontarsi in merito all'esecuzione dell'ordine. Anche in questo caso, l'unico modo di assicurare la vittoria è garantire il consenso in merito all'ordine del generale.

Per avere una valida soluzione l'algoritmo deve soddisfare due condizioni:

1. Tutti i generali onesti devono aderire sul piano da attuare;
2. Un piccolo numero di traditori non può causare l'adozione di un piano sbagliato da parte dei generali onesti.

La seconda condizione è più difficile da definire formalmente in quanto non è facile determinare le caratteristiche di un piano "sbagliato". Nonostante ciò, l'aspetto importante è piuttosto la modalità con cui i generali arrivano al consenso.

Una soluzione al problema consiste nell'individuare un algoritmo che rispetti due ulteriori condizioni. L'ordine del generale deve essere impartito ai tenenti in modo tale che:

1. I tenenti onesti obbediscano allo stesso ordine;
2. Se il comandante è onesto, tutti i tenenti onesti obbediscano al suo ordine.

È a questo punto facile verificare che, nel caso in cui il comandante sia onesto, il rispetto della condizione 1 è conseguenza della condizione 2. Ma il comandante non deve essere per forza onesto.

Nel caso più semplice di un comandante e due tenenti, è facile dimostrare come la presenza di un traditore renda impossibile l'esistenza di un protocollo che rispetti le due condizioni di cui sopra. Nel caso in cui il

traditore sia un tenente, il generale impartirà ad entrambi l'ordine di attaccare, ma il primo comunicherà al secondo tenente di aver ricevuto l'ordine di ritirarsi. Essendo il traditore libero di non seguire l'ordine, ma il tenente onesto costretto a seguire l'ordine del generale nel rispetto della condizione 2, i due non raggiungeranno la stessa decisione.

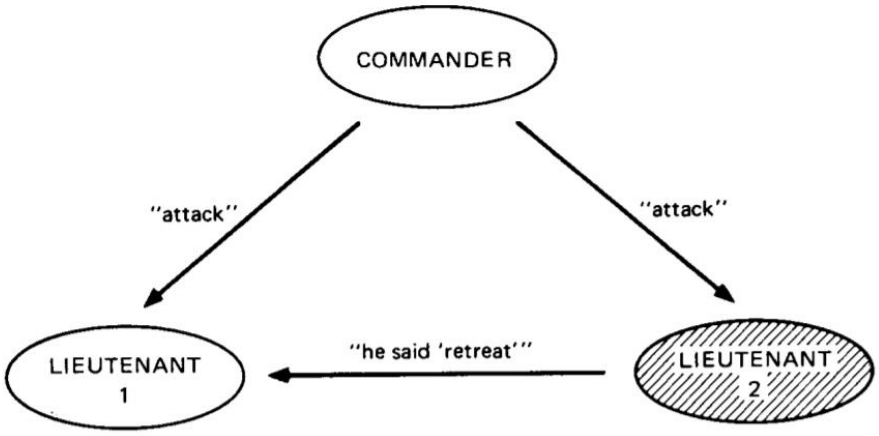


Fig. 1. Lieutenant 2 a traitor.

[18]

Nel caso in cui il generale sia il traditore, questo invierà diversi ordini ai tenenti. I due, dunque, si scambieranno informazioni conflittuali in merito all'ordine del comandante, ma non potendo stabilire chi sia il traditore, decideranno di comportarsi secondo la condizione 1, arrivando di nuovo a conclusioni differenti.

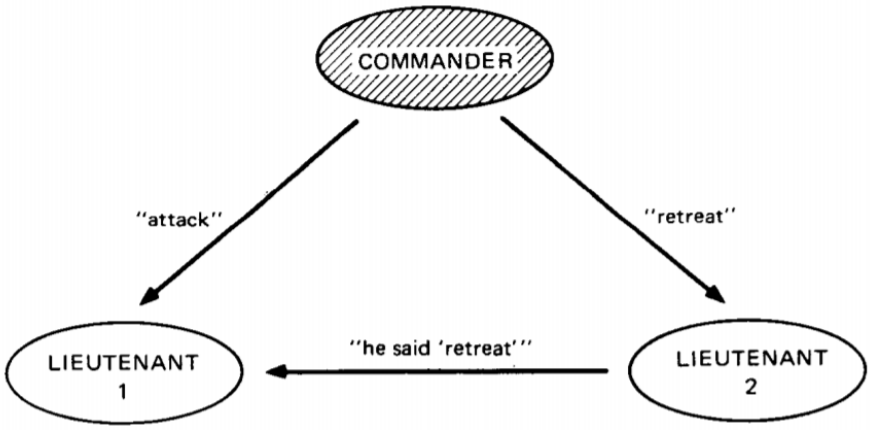


Fig. 2. The commander a traitor.

È possibile dimostrare come l'impossibilità di trovare una soluzione si possa estendere al caso in cui vi sia un numero di generali pari a *3n* di cui *n* sono traditori. Ciononostante, gli autori dell'articolo furono in grado di descrivere il funzionamento di un algoritmo in grado di funzionare nel caso di *3n+1* generali in presenza di un numero massimo *n* di traditori.

[18] Questa figura e la successiva sono tratte dall'articolo di cui alla nota 16.

Il problema di elaborare un protocollo di consenso distribuito per la condivisione di dati tra una rete di computer era dunque noto più di trent'anni prima della nascita di Bitcoin e nel tempo diversi algoritmi tolleranti al problema dei generali bizantini sono stati proposti. Bitcoin rappresenta una nuova soluzione al problema, attraverso l'utilizzo di una tecnologia non presente al momento della sua formulazione, il Proof of Work Algorithm, e di un incentivo economico in grado di favorire il comportamento onesto da parte dei nodi.

2.1.2. Il Sistema di identificazione degli utenti: l'indirizzo Bitcoin

Per risolvere il problema dei generali bizantini in modo efficiente, è innanzitutto necessario stabilire un sistema di comunicazione sicuro. Per fare ciò, Bitcoin utilizza una tipologia di crittografia, definita crittografia asimmetrica, grazie alla quale è possibile identificare in modo univoco un utente attraverso una coppia di stringhe alfanumeriche: la chiave pubblica e la chiave privata. Due importanti caratteristiche della funzione crittografica usata per generare le chiavi sono la corrispondenza univoca tra chiave privata e chiave pubblica e l'elevatissima potenza computazionale richiesta per risalire alla chiave privata partendo da quella pubblica. Quest'ultima può dunque essere condivisa a tutti i nodi della rete sopportando un rischio irrisorio di compromissione dell'identità degli utenti.

I passaggi per l'assegnazione di un indirizzo ad un utente sono i seguenti:

1. Una chiave privata viene generata casualmente e assegnata ad un nuovo utente.
2. Attraverso l'algoritmo *ECDSA (Elliptic Curve Digital Signature Algorithm)* viene creata una chiave pubblica univocamente associata alla chiave privata.
3. Alla chiave pubblica viene applicata un'operazione di *Double Hash* composta dagli algoritmi *SHA-256* e *RIPEDM160* ricavandone il corrispondente *hash*.
4. Si applica l'algoritmo *Base58Check encode* per trasformare l'hash del passo precedente in una stringa di 58 valori alfanumerici rendendo l'indirizzo facilmente leggibile da un essere umano e digitabile tramite tastiera.[19]

L'indirizzo Bitcoin così ottenuto può finalmente essere utilizzato per identificare l'utente e autorizzare le transazioni. L'utente che voglia effettuare una transazione deve inviare un messaggio al destinatario contenente la quantità di bitcoin desiderata. Per fare ciò, il mittente A firma il messaggio con la propria chiave privata e con quella pubblica del destinatario B. In questo modo è possibile identificare con certezza A usando la corrispondente chiave pubblica per decifrare il messaggio. La chiave pubblica di B serve invece ad effettuare il trasferimento del diritto di proprietà sulla quantità di bitcoin inviata. Se la transazione viene ritenuta valida dal sistema (vedi paragrafo IV di questo capitolo), essa viene registrata. Avvenuto ciò, solo il destinatario avrà la possibilità di spendere i bitcoin nella prossima transazione: il diritto di proprietà dell'utente B è certificato dalla chiave pubblica utilizzata per firmare l'ultima transazione con cui sono stati inviati. Per effettuare un

[19] La descrizione dei passaggi è tratta da: MIT OpenCourseWare, Massachussets Institute of Technology, Blockchain and Money, Prof. Gary Gensler, Session 4: Blockchain Basics & Consensus.

successivo trasferimento, solo la chiave privata di B potrà essere utilizzata per inviare bitcoin ad un nuovo indirizzo senza causare il rigetto della transazione.

2.1.3. Il Proof of Work di Adam Back

Il Proof of Work Algorithm di Adam Back, citato nel paragrafo III del capitolo 1, consiste nel cercare di evitare che utenti malintenzionati decidano di sovraccaricare un terminale di rete inviando una quantità di richieste superiori alle sue possibilità di gestione. Per comprenderne il funzionamento è più semplice descriverne l'applicazione al caso dello spam e-mail. In tale circostanza, l'utente malintenzionato vuole sfruttare la possibilità di poter inviare una elevata quantità di messaggi standardizzati ad un gran numero di utenti. L'unico sforzo richiesto per il raggiungimento dell'obiettivo è la conoscenza dell'indirizzo e-mail dei destinatari. L'idea di Back fu quella di incrementare la difficoltà di condurre l'attacco richiedendo al mittente di dimostrare di avere impiegato una parte delle proprie risorse computazionali per poter inviare il messaggio. Per fare ciò fa uso di una funzione, detta funzione di hash, con le seguenti proprietà:

- Unidirezionalità: dato l'input della funzione deve essere particolarmente facile calcolarne l'output, ma estremamente difficile realizzare l'operazione inversa;
- Resistenza alle collisioni: deve essere pressoché impossibile trovare due diversi input in grado di restituire lo stesso output;
- Output di dimensione fissa: dato un messaggio di lunghezza arbitraria, il risultato deve essere una stringa alfanumerica di lunghezza predefinita (chiamata hash del messaggio).

Stabilita la funzione di hash da utilizzare, gli input da utilizzare sono determinati a partire dall'intestazione dell'e-mail (una serie di informazioni in grado di identificarla in modo univoco, come ad esempio l'indirizzo del mittente, quello del destinatario e la data e l'ora in cui il messaggio è stato scritto).

La prova del lavoro consiste nel richiedere al mittente di reiterare il calcolo della funzione di hash fino ad ottenere un output che rispetti una specifica condizione. Gli argomenti da inserire nella funzione sono due: l'intestazione dell'e-mail ed un numero intero arbitrario, il cosiddetto *nonce*. La condizione imposta sull'output è di avere come valori inziali una combinazione di valori alfanumerici prestabilita.

Una conseguenza dell'unidirezionalità è il fatto che una minima variazione nell'input causa una variazione notevole nell'output, rendendo dunque infattibile trovare una chiara associazione tra tutti i possibili input e gli output. Ciò fa sì che l'unico modo per il mittente di trovare l'output che soddisfi la condizione è attraverso una serie di tentativi ed errori. Prima di inviare la mail, il programma avvia il processo di calcolo dell'hash. Viene selezionato un primo numero casuale e inserito insieme all'intestazione come argomento per il calcolo della funzione. Se l'hash non gode della proprietà sopra descritta, il processo ripete il calcolo inserendo come primo argomento il numero intero successivo a quello già utilizzato. Il procedimento viene ripetuto finché l'hash calcolato non soddisfa la condizione richiesta.

Trovato l'hash, il mittente lo allega al contenuto dell'e-mail insieme all'intestazione e al nonce che lo hanno generato. Il mittente impiega dunque un tempo, nell'ordine dei millisecondi, per verificare la corrispondenza tra argomenti ed hash.
Aumentando e diminuendo il numero di valori alfanumerici iniziali dell'hash si ha una modifica della complessità del calcolo richiesto. È quindi possibile definire il tempo medio richiesto per il calcolo dell'hash modificando la condizione imposta sull'hash stesso. Scegliendo una quantità di tempo sufficientemente contenuta per trovare l'hash è possibile far sì che un utente benevolo non abbia problemi ad impiegare pochi secondi per il calcolo, mentre un utente malintenzionato vedrà ridotta la convenienza dell'attacco.
L'ultimo passo richiesto al destinatario consiste nella verifica della corrispondenza tra argomenti e immagine della funzione. Se la corrispondenza viene verificata con successo, l'algoritmo classifica la mail come "importante" e la mostra al destinatario nella sezione "posta ricevuta". In caso contrario, la mail viene classificata come "spam".

2.1.4. Il protocollo

Come ben descritto all'interno del Whitepaper di Ethereum, "il tentativo di creare un sistema valutario decentralizzato richiede la combinazione di un meccanismo di transizione di stato con un protocollo di consenso per assicurare che ci sia accordo in merito all'ordine delle transazioni. In Bitcoin questo si traduce nel tentativo da parte dei nodi della rete di produrre pacchetti di transazioni chiamati "blocchi". La finalità della rete è quella di produrre un blocco ogni dieci minuti, con ogni blocco contente una data, un nonce, un riferimento al blocco precedente (ossia l'hash) e una lista delle transazioni avvenute a partire dal blocco precedente. Nel tempo, questo crea una persistente, continuamente in crescita, "catena di blocchi" che si aggiorna costantemente per riflettere lo stato più recente del registro Bitcoin.
L'algoritmo per la verifica della correttezza dei blocchi è strutturato nel modo seguente:

1. Verifica se il blocco precedente a cui si riferisce il blocco corrente esiste ed è valido;
2. Verifica se la data contenuta nel blocco è maggiore di quella del blocco precedente e distante da esso meno di due ore;
3. Verifica che la Proof of Work eseguita sul blocco sia valida;
4. Per ogni transazione contenuta all'interno del blocco verifica che sia valida;
5. Se la verifica delle transazioni non restituisce errori, aggiungere il blocco alla catena."[20]

La Proof of Work utilizzata nel protocollo funziona in modo simile all'algoritmo ideato da Back. I nodi nella rete hanno la possibilità di partecipare alla validazione dei blocchi destinando le risorse computazionali a loro disposizione. Questi nodi calcolano un hash, che sarà l'hash del blocco corrente, a partire da una serie di dati: la data in cui il blocco è stato formato, l'hash del blocco precedente, le transazioni inserite nel blocco e un nonce. La prova del lavoro consiste, come descritto nel paragrafo precedente, nel trovare il nonce che consenta

[20] Ethereum Whitepaper.

alla funzione di hash di restituire come risultato un hash che cominci con un numero di 0 iniziali stabilito dinamicamente. La difficoltà di trovare l'hash è modificata ogni 2016 blocchi, variando il numero di 0 con cui deve iniziare l'hash del blocco, per fare sì che la validazione di ogni blocco avvenga approssimativamente ogni dieci minuti. Il primo nodo a trovare l'hash invia il risultato agli altri validatori, i quali verificano, come il destinatario della mail nel paragrafo precedente, che vi sia corrispondenza tra input e output della funzione di hash.

Per verificare la validità delle transazioni, viene invece utilizzato il sistema di indirizzi descritto nel paragrafo precedente. Tramite la coppia chiave pubblica-chiave privata chiunque può verificare che il mittente della valuta abbia effettivamente titolo a spenderla, riassegnando tale diritto alla chiave privata del destinatario inserendo nella transazione la chiave pubblica di quest'ultimo.

Di seguito si riporta un esempio che aiuti a comprendere la garanzia di sicurezza offerta dal protocollo. Ipotizziamo l'esistenza di un utente malintenzionato che effettui una transazione per regolare un'obbligazione contrattuale. Nel caso di acquisto di un bene la cui consegna sia immediata, il venditore potrebbe decidere di attendere la validazione del blocco prima di trasferire il bene. A questo punto il compratore, ottenuta la merce, valida un nuovo blocco, in sostituzione del precedente, nel quale non compare la transazione. Per comprendere quale sia la catena di blocchi su cui proseguire, i validatori si basano sulla catena più lunga. A parità di lunghezza, i nodi decideranno diversamente in merito a quale blocco dal quale partire per estendere la catena. Nel caso qui presentato, i nodi onesti godranno di un vantaggio. Il primo blocco ricevuto dagli altri nodi è quello contenente la transazione con cui lo scambio viene regolato. Essi godranno dunque di un vantaggio temporale nella validazione del blocco successivo. Per completare l'attacco, il nodo disonesto deve impiegare meno tempo dei restanti nodi per estendere la catena. Essendo necessaria una prova del lavoro per la validazione del blocco, fino a che i nodi disonesti non controlleranno la maggioranza della potenza di calcolo della rete, i nodi onesti manterranno il controllo della stessa impiegando meno tempo ad estendere la catena. L'utente malevolo, dovrà dunque controllare il 51% della potenza di calcolo dell'intera rete per poter eseguire l'attacco con successo, sostenendo un costo estremamente elevato per ottenere un beneficio pari solamente ad una frazione di esso. Inoltre, bisogna considerare che Bitcoin presenta le caratteristiche di un'economia di rete. Come avviene per la telefonia mobile, o per Internet, il suo valore aumenta all'aumentare del numero degli utenti. La corruzione del sistema attraverso una *doppia spesa* comporterebbe la perdita della sua funzionalità come sistema di scambio monetario, causando la cessazione dell'utilizzo da parte degli utenti e azzerandone il valore, rendendo totalmente priva di valore la transazione corrotta.

All'argomentazione di cui sopra si può aggiungere un ulteriore incentivo all'onestà degli operatori. Il validatore, che abbia correttamente speso potenza di calcolo per validare un blocco successivamente aggiunto alla catena, guadagna il diritto di aggiungere all'interno del blocco una transazione a suo beneficio generatrice di nuova valuta, la cosiddetta *coinbase transaction*. In analogia al lavoro compiuto dalle compagnie di estrazione aurifera, i validatori della blockchain sono comunemente chiamati *miners*. Il meccanismo di emissione è interamente regolato dalle coinbase transactions. Ogni 210,000 blocchi, la quantità di bitcoin che

i miners hanno diritto di attribuirsi si dimezza, fenomeno noto con il nome di *halving*. Diretta conseguenza è la riduzione del tasso di inflazione nel corso del tempo, conferendo ai bitcoin l'importante caratteristica di moneta disinflazionistica. Visto che il tempo di validazione dei blocchi si mantiene pressoché costante, l'halving avviene con cadenze di circa quattro anni. Nel 2009, il reward per i miners ammontava a 50 BTC ($2,150,000 ai prezzi attuali). A seguito dell'ultimo halving, avvenuto circa alle 15:00 dell'11 maggior 2020, il reward si è nuovamente dimezzato per un valore di 6.25 BTC. La presenza di un incentivo economico alla validazione dei blocchi conferisce un secondo incentivo al comportamento onesto, assicurando che il miner non sia disposto a compromettere il registro per non perdere il valore economico della remunerazione.
Questo è, non senza approssimazioni, il meccanismo di funzionamento di Bitcoin. Nonostante sia stato il primo protocollo a rendere possibile una forma di consenso distribuito non basato sulla fiducia in un'autorità centrale, le successive evoluzioni degli algoritmi di consenso (Proof of Stake, Delegated Proof of Stake, Proof of History…) sono varianti che ripropongono buona parte dei meccanismi fondamentali di Bitcoin. Tali varianti verranno descritte nel capitolo X, quando si discuteranno altri protocolli blockchain con interessanti casi di utilizzo nel settore finanziario. Prima, però, è necessario descrivere un secondo passo che la tecnologia ha dovuto affrontare per rendere possibile una prima approssimazione della società descritta nell'articolo di Wei Dai. Con la realizzazione della prima blockchain di seconda generazione, è stato possibile il passaggio da mera tecnologia di contabilità decentralizzata, a piattaforma trustless per l'esecuzione di *smart contracts*.

2.2. La Blockchain di seconda generazione: il protocollo Ethereum

2.2.1. L'Account Ethereum

Una prima differenza tra Bitcoin ed Ethereum è la tipologia di informazione mantenuta dal registro. In Bitcoin la contabilità è tenuta annotando le transazioni effettuate dagli utenti. Lo stato è dunque definito dall'ammontare di bitcoin trasferiti ai vari indirizzi per mezzo delle transazioni. Ethereum, invece, identifica gli utenti attraverso un Account. La blockchain, quindi, riporta la quantità di valuta nella disponibilità degli utenti modificando direttamente il bilancio dell'Account. Ogni Account è identificato da quattro dati:

1. Il nonce, un contatore che si occupa di assicurare che ogni transazione avvenga una sola volta;
2. Il bilancio di ether (la valuta nativa della blockchain) disponibile;
3. Il codice del contratto, se presente;
4. Lo spazio di archiviazione disponibile, vuoto di default.

La principale funzione svolta da Ether è il pagamento delle commissioni di transazione. Esistono due tipologie di account: account di proprietà esterna e account di contratto. I primi sono controllati dalle chiavi private degli utenti, i secondi dal rispettivo codice di contratto. Gli account di proprietà esterna non hanno codice. È inoltre possibile inviare messaggi da un account di proprietà esterna firmando e creando transazioni. Negli account di contratto, invece, la ricezione di un messaggio innesca l'esecuzione del codice al quale è consentito di leggere e scrivere nello spazio di archiviazione interno, di inviare altri messaggi o di creare nuovi contratti.

Prima di proseguire, una precisazione, seppur banale. Nonostante l'utilizzo del termine "contratto", la differenza rispetto all'utilizzo del termine in ambito giuridico è evidente. I contratti di Ethereum sono in realtà delle porzioni di codice che eseguono una logica arbitraria frutto del preventivo accordo tra le parti. Più che essere la rappresentazione di un vincolo contrattuale atto a fornire la prova di un rapporto giuridico in sede di giudizio, esso è piuttosto lo strumento di esecuzione automatica dei termini a cui le parti hanno aderito.

2.2.2. I messaggi e le transazioni

Con il termine "transazione" in Ethereum ci si riferisce al pacchetto di dati firmato da un conto di proprietà esterna che memorizza un messaggio da inviare. Come riportato nel whitepaper di Ethereum, "le transazioni contengono:

1. Il destinatario del messaggio;
2. Una firma che identifica il mittente;
3. La quantità di etere da trasferire dal mittente al destinatario;
4. Un campo dati opzionale;
5. Un valore STARTGAS, che rappresenta il numero massimo di passi di calcolo che l'esecuzione della transazione può richiedere;
6. Un valore GASPRICE, che rappresenta la tassa che il mittente paga per ogni passo di calcolo."

Chiara è l'analogia delle prime tre componenti con le transazioni di Bitcoin. Il campo dati opzionale è invece un contenitore al quale il contratto ha la possibilità di accedere per recuperare le informazioni sulla base delle quali eseguire il codice. Nel whitepaper di Ethereum è presente un chiaro esempio dell'utilizzo che un contratto può fare di tali dati. "Se un contratto funziona come un servizio di registrazione di domini on-blockchain, allora potrebbe voler interpretare i dati che gli vengono passati come contenenti due "campi", il primo campo essendo un dominio da registrare e il secondo campo essendo l'indirizzo IP a cui registrarlo. Il contratto leggerebbe questi valori dai dati del messaggio e li metterebbe opportunamente in memoria."

Gli ultimi due campi, lo STARTGAS e il GASPRICE sono utilizzati per prevenire l'utilizzo da parte di utenti malintenzionati delle risorse messe a disposizione dalla blockchain. Ogni transazione deve infatti dichiarare la quantità massima di istruzioni che può essere eseguita tramite il codice. L'obiettivo è quello di impedire cicli di esecuzione infiniti o "altri sprechi computazionali". Il cosiddetto *gas* è l'unità fondamentale rappresentativa del calcolo. Generalmente l'esecuzione di ogni istruzione costa un *gas*, con l'eccezione di alcune istruzioni più complesse al quale è assegnato un valore maggiore in termini di *gas*. Ad ogni singolo byte presente nella transazione è invece assegnato un valore pari a 5 *gas*. In questo modo, all'utilizzatore dell'ambiente di esecuzione di Ethereum è richiesto un pagamento che sia quanto meno approssimativamente proporzionale alla quantità di risorse consumate. Tale sistema può essere visto come un'ulteriore assicurazione contro gli utilizzi impropri da parte di un utente malintenzionato.

È già stata menzionata la possibilità in capo ad un contratto di inviare "messaggi" ad altri contratti. I messaggi "sono oggetti virtuali che non sono mai serializzati ed esistono solo nell'ambiente di esecuzione di Ethereum. Un messaggio contiene:

1. Il mittente del messaggio (implicito);
2. Il destinatario del messaggio;
3. La quantità di etere da trasferire insieme al messaggio;
4. Un campo dati opzionale;
5. Un valore STARTGAS."

Un messaggio può dunque essere visto come una transazione, con la differenza che a produrlo è un contratto e non un soggetto esterno. La finalità dei messaggi è sostanzialmente quella di rendere possibile l'interazione tra di essi come per gli account di proprietà esterna.

2.2.3. La Funzione di Stato

Con il termine funzione di stato si intende indicare i criteri di modifica apportati allo stato iniziale di un sistema in modo tale da ottenerne lo stato finale. La funzione di stato (o funzione di transizione di stato) è quindi la formalizzazione delle modifiche rappresentanti una transizione dallo stato iniziale S del sistema allo stato finale S'. Nel protocollo Bitcoin, la funzione di stato è rappresentata dall'insieme di transazioni aggiunte attraverso la validazione di un nuovo blocco. In Ethereum invece, "la funzione di transizione di stato", formalmente descritta come "APPLY (S, TX) -> S', può essere definita come segue:

1. Controllare se la transazione è ben formata (cioè ha il giusto numero di valori), la firma è valida, e il nonce corrisponde al nonce nell'account del mittente. In caso contrario, restituire un errore;
2. Calcolare la commissione di transazione come STARTGAS * GASPRICE, e determinare l'indirizzo di invio dalla firma. Sottrarre la tassa dal saldo del conto del mittente e incrementare il nonce del mittente. In caso di saldo insufficiente, restituire un errore;
3. Inizializzare GAS = STARTGAS, e togliere una certa quantità di gas per byte per pagare i byte della transazione;
4. Trasferire il valore della transazione dal conto del mittente al conto ricevente. Se il conto ricevente non esiste ancora, crearlo. Se il conto ricevente è un contratto, eseguire il codice del contratto fino al completamento o fino a quando l'esecuzione non esaurisce il gas;
5. Se il trasferimento di valore è fallito perché il mittente non aveva abbastanza denaro, o l'esecuzione del codice ha consumato tutto il gas, ripristinare tutti i cambiamenti di stato tranne il pagamento delle commissioni, e aggiungere le commissioni al conto del miner;
6. Altrimenti, rimborsare le commissioni per tutto il gas rimanente al mittente, e inviare le commissioni pagate per il gas consumato al miner."

Per un esempio di esecuzione della funzione di stato, si rimanda al Whitepaper di Ethereum.

2.2.4. Il protocollo

Un'importante differenza tra Ethereum e Bitcoin a riguardo dell'architettura della blockchain è che Bitcoin contiene una lista delle transazioni effettuate mentre Ethereum contiene sia una lista delle transazioni che una copia dello stato più recente. "L'algoritmo di convalida del blocco di base in Ethereum è il seguente:

1. Controllare se il blocco precedente a cui si fa riferimento esiste ed è valido;
2. Controllare che il *timestamp* del blocco sia maggiore di quello del blocco precedente a cui si fa riferimento e meno di 15 minuti nel futuro;
3. Controllare che il numero del blocco, la difficoltà, la radice della transazione, la radice dello zio e il limite del gas (vari concetti di basso livello specifici di Ethereum) siano validi;
4. Controllare che la prova di lavoro del blocco sia valida;
5. Sia S [0] lo stato alla fine del blocco precedente;
6. Sia TX la lista delle transazioni del blocco, con n transazioni. Per tutti gli i in 0...n-1, impostare S[i+1] = APPLY(S[i], TX[i]). Se qualsiasi applicazione restituisce un errore, o se il totale del gas consumato nel blocco fino a questo punto supera il GASLIMIT, restituisce un errore;
7. Lasciamo che S_FINAL sia S[n], ma aggiungendo la ricompensa del blocco pagata al minatore;
8. Controllare se la radice dell'albero di Merkle dello stato S_FINAL è uguale alla radice dello stato finale fornito nell'intestazione del blocco. Se lo è, il blocco è valido; altrimenti, non è valido."

"Una domanda comunemente posta è "dove" viene eseguito il codice del contratto, in termini di hardware fisico. Questo ha una risposta semplice: il processo di esecuzione del codice del contratto è parte della definizione della funzione di transizione di stato, che è parte dell'algoritmo di convalida del blocco; quindi, se una transazione viene aggiunta nel blocco B l'esecuzione del codice generato da quella transazione sarà eseguita da tutti i nodi, ora e in futuro, che scaricano e convalidano il blocco B".

2.3. L'interoperabilità con i sistemi esterni: ChainLink

La necessità di realizzare l'interoperabilità tra sistemi blockchain e le esistenti infrastrutture di mantenimento e condivisione dati è un importante argomento affrontato dal World Economic Forum in un paper pubblicato nel dicembre 2020[21]. L'avvento di Ethereum, con la possibilità di garantire il rispetto di vincoli contrattuali tramite porzioni di codice eseguite su una piattaforma decentralizzata, ha avviato un dibattito in merito ai possibili casi di utilizzo degli smart contracts nel mondo reale. Purtroppo, con i mezzi messi a disposizione da Ethereum e dalle blockchain programmabili nate dopo di esso, ad esempio Polkadot e Algorand, non è possibile scambiare dati con fornitori di dati esterni ad un ambiente blockchain senza mettere a rischio i vantaggi derivanti dai protocolli di consenso. Allo stesso tempo, non permettere la comunicazione con sistemi

[21] Nazarov, Sergey; Shukla, Punit, Bridging the Governance Gap: Interoperability for blockchain and legacy systems. World Economic Forum, Center for the Fourth Industrial revolution, dicembre 2020.

esterni limita le applicazioni reali degli smart contracts. Basti pensare ai dati in merito all'annullamento o il ritardo di un volo aereo necessari ad eseguire i termini di un contratto di assicurazione sul volo stesso. Per eseguire un simile contratto senza rinunciare alle caratteristiche di sicurezza offerte dagli smart contracts è fondamentale interrogare una fonte dati esterna che possa fornire le informazioni necessarie. Per superare le limitazioni dei protocolli esistenti, Chainlink propone di inserire un ulteriore strato di decentralizzazione tra le richieste effettuate dalle porzioni di codice on-chain e le risposte da parte dei data providers[22]. Per fare ciò è stato realizzato un protocollo di reperimento, aggregazione e condivisione dati provenienti da sistemi esterni attraverso reti decentralizzate di nodi specializzate nella fornitura di particolari dati, quali ad esempio tassi di interessi, corsi azionari, temperature. Ciascun nodo di ogni singola rete è a tutti gli effetti un data provider, il quale, però, non condivide i dati direttamente con il richiedente. Questi, infatti, vengono trasmessi al contratto Chainlink che si occupa di garantirne la correttezza attraverso un proprio protocollo di consenso e un meccanismo di disincentivi al comportamento disonesto.

2.3.1. L'architettura on-chain

La componente *on-chain* del contratto ChainLink è costituita a sua volta di tre contratti: un contratto di reputazione, un contratto di corrispondenza degli ordini e un contratto di aggregazione. Il primo tiene traccia delle prestazioni dei singoli oracoli riportando sulla blockchain alcune statistiche come il numero di richieste assegnate e soddisfatte, il tempio medio di risposta o l'ammontare delle penalità pagate (cfr. paragrafo 2.3.2.). Il secondo registra le richieste esterne e raccoglie le offerte da parte dei fornitori di dati. Infine, il contratto di aggregazione raccoglie i dati forniti e procede a calcolare il risultato finale della richiesta. Il flusso di esecuzione del contratto è composto di tre fasi: selezione dell'oracolo, fornitura dei dati, aggregazione dei risultati.

La selezione dell'oracolo può avvenire manualmente o automaticamente. Il processo manuale prevede il raggiungimento di un accordo tra il fornitore dei dati e il richiedente secondo le esigenze espresse da quest'ultimo. Altrimenti, il richiedente può compilare il contratto di corrispondenza degli ordini specificando le caratteristiche della richiesta lasciando al contratto il compito di selezionare gli oracoli che soddisfano la richiesta interrogando il contratto di reputazione. Individuati gli oracoli il contratto viene registrato nella blockchain, dando inizio alla fase di fornitura dei dati. In questa fase gli oracoli eseguono il contratto, firmano il messaggio contente i dati richiesti e lo inviano al contratto di aggregazione. Nell'ultima fase il contratto di aggregazione si occupa del calcolo di un risultato ponderato a partire dai dati messi a disposizione dagli oracoli. La ponderazione avviene diversamente a seconda della tipologia di dato richiesta e delle necessità del richiedente. Ad esempio, se il dato oggetto della richiesta fosse il tasso LIBOR a tre mesi rispetto al dollaro americano il contratto di aggregazione procederebbe a sottrarre dall'insieme dei dati forniti dagli oracoli (le maggiori banche globali) il maggiore e minore tasso riportato e a calcolare una media dei restanti tassi. Il

[22] Ellis, Steve; Juels, Ari; Nazarov, Sergey, ChainLink A decentralized oracle network, 4 settembre 2017.

contratto ChainLink mette a disposizione una serie di contratti di aggregazione standard, nonostante il richiedente goda sempre della libertà di configurare il contratto a sua discrezione.

2.3.2. La decentralizzazione degli oracoli

L'approccio alla decentralizzazione di ChainLink si fonda su tre pilastri: la distribuzione delle fonti, la distribuzione degli oracoli e l'utilizzo di *trusted hardware*. La distribuzione delle fonti richiede al singolo oracolo di determinare la propria risposta sulla base di dati di diversa provenienza. Ogni oracolo è libero di utlizzare poi la logica che ritiene più adatta per aggregare i dati ricevuti in un'unica risposta. Un ulteriore passo verso la decentralizzazione è costituito dalla distribuzione degli oracoli. Piuttosto che affidare la soddisfazione di una richiesta ad un singolo oracolo ChainLink si affida ad una rete di oracoli quanto più differenziati possibili in termini di fonti consultate. Di conseguenza, la risposta finale alla query sarà rappresentata dall'insieme delle risposte fornite dagli oracoli. Si presenta a questo punto il problema della possibile manomissione di uno più oracoli. Questo problema viene risolto attraverso un complesso consenso di protocollo che fa uso di concetti crittografici all'avanguardia come le *Schnorr Signatures*. Infine, per garantire confidenzialità nella condivisione dei dati da parte degli oracoli, ChainLink propone l'utilizzo da parte degli oracoli di particolari hardware in grado di impedire l'accesso ad alcuni processi allo stesso proprietario, rendendo possibile interrogare una fonte dati e restituire il risultato senza venirne a conoscenza.

3. LE APPLICAZIONI FINANZIARIE

Uno dei primi utilizzi dell'infrastruttura decentralizzata messa a disposizione da Ethereum è stata la possibilità di ottenere in prestito asset digitali utilizzando come collaterale altri asset digitali. Poco dopo la nascita di Compound, il primo protocollo per i *decentralized loans* sviluppato su Ethereum, nel novembre 2018 è nato Uniswap, il primo Decentralized Exchange, o DEX. Per garantire il funzionamento dell'Exchange in assenza di fornitori di liquidità centralizzati, Uniswap ha introdotto un meccanismo di gestione della liquidità noto come Automated Market Making. L'utilizzo del AMM verrà proposto dai successivi DEX come Curve, SushiSwap e Balancer. Più tardi, nel gennaio 2020 è stato pubblicato il whitepaper della piattaforma di peer-to-peer lending che ha conquistato la posizione di leader nel settore dei prestiti decentralizzati per valore totale di depositi: Aave. [Infine, con la nascita di Solana, una blockchain programmabile dotata di un algoritmo di validazione dei blocchi che le consente di gestire fino a 50.000 transazioni al secondo, è stato possibile superare le inefficienze degli AMM, programmando il primo Exchange decentralizzato in grado di offrire un meccanismo di gestione della liquidità identico a quello degli Exchange centralizzati.] Le applicazioni finanziarie della blockchain non si esauriscono con lo scambio e i prestiti di asset digitali. Un interessante ed emergente caso di utilizzo riguarda il settore assicurativo: l'assicurazione parametrica decentralizzata.

3.1. Decentralized peer-to-peer lending

Una prima inefficienza rilevata nel settore della DeFi consisteva nell'impossibilità di prendere a prestito i token nativi dei nuovi progetti che nascevano su Ethereum. Alla fine del 2017 molti di questi raggiunsero valutazioni eccessive. In assenza di piattaforme che permettessero di ottenere prestiti denominati nel token di interesse non era possibile effettuare vendite allo scoperto rappresentanti un importante strumento di ritorno ad equilibrio dei prezzi. Un'altra possibile applicazione su cui i programmatori specularono fu la cosiddetta *tokenizzazione* dei tradizionali asset finanziari. Questa consiste nell'emissione di *crypto-token* la cui funzione è di rappresentare titoli azionari di società quotate a fini esclusivamente speculativi. Quest'ultima applicazione è stata recentemente oggetto di una regolamentazione da parte degli istituti di vigilanza e controllo finanziari di alcuni Stati Membri dell'Unione Europea, tra cui la Consob, che ha imposto a Binance, piattaforma leader nello scambio di criptovalute, la cessazione dell'offerta di servizi legati agli strumenti finanziari *tokenizzati* e di derivati sulle criptovalute. Per soddisfare tali bisogni, nacquero diverse piattaforme di peer-to-peer lending, tra cui le già citate Compound ed Aave. La prima fu in grado di risolvere la carenza di piattaforme di prestito decentralizzate attraverso l'offerta di servizi limitati, seppur innovativi. Con lo sviluppo di Aave, invece, fu possibile allargare la gamma di prodotti finanziari introducendo, in aggiunta ai prestiti a tempo indeterminato e tasso variabile offerti da Compound, la possibilità di ottenere prestiti in criptovalute a tempo indeterminato

e tasso relativamente fisso e una forma di prestito possibile su larga scala soltanto grazie alle caratteristiche di integrità e certezza della blockchain: i *flash loans*[23].

3.1.1. Aave

"Aave è un protocollo Open Source e non-custodial per guadagnare interessi su depositi e attività di prestito"[24]. Per rendere possibile ciò, Aave raccoglie i depositi degli utenti in *pool* di riserve e stabilisce algoritmicamente la quantità di collaterale che deve essere depositata per garantire il debito, le modalità di liquidazione del prestito nel caso in cui una riduzione di valore del collaterale e l'ammontare dei tassi di interesse fissi e variabili da corrispondere. Un importante meccanismo implementato nel protocollo è la tokenizzazione delle riserve, ovvero la creazione e distruzione di rappresentazioni digitali dei token depositati sulla piattaforma. Quando un utente invia i propri fondi al contratto di Aave riceve in cambio altri token generati dal contratto, definiti "*aTokens*", la cui funzione è quella di rappresentare il deposito e l'ammontare degli interessi maturati su di esso. Ogni *pool* possiede delle riserve liquide la cui funzione è di garantire la possibilità di ritiro in qualunque momento. Per prendere a prestito dalle riserve è necessario depositare un collaterale rappresentato dalle valute che la *pool* decide di accettare a garanzia del prestito. La quantità di valuta che può essere presa a prestito dipende dalla disponibilità delle riserve stesse e dall'ammontare del collaterale depositato. Per ciascuna di esse viene infatti calcolato il Loan-To-Value (LTV) come media ponderata dei singoli LTV di ogni valuta nella riserva, utilizzando come coefficiente di ponderazione il valore equivalente in ETH del collaterale depositato.

Le variazioni del controvalore in ETH del collaterale possono causare la liquidazione dello stesso. Per determinare la soglia di liquidazione si utilizza l'omonimo indicatore, calcolato anch'esso come media ponderata delle soglie di liquidazione scelte per ogni valuta presente nella riserva. Se il valore in ETH della percentuale di collaterale rappresentata dalla soglia di liquidazione scende al di sotto del valore totale in ETH preso a prestito dalla *pool* più i costi di transazione per trasferire i fondi in caso di liquidazione, l'algoritmo procede alla vendita forzata del collaterale. Questa consiste nella possibilità da parte degli utenti con sufficiente liquidità di acquistare il collaterale ad un prezzo scontato e destinando una quota di esso al rimborso del prestito in tal modo ripristinando l'equilibrio.

Caratteristica dei prestiti è quella di essere a tempo indeterminato, con la possibilità di scegliere tra tasso variabile e fisso. Il rimborso può avvenire parzialmente o totalmente in qualunque momento. Per la determinazione del tasso di interesse variabile si fa riferimento al concetto di utilizzazione ottimale. Per ogni valuta nella riserva l'utilizzazione ottimale determina l'intensità con cui una variazione nella liquidità disponibile comporta una variazione nel tasso di interesse. Al di sotto della soglia ottimale, il tasso di interesse, a partire da un valore fisso minimo, aumenta gradualmente fino a raggiungere il tasso applicato in

[23] Si veda il sottoparagrafo successivo.
[24] Aave, 2021: https://aave.com/.

corrispondenza della coincidenza tra ammontare preso in prestito e ammontare di utilizzazione ottimale. Superata tale soglia, l'aumento del tasso a seguito di una riduzione di liquidità aumenta di intensità[25].

Come menzionato nello stesso whitepaper, l'implementazione di un tasso fisso per un prestito a tempo indeterminato causa complessi problemi di gestione dei rischi. Sono le condizioni di mercato ad imporre l'applicazione di un determinato tasso. Variazioni repentine in tali condizioni, ad esempio nel caso di una "corsa agli sportelli", possono causare variazioni eccessivamente inique nelle condizioni di prestito offerte ai nuovi debitori. Per questo motivo gli sviluppatori della piattaforma hanno deciso di adottare una restrizione temporale alla costanza del tasso. Anziché assicurare un valore fisso a tempo indeterminato, si è voluto assicurare valori del tasso costanti per periodi di tempo determinati.

La determinazione del tasso segue la formula descritta per quello variabile, con l'eccezione della determinazione del valore minimo. Questo è calcolato tramite una media ponderata per il volume di prestiti dei tassi di interesse applicati da altre piattaforme, centralizzate e decentralizzate. Tale tasso si applica solo alle nuove posizioni aperte. Tuttavia, per mantenere contenute le differenze nei tassi di interesse applicati ai diversi utenti è stato introdotto un meccanismo di ribilanciamento del tasso, mentendo l'insieme dei tassi fissi applicati all'interno di una banda di oscillazione predeterminata[26].

L'ultima ma non meno importante funzionalità resa possibile da Aave sono i *flash loans*. Un *flash loan* consiste nella possibilità da parte dell'utente di prendere a prestito, nei limiti della liquidità disponibile, una somma qualunque senza mettere a disposizione un collaterale a garanzia. Per rendere possibile un simile prestito, le azioni che l'utente intende eseguire con la somma devono essere programmate in un contratto che rispetti gli standard stabiliti da Aave. L'esecuzione del contratto segue la seguente logica indicata nella figura.

Come indicato nella figura 12 del Whitepaper, Aave esegue le azioni del contratto e verifica che al termine di esse l'utente restituisca alle riserve la liquidità presa a prestito più una certa commissione. Se le azioni eseguite verificano tale condizione di rimborso, il contratto è eseguito con successo e il risultato registrato nella blockchain. Essendo le azioni eseguite in un arco temporale più breve rispetto a quello di validazione del blocco successivo, un insuccesso delle azioni consente di annullare gli effetti prodotti dal contratto di esecuzione semplicemente annullando la registrazione delle transazioni effettuate dall'utente con la liquidità presa a prestito. Il principale utilizzo dei *flash loans* consiste nell'esecuzione di strategie di arbitraggio tra i token disponibili sulla piattaforma stessa. Il loro fascino, tuttavia, consiste nel dare la possibilità a chiunque trovi opportunità di arbitraggio profittevole di eseguirle in assenza del capitale necessario a renderle sufficientemente profittevoli. Riassumendo con le parole usate in un paper recentemente pubblicato da ING

[25] Per visualizzare la formula, si rimanda alla sesta pagina del whitepaper di Aave: https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf.

[26] Per un approfondimento del meccanismo vedere pagina 18 del whitepaper di cui alla nota precedente.

Group: "I flash loan consentono ai debitori senza disponibilità di capitale di eseguire scambi (spesso arbitraggi) prendendo a prestito fino a milioni di dollari senza la necessità di depositare collaterale"[27].

Attualmente, il valore totale dei prestiti concessi su Aave si aggira intorno ai 19 miliardi di dollari. Nonostante l'innovatività di una simile piattaforma, non mancano problemi principalmente legati alla compliance con le normative di antiriciclaggio e Know Your Customer attualmente in vigore sia in Europa che negli Stati Uniti. Ulteriori complicanze derivano dall'assenza di un'assicurazione sui depositi in criptovalute, limitando l'attuale utilizzo ad investitori retail disposti a sopportare il rischio per beneficiare di tassi migliori rispetto all'attuale mercato monetario. Un'evoluzione è certamente in atto, ma per garantire la futura espansione di piattaforme come Aave, è decisamente necessaria non solo maggiore chiarezza normativa, ma anche l'implementazione di tecnologie che rendano possibile integrare direttamente sulle piattaforme meccanismi di applicazione della legge vigente[28].

3.2 Decentralized Exchanges

Con la nascita di migliaia di nuovi token su Ethereum è inevitabilmente aumentata la domanda di piattaforme di scambio di tali token. Ad oggi, esistono due tipologie di *exchange* di criptovalute: centralizzati e decentralizzati. Il funzionamento degli *exchange* centralizzati non porta con sé nessun carattere di innovatività rispetto al funzionamento degli *exchange* tradizionali se non per quanto riguarda la tipologia di *asset* scambiata. Il meccanismo di esecuzione e gestione degli ordini si basa come al solito su un *centralized limit orderbook e* sull'attività di fornitura di liquidità da parte dei market makers remunerata attraverso l'applicazione di un *bid-ask spread* sul prezzo di mercato. Il cuore del funzionamento di un Decentralized Exchange (o DEX) consiste invece nell'utilizzo di un meccanismo di gestione algoritmica della liquidità noto con il nome di *Automated Market Making*, di cui si discuterà a breve. Nonostante l'innovatività introdotta dai DEX, l'*Automated Market Making* porta con sé un serie di rischi e svantaggi per la fornitura di liquidità che non consentono il raggiungimento dei livelli di efficienza offerti dalla concorrenza centralizzata. Inoltre, essendo un DEX, nei casi più rilevanti, un insieme di *smart contracts* operanti su Ethereum, l'ordine di esecuzione delle transazioni e la conferma della finalità delle stesse avviene solo nel momento in cui queste sono state registrate sulla blockchain. Essendo lo spazio di archiviazione dei singoli blocchi limitato, i miners tenderanno a dare precedenza agli ordini disposti a pagare commissioni di transazione più elevate, aumentando le latenze sopportate dagli investitori meno abbienti. Nonostante ciò, la democratizzazione nella partecipazione al funzionamento dei meccanismi finanziari rappresenta tutt'ora un fattore critico di successo per l'utilizzo su larga scala dei *Decentralized Exchanges*.

[27] Meegan, X.; Koens, T., Lessons learned from Decentralised Finance: https://new.ingwb.com/binaries/content/assets/insights/themes/distributed-ledger-technology/defi_white_paper_v2.0.pdf.

[28] Auer, Raphael, Embedded supervision: how to build regulation into blockchain finance. BIS working paper, 16 settembre 2019: https://www.bis.org/publ/work811.htm.

3.2.1. Automated Market Making

L'*automated market making* è un algoritmo impiegato per la gestione decentralizzata della liquidità utilizzando delle riserve di asset, le cosiddette *pool*, depositati da utenti volenterosi di beneficiare delle commissioni di scambio. Esso prevede che gli utenti che vogliano fornire liquidità depositino sulla piattaforma quantità di due diversi crypto-asset di egual valore secondo il prezzo di mercato al momento del deposito. Contro il deposito l'utente riceve un token rappresentativo del diritto di ritirare i token inizialmente depositati. Per gestire la liquidità buona parte dei DEX utilizzano la formula del prodotto costante. Tale formula prevede che il prodotto tra le quantità dei due token inizialmente depositati debba mantenersi costante nel tempo. Ciò significa che un aumento della domanda di un token rispetto ad un altro determina una riduzione della quantità del primo rispetto al secondo nelle disponibilità del fornitore. Un esempio numerico può aiutare a comprendere il meccanismo.

Ipotizziamo che il prezzo attuale di un ETH sia di 100 USDT[29]. L'utente deposita quantità di egual valore in una pool di liquidità per un determinato cambio, in questo caso per il cambio ETH/USDT vengono depositati 1 ETH e 100 USDT. Il prodotto di tali quantità è mantenuto costante per definizione. Il prezzo, invece, è definito come il rapporto tra la quantità di USDT presenti nella pool rispetto a quella di ETH. Le formule [1] e [2] formano il sistema di equazioni impiegato per la gestione della liquidità.

$$Quantità_{ETH} \times Quantità_{USDT} = costante \qquad [1]$$

$$Prezzo_{ETH} = \frac{Quantità_{USDT}}{Quantità_{ETH}} \qquad [2]$$

Da tale sistema di equazioni è possibile determinare come la variazione del prezzo influenza le quantità di token presenti nella pool.

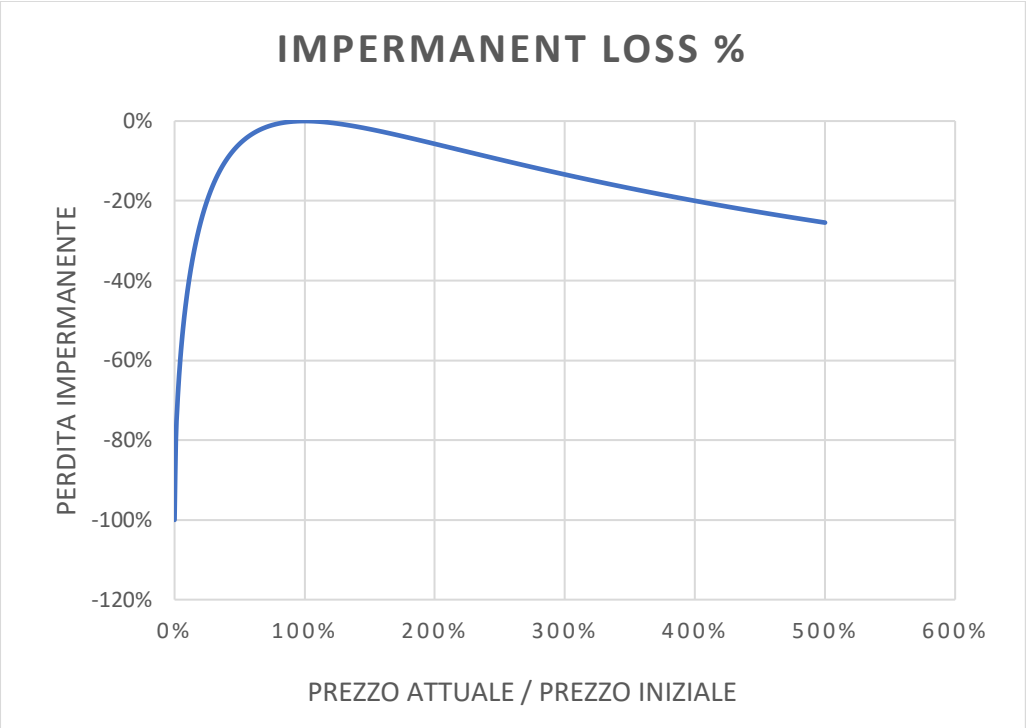
$$Quantità_{ETH} = \sqrt{\frac{costante}{Prezzo_{ETH}}} \qquad [3]$$

$$Quantità_{USDT} = \sqrt{costante \times Prezzo_{ETH}} \qquad [4]$$

Ipotizziamo che il prezzo aumenti a 130 USDT per ETH. Secondo le formule [3] e [4] le quantità di token della pool saranno di circa 114.018 USDT e 0.877 ETH, per un valore totale di 219.26 USDT. Da questo risultato emerge il rischio a cui i fornitori di liquidità sono esposti. Se i token non fossero stati depositati nella

[29] Il dollaro Tether (USDT) è una criptovaluta il cui valore è ancorato al dollaro la cui funzione principale è di semplificare la gestione della liquidità sulle piattaforme di negoziazione di criptovalute.

pool, sulla base del nuovo prezzo, il loro valore sarebbe di 220 USDT. La fornitura di liquidità è dunque costata 0.74 USDT. Le perdite di questo tipo vengono definite *impermanent loss* in quanto esse vengono annullate dall'eventuale ritorno del prezzo al suo valore iniziale, escludendo le commissioni di scambio ricevute. Sempre sulla base del sistema di equazioni inizialmente definito, è possibile derivare il rapporto tra la variazione del valore degli asset nella pool e il loro valore se non fossero stati depositati, in funzione della variazione percentuale del prezzo.



[30]

Osservando il grafico si può notare come le variazioni del prezzo in entrambe le direzioni causino una perdita al fornitore di liquidità, la cui speranza è quella di beneficiare dal pagamento delle commissioni in misura maggiore rispetto alle perdite subite.

La formula del prodotto costante non è l'unica ad essere utilizzata nel settore dell'AMM, ma è decisamente il meccanismo preferito dalla maggior parte dei DEX. Tra questi, Uniswap rappresenta un interessante esempio.

3.2.1. Uniswap

"Uniswap è un protocollo per lo scambio automatizzato di token su Ethereum. È costruito sulla base della semplicità di utilizzo, efficienza nell'utilizzo del gas, resistenza alla censura e alle influenze politiche. È utile ai traders e funziona particolarmente bene come una componente di altri *smart contracts* che richiedono garanzie di liquidità *on-chain*"[31].

[30] Figura realizzata tramite Excel.
[31] Uniswap Whitepaper: https://hackmd.io/C-DvwDSfSxuh-Gd4WKE_ig.

La nascita di Uniswap può essere fatta risalire ad un'idea proposta da Buterin nel 2016 per l'implementazione di un sistema di market making decentralizzato. Un anno dopo, Hayden Adams iniziò a lavorare alla realizzazione di questa idea trasformandola in prodotto finale. Dopo aver ricevuto fondi per $100,000 dalla Fondazione Ethereum, Uniswap venne lanciato nel novembre del 2018. Il protocollo ha fin da subito attirato l'attenzione di molti investitori, raggiungendo in un anno volumi di scambio nell'ordine delle decine di milioni di dollari[32]. Nei tre anni successivi al lancio Adams si è dedicato al miglioramento del protocollo riconoscendo alcune inefficienze proprie del meccanismo di fornitura della liquidità descritto nella sezione precedente. Con l'implementazione di due nuove versioni del protocollo sono state aggiunte diverse funzionalità, le più interessanti delle quali sono la possibilità di fornire liquidità esclusivamente in un range di prezzo prestabilito dall'utente e la creazione di un meccanismo di scambio simile al prestito istantaneo di Aave: i flash swaps. All'introduzione di questi nuovi prodotti è seguito un aumento nel valore della liquidità fornita. Si è infatti passati da un valore di circa 100 milioni di dollari nell'agosto 2020 fino ad un massimo di 8 miliardi nel maggio 2021. Secondo i dati aggiornati al 2 settembre 2021, Uniswap è il secondo DEX più liquido, con circa 7 miliardi di liquidità disponibile.[33]

3.3. Assicurazione parametrica decentralizzata

L'assicurazione parametrica, anche detta assicurazione *index-based*, è un tipo di assicurazione che affida ad un indicatore, calcolato sulla base dei dati forniti da terze parti indipendenti, la determinazione dell'entità dei pagamenti da elargire agli assicurati. Ad esempio, un possibile *payout* potrebbe essere determinato sulla base della quantità di pioggia giornaliera verificatasi in una determinata località. L'entità del pagamento assicurativo potrebbe essere stabilita in misura proporzionale all'eccedenza di un particolare valore soglia di pioggia caduta. Ad ogni modo, qualunque parametro può essere preso a riferimento per l'individuazione di un contratto di assicurazione parametrica, nel rispetto che sia oggettivamente misurabile e goda di una certa correlazione con le perdite subite dall'assicurato. Rispetto ai normali contratti di assicurazione, dove la determinazione dei rimborsi dipendono dalla perizia di un esperto scelto dalla società di assicurazione, l'assicurazione parametrica garantisce una maggiore velocità di rimborso del danno emergente o del lucro cessante, l'oggettività nella determinazione dell'entità del rimborso e la possibilità di offrire assicurazione su eventi difficili da rappresentare con modelli statistici.

Un'ulteriore caratteristica è la flessibilità offerta dai contratti. Ciascun cliente ha infatti la possibilità di scegliere i termini contrattuali che ritiene più consoni ai rischi sostenuti. Ciò che deve fare è concordare i pagamenti corrispondenti al raggiungimento di particolari valori da parte dell'indicatore scelto. Inoltre, le possibilità offerte dall'assicurazione parametrica estendono l'attuale copertura del mercato assicurativo. Infatti, la possibilità di automatizzare i pagamenti e l'inutilità di una perizia per la determinazione

[32] Fonte dati: DeFi Pulse: https://defipulse.com/uniswap.

[33] Fonte dati: DeFi Pulse: https://defipulse.com/.

del danno riducono i costi di transazione. Ciò consente di offrire servizi di cosiddetta micro-assicurazione. Un esempio può essere l'assicurazione contro ritardi o cancellazioni di voli aerei.
Tuttavia, l'assicurazione parametrica comporta l'assunzione da parte dell'assicurato di una nuova forma di rischio. Stabilire il pagamento sulla base di un indicatore non significa infatti garantire la copertura delle perdite. Il grado di correlazione tra l'evento casuale misurato nell'indicatore e le perdite subite difficilmente risulta costante nel tempo. L'assicurato dovrà dunque sopportare il rischio di ricevere un rimborso inferiore rispetto all'entità del danno subito. Tale rischio non consente l'applicazione dell'assicurazione a settori in cui l'importanza della copertura dalla perdita di valore supera la velocità di ottenimento dei fondi assicurativi. Tuttavia, l'assicurazione contro calamità naturali in grado di generare danni di notevole entità può essere considerato un possibile caso di applicazione. Spesso, in seguito a tali eventi, la necessità di liquidità per far fronte a misure di ripresa dalla crisi giustifica il rischio di un discostamento della somma ottenuta rispetto al danno subito.
Per ora non si è ancora parlato della caratteristica di decentralizzazione menzionata nel titolo del paragrafo. È facile, però, inserire il concetto di assicurazione parametrica nel contesto della decentralizzazione permessa dall'utilizzo di contratti intelligenti sulla blockchain. Infatti, una prima necessità per l'automazione dell'esecuzione dei pagamenti è rappresentata dalla garanzia di immutabilità del codice che esegue la transazione. Uno *smart contract* soddisfa perfettamente tale bisogno di garanzia. Una volta programmato il contratto con i parametri convenuti dalle parti, la sua pubblicazione sul registro distribuito consente la verifica dell'esattezza dei termini dell'accordo e garantisce la correttezza di esecuzione del contratto.
Un secondo ordine di problemi riguarda l'affidabilità delle fonti di dati esterne. Anche in questo caso, l'infrastruttura decentralizzata della blockchain offre una soluzione tramite l'impiego di un oracolo come ChainLink, descritto al paragrafo 2.3. Non a caso, è proprio quest'ultimo protocollo ad essere utilizzato per la fornitura di dati ad uno dei servizi di assicurazione parametrica il cui funzionamento è interamente basato sull'impiego della tecnologia blockchain: Arbol.

3.3.1. Arbol

Arbol è una società con sede a New York operante nel settore delle assicurazioni che utilizza la blockchain Ethereum e il sistema di oracoli decentralizzato ChainLink per offrire prodotti di assicurazione parametrica nel settore agricolo ed energetico. Tra i prodotti offerti da Arbol figura l'assicurazione sul rendimento dei raccolti basata sulle rilevazioni di pioggia caduta, temperatura e umidità nelle località nelle quali operano gli assicurati. La società promette di ridurre consistentemente i costi e le tempistiche delle tradizionali società di assicurazione. Nel gennaio del 2021 Arbol ha annunciato di aver completato il primo round di finanziamenti da parte di *Venture Capitalists* raggiungendo una somma pari a 7 milioni di dollari in nuovo capitale di

rischio[34]. La stipula del contratto assicurativo avviene attraverso la registrazione alla piattaforma *web*, la selezione del settore di interesse e la scelta dell'indicatore da prendere a riferimento per il calcolo dei *pay-out*. Definiti i termini del contratto, il sito si occupa del loro inserimento nella logica del programma e della registrazione di quest'ultimo sulla blockchain. Attualmente, il portafoglio prodotti di Arbol consiste di 25 prodotti assicurativi. Inoltre, la società vanta più di 700 clienti istituzionali e un miliardo di dollari in capacità di assorbimento dei rischi.

La crisi pandemica globale causata dal COVID-19 ha mostrato le fragilità di diversi settori economici, incluso quello assicurativo. La situazione di crisi vissuta in particolare dalle piccole e medie imprese è stata esacerbata dalla lentezza delle tradizionali imprese assicurative nel fornire la liquidità necessaria alla sua gestione. Si pensi al caso della società americana Century 21, la quale ha dichiarato di essere stata costretta a presentare richiesta di protezione dalla bancarotta per il rifiuto da parte della società di assicurazione di pagare circa 175 milioni di dollari dovuti secondo contratto[35]. La riduzione delle tempistiche di erogazione dei fondi assicurativi è un tema di estrema rilevanza per la diffusione dei servizi di assicurazione parametrica. Nonostante quest'ultima non sia da ritenersi un'alternativa completa ai tradizionali modelli di business del settore, una maggiore sensibilità nella percezione dei rischi, in buona parte legata alla maggiore instabilità causata dalla crisi climatica in settori economici quali quello agricolo, logistico e del turismo, rappresenta un fattore critico per l'aumento della quota di mercato da parte delle società che propongono questo nuovo modello. In più, le caratteristiche di trasparenza, finalità e flessibilità offerte dalla blockchain hanno la possibilità di contribuire in modo rilevante ad incentivare l'utilizzo di questa nuova tecnologia nel processo innovativo che sta interessando il settore finanziario tradizionale.

[34] Smith, Ian; "Investors flood into parametric insurance", Financial Times: https://www.ft.com/content/f77f3471-fa94-4971-809f-49d8414deed2.

[35] Thomas, Lauren; "Discount retailer Century 21 files for Chapter 11 bankruptcy and is closing all of its 13 stores", CNBC: https://www.cnbc.com/2020/09/10/discount-retailer-century-21-files-for-bankruptcy-to-close-all-stores.html.

4. IL CONTESTO NORMATIVO

L'approccio all'elaborazione di un quadro normativo per le "cripto-attività" e le valute virtuali ha seguito, specialmente in Europa e negli Stati Uniti, un approccio *bottom-up*. L'iniziale scarsa rilevanza di questa nuova tipologia di *asset* per la protezione degli investitori e la trascurabile contribuzione all'aumento del rischio sistemico hanno contribuito a far sì che in un primo momento la relativa regolamentazione fosse adottata in modo discrezionale dai singoli Stati. Con il tempo, la maggiore rilevanza acquisita in termini di valore scambiato e capitalizzazione di mercato delle criptovalute ha richiesto un approccio federale da parte del Congresso degli Stati Uniti e della Commissione Europea. Ad oggi, le istituzioni interessate dalla produzione normativa sono diverse.

Negli Stati Uniti la nomina di Gary Gensler, ex titolare di un corso riguardante blockchain e protocolli di consenso al MIT, a presidente della *Securities and Exchange Commission* il 17 aprile 2021[36] è stato un chiaro segno dell'intenzione di elaborare una regolamentazione esaustiva e in grado di mantenere la sua efficacia nonostante i rapidi cambiamenti tecnologici che caratterizzano un settore che si trova ancora nella sua fase di sviluppo. Ma la competenza della SEC è limitata, secondo il *Securities Exchange Act*[37], alla regolamentazione di entità e attività legate alla definizione di contratto finanziario. La Corte Suprema di Giustizia americana ha definito nella causa *SEC v. WJ Howey Co*[38] gli elementi essenziali di un contratto di investimento: l'investimento di moneta (1) in un'impresa comune (2) con l'aspettativa di ottenere profitto (3) esclusivamente dal lavoro altrui (4)[39]. Al di là della difficoltà delle corti di appello dei circuiti federali americani di convenire sulla definizione di impresa comune, la definizione della Corte Suprema pone problemi relativamente alle cripto-attività non configurabili come contratti di investimento. A tal riguardo, il 6 febbraio 2018, in una testimonianza scritta dinanzi al *Senate Banking Committee*, il presidente della *Commodities Futures Trading Commission*, ha affermato la competenza dell'ente nella regolamentazione e supervisione dello scambio di derivati con sottostante bitcoin ai sensi della definizione di *commodity* nel *Commodity Exchange Act*[40]. Ad aumentare la frammentarietà delle fonti normative è poi la normativa in materia fiscale delegata *all'Internal Revenue Service*. Il numero delle istituzioni coinvolte richiede un elevato grado di cooperazione tra le stesse e il raggiungimento di un non facile accordo in merito a definizioni condivise di *crypto-assets*, *commodities* e contratti finanziari.

La stessa frammentarietà riguarda il contesto europeo, con le diverse scelte di regolamentazione fiscale e finanziaria delle cripto-attività operate dalle autorità competenti dei vari Stati Membri. Tuttavia, anche

[36] Press Release, Securities and Exchange Commission: https://www.sec.gov/news/press-release/2021-65.
[37] https://www.govinfo.gov/content/pkg/COMPS-1885/pdf/COMPS-1885.pdf.
[38] Securities and Exchange Commission v. W. J. Howey Co. et al., Cornell Law School: https://www.law.cornell.edu/supremecourt/text/328/293.
[39] James D. Gordon III, Defining a common enterprise in investment contracts: https://kb.osu.edu/bitstream/handle/1811/71438/OSLJ_V72N1_0059.pdf.
[40] Written Testimony of Chairman J. Christopher Giancarlo before Senate Banking Committee, Washington, D.C.: https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo37.

nell'Unione Europea sta emergendo la necessità di una regolamentazione unica che fornisca un chiaro riferimento per l'offerta di servizi legati a una tecnologia intrinsecamente sovranazionale. La rilevanza della blockchain nella rivoluzione finanziaria in atto non può più essere ignorata e se l'Unione Europea vuole rimanere coerente con i propri valori di innovatività e competitività alle sue istituzioni è richiesta la produzione di normative in grado di favorire lo sviluppo di nuove tecnologie in un contesto sicuro e trasparente.

4.1. Il contesto normativo europeo

4.2.1. La situazione giuridica attuale

I primi passi sono stati mossi dalla Corte di Giustizia dell'Unione Europea, che nel 2015 ha espresso il proprio giudizio in merito all'applicazione della *Value Added Tax* al servizio di compravendita di bitcoin offerto da un cittadino svizzero. La decisione della corte è stata quella di escludere l'applicazione dell'imposta, nonostante l'attività svolta costituisse fornitura di servizi[41]. Successivamente, nel gennaio del 2020 è entrata in vigore la *Fifth Anti-Money Laundering Directive* (5AMLD). Essa introduce quattro importanti novità per il settore delle criptovalute. Innanzitutto, predispone una modifica alla precedente direttiva (4AMLD) nel primo articolo, dedicato alle definizioni, inserendo quella di "valute virtuali": "una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente"[42]. Nonostante la definizione sia più ampia rispetto a quella americana di "*crypto-asset*", tale definizione coinvolge senza dubbio anche le valute emesse tramite tecnologia blockchain, estendendo l'applicazione della normativa a quest'ultime. Una prima estensione riguarda l'applicazione degli obblighi di informazione degli emittenti e degli *exchange* di criptovalute nei confronti delle *Financial Intelligence Units* competenti. Tra i processi informativi *standard* da adottare figurano le procedure di *Know Your Customer*, *Customer Due Diligence* e *Suspicious Activity Reports*: le prime due sono volte a permettere l'identificazione del cliente tramite l'associazione degli indirizzi del suo portafoglio digitale con alcune sue informazioni personali; la terza richiede la condivisione con le autorità competenti di attività sospette che possano implicare il coinvolgimento del cliente in attività di riciclaggio o finanziamento del terrorismo. Inoltre, alle autorità è anche concesso il diritto di richiedere informazioni su particolari clienti, facendo venir meno la caratteristica di pseudo-anonimità che la blockchain era inizialmente in grado di offrire. Infine, l'ultima novità introdotta dalla direttiva riguarda l'obbligo di registrazione degli emittenti e dei fornitori di servizi legati alle criptovalute presso le autorità finanziarie dello Stato Membro presso cui la persona fisica o giuridica emittente o fornitrice ha la residenza o la sede legale.

[41] CJEU Case C-264/14 Hedqvist: Bitcoin: https://circabc.europa.eu/sd/a/add54a49-9991-45ae-aac5-1e260b136c9e/892%20-%20CJEU%20Case%20C-264-14%20Hedqvist%20-%20Bitcoin.pdf.
[42] Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio, Articolo 1 (2) (d): https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32018L0843&from=EN.

Un'ulteriore modifica al regime giuridico antiriciclaggio applicato al settore delle criptovalute si è avuta con l'entrata in vigore nel dicembre 2020 della *Sixth Anti-Money Laundering Directive* (6AMLD). Essa consiste nell'inserire obblighi di adeguamento dei processi informativi e di controllo più stringenti, classificando i reati di natura informatica tra quelli sui quali le società emittenti o fornitrici di servizi relativi alle criptovalute hanno l'obbligo di vigilanza.

Per quanto riguarda lo scambio di criptovalute e cripto-attività nell'Unione Europea, esse vengono considerate come Strumenti Finanziari Qualificati. Ciò significa che nessuna società autorizzata tramite licenza allo scambio di tali strumenti subisce limiti alla compravendita di cripto-attività. Allo stesso tempo, ciò richiede che i nuovi fornitori di servizi in cripto-attività debbano adeguarsi al rispetto delle normative a cui sono soggetti gli istituti finanziari europei tra cui la *Markets in Financial Instruments Directive II* e la *Electronic Money Directive II*.

4.2.2. Futuri sviluppi

Nel settembre 2020 la Commissione Europea ha presentato una proposta per l'adozione di un Regolamento avente ad oggetto i "Mercati in cripto-attività". Secondo quanto riportato nella sezione "Contesto della Proposta", essa "fa parte del pacchetto sulla finanza digitale, un pacchetto di misure volte a consentire e sostenere l'ulteriore sfruttamento del potenziale della finanza digitale in termini di innovazione e concorrenza, attenuando allo stesso tempo i rischi"[43]. Gli obiettivi perseguiti sono quattro: la certezza del diritto, il sostegno all'innovazione, la garanzia di tutela dei consumatori e degli investitori e la garanzia di stabilità finanziaria. Il Titolo I si occupa di dare alcune importanti definizioni al fine di stabilire l'ambito di applicazione della disciplina, il suo oggetto e i soggetti coinvolti. Tra le più importanti vi è quella di cripto-attività, "una rappresentazione digitale di valore o di diritti che possono essere trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga", e quella di *token* collegato ad attività ossia "un tipo di cripto-attività che intende mantenere un valore stabile facendo riferimento al valore di diverse monete fiduciarie aventi corso legale, di una o più merci o di una o più cripto-attività, oppure di una combinazione di tali attività". Queste due categorie di cripto-attività, insieme ai "*token* di moneta elettronica"[44], individuano tre regimi giuridici specifici per ogni tipologia di *token*. Infatti, il Titolo II è dedicato a definire obblighi e responsabilità degli emittenti di cripto-attività diverse dai *token* collegati ad attività e dai *token* di moneta elettronica, che desiderino offrire al pubblico, *token* in cambio di moneta fiduciaria avente corso legale o altre cripto-attività o che richiedano l'ammissione alla negoziazione in una piattaforma di scambio. Le più importanti misure di tutela degli investitori riguardano la necessità di redigere,

[43] Proposta di Regolamento del Parlamento europeo e del Consiglio relativa ai Mercati in cripto-attività, Commissione Europea: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52020PC0593&from=EN.

[44] Secondo la proposta: "un tipo di cripto-attività il cui scopo principale è quello di essere utilizzato come mezzo di scambio e che mira a mantenere un valore stabile facendo riferimento al valore di una moneta fiduciaria avente corso legale".

notificare alle autorità competenti, ossia l'autorità finanziaria dello stato membro in cui l'emittente ha la sede legale o la residenza, e pubblicare sul proprio sito un *Whitepaper* che contenga informazioni corrette, chiare e non fuorvianti. Solo dopo la pubblicazione dello stesso è possibile procedere all'offerta al pubblico dei *token*. Il contenuto minimo obbligatorio e la forma sono disciplinati dall'articolo 5. La fase di notifica è invece volta a consentire all'autorità competente la verifica della correttezza formale e sostanziale. Nonostante l'autorità non sia delegata a concedere o negare l'autorizzazione all'emissione, può richiedere che vengano modificate o integrate informazioni nel *Whitepaper*, posticipando l'offerta al pubblico al momento in cui tali contenuti siano in linea con le disposizioni dell'articolo 5. La pubblicazione della versione finale del documento espone l'emittente a responsabilità per danni arrecati dalla pubblicazione di informazioni incomplete, non corrette, poco chiare o fuorvianti nei confronti dei partecipanti all'offerta. In tal caso l'onere della prova è a carico del possessore di cripto-attività danneggiato e l'esercizio del diritto di risarcimento sancito secondo il regolamento non esclude ulteriori azioni risarcitorie in conformità del diritto nazionale.

L'obbligo di redazione del *Whitepaper* è valido anche per gli emittenti di *token* collegati ad attività, ad eccezione degli enti creditizi che abbiano ricevuto autorizzazione conformemente all'articolo 8 della direttiva 2013/36/UE. In tal caso, però, il contenuto informativo è più ampio. Lo scopo è quello di assicurare la stabilità finanziaria evitando che le riserve detenute a garanzia del valore del *token* non siano in grado di soddisfare le richieste di rimborso diretto o l'esecuzione dei diritti di credito che i possessori vantano su tali riserve. Inoltre, in questo caso è necessaria l'autorizzazione dell'autorità competente, previa consultazione dell'ABE e dell'ESMA le quali elaborano pareri non vincolanti ad ausilio della decisione. Oltre che al diritto di negare l'autorizzazione, le autorità competenti hanno anche l'obbligo di revocare l'autorizzazione nel momento in cui vengano meno uno o più requisiti sulla base dei quali la stessa è stata concessa. Ovviamente, anche le modalità di mantenimento e gestione degli *asset* che costuiscono la riserva sono soggette al rispetto di vincoli riguardanti la tipologia di enti che possono custodire tali *asset* e la chiarezza delle politiche di investimento di tali riserve, che in ogni caso devono essere impiegate in mercati con un contenuto livello di rischio di credito, di mercato e di liquidità. Altrettanto importanti sono le modalità e le procedure utilizzate per l'esercizio dei diritti di rimborso e di credito dei possessori dei *token*, le quali devono essere chiaramente definite dall'emittente. È inoltre prevista una distinzione tra token collegati ad attività significativi e non significativi. La principale differenza consiste nel passaggio di responsabilità in capo all'ABE in materia di supervisione dell'ente in concomitanza con l'applicazione di obblighi di riserva più stringenti a garanzia della continuità dell'operatività anche in situazioni di stress di liquidità.

Per quanto riguarda i *token* di moneta elettronica, la loro disciplina è assoggettata alle disposizioni della direttiva 2009/110/CE. Le uniche eccezioni riguardano l'obbligatorietà di notifica all'autorità competente e pubblicazione del *Whitepaper* nel momento in cui il valore dei *token* emessi superi il valore di cinque milioni di euro e il divieto di concedere interessi legati al periodo di detenzione dei *token*.

L'altra categoria di soggetti regolati sono i fornitori di servizi legati alle cripto-attività. Similmente agli emittenti di *token* legati ad attività, tali servizi non possono essere offerti in assenza di un'autorizzazione

concessa dalle stesse autorità competenti in materia di token legati ad attività. Tali fornitori sono inoltre soggetti ad una serie di obblighi, quali requisiti prudenziali e organizzativi, l'obbligo di agire in modo onesto, corretto, professionale e nel migliore interesse dei clienti, l'obbligo di fornire a quest'ultimi informazioni chiare, corrette e non fuorvianti, l'obbligo di prevenire, individuare, gestire e comunicare eventuali conflitti di interesse e obblighi legati alla garanzia di corretto funzionamento della piattaforma e custodia delle cripto-attività.

Il Titolo VII della proposta riguarda, infine, l'attività svolta dalle autorità competenti. Al vertice del sistema di supervisione vi sono l'Associazione Bancaria Europea e l'*European Securities and Markets Authority*, le quali condividono tra loro le informazioni necessarie allo svolgimento dei loro compiti. Sotto la supervisione e il coordinamento delle due autorità europee operano poi le autorità dei singoli Stati Membri. Il regolamento conferisce a ciascuno di essi la possibilità di individuare autonomamente l'autorità competente in materia di supervisione. Nel caso in cui lo Stato Membro affidi la competenza a diverse autorità, è necessario definire chiaramente i compiti affidati a ciascuna di esse. Anche i poteri minimi attribuibili a tali autorità sono stabiliti dal regolamento, e riguardano nella maggior parte dei casi il potere di richiedere ulteriori informazioni ai soggetti interessati e di sospendere o cessare le loro attività nel momento in cui vi siano ragionevoli dubbi di violazione del regolamento o nel momento in cui tali dubbi siano stati confermati da successive indagini. Particolare enfasi è posta sulla cooperazione tra le autorità e gli articoli 83-85 e 90 disciplinano le modalità attraverso cui essa deve essere realizzata.

Il Capo 2 del Titolo VII si occupa di stabilire le sanzioni amministrative minime che le autorità competenti individuate dallo Stato Membro devono poter imporre ai soggetti che operano in violazione del regolamento. Infine, i Capi 3 e 4 definiscono le responsabilità, i poteri e le competenze dell'ABE sui *token* di moneta elettronica e i *token* collegati ad attività che sono classificati come "significativi", ossia rilevanti dal punto di vista della protezione degli investitori e consumatori e della stabilità finanziaria, dalla normativa.

5. RISCHI ED OPPORTUNITA' DELLA DECENTRALIZZAZIONE FINANZIARIA

5.1. Rischi e limiti della blockchain

5.1.1. Gli Hard Forks

Un primo limite della blockchain riguarda la difficoltà di gestione degli *upgrade* del codice sottostante. Essendo la logica di sviluppo *open source*, la partecipazione di una *community* di sviluppatori e validatori comporta la possibilità che una parte di questi decida di non accettare le modifiche proposte dalla maggioranza. La conseguenza di tale divisione è un "*hard fork"*[45]. A seguito dell'aggiornamento, la parte dei validatori che ha aderito modificherà le modalità di validazione dei blocchi. La parte di validatori che, invece, si è rifiutata di accettare le variazioni nel codice lavorerà su una diversa estensione della *blockchain* originale, dando vita, a tutti gli effetti, ad una nuova ed indipendente *blockchain*. Il rischio posto dagli *hard fork* è quello di un periodo di vulnerabilità in cui la *blockchain* è esposta al rischio di attacchi. Prima che la difficoltà della prova del lavoro diminuisca in risposta al minor numero di potenza di calcolo disponibile è possibile che un numero ristretto di *miners* controlli la *blockchain* e tenti di effettuare una doppia spesa. La nascita di Bitcoin Cash è dovuta proprio ad un simile evento ed ha esposto la *blockchain* di Bitcoin al rischio di un attacco. Sebbene negli ultimi anni il numero di *hard fork* sia diminuito, la possibilità che se ne verifichino degli altri è motivo di preoccupazione per il rischio posto al funzionamento dell'ecosistema finanziario operante su una *blockchain*.

5.1.2. Il difficile equilibrio tra privacy e trasparenza

Le diverse esigenze in termini di privacy e trasparenza di regolatori e utenti tendono a creare delle tensioni che complicano il raggiungimento di un equilibrio tra le due. La caratteristica di *privacy* garantita dalla *blockchain*, e in particolare da alcune criptovalute note come *privacy-coins*, è per molti utenti un fattore critico nella scelta di utilizzare questa tecnologia per detenere parte della loro ricchezza e scambiarla. D'altra parte, senza informazioni necessarie le autorità competenti in termini di supervisione si ritrovano impossibilitate nel portare avanti le prerogative a loro delegate. Tuttavia, alcune soluzioni a questa *impasse* sono state proposte. Tra queste, l'utilizzo di primitive crittografiche come le *zero knowledge proofs (ZKPs)*. Queste furono proposte per la prima volta nel 1982 da alcuni ricercatori del MIT, tra cui il premio Turing, Silvio Micali. Sebbene i calcoli matematici necessari alla dimostrazione della loro validità siano decisamente fuori dagli scopi di questa tesi, un esempio concreto può comunque aiutare a comprenderne la rilevanza nel risolvere il dilemma *privacy*-trasparenza. Le ZKP potrebbero essere usate per dimostrare che un individuo ha l'età legale

[45] Con il termine ci si riferisce ad una divisione di una catena di blocchi in due blockchain indipendenti a seguito di un aggiornamento nel codice sorgente.

per bere alcolici, senza rivelare la sua data di nascita. In questo caso, non deve mostrare per forza un documento al venditore e condividere la sua età, ma è sufficiente utilizzare un meccanismo in grado di verificare che sia nato prima di una certa data. Allo stesso modo, un individuo che sia accusato della violazione di una disposizione normativa, tramite le ZKPs, ha la possibilità di dimostrare che le sue azioni sono rimaste nell'ambito della legalità, senza dover necessariamente mostrare le azioni compiute.
Un'altra problematica, seppur circoscritta al contesto europeo, è la difficoltà di tutelare il diritto all'oblio, che nella normativa GDPR si traduce nel diritto alla rimozione dei propri dati personali dai server in cui sono stati registrati, nel contesto di un registro immutabile come la *blockchain*.
Ulteriori problemi nascono a livello di cybersecurity, in quanto i rischi per la stabilità finanziaria aumentano nel momento in cui la custodia di *asset* finanziari affidati ad un registro distribuito rimette la sicurezza di tali asset al possesso della chiave privata corrispondente all'indirizzo a cui appartengono. Perdere la chiave privata, significa perdere gli asset. Di conseguenza viene a crearsi, soprattutto per i maggiori istituti finanziari, una considerevole asimmetria in termini di rischi e benefici. A differenza delle convenzionali autenticazioni tramite *password*, la perdita di una chiave privata non prevede alcun meccanismo di recupero. Una volta persa o hackerata la chiave, la perdita è irrecuperabile e potenzialmente nell'ordine dei milioni se non dei miliardi di dollari per simili istituti.

5.1.3. Il trilemma della blockchain

Tre sono gli aspetti più importanti per l'adozione di massa della *blockchain* come infrastruttura per un sistema finanziario decentralizzato: sicurezza, decentralizzazione e scalabilità. La sicurezza è la caratteristica fondamentale. Senza di essa, la decentralizzazione e la scalabilità passano in secondo piano. La decentralizzazione rappresenta un aspetto chiave per mantenere la promessa di un sistema finanziario più accessibile. Senza decentralizzazione, la disponibilità della semplice connessione ad Internet non sarebbe sufficiente a permettere la diffusione di servizi finanziari nei Paesi più poveri, dove i costi di gestione di un sistema centralizzato non rendono conveniente l'offerta di tali servizi. Infine, la scalabilità definisce la possibilità di una *blockchain* di validare un numero sempre maggiore di transazioni al secondo. Attualmente, Visa è in grado di gestire un numero di transazioni nell'ordine delle decine di migliaia al secondo, un numero di molto superiore rispetto alle attuali *blockchain* più performanti che sono in grado di gestire tra le quattromila e le cinquemila transazioni al secondo.
Il trilemma della blockchain, presentato esposto per la prima volta da Vitalik Buterin per evidenziare gli attuali e potenzialmente futuri limiti della *blockchain*, riguarda l'impossibilità di migliorare una delle tre caratteristiche sopra descritte senza sacrificare le altre. Nonostante la verità di tale affermazione, per la maggior parte delle *blockchain* esistenti all'epoca in cui il trilemma è stato formulato, nel tempo sono nati nuovi protocolli in grado di superare l'ostacolo. Come nel caso della tensione tra *privacy* e trasparenza descritta nel paragrafo 5.1.2., è stato ancora una volta rilevante il contributo del Professor Silvio Micali. Il meccanismo

di funzionamento del protocollo *blockchain* ideato da quest'ultimo ha infatti gettato le basi per il superamento del trilemma e ha comportato la presenza di Algorand tra le cinquanta maggiori *blockchain* per capitalizzazione di mercato.

5.2. Opportunità

Secondo un articolo pubblicato il 5 maggio 2021 dal *Word Economic Forum*, circa 1,7 miliardi di persone non hanno accesso ad un conto bancario, trovandosi dunque in una situazione di svantaggio rispetto alle maggiori economie che nel frattempo riducono la circolazione di contante fisico[46]. La rimozione di autorità centralizzate che caratterizza la *blockchain* consente l'accesso a servizi finanziari, quali operazioni di deposito e prestito, attraverso la semplice disponibilità di una connessione a Internet. Con la conversione della rappresentazione di valore di un'economia in via di sviluppo da denaro contante a criptovalute effettuare transazioni non solo sarebbe costoso, ma consentirebbe a chi deriva la propria sussistenza dall'economia interna di depositare la valuta su piattaforme come Aave e usarla come collaterale per prendere a prestito il denaro per finanziare un'impresa.

Una seconda opportunità è rappresentata dalla possibilità di gestire le microtransazioni. La riduzione dei costi di transazione garantita dalle *blockchain* attualmente più performanti consente di effettuare transazioni di valore nell'ordine di frazioni di centesimi. L'utilità di simili transazioni è evidente se si considera l'esempio del modello di *business* delle riviste online. I principali guadagni di queste derivano dagli spazi pubblicitari offerti sulla rivista e dal numero di abbonamenti venduti. Tuttavia, restringere l'accesso ai contenuti pubblicati dalla rivista ai non abbonati riduce il benessere sociale. Gli individui interessati a leggere un singolo articolo che non sono disposti a pagare il valore di un intero abbonamento rinunceranno alla consultazione lasciando invariato numero di abbonati. D'altra parte, la possibilità di acquistare singolarmente gli articoli di interesse potrebbe avere effetti rilevanti sia per i lettori che per i pubblicatori. Per fare ciò, è necessario un meccanismo di gestione delle microtransazioni. Soprattutto nei protocolli di consenso diversi dalla *proof of work*, il valore economico della transazione non ha rilevanza nel momento in cui le risorse computazionali necessarie al suo inserimento nella catena di blocchi sono fornite da un elevato numero di partecipanti. La riduzione dei costi di transazione così realizzata apre le porte a nuove possibilità nello scambio di valore in Internet. In particolare, la trasformazione dei modelli di business basati sulla pubblicità in modelli di business basati sui contenuti.

Una terza opportunità è rappresentata dalla possibilità di automazione nell'esecuzione dei contratti finanziari. Come già visto nel paragrafo 3.3.1. con la blockchain è possibile elaborare contratti finanziari che si eseguono automaticamente sulla base della logica definita. Esistono numerosi casi nei quali l'esecuzione del contratto può essere automatizzata una volta che la blockchain sia in grado di scambiare in modo sicuro con fonti esterne i dati necessari all'esecuzione del contratto. Ad esempio, uno swap sui tassi di interesse potrebbe essere

[46] Kirill Evstratov, How Technology can help unbanked access e-commerce: https://www.weforum.org/agenda/2021/05/technology-help-unbanked-access-ecommerce/#:~:text=Worldwide%2C%201.7%20billion%20adults%20do,and%20not%20be%20left%20behind..

interamente gestito da un Decentralized Exchange. Le controparti potrebbero firmare il contratto impostando il tasso soglia e il nozionale di riferimento e lasciare che sia lo smart contract a gestire i flussi di casa sulla base del valore attuale dei tassi e dei periodi di regolamento in contanti. Nonostante non manchino problematiche, soprattutto dal punto di vista normativo, per l'effettiva automazione e decentralizzazione dell'infrastruttura finanziaria attuale, l'esistenza di questa possibilità rende probabile un futuro in cui istituti di intermediazione finanziaria centralizzati e programmatori blockchain collaborino per superare gli ostacoli alla realizzazione di un settore finanziario più decentralizzato, efficiente e inclusivo.

CONCLUSIONI

La fiducia è un elemento fondamentale per il corretto funzionamento di qualunque sistema finanziario. Depositare denaro in banca richiede fiducia nell'amministrazione della stessa, investire in un fondo richiede fiducia nella sua sana e prudente gestione. Fino a poco più di un decennio fa, questa fiducia non poteva che essere riposta nelle persone a cui era affidata la gestione dei più importanti istituti di intermediazione finanziaria. Grazie alla blockchain è adesso possibile accedere, sebbene in un ambito ancora molto ristretto rispetto al sistema finanziario tradizionale, a prodotti finanziari la cui garanzia di funzionamento non risiede nell'amministrazione di una società privata, ma nella tecnologia che elimina la fiducia nella controparte come elemento fondamentale per lo scambio di valore. La blockchain è infatti un protocollo informatico per il raggiungimento del consenso sociale. In particolare, il consenso riguarda lo stato di un registro in cui sono riportate le transazioni eseguite dagli utenti.

La possibilità di eseguire codice informatico attraverso un meccanismo sicuro e decentralizzato rende possibile trasferire la logica di esecuzione di moltissimi contratti finanziari direttamente sulla blockchain, consentendo automazione, efficienza e trasparenza. L'inclusività che tale trasferimento comporta è evidente nel caso delle piattaforme di prestito decentralizzate come Aave. Chiunque ha la possibilità di fornire liquidità a chi ne fa domanda ponendo la propria fiducia non tanto nella capacità dell'intermediario di selezionare accuratamente il destinatario dei fondi, quanto nella garanzia di funzionamento data dal codice sorgente della piattaforma. Ad ogni modo, i problemi della decentralizzazione finanziaria sono altrettanto evidenti. La difficoltà di proteggere gli investitori meno educati dalle truffe, che sempre più spesso vengono realizzate per mezzo di complicati programmi, è uno di questi. Anche per via di tale difficoltà si sta procedendo all'aggiornamento del quadro normativo. L'obiettivo è quello di espandere la protezione degli investitori ai nuovi prodotti finanziari offerti tramite le tecnologie emergenti.

Sebbene il sogno anarchico che ha per molto tempo ispirato buona parte dei crittografi renda molto affascianti le promesse di completa decentralizzazione del sistema finanziario, potrebbe non arrivare mai il giorno in cui la finanza mondiale opererà in assenza di istituti di intermediazione per mezzo di un registro distribuito di transazioni e applicazioni. Tuttavia, le possibilità di efficientamento dei processi offerte dalla blockchain rendono estremamente probabile l'impiego di questa tecnologia da parte degli istituti finanziari del XXI secolo. Nei dieci anni seguenti la sua prima manifestazione, migliaia di ingegneri e sviluppatori hanno dedicato tempo e risorse a migliorarne le caratteristiche. Le basi per l'armoniosa integrazione tra blockchain e finanza sono state costruite. La decisione, adesso, spetta agli operatori tradizionali.

Bibliografia:

Chaum, David; *Blind Signatures for Untraceable Payments*; Department of Computer Science, University of California Santa Barbara.

Brands, Stefan; Chaum, David; *"Minting" elettronic-cash*, 4 gennaio 1999.

Cay, Timothy; *The Crypto Anarchist Manifesto*, 1988.

Back, Adam; *Hashcash – A Denial of Service Counter-Measure*, 1 Agosto 2002.

Ethereum Whitepaper.

Akkoyunlu, E. A.; Ekanadham, K.; Huber, R.V; *Some constraints and trade-offs in the design of network communications*, ,1975.

Lamport, Leslie; Shostak, Robert; Pease, Marshall; *The Byzantine Generals Problem*.

MIT OpenCourseWare, Massachussets Institute of Technology, Blockchain and Money, Prof. Gary Gensler, Session 4: *Blockchain Basics & Consensus.*

Nazarov, Sergey; Shukla, Punit; *Bridging the Governance Gap: Interoperability for blockchain and legacy systems.* World Economic Forum, Center for the Fourth Industrial revolution, dicembre 2020.

Ellis, Steve; Juels, Ari; Nazarov, Sergey, *ChainLink A decentralized oracle network*, 4 settembre 2017.

Aave Whitepaper.

Meegan, X.; Koens, T., *Lessons learned from Decentralised Finance*.

Auer, Raphael, *Embedded supervision: how to build regulation into blockchain finance*. BIS working paper, 16 settembre 2019.

Uniswap Whitepaper.

Smith, Ian; *Investors flood into parametric insurance*, Financial Times.

Thomas, Lauren; *Discount retailer Century 21 files for Chapter 11 bankruptcy and is closing all of its 13 stores*, CNBC.

Securities and Exchange Commission v. W. J. Howey Co. et al., Cornell Law School.

James D. Gordon III, *Defining a common enterprise in investment contracts*.

Written Testimony of Chairman J. Christopher Giancarlo before Senate Banking Committee, Washington, D.C.

CJEU Case C-264/14 Hedqvist: Bitcoin.

Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio.

Proposta di Regolamento del Parlamento europeo e del Consiglio relativa ai Mercati in cripto-attività, Commissione Europea.

Evstratov, Kirill; *How Technology can help unbanked access e-commerce*.