Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica per il Management

LIBRA: UNA NUOVA FRONTIERA PER LE CRIPTOVALUTE

Relatore:
Chiar.mo Prof.
GABRIELE D'ANGELO
STEFANO FERRETTI

Presentata da:
DAVIDE MENETTO

III Sessione
Anno Accademico 2018/2019

alla mia famiglia ...

Introduzione

Le criptovalute sono una naturale evoluzione del concetto di denaro. Sviluppatesi e rese famose con il Bitcoin nel 2008, le criptovalute sono passate in poco tempo da materia per pochi appassionati ad argomento capace di catturare l'attenzione del pubblico mondiale. In un mercato a oggi composto da più di 2000 criptovalute e con un valore stimato a oltre 200 miliardi di dollari, l'interesse di banche e governi si fa sempre più vivo sia dal lato dei possibili guadagni che per la tecnologia che le accomuna: la blockchain.

La nuova entrata nel mercato è Libra, la criptovaluta di Facebook. Con la presentazione del progetto a Giugno 2019, gli appassionati di blockchain e criptovalute sono stati attratti dalle potenzialità offerte da questa nuova realtà. Allo stesso modo le banche e i governi di tutto il mondo si sono subito messi in guardia dalle potenzialità destabilizzanti che questa criptomoneta potrebbe portare all'economie nazionali e non si sono certo fatti risparmiare le critiche.

Una cosa è certa: il progetto è assolutamente ambizioso, la potenziale user base è immensa, stimata sui 3 miliardi, pone questa criptovaluta in una posizione estremamente competitiva rispetto alle due più grandi criptomonete, Bitcoin ed Ethereum, che contano complessivamente poco più di 60 milioni di utenti. L'obiettivo che si pone Libra è altresì ambizioso e nobile, con lo scopo di ridurre al minimo la popolazione *unbanked* del mondo, ovvero che non ha accesso diretto alle banche e ai servizi finanziari. Questo progetto potrebbe dare inizio ad una rivoluzione globale per l'introduzione di criptovalute e sistemi blockchain nazionali e cambiando per sempre il modo in cui

concepiamo il denaro.

La tesi è strutturata come segue:

- Nel primo capitolo si ripercorre la storia delle criptovalute, con i concetti e gli studi degli anni '90 che hanno dato vita al Bitcoin. Vengono analizzate in breve le blockchain, i potenziali ambiti di applicazione e il funzionamento della tecnologia.

- Nel secondo capitolo si introduce Libra e le organizzazioni che ruotano attorno al progetto e vengono analizzati gli obiettivi del progetto.

- Il terzo capitolo è un capitolo più tecnico, che analizza il protocollo di Libra e ne illustra il funzionamento. Viene analizzato il ciclo di vita di una transazione, dalla sua creazione al caricamento sulla blockchain, e si mostra il funzionamento del protocollo di consenso. Infine viene mostrato un esempio di un test di una transazione con il prototipo del protocollo di Libra, il testnet.

- Nel quarto ed ultimo capitolo vengono formulate delle teorie sui possibili scenari futuri di Libra. Si ripercorrono le critiche e i dubbi che sono state portate avanti dai governi e infine si analizzano le principali differenze con le altre criptomonete.

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

Introduzione alle criptovalute e al sistema Blockchain

1.1 Storia delle criptovalute

L'idea di una valuta digitale non è di certo recente, ma bensì risale a ben prima di quanto si possa immaginare. L'ormai conosciutissimo Bitcoin, creato da una persona sotto lo pseudonimo di Satoshi Nakamoto, e pubblicato nel 2008 con il pioneristico white paper *"Bitcoin: A Peer-to-Peer Electronic Cash System"*[1], non è in realtà il primo tentativo di una valuta digitale.

Il fondatore di Bitcoin infatti si avvalse di tecnologie preesistenti ed introdotte decenni prima da diversi matematici e ingegneri informatici. Primo fra tutti il lavoro avanguardistico svolto dal crittografo Ralph Merkle che nel 1980 descrisse i Merkle Trees[2]: una metodologia di hashing che garantiva sicurezza e controllo di grandi strutture dati e che fu per questo implementata trent'anni dopo nel protocollo di Bitcoin.

Nel 1991 viene teorizzato un primo prototipo di catena di blocchi firmata crittograficamente, ben 17 anni prima della pubblicazione del white paper di Bitcoin, da parte dei crittografi Stuart Haber e W. Scott Stornetta[3]. La tecnologia concepita aveva come scopo quello di ottenere il timestamp (marcatura temporale) di documenti digitali, garantendone l'autenticità e

permettendo di risolvere questioni come i diritti di proprietà intellettuale. Tale protocollo fu talmente importante per lo sviluppo e la creazione di Bitcoin, che ben tre degli 8 articoli che vengono citati nel paper di Satoshi Nakamoto e a cui egli si è ispirato riportano il nome di Haber e Stornetta.

Un altro importante tassello che ha contribuito alla nascita delle criptovalute è stato il sistema di proof of work "Hashcash" formalizzato da Adam Back nel 1997[4]. Tale meccanismo di proof of work usato per limitare l'email spam e attacchi di denial of service, viene proprio ripreso nel funziamento di Bitcoin ed implementato efficacemente come parte dell'algoritmo di mining. Per i dettagli tecnici del suo funzionamento si rimanda alle letture inerenti.

Prima di arrivare alle prime sperimentazioni vere e proprie di criptovalute, vi sono state diversi tentativi di implementazione di sistemi elettronici di pagamento. Uno di questi fu l'esperienza infruttuosa del crittografo David Chaum che nel 1983 pubblicò il documento "Blind Signatures for Untraceable Payments"[5], un sistema di crittografia che dava soluzione alla realizzazione di un anonimo sistema di pagamento per Internet. Nel 1994 tale progetto ebbe vita con la fondazione di DigiCash, la prima azienda attiva nell'ambito della moneta elettronica e dei pagamenti online, che purtroppo si insediò nel mercato prima della vera diffusione dell'e-commerce. Per questo e altri motivi[6] DigiCash dichiarò bancarotta nel 1998 e l'azienda si riorganizzò sotto il nome di e-Cash. Nonostante ciò il lavoro di Chaum gettò le fondamenta per lo sviluppo nei primi anni duemila dei più grandi colossi dei pagamenti online e di monete elettroniche come PayPall, Skrill, Stripe.

Per quanto riguarda propriamente l'ideazione di criptovalute basate su sistema blockchain, vi sono state diverse sperimentazioni prima dell'effettiva introduzione di Bitcoin nel 2008. Primo fra tutti il lavoro svolto dall'ingegnere informatico Wei Dai che nel 1998 pubblicò *"B-Money, an Anonymous, Distributed Electronic Cash System"*[7] dove introdusse l'idea di un mezzo di scambio che fosse decentralizzato, che utilizzasse un protocollo di proof of work e dove i partecipanti fossero anonimi. Nonostante il progetto B-Money non ebbe mai luce, il lavoro di Wei Dai fu fondamentale sia per lo sviluppo

di Bitcoin che per Ethereum a tal punto che la più piccola unità di Ether viene chiamata *"wei"* proprio in onore del creatore di B-Money.

Lo stesso anno un altro tentativo di criptovaluta sotto il nome di Bit-Gold fu formalizzato dall'informatico Nick Szabo. Spinto dalle inefficienze del sistema finanziario tradizionale, come la necessità di avere un intermediario di fiducia per permettere transazioni, e ispirato dalla visione di Timothy May dipinta nel manifesto *The Crypto Anarchist Manifesto*[8], l'obiettivo di Szabo, così come quello di Wei Dai, fu quello di creare una valuta digitale decentralizzata. Di seguito un estratto del documento[9] di Szabo che riassume la sua visione e che verrà ripresa in toto dall'inventore di Bitcoin:

> *"Traditional security is costly and risky... When a protocol designer invokes or assumes a TTP, (s)he is creating the need for a novel organization to try to solve an unsolved security problem via traditional security and control methods. Especially in a digital context these methods require continuing high expenditures by the TTP and the TTP creates a bottleneck which imposes continuing high costs and risks on the end user...*
>
> *The best "TTP" of all is one that does not exist, but the necessity for which has been eliminated by the protocol design, or which has been automated and distributed amongst the parties to a protocol... The latter strategy has given rise to the most promising areas of security protocol research including digital mixes, multiparty private computations, and Byzantine resiliant databases. These and similar implementations will be used to radically reduce the cost of current TTPs and to solve the many outstanding problems in privacy, integrity, property rights, and contract enforcement while minimizing the very high costs of creating and operating new TTP institutions..."*

1.2 Successo di Bitcoin

Il 18 Agosto 2008 viene registrato il dominio Bitcoin.org e poco dopo viene pubblicato il protocollo di funzionamento della criptovaluta dall'anonimo

autore Satoshi Nakamoto. Come si può notare la fondazione di Bitcoin è stata in parte una diretta conseguenza della crisi dei subprime del 2008 e del successivo tracollo dei mercati globali, che ha di seguito alimentato una crescente sfiducia di Nakamoto nei confronti dei grandi istituti finanziari. Il Genesis Block fu creato solo il 3 Gennaio 2009, che fu il giorno che sancisce ufficialmente la nascita dell'infrastruttura che sta alla base del Bitcoin: la blockchain.

Dalla prima transazione tra due utenti per l'acquisto di una pizza nel 2010 (pagata 10,000 bitcoin) al lancio di prodotti finanziari basati sui Bitcoin, come i futures autorizzati dal CME di Chicago nel 2017, questa criptovaluta sta avendo un notevole impatto rivoluzionario verso il modo in cui vengono concepite le valute e i sistemi di pagamento tradizionali.

Dalla sua fondazione ad oggi il prezzo di acquisto di un singolo bitcoin è passato da 0.003$, primo valore segnato dal New Liberty Standard exchange, al picco di 20,000$ del 17 Dicembre 2017 come si vede in figura 1.1.

Figura 1.1: Evoluzione del prezzo del Bitcoin

Nonostante il forte problema della volatilità dei prezzi, l'interesse di aziende, governi ed istituti finanziari in merito all'argomento è aumentato sempre di più. La crescita e la diffusione di sistemi di pagamento affidabili che permettono lo scambio di Bitcoin ha portato negli ultimi anni ad un aumento esponenziale delle aziende che accettano pagamenti con la criptovaluta.

Dal 2014 a questa parte l'ecosistema di startup legate al Bitcoin è cresciuto enormemente: servizi di portafogli online, exchange, cloud mining, servizi finanziari. Figure di spicco come Marc Andreessen, fondatore di Netscape, e Reid Hoffman, fondatore di LinkedIn, hanno investito 315 milioni di dollari solo nel 2014 in aziende legate alla criptovaluta.

La crescita e il successo di Bitcoin comincia proprio nel 2015, quando la criptovaluta compare per la prima volta sulla copertina dell'Economist[10]. Da qui è un crescendo. Il grande pubblico ne viene a conoscenza e Bitcoin attraversa un periodo di insolità stabilità, attestandosi ad un presso di 1000$ per coin per la fine del 2016.

Il 2017 è l'anno definitivo per la criptovaluta di Nakamoto che sarà oggetto di dibattito in tutto il mondo per via del rapidissimo rialzo dei prezzi. Nonostante alcune battute di arresto occorse a Settembre a causa di forti dichiarazioni di alcune figure, come il CEO di JPMorgan che definì Bitcoin una "frode che alimenta un'economia criminale"[11], e nonostante la China dichiarò illegali gli exchange di criptovalute nel paese, il prezzo riprese subito il suo naturale corso di rialzo fino a toccare a Dicembre quota 20000$.

I due anni successivi sono stati decisamente più in sordina per Bitcoin. Nonostante ciò il suo successo ha aperto la strada per la creazione di criptovalute alternative e per lo sviluppo di protocolli sempre più avanzati per le Blockchain. La rivoluzione messa in piedi da Satoshi Nakamoto ha portato diversi istituti finanziari a sviluppare internamente criptovalute e blockchain regolamentate, come il caso emblematico di JP Morgan che a inizio 2019 ha annunciato JPM Coin[12] per permettere inzialmente ai grandi clienti corporate di effettuare pagamenti internazionali istantanei.

Nel prossimo capitolo analizzeremo le motivazioni che stanno alla base del successo delle criptovalute ed in particolare al successo della blockchain.

Coin	Market Cap. (Mrd $)	Prezzo ($)
Bitcoin	156.7	8.507,04
Ethereum	18.9	173,19
XRP	10.1	0,230263
Bitcoin Cash	6.2	343,58
Bitcoin SV	4.6	253,95
Tether	4.1	0,901417
Litecoin	4.0	64,51
EOS	3.6	3,85
Binance Coin	2.6	16,79
Cardano	1.3	0,051836

Tabella 1.1: Prime 10 criptovalute per Market Cap. *2 Febbraio 2020*

1.3 La tecnologia blockchain

La blockchain è un libro mastro ("ledger") digitale, decentralizzato e distribuito su un network, strutturato come una catena di registri (i "blocchi") responsabili dell'archiviazione dei dati (dalle transazioni di valore ad intere applicazioni digitali). E' possibile aggiungere nuovi blocchi di informazioni, ma non è possibile la modifica o la rimozione di blocchi precedentemente aggiunti alla catena. In questo ecosistema, la crittografia e i protocolli di consenso garantiscono sicurezza ed immutabilità. Il risultato è un sistema aperto , neutrale, affidabile e sicuro, dove la nostra capacità di utilizzare e di avere fiducia non dipendono dalle intenzioni di nessun individuo o istituzione.

Questo è ciò che la blockchain è stata in grado di conquistare: il problema della fiducia è stato risolto cambiando totalmente le fondamenta del sistema, sviluppando una tecnologia in cui la fiducia è costruita intrinsecamente all'interno della tecnologia stessa. La nostra società si regge su fondamenta di *trust* costruite da diversi attori, perciò se perdessimo fiducia anche in un solo anello della catena, nessuna transazione sarebbe più possibile.

1.3.1 Le applicazioni

Le possibili applicazioni di tale tecnologia sono innumerevoli. Diversi settori stanno adottando blockhain proprietarie per far fronte a problemi differenti. Come mostrato nella figura 1.2, numerose aziende investiranno nel 2020 in progetti legati alla blockchain secondo uno studio condotto da Deloitte[13].

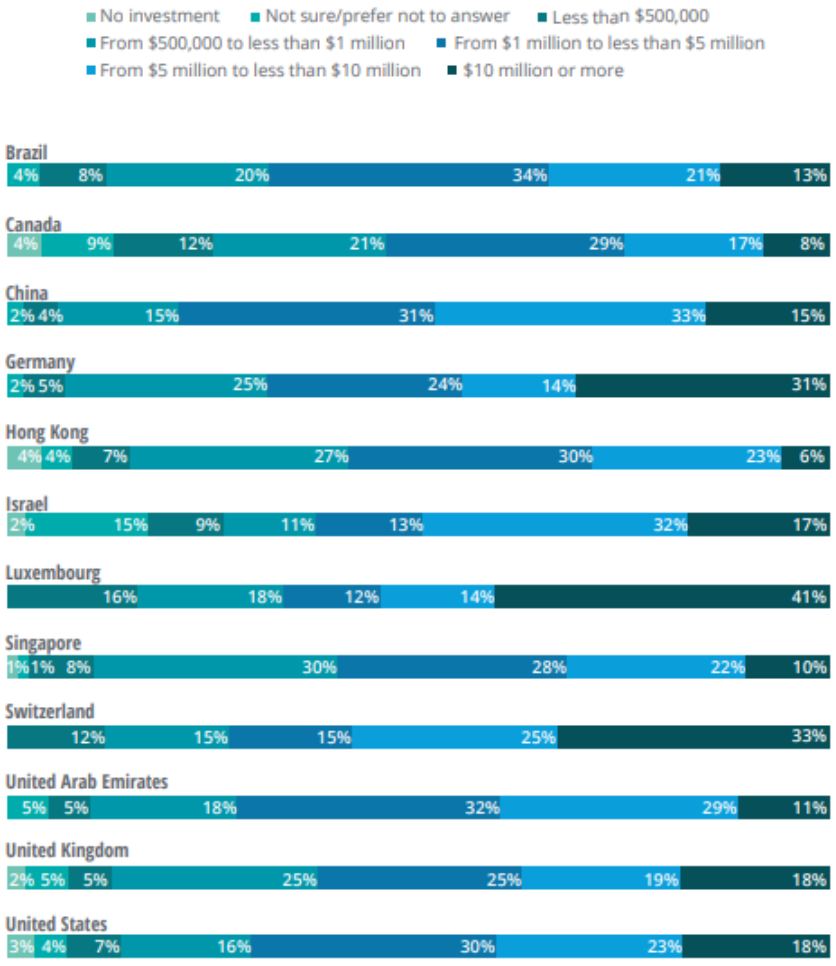

Figura 1.2: Investimenti in progetti blockchain nel 2020. Fonte: *Deloitte's 2019 Global Blockchain Survey*

Servizi finanziari

Il settore finanziario, considerato uno dei settori più lenti ad adattarsi alle nuove tecnologie, in quanto spesso rimane legato a sistemi obsoleti che ne ostacolano l'innovazione, sarebbe sicuramente migliorato in diversi aspetti: gestione dei pagamenti, custodia degli asset o trading. Un report di Santander stima un risparmio complessivo per le banche di 20 miliardi di dollari l'anno grazie all'implementazione di tecnologie blockchain [14]. Analogamente *Harvard Business School* assicura che la blockchain sarà per i servizi finanziari quello che Internet è stato per i media [15].

Anche il trasferimento di valore, che è sempre stato un processo lento e costoso, specialmente quando si tratta di pagamenti cross-border, può essere impattato positivamente dall'uso di blockhain. Per trasferire denaro al di fuori dell'Unione Europea le commisioni bancarie sono spesso elevate e i tempi di esecuzione di sicuro non sono istantanei. La tecnologia blockhain è in grado di semplificare questo processo, eliminando gli intermediari, aumentando drasticamente la velocità e diminuendo i costi. Accenture ha stimato che l'utilizzo della blockchain potrà portare alle banche risparmi complessivi per oltre 8 miliardi di dollari l'anno [16].

Supply chain

La *supply chain* (o catena di distribuzione) è la filiera logistica-produttiva che porta un prodotto da un'organizzazione a un cliente. Essa comprede il reperimento delle materie prime e dei componenti necessari all'ottenimento del prodotto finito. Oggi giorno questi processi sono diventati estremamente complessi, richiedendo decine e decine di fasi per il completamento della filiera di produzione. I problemi che intercorrono in questi passaggi sono di varia natura, come la perdita di informazioni, la complessa gestione delle diverse parti coinvolte nella logistica e i ritardi causati dalla lenta e macchinosa burocrazia. La tecnologia blockchain può aiutare questi insieme di processi fornendo tracciabilità e trsparenza dei prodotti: grazie alla sua intrinseca caratteristica di immutabilità e sicurezza dei dati è possibile salvare

ogni singolo passaggio di produzione all'interno di una blockchain, rendendolo visibile e accessibile a tutte le parti autorizzate. Anche il consumatore finale ne beneficierebbe in quanto è in grado di verificare la provenienza e l'autenticità del prodotto acquistato.

Energia

Negli ultimi anni il settore delle energie rinnovabili è cresciuto enormemente, grazie anche alla riduzione dei costi (pannelli solari) e alle politiche di incentivo per investimenti nel settore. Sembra difficile pensare ad un utilizzo di tecnologie blockchain in questo ambito così distante dal mondo dell'informatica. L'uso principale riguarda la crezione di piattaforme di scambio *peer-to-peer*, dove diventa possibile per gli utenti vendere o comprare energia senza dover necessariamente passare per degli intermediari. Un report di Pwc mostra in modo dettagliato come molte startup stiano lavorando in questo senso [17].

Applicazioni in ambito governativo

Le applicazione della tecnologia blockchain in ambito governativo e della pubblica amministrazione sono svariate. I limiti che ne rallentano lo sviluppo sono principalmente di natura burocratica piuttosto che tecnologica. Di seguito vedremo una breve lista di applicazioni nel settore pubblico:

- **Identità digitale**
  Tecnologie blockchain permettono di trovare soluzione al problema di realizzare un sistema globale di riconoscimento e di verifica di identità facilmente accessibile e non modificabile. Implementare quindi un'identità digitale per ogni essere umano, slegata dal controllo governativo e non dipendente dai documenti di identità dei vari Paesi.

- **Voto digitale**
  E' facilmente intuibile come, avendo un sistema di riconoscimento digitale per ogni cittadino, si possa ottimizzare lo scenario di un voto

tramite blockchain, riducendo sensibilmente i rischi legati a corruzione, modifica delle schede elettorali e vendita di voti. Inoltre il conteggio dei voti diventa immediato, garantendo un notevole risparmio economico.

- **Sanità**
  La blockchain può essere utilizzata per la gestione delle cartelle cliniche, con la possibilità di tenere traccia della storia medica di ogni paziente e permettendo la condivisione di queste informazioni con soggetti autorizzati oltre i confini nazionali in maniera rapida e sicura.

- **Istruzione**
  La comunità Europea ha pubblicato un report sulle possibili applicazioni della blockchain nel campo dell'istruzione [18]. Il report focalizza la sua attenzione sulla possibilità di tracciare in modo digitalizzato le conoscenze e competenze raggiunte dagli studenti in ambito accademico, disegnando quindi un profilo unico e immutabile del percorso di studi di ciascuna persona.

1.3.2 Panoramica del funzionamento

Il network

Come abbiamo definito in precedenza, la blockchain è un registro digitale immutabile e decentralizzato distribuito su un *network*. L'architettura di rete su cui si basano le blockchain è di tipo *peer-to-peer (P2P)*, ovvero ogni macchina connessa alla rete blockchain non è gerarchizzata sotto forma di client o server fissi ma sono considerate *nodi paritari* (peer).

In una rete decentralizzata, le risorse sono distribuite e possibilmente replicate nei nodi della rete e, di conseguenza, un'applicazione viene eseguita da tutti i suoi partecipanti senza generare un singolo punto di possibile fallimento infrastrutturale. Vedi figura 1.3

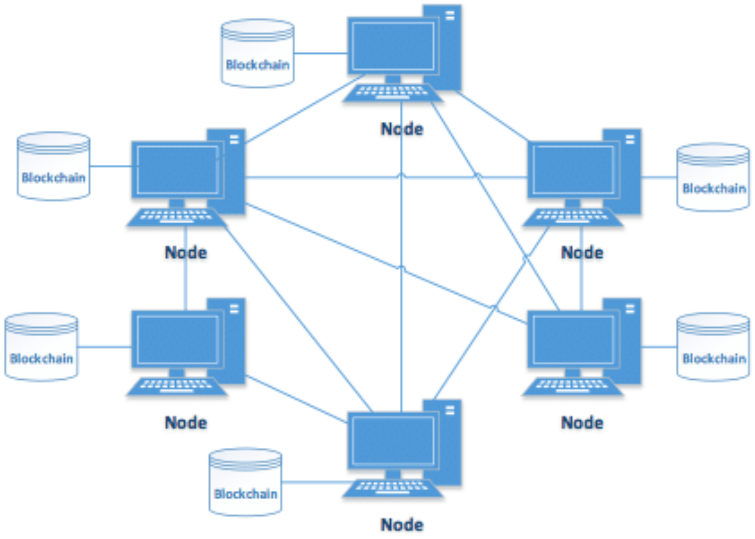

Figura 1.3: Rete P2P

Solitamente vi sono due tipologie di nodi:

- **Light-node**
  E' la tipologia di nodo tipicamente utilizzato dall'utente medio, permette di ricevere i dati di cui ha bisogno da un full-node ed effettua transazioni. Non ha la capacità di verificare in modo indipendente la correttezza dei dati/transazioni.

- **Full-node**
  Il suo compito, oltre a quello del light-node, è di scaricare e archiviare una copia completa della blockchain e controllare che ogni transazione segua le regole definite dal sistema.

Blocchi e Hashing

Come suggerisce il termine, la blockchain è letteralmente una "catena di blocchi" disposti in maniera sequenziale. La connessione tra blocchi avviene

tramite una funzione crittografica di *hash* che fornisce un collegamento matematico indissolubile tra essi. Tale funzione è utilizzata per mappare dati di dimensioni arbitrarie in dati di dimensioni fisse. E' una funzione unidirezionale: è computazionalmente molto facile generare un hash a partire da qualsiasi input, ma è molto complesso calcolare l'input partendo dall'hash. L'unico modo per passare dall'hash all'input è provare tutte le combinazioni possibili (metodo brute-force). Poichè una piccola modifica dell'input altera completamente l'hash, una volta calcolato l'hash di un blocco, qualora il blocco venisse modificato anche il relativo hash subirebbe delle modifiche.

Transazioni e Consenso

Una transazione valida è l'unità elementare di informazione che viene scritta sulla blockchain. Una blockchain ha un solo possibile stato al tempo t che sia ritenuto valido dal network. Una transazione valida implica un cambio di stato nella blockchain. Le transazioni possono essere monetarie, come l'invio di denaro, o coinvolgere altri asset digitali (stock, certificati di proprietà ecc.).

Poichè non esiste un'autorità centrale, risulta necessario trovare un modo per raggiungere un accordo sullo stato corretto della blockchain, e cioè decidere quali transazioni sono avvenute e in quale ordine. Il consenso rappresenta l'unica verità possibile sul corretto stato della blockchain, di conseguenza una transazione è valida soltanto se approvata dal network.

Una volta che una transazione è stata creata e firmata digitalmente[19], può essere propagata ai nodi limitrofi, i quali hanno il compito di verificarne la validità e decidere se propagarla ulteriormente o meno. La transazione valida viene quindi propagata ai nodi del network, ma non è ancora registrata sulla blockchain.

Il network deve arrivare ad una decisione comune seguendo un processo chiamato consenso, con l'obiettivo di validare la transazione ed inserirla nel registro immutabile che è la blockchain. I nodi che partecipano attivamente

a tale processo e che quindi aggiungono nuovi blocchi di transazioni validate sono chiamati *miner* e svolgono un processo definito *mining*.

Sono stati sviluppati diversi algoritmi per risolvere il problema del consenso in un sistema dove non ci si può fidare di nessuno. I due algoritmi più utilizzati nell'ambito delle blockchain sono la *Proof of Work (PoW)* e la *Proof of Stake (PoS)*.

Concretamente il protocollo di Proof of Work si basa sulla ricerca di un numero computazionalmente difficile da trovare, ma una volta trovato diventa facile per tutti gli altri nodi verificarne la correttezza. In un sistema di PoW, un blocco è valido solo se contiene una soluzione valida al Pow. Nel Pow-mining, i nodi del network competono per risolvere un problema matematico complesso dove l'unico modo per trovare soluzione è provare tutte le possibili combinazioni. Il primo miner che risolve il problema ha il diritto di creare il blocco successivo che viene trasmesso alla rete in attesa che gli altri nodi ne verifichino la validità. Se il blocco è ritenuto valido, il miner si aggiudica le commissioni di transazione in esso contenute ed il blocco viene definitivamente aggiunto alla blockchain.

Per incentivare i miner a generare nuovi blocchi e mantenere il network sicuro, sono previste delle ricompense come le commissioni delle transazioni incluse nel blocco ed eventualmente le criptovalute create insieme al blocco (block-reward). In questo momento, per esempio, nel Bitcoin, per ogni blocco generato, vengono generati 12.5 bitcoin che vengono assegnati al miner che crea il nuovo blocco. Di solito il numero di nuove criptovalute che vengono generate con ogni blocco diminuisce nel tempo, poichè la maggior parte delle criptovalute ha un limite nel numero massimo di coin esistenti (nel caso del Bitcoin il limite è fissato 21 milioni [20]).

Il vantaggio principale del Proof of Work è la forte garanzia di immutabilità. E' quasi impossibile modificare una transazione dopo che questa sia stata inserita in un blocco e successivamente confermata nella blockchain. Perciò modificare una transazione diventa progressivamente più difficile a mano a mano che nuovi blocchi vengono generati, in quanto bisognerebbe

ricalcolare la Proof of Work di tutti i blocchi seguenti prima che gli altri miner riescano a generare un nuovo blocco. Vedi figura 1.4

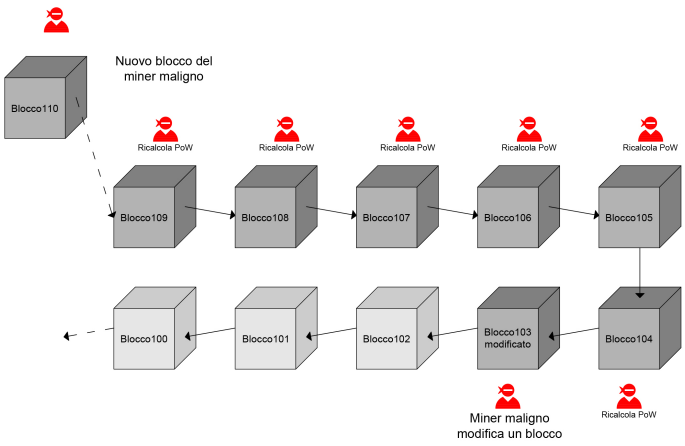

Figura 1.4: Ipotesi di modifica di un blocco da parte di un utente maligno

L'utente maligno per fare ciò dovrebbe essere in possesso di una enorme potenza di calcolo, che però a questo punto potrebbero essere sfruttate in maniera più redditizia seguendo le regole della blockchain e dei relativi rewards.

Tuttavia vi sono dei limiti nell'utilizzo di questo sistema di consenso. Uno di questi è la difficoltà nello scalare i sistemi che adottano la PoW. Molti sostengono che la lentezza delle transazioni e le commissioni elevate delle tecnologie che sfruttano la PoW stiano rallentando l'adozione su larga scala delle blockchain. E' però possibile usare soluzioni alternative senza modificare l'algoritmo di consenso, implementando soluzioni off-chain (nel caso di Bitcoin o simili, si parla di Lighting Network[21]) o modificando la dimensione del blocco.

Un altro fattore che ha sollevato diverse polemiche soprattutto tra gli ambientalisti, è relativo al massiccio consumo di energia che le reti blockchain con Proof of Work utilizzano. E' stato stimato che Bitcoin, il più grande pro-

getto che utilizza il Pow, consuma attualmente circa lo 0.3% dell'elettricità mondiale (oltre 1 milione di dollari al giorno tra elettricità e hardware per il mining [22]). Figura 1.5

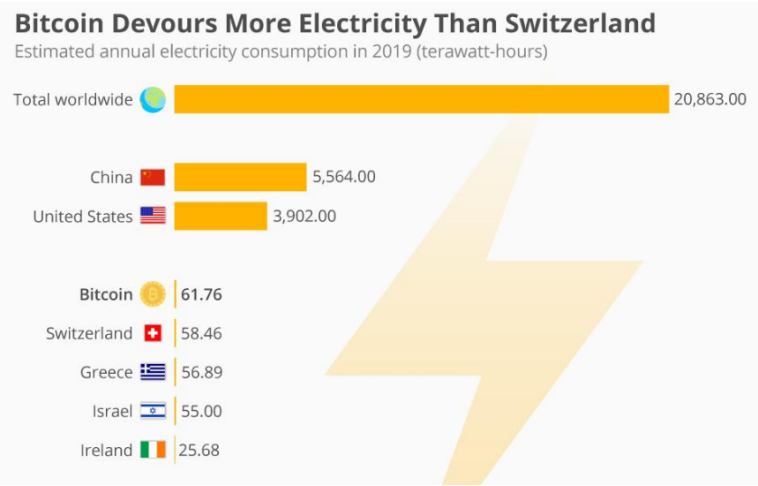

Figura 1.5: Consumo energetico Bitcoin

Come è ben evidente questi sistemi non possono essere sostenibili nel lungo periodo. Per fortuna diverse aziende stanno modificando il loro algoritmo di consenso in favore di soluzioni più *green*. Ethereum, la seconda criptovaluta per capitalizzazione di mercato, ha annunciato che è al lavoro per passare dalla PoW alla PoS (Proof of Stake) entro il 2020 [23].

Dopo questa breve analisi del funzionamento e degli applicativi della blockchain, che hanno avuto lo scopo di fissare i concetti e le potenzialità della tecnologia, il prossimo capitolo analizzerà a fondo e con spirito critico il progetto *Libra* e ne fornirà i dettagli tecnici per permetterne la comprensione.

Capitolo 2

Libra: una nuova entrata nel panorama delle criptovalute

2.1 Introduzione al progetto

Facebook introduce per la prima volta il progetto Libra il 18 Giugno 2019 con la pubblicazione del White Paper *An Introduction to Libra*[24].

> *"Libra's mission is to enable a simple global currency and financial infrastructure that empowers billions of people."*

Libra sarà gestita dalla *Libra Association*, un'organizzazione indipendente senza scopo di lucro che supervisiona il funzionamento della criptovaluta.

L'obiettivo individuato da Mark Zuckerberg è quello di realizzare una nuova blockchain decentralizzata, una criptovaluta a bassa volatilità e una piattaforma per gli *smart contract* che insieme possono creare nuove opportunità per lo sviluppo e l'innovazione di servizi finanziari differenti.

2.1.1 Il problema da risolvere

L'avvento di Internet e della banda larga ha reso possibile l'accesso a miliardi di persone ad una miriade di informazioni e a servizi a basso costo estremamente efficienti. Nonostante questo progresso, una grande porzione

della popolazione mondiale è rimasta tagliata fuori dai sistema finanziario con nessuna possibilità di accedere ai servizi offerti dalle banche tradizionali [24]. Vedi figura 2.1

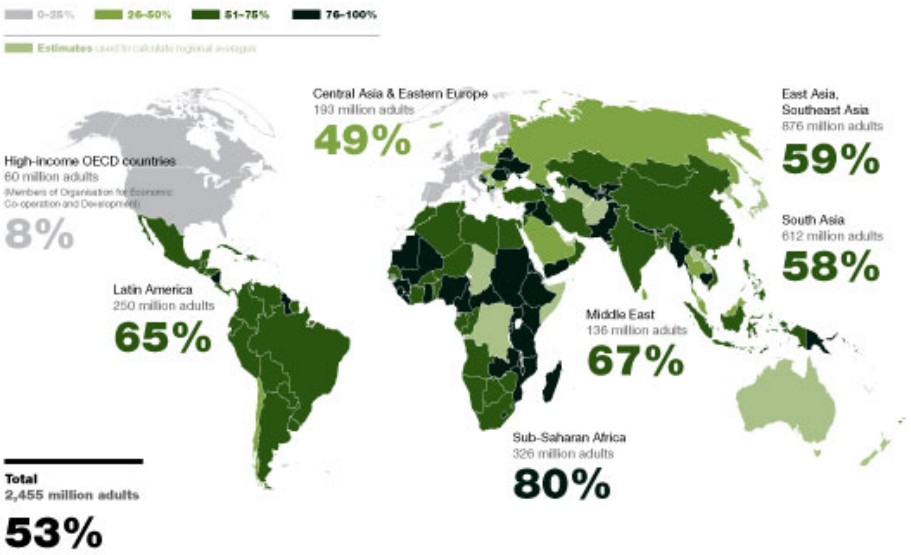

Figura 2.1: Popolazione tagliata fuori dal sistema bancario

Le persone che non possono accedere alle banche spesso è perchè non hanno fondi sufficienti per aprire un conto, o perchè gli istituti si trovano troppo distanti o anche perchè mancano della necessaria documentazione.

Questo problema è risolvibile attraverso l'utilizzo di blockchain e criptovalute che, come abbiamo detto nel capitolo precedente, eliminano l'intermediario pur garantendo fiducia e sicurezza. L'utilizzo massivo delle blockchain e delle criptovalute preesistenti è stato però frenato dalla forte volatilità di quest'ultime e dalla loro bassa scalabilità.

Libra si propone di collaborare con il settore finanziario, includendo enti regolatori ed esperti provenienti da tutte le branche dell'economia, in modo da assicurare che un sicuro, sostenibile e affidabile framework sia alla base di questo nuovo sistema.

2.1.2 The Libra Blockchain

L'obiettivo della *Libra Blockchain* è di fornire una solida base per la costruzione di servizi finanziari complessi, inclusa una nuova criptovaluta globale, che possa andare incontro ai fabbisogni finanziari di miliardi di persone.

I 2 requisiti più importanti che la blockchain dovrà soddisfare sono:

- Alta scalabilità, per garantire un numero elevato di transazioni a bassa latenza
- Elevato livello di sicurezza, per assicurare la protezione di fondi ed informazioni sensibili

Rispetto alle comuni blockchain, come Bitcoin ed Ethereum, Libra sarà una *permissioned blockchain*, ovvero i nodi validatori saranno scelti previa autorizzazione. In una *permissionless blockchain*, invece, chiunque abbia i requisiti può essere un nodo validatore e contribuire al processo di consenso (Vedi tabella 2.1). L'obiettivo finale di Libra sarà in ogni caso quello di diventare permissionless entro 5 anni dal lancio.

Caratteristiche	**Permissioned**	**Permissionless**
Accesso	Solo ai membri approvati	Aperto e trasparente
Performance	Veloce	Lenta
Costi transazione	Bassi	Elevati
Scalabilità	Potenzialmente illimitata	Limitata
Identità	Nota	Ignota o parzialmente oscurata
Trust	Trusted environment	Trust-free

Tabella 2.1: Permissioned vs Permissionless blockchain

Per lo sviluppo della blockchain e la creazione di smart contracts è stato ideato un nuovo linguaggio di programmazione: *Move*. Il linguaggio è stato progettato per rendere relativamente facile lo sviluppo di applicazioni sulla

blockchain, riducendo al minimo il rischio di brecce nella sicurezza o di bug non intenzionali.

Il funzionamento della blockchain, il protcollo di consenso e i tecnicismi riguardanti il linguaggio verranno descritti più dettagliatamente nel prossimo capitolo.

2.1.3 The Libra Reserve

Poichè la maggior parte delle criptovalute soffre di elevata volatilità dei prezzi, Libra è stata progettata per essere una *stable coin*, ovvero ancorata ad un altro tipo di attivo finanziario, come un euro, un dollaro americano o una commodity come l'oro. Questo paniere di asset reali sarà costituito dalla *Libra Reserve* e sarà composto principalmente da asset a bassa volatilità, cosicchè i possessori di Libra potranno avere delle garanzia sulla stabilità del valore della moneta. Questi asset verranno gestiti da un numero indefinito di enti distribuiti geograficamente con un elevato rating creditizio, che garantiranno decentralizzazione e sicurezza.

2.1.4 The Libra Association

The Libra Association è un'organizzazione indipendente, no-profit fondata a Ginevra, Svizzera, con l'obiettivo di coordinare e supportare lo sviluppo e l'integrazione di Libra nel mercato. L'associazione, al momento del lancio, ha ottenuto il sostegno di 27 aziende tra le quali Visa, Mastercard, PayPal, PayU, Spotify, Iliad e Coinbase. Nonostante alcune di queste si sono allontanate dal progetto per motivi che analizzeremo in seguito, il traguardo fissato da Libra Association è di raggiungere 100 partner entro metà del 2020.

Chiunque rispetti i requisiti fissati da Libra Association può entrare a far parte dei membri fondatori, con un deposito iniziale fissato a 10 milioni di dollari per ciascun membro.

Uno dei compiti più importanti dell'associazione sarà quello di gestire la *Libra Reserve* e dunque la stabilità e la crescita dell'economia di Libra.

L'associazione sarà inoltre l'unico ente in grado di creare o distruggere Libra. I coin verranno creati solamente quando un reseller autorizzato li comprerà con denaro *fiat* (legale), e verranno distrutti quando verranno venduti alla Libra Reserve in cambio degli asset sottostanti.

I membri fondatori inoltre serviranno come nodi validatori nei primi anni della moneta, con il compito effettivo di validare le transazioni ed assicurarsi il corretto funzionamento del protcollo di consenso.

2.1.5 Calibra: un wallet per Libra

Calibra è una sussidiaria di Facebook annunciata il 18 giugno 2019 e che farà il suo debutto nel 2020. Il suo compito sarà quello di lavorare su prodotti e servizi legati a Libra ed in particolare offrirà un wallet, un portafogli digitale per gestire i propri fondi. Sarà possibile inviare denaro a un contatto, senza alcun costo di commissione, con un gesto del tutto simile a quello che oggi si compie per spedire un messaggio o una foto all'interno delle chat.

A differenza di quanto avviene con altre criptovalute come Bitcoin, l'anonimato delle transazioni non sarà una delle caratteristiche di Libra. Anzi, come si legge sul sito ufficiale di Calibra, per poter entrare a far parte del network sarà necessario autenticarsi fornendo un documento d'identità valido.

Per quanto concerne la sicurezza, verrà garantita la tutela dei fondi con sistemi antifrode e tecnologie di protezione equiparabili a quelle impiegate dagli istituti bancari.

L'iniziativa guarda anche al mondo retail e all'e-commerce. Sarà possibile pagare in LBR gli acquisti nei negozi fisici e sugli store online, mediante un sistema basato su codici QR. A tal proposito, ai commercianti dovrebbe essere applicata una commissione al momento non ancora quantificata.

Il prossimo capitolo andrà ad analizzare i dettagli implementativi di Libra, il funzionamento tecnico della blockchain e del sistema di consenso utilizzato e saranno fornite delle simulazioni pratiche del funzionamento delle transazioni.

Capitolo 3

Analisi tecnica del funzionamento di Libra

3.1 Introduzione

Come abbiamo anticipato nei capitoli precedenti, Libra è una criptovaluta basata sulla Libra Blockchain, gestita dalla Libra Association e coperta da diversi asset che garantiscono stabilità nel suo valore.

Il linguaggio creato per sviluppare sulla blockchain si chiama *Move*. Move è stato progettato per essere sicuro ed affidabile: in particolare rende l'esperienza di sviluppo di applicativi sulla blockchain facile ed intuitiva, prevenendo la clonazione di asset e di bug non intenzionali. Inoltre rende agile e sicura l'implementazione delle policies di governance dell'ecosistema di Libra, come la gestione della criptovaluta e il network dei nodi validatori.

3.1.1 Il protocollo di Libra

La blockchain di Libra è fondamentalmente un database autentificato crittograficamente e mantenuto insieme dal protocollo di Libra. Questo database contiene un *ledger* di risorse programmabili, come ad esempio i Libra *coins*. Queste risorse sono possedute da diversi account autenticati grazie

alla crittografia a chiave pubblica. Il possessore di un account può effettuare delle transazioni contenenti le risorse detenute dall'account.

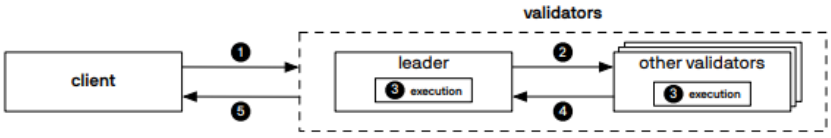

Figura 3.1: Panoramica del protocollo di Libra

La figura 3.1 mostra i due tipi di entità che interagiscono usando il protocollo di Libra: i nodi validatori, che mantengono il database, e i client, che effettuano richieste al db ed inviano le transazioni per modificarlo. I nodi validatori hanno il compito di processare le transazioni effettuate dai client e convalidarle utilizzando un protocollo di consenso distribuito (LibraBFT) che analizzeremo successivamente nel dettaglio. Un validatore *leader* invia un blocco di transazioni (sia quelle ricevute direttamente dal client che quelle ricevute indirettamente dagli altri nodi validatori) agli altri nodi validatori (2). Successivamente tutti gli altri nodi validatori eseguono le transazioni (3) e creano un struttura dati autenticata che contiene la nuova *ledger history*.

I client possono richiedere ai nodi validatori di leggere i dati contenuti sul database. Poichè il database è autenticato, i client sono certi dell'accuratezza e dell'autenticità della risposta.

3.1.2 Struttura di un account

A livello logico, un account è una collezione di risorse e moduli salvati sotto l'*account address*. Il protocollo di Libra utilizza un modello di dati account-based per codificare il *ledger state* (stato del libro mastro). Esso è strutturato secondo il modello key-value, che mappa le chiavi degli *account address* agli *account values*.

Un account address è un valore a 256-bit. Quando viene creato un account, viene generata una coppia di chiavi (*vk,sk*): una per la firma digitale,

usata per firmare le transazioni, e l'altra, trasformata in hash, viene usata per l'indirizzo dell'account `a` = `H`*(vk)*.

Il protocollo di Libra non collega gli account alle identità reali degli utenti. Un utente è libero di creare molteplici account generando le diverse coppie di chiavi.

Gli account contengono risorse e moduli. I moduli, in *Move*, sono l'equivalente degli smart contracts per le altre blockchain. Le risosrse hanno un tipo dichiarato da un modulo. Le risorse fanno riferimento ad un modulo dichiarato da un account. La figura 3.2 mostra la struttura del *ledger state* con 4 account.

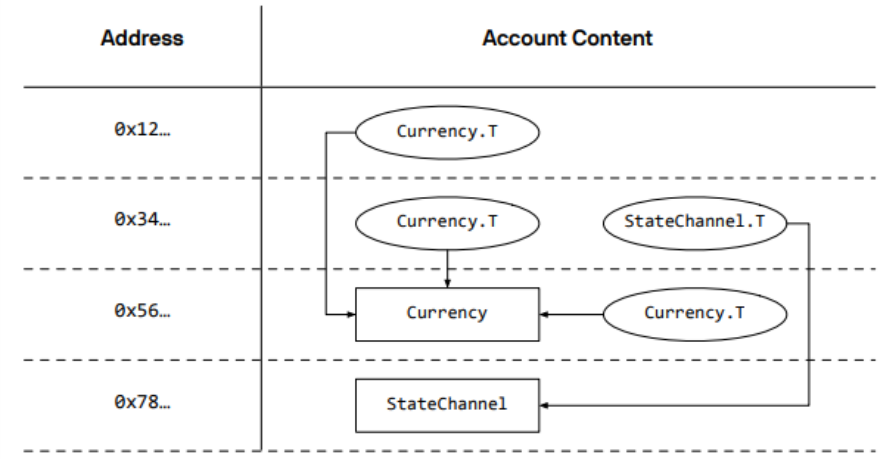

Figura 3.2: Struttura del ledger state

Nel diagramma soprastante, gli ovali raprresentano le risorse e i rettangoli rappresentano i moduli. Le freccie che collegano le risorse ai moduli, significano che quel tipo di risorsa è stato dichiarato da quel specifico modulo. L'account `0x12`, per esempio, contiene la risorsa `Currency.T` dichiarata dal modulo `Currency`. Il codice del modulo `Currency` è immagazzinato nell'account all'indirizzo `0x56`. L'account all'indirizzo `0x34` contiene sia la risorsa `Currency.T` che la risorsa `StateChannel.T`, la quale è dichiarata dal modulo salvato all'indirizzo `0x78`.

Il protocollo attuale non permette la modifica dei moduli. Una volta che un modulo è stato dichiarato sotto l'indirizzo di un account, non può essere modificato o eliminato.

Ogni account Libra ha una risorsa `LibraAccount.T`. Si può interagire con l'account in due modi: leggendo i dati dalla risorsa `LibraAccount.T` oppure chiamare le procedure del modulo `LibraAccount`.

```
module LibraAccount {
  import 0x0.LibraCoin;
  import 0x00.Hash;

  resource T {
      balance: R#LibraCoin.T,

      authentication_key: bytearray,

      sequence_number: u64,

      sent_events_count: u64,

      received_events_count: u64
  }

  ...
}
```

Figura 3.3: Modulo LibraAccount in *Move*

Come si può vedere dalla porzione di codice soprastante, ad ogni `LibraAccount` fa riferimento una risorsa `LibraAccount.T` che contiene i seguenti valori:

- Il saldo dell'account in Libra Coin
- La chiave di autenticazione
- Il numero di sequenza
- Gli eventi ricevuti

3.1.3 Il modello di rappresentazione dei dati

Tutti i dati della Libra Blockchain sono contenuti in un singola versione del database. Il numero di versione corrisponde al numero di transazioni che il sistema ha seguito. Ad ogni versione n, il database contiene le tuple che vanno da 1 a n (T_n, O_n, S_n), che rappresentano rispettivamente la transazione (T_n), l'output della transazione (O_n), e il ledger state (S_n). Il processo che avviene quando una transazione viene eseguita è il seguente: la transazione (T_n) viene eseguita contro un ledger state (S_{n-1}) che produce un output (O_n) e un nuovo stato (S_n). La funzione $F(S_{n-1}, T_n) \rightarrow (O_n, S_n))$ è una funzione deterministica. F produce sempre lo stesso stato finale per uno specifico stato iniziale ed una specifica transazione. Se lo stato corrente della blockchain è (S_{n-1}) e la transazione (T_n) è eseguita sullo stato (S_{n-1}), il nuovo stato della blockchain sarà sempre (S_n).

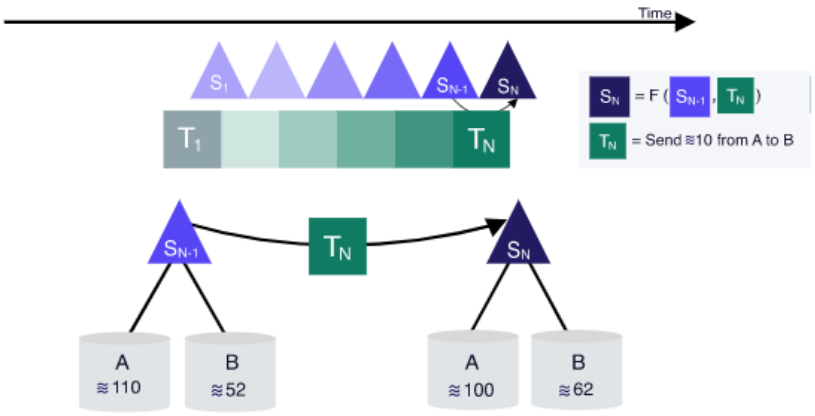

Figura 3.4: Modifica dello stato della blockchain

Eseguire una transazione cambia quindi lo stato della blockchain (vedi figura 3.4). Per esempio allo stato (S_{n-1}), Alice possiede 110 LBR e Bob possiede 52 LBR. Quando Alice decide di trasferire 10 LBR a Bob, la transazione viene applicata alla blockchain e viene generato un nuovo stato. Per passare da (S_{n-1}) a (S_n), viene eseguita la transazione (T_n) contro lo stato

(S_{n-1}). Questo comporta che il saldo di Alice diminuisce di 10 LBR e il saldo di Bob aumenta di 10 LBR. Il nuovo stato (S_n) mostra i saldi aggiornati.

3.2 Ciclo di vita di una transazione

Nel protocollo di Libra l'unico modo per cambiare lo stato della blockchain è eseguire transazioni. Per capire al meglio il ciclo di vita di una transazione Libra, la seguiremo lungo tutto il percorso che la porterà ad essere caricata sulla blockchain. Inoltre verranno analizzati i componenti logici dei nodi validatori per capirne le utilità e le interazioni con gli altri componenti.

I prerequisiti

Conoscere lo stato iniziale. Tutti i nodi validatori devono concordare sullo stato iniziale del sistema, o stato *genesi*.

Determinismo. L'esecuzione delle transazioni deve essere deterministica, cioè che l'output delle transazioni è totalmente predicibile e basato sulle informazioni contenute nella transazione e sullo stato corrente della blockchain. Questo tipo di esecuzione assicura che i diversi nodi validatori possono concordare sullo stato finale dalla stessa sequenza di transazioni anche se le transazioni vengono eseguite indipendentemente da ogni validatore.

Fees. Per gestire il carico computazionale sulla blockchain, il protocollo di Libra applica dei costi di transazione. Il comportamento è simile al *gas model* reso popolare da Ethereum [26]. L'unico obiettivo di questa tassa è di ridurre la domanda quando il sistema è sotto stress, ad esempio a causa di un attacco DoS. Il costo delle transazioni è determinato da due fattori: *gas price* e *gas cost*. Ogni transazione specifica un prezzo in Libra per unità di gas che l'utente è disposto a pagare. L'esecuzione di una transazione rappresenta e il costo computazionale associato ad essa vengono espressi sotto forma di *gas cost*. I nodi validatori danno la priorità alle transazioni con alti *gas prices*

quando il sistema è congestionato, così da ridurre la richiesta di transazioni quando il sistema è sotto stress.

Struttura di una transazione

Una transazione è un messaggio firmato che contiene le seguenti informazioni:

- **Indirizzo del mittente:** l'indirizzo dell'account del mittente è un valore di 256-bit. Non vi è collegamento tra l'account e l'identità reale dell'utente, il che garantisce pseudoanonimato agli utenti.

- **Chiave pubblica del mittente:** la chiave pubblica a cui corrisponde una chiave privata usata per firmare digitalmente la transazione. L'hash di questa chiave pubblica deve corrispondere alla chiave di autenticazione salvata nell'account del mittente.

- **Il programma:** uno script in *Move* che definisce l'operazione che il client invia al nodo validatore. L'operazione può essere una semplice richiesta di trasferimento fondi da un account ad un altro, oppure può riguardare delle interazioni con smart contracts.

- **Gas price:** il numero di Libra coins che il mittente è disposto a pagare per unità di gas, per eseguire la transazione.

- **Quantità massima di gas:** il massimo quantitativo di unità di gas che la transazione è autorizzata a consumare prima che si blocchi.

- **Numero di sequenza:** indica il numero di transazioni effettuate dall'account. Viene incrementato di uno ogni volta che una transazione viene inviata da quell'account e salvata sulla blockchain. Una transazione viene eseguita solo se corrisponde al numero di sequenza dell'account del mittente, così da prevenire i cosiddetti *replay attacks*.

Eseguire una transazione

L'esecuzione di una transazione procede attraverso una sequenza di 6 step all'interno della *Virtual Machine* del nodo validatore. In primis la transazione viene eseguita come parte di un tentativo di raggiungere il consenso sulla sua validità; solamente dopo il raggiungimento di un accordo e consenso comune la transazione viene salvata sulla blockchain.

Gli step che i nodi validatori devono eseguire sono i seguenti:

- **Check della firma digitale.** La firma della transazione deve corrispondere alla public key del mittente. Questo step è una funzione solamente della transazione e non vengono lette le informazioni del mittente durante questa fase.

- **Run del prologo.** Il prologo permette l'autenticazione del mittente della transazione, assicurandosi che abbia sufficienti *Libra coin* per pagare il numero di *gas unit* specificate nella transazione e garantendo che la transazione non è un *replay* di una transazione precedente. Più nel dettaglio, la funzione `prologue` definita in *Move* esegue le seguenti operazioni:

  - Controlla che l'hash della public key del mittente sia uguale alla sua chiave di autenticazione salvata nell'account.
  - Controlla che il `gas_price * max_gas_amount <= sender_account_balance`. Senza questo check, la transazione fallisce nell'epilogo perchè non sarebbe in grado di pagare le commissioni di transazione.
  - Si assicura che il numero di sequenza è uguale a quello salvato nell'account del mittente. Senza questo controllo un utente malintenzionato potrebbe effettuare il *replay* di vecchie transazioni.

- **Verifica dei moduli.** Una volta che il prologo ha avuto successo, la VM effettua dei controlli (*type-safety, reference-safety, resource-safety*) sui moduli. I moduli, come abbiamo definito in precedenza, sono delle unità di codice pubblicate sul libro mastro per la creazione di risorse.

- **Pubblicazione dei moduli.** Ogni modulo è pubblicato sotto l'account del mittente della transazione. I moduli duplicati sono proibiti, per esempio se una transazione tenta di pubblicare un modulo chiamato `M` su un account che contiene già il modulo chiamato `M`, lo step fallisce.

- **Run dello script della transazione.** La VM esegue lo script della transazione: se l'esecuzione ha successo, l'output viene committato sullo stato globale; se l'esecuzione fallisce nessun cambiamento viene formalizzato sullo stato globale del libro mastro.

- **Run dell'epilogo.** Al termine di tutto, la VM commissiona all'utente la quantità di gas utilizzata e incrementa il numero di sequenza dell'account. Il prologo e l'epilogo lavorano insieme per assicurare che tutte le transazioni che sono accettate nel *ledger history* vengano commissionate del quantitativo di gas definito.

3.2.1 Percorso di una transazione

Il ciclo di vita di una transazione è mostrato in figura 3.5

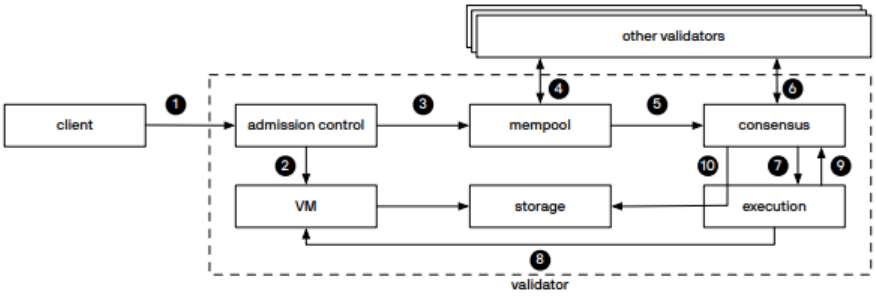

Figura 3.5: Ciclo di vita di una transazione

Una richiesta inizia quando un client effettua una transazione.

Admission control. Una volta ricevuta la transazione, l'*admission control* del nodo validatore effettua i primi controlli sintattici (1) al fine di scartare

le transazioni errate che non possono essere eseguite. Eseguire questi controlli preliminari riduce il rischio di sovraccaricamento del sistema dovuto a richieste errate. L'admission control può richiedere l'accesso alla VM (2) per effettuare ulteriori controlli, come assicurarsi che l'account ha gas sufficiente per pagare la transazione. Il nodo validatore può lanciare diverse istanze di questa componente, così da permettere di processsare più transazioni e per mitigare eventuali attacchi DoS.

Mempool. Le transazioni che passano i controlli dell'admission control sono inviate alla *mempool* del validatore, che contiene le diverse transazioni che aspettano di essere eseguite(3). La mempool può contenere molteplici transazioni provenienti dallo stesso indirizzo. Questa componente può effettuare delle operazioni che l'admission control non riesce, come assicurarsi che tutte le transazioni provenienti dallo stesso account possono pagare per il gas. Attraverso il protocollo di *shared-mempool* (4), un nodo validatore condivide le transazioni all'interno della sua mempool con gli altri nodi validatori e inserisce le transazioni ricevute dagli altri validatori nella sua mempool.

Consenso. I nodi validatori creano diversi blocchi selezionando una sequenza di transazioni provenienti dalla propria mempool. Quando un validatore che agisce come leader del protocollo di consenso, forma un blocco di transazioni dalla sua mempool. Questo blocco viene poi proposto agli altri validatori (6). Il consenso, che è la componente responsabile del raggiungimento di un accordo tra tutti i nodi validatori per l'esecuzione e la validazione di questi blocchi di transazioni, utilizza il protocollo LibraBFT che verrà analizzato nella prossima sezione.

Esecuzione della transazione. Il blocco di transazioni viene inviato alla componente di esecuzione (7), che si occupa di eseguire le transazioni nella VM (8)(vedi paragrafo precedente). Dopo l'esecuzione delle transazioni del blocco, viene costruito uno storico di queste transazioni. Infine lo storico

viene restituito alla componente di consenso (9) per concludere le operazioni di accordo.

Il blocco viene committato. Una volta che l'algoritmo di consenso ha raggiunto l'*agreement*, il validaotre legge il risultato dell'esecuzione del blocco dalla cache della componente di esecuzione e aggiorna il suo database locale (10).

3.3 Il protocollo di consenso LibraBFT

3.3.1 Il problema dei generali bizantini

Nel capitolo 1 è stato introdotto il concetto di consenso, ovvero il sistema che tiene in piedi i sistemi trustless come le blockchain dove manca l'intermediario di fiducia. Come sappiamo, raggiungere il consenso all'interno di un network distribuito non è compito facile.

Quindi, come può un network distribuito di nodi concordare su una decisione se alcuni dei nodi potrebbero fallire o agire in modo disonesto? Questa è la domanda fondamentale del cosidetto problema dei Generali Bizantini, il quale ha dato vita al concetto di Byzantine fault tolerance (BFT). Le implementazioni più comuni sono la Proof of Work (PoW) e la Proof of Stake (Pos), rispettivamente utilizzate da Bitcoin ed Ethereum, che però non sono Byzantine Fault Tolerant al 100%.

Il Problema dei Generali Bizantini è stato ideato nel 1982 [27]. Si tratta di un dilemma logico che illustra come un gruppo di generali bizantini potrebbe avere problemi di comunicazioni quando cerca di accordarsi sulla prossima mossa.

Il dilemma suppone che ciascun generale abbia la propria armata e che ciascun gruppo sia situato in diversie posizioni intorno alla città che intendono attaccare. I generali devono decidere se attaccare o ripiegare. Non importa se attaccano o ripiegano, purchè tutti i generali raggiungano il con-

senso, ovvero che tutti concordino su una decisione comune per eseguirla in modo coordinato.

I problemi di comunicazione sono legati al fatto che un generale è in grado di comunicare con un altro soltanto tramite messaggi, recapitati da un messaggero. Di conseguenza, la sfida centrale del problema dei Generali Bizantini è che questi messaggi possono arrivare in ritardo, essere distrutti o smarriti. Inoltre anche i generali stessi possono decidere (per qualsiasi ragione) di agire in modo disonesto e inviare un messaggio falso per confondere gli altri generali, portando a un totale fallimento.

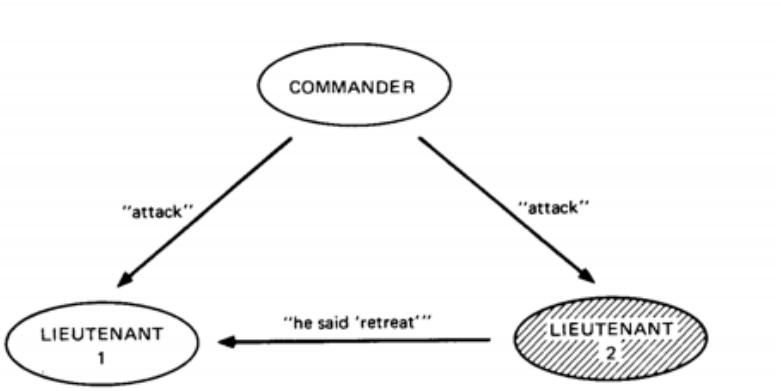

Fig. 1. Lieutenant 2 a traitor.

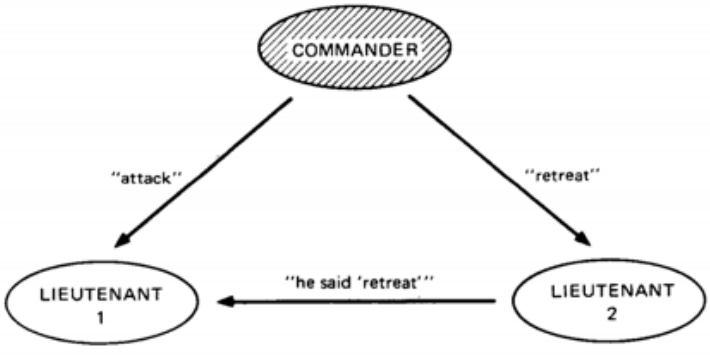

Fig. 2. The commander a traitor.

Figura 3.6: Problema dei generali bizantini nella forma "Comandante-Luogotenente"

In poche parole, la Byzantine fault tolerance (BFT) è la proprietà di un sistema che riesce a resistere alla classe di fallimenti derivata dal Problema dei Generali Bizantini. Questo significa che un sistema BFT è in grado di operare anche se alcuni nodi falliscono o agiscono in modo disonesto.

Esiste più di una soluzione al Problema dei Generali Bizantini e, di conseguenza, più di un modo per costruire un sistema BFT. Allo stesso modo, ci sono vari approcci diversi per una blockchain che intende ottenere la Byzantine fault tolerance e questo ci porta ai cosiddetti algoritmi di consenso.

3.3.2 La soluzione di Libra

Il protocollo utilizzato da Libra viene denominato LibraBFT che appartiene alla classe dei tipici algoritmi di consenso BFT. In particolare si basa su un algoritmo di consenso chiamato *HotStuff* [28], il quale a sua volta è basato su un altro algoritmo di consenso BFT chiamato Practical Byzantine Fault Tolerance (pBFT) [29].

Practical Byzantine Fault Tolerance

Il pBFT, introdotto nel 1999, utilizza un modello di sistema asincrono e distribuito dove i processi sono connessi da un network. All'interno del network possono sussistere degli errori: i messaggi possono essere duplicati, ritardati o inviati in ordine sbagliato. Se `N` è il numero totale di nodi all'interno del network e `f` è il numero dei nodi difettosi, allora il pBFT necessita di $N \geq 3f + 1$ nodi per garantire tolleranza contro i fallimenti Bizantini. In pratica il numero dei nodi maligni non deve essere equivalente o eccedere 1/3 dei nodi totali del sistema.

Essenzialmente, nel protocollo pBFT i nodi sono ordinati in sequenza dove un nodo è il *leader* e gli altri sono definiti nodi di *backup*. Il consenso si sviluppa attraverso diverse tappe chiamate *views*, dove ogni tappa raggiunge un accordo su alcuni step del processo di consenso. La figura seguente mostra le 4 fasi in cui è suddiviso il consenso. Questo sistema segue più il modello

"Comandante e Luogotenente" che il puro e semplice "Problema dei Generali Bizantini", a causa della presenza del nodo leader.

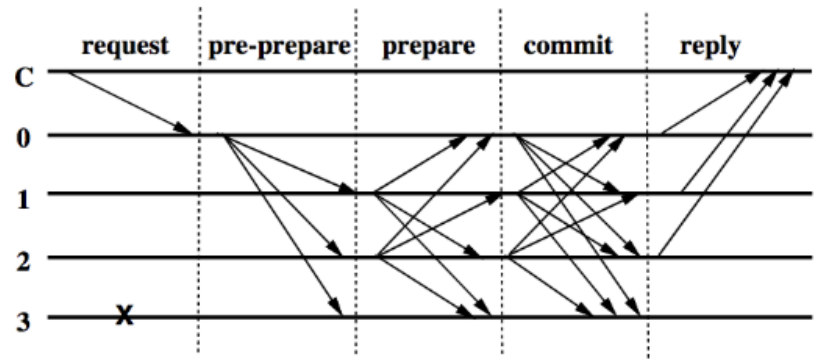

Figura 3.7: pBFT steps per il raggiungimento del consenso

1. Un client `C` invia una richiesta al nodo leader `0` per un operazione di servizio.

2. La richiesta viene inoltrata anche a tutti i nodi backup del sistema `1,2` e `3`.

3. La richiesta viene eseguita ed inviata una risposta al client.

4. Il client attende le `f + 1` (`f` è il numero massimo di nodi che possono essere difettosi) risposte con lo stesso risultato. Questo risultato è il risultato dell'operazione.

Nel caso in cui il leader fallisca, viene lanciato un protocollo di *view-change* per prevenire che i nodi di back-up attendano all'infinito messaggi dal leader. Questo tipo di situazione può essere frequente in un grande network distribuito, quindi è opportuno tenerne conto per calcolare il livello di complessità dell'algoritmo. La complessità di esecuzione del pBFT con view-change è $O(n^3)$, dove `n` è il numero di nodi attivi nel network.

Il protocollo garantisce sicurezza solo se tutti i nodi non difettosi riproducono lo stesso risultato. Questo significa che `N - f` nodi devono restituire al client lo stesso identico risultato.

Protocollo HotStuff

Il consenso HotStuff introduce delle migliorie al protocollo pBFT per quanto riguarda la complessità computazionale per raggiungere il consenso. In particolare, se il leader non fallisce, la complessità passa da $O(n^2)$ a $O(n)$, mentre nel caso peggiore in cui vi siano dei fallimenti a cascata dei leader designati e quindi viene azionato il protocollo *view-change*, la complessità passa da $O(n^3)$ a $O(n^2)$.

Protocollo	**Leader valido**	**Leader failure (view-change)**	***f* leader failures**
DLS	$O(n^4)$	$O(n^4)$	$O(n^4)$
PBFT	$O(n^2)$	$O(n^3)$	$O(fn^3)$
SBFT	$O(n)$	$O(n^2)$	$O(fn^2)$
Tendermint/Casper	$O(n^2)$	$O(n^2)$	$O(fn^2)$
Hotstuff SV	$O(n)$	$O(n)$	$O(fn)$

Tabella 3.1: Costi computazionali dei principali algoritmi di consenso BFT

HotStuff introduce anche il teorema di *liveness* del sistema che può essere riassunto come segue: sotto certe circostanze, esiste un limite di tempo entro il quale tutti i nodi non difettosi eseguono un comando e passano al turno successivo.

Theorem 4. *After GST, there exists a bounded time period T_f such that if all correct replicas remain in view v during T_f and the leader for view v is correct, then a decision is reached.*

Figura 3.8: Teorema di liveness di HotStuff

Inoltre, nel design del procollo HotStuff, vi è una miglioria nel processo di votazione. Infatti quando vi è il processo di votazione su una decisione del

nodo leader, i nodi backup inviano il loro voto firmato digitalmente solamente al nodo leader e non a tutti gli altri nodi (vedi figura 3.8).

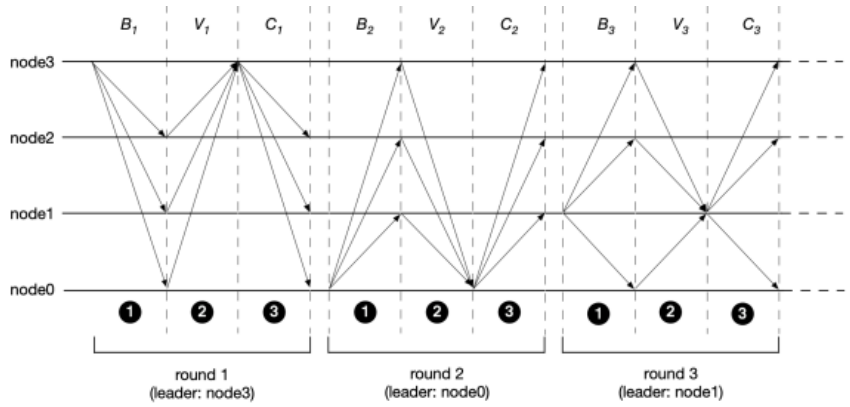

Figura 3.9: Dinamiche del protocollo HotStuff

Nell'immagine soprastante, le lettere B, V, C indicano rispettivamente "blocco", "voto" e "quorum certificate". Come si può notare i nodi leader inviano i loro voti solamente al leader e non a tutti gli altri nodi come accade nel pBFT.

Protocollo LibraBFT

Come abbiamo detto in precedenza, LibraBFT è basato su HotStuff. Secondo gli autori di Libra, sono 3 i motivi per i quali è stato scelto il protocollo HotStuff come base:

- Semplicità e modularità
- Possibilità di integrare facilmente il processo di consenso con l'esecuzione
- Elevate performance per i primi esperimenti

LibraBFT e HotStuff sono molto simili di per sè. Il design dell'infrastruttura è praticamente la stessa, come per esempio il fatto che i nodi inviano i

loro voti soltanto al loro leader e non a tutti gli altri nodi. Tuttavia, in questo protocollo viene richiesto che i nodi non leader (di backup , come abbiamo detto prima) effettuano dei *broadcast* per sincronizzare il proprio stato e per inviare dei messaggi di timeout agli altri nodi nel caso in cui ci sia un nodo leader difettoso o dei generici problemi nel network. Nonostante questo broadcast addizionale aumenti l'affidabilità e la *liveness* della rete, la complessità algoritmica della comunicazione tra nodi aumenta considerevolmente.

Inoltre LibraBFT ha la proprietà di rimanere attiva finchè esiste un *global stabilization time* (GST) dopo il quale tutti i messaggi tra validatori onesti vengono recapitati ad altri validatori onesti entro un massimo ritardo di rete δ (questo è il modello di sincronia parziale introdotto da DLS [30]). In aggiunta a ciò, LibraBFT rimane sicura e garantisce *liveness* quando i validatori crashano e restartano, anche quanto tutti i validatori crashano allo stesso momento.

LibraBFT introduce anche un ulteriore miglioria rispetto ad HotStuff per quanto riguarda il meccanismo con cui viene selezionato il leader. Il meccanismo di elezione del leader di un round è determinato dal proponente dell'ultimo blocco utilizzando una funzione casuale verificabile VR [31]. Questo meccanismo limita la finestra di tempo nella quale un nodo avversario può lanciare un attacco di denial-of-service contro il leader. In ogni caso il protocollo "LibraBFT" è ancora *work-in-progress* pertanto non sappiamo se vi saranno delle implementazioni e features aggiuntive (oltre quelle poche già citate) rispetto ad HotStuff.

3.4 Testing della Libra Blockchain

In questa sezione conclusiva verranno mostrati i risultati dei vari test che ho effettuato sul prototipo della blockchain di Libra. In particolare vengono mostrate come si svolgono le transazioni all'interno del protocollo.

In primo luogo vengono creati tre account, che chiameremo per convenienza Davide, Caterina e Luca.

```
User account index: 0, address: 32342a442c63b622f91dd488ce40de17af33a55c2
95b15965d07f22c10139828, sequence number: 3, status: Persisted
User account index: 1, address: 2d07dd9865fc406720b1cb68fac16dd2c41b476e6
c65394a8e6361712a307d15, sequence number: 1, status: Persisted
User account index: 2, address: 7a87e454330077ac576a1c8d0b7468a33e7b607ce
a25249f18add6e30f64c93f, sequence number: 0, status: Persisted
```

Figura 3.10: Vengono creati 3 account

L'output che si presenta nella figura soprastante ha la seguente configurazione: il primo numero, rispettivamente *0, 1, 2*, rappresenta l'indice dell'account di Davide, Caterina e Luca. Questo numero non ha alcun significato a livello di blockchain, è solo un modo semplice per riferirsi ad un account senza usare l'indirizzo. Il valore alfanumerico seguente infatti è l'hash dell'indirizzo dell'account che viene usato dal protocollo per riferirsi ad un determinato account. Gli account, inoltre, non vengono inseriti nella blockchain fino al momento in cui non si coniano dei coins all'interno di essi, oppure finchè non vengono trasferiti dei fondi tra un account e un altro. L'ultimo valore infine rappresenta il numero di sequenza, che corrisponde al numero di transazioni che sono partite da quell'account.

Successivamente vengono generati nell'account di Davide 31 LBR e 22 LBR in quello di Caterina. Viene deciso di trasferire 15 LBR da Davide a Caterina.

```
libra% transfer 0 1 15
>> Transferring
Transaction submitted to validator
```

La transazione viene inviata ad un nodo validatore del testnet e viene inclusa nella sua mempool. Questo non significa che la transazione viene eseguita. Infatti, se il sistema fosse rallentato per qualunque motivo, la transazione impiegherebbe un po di tempo prima di essere eseguita e bisognerebbe

effettuare delle *balance query* agli account per verificarne il successo o meno. Le informazioni della transazione inviata sono elencate di seguito.

```
libra% query txn_acc_seq 0 3 true
>> Getting committed transaction by account and sequence number
Committed transaction: SignedTransaction {
 raw_txn: RawTransaction {
         sender: 32342a442c63b622f91dd488ce40de17af33a55c295b15
         965d07f22c10139828,
         sequence_number: 3,
         payload: {,
                 transaction: peer_to_peer_transaction,
                 args: [
                         {ADDRESS: 2d07dd9865fc406720b1cb68fac
                         16dd2c41b476e6c65394a8e6361712a307d15},
                         {U64: 15000000},
                      ]
                 },
                 max_gas_amount: 140000,
                 gas_unit_price: 0,
                 expiration_time: 1583233202s,
},
 public_key: Ed25519PublicKey(1660178550d6c216820a4
 6621040485a5a8fef12b8706b7af89312e8b1ee01d7),

 signature: Ed25519Signature(
    Signature( R: CompressedEdwardsY: [104, 41, 95, 90, 221, 143,
    206, 203, 115, 178, 118, 79, 154, 188, 169, 46, 180, 38, 171,
    12, 112, 59, 230, 214, 72, 69, 73, 13, 115, 243, 246, 228],
    s: Scalar{
    bytes: [225, 120, 229, 145, 142, 148, 229, 19, 92, 151, 81,
    207, 150, 211, 54, 113, 228, 51, 157, 74, 192, 85, 34,
```

```
    66, 248, 148, 25, 89, 175, 177, 182, 3],
    } ),
),
 }
Events:
ContractEvent { key: 010000000000000032342a442c63b622f91dd488
              ce40de17af33a55c295b15965d07f22c10139828,
              index: 2,
              type: Struct(StructTag { address: 000000000000
              0000000000000000000000000000000000000000,
              module: Identifier("LibraAccount"),
              name: Identifier("SentPaymentEvent"),
              type_params: [] }),
              event_data: SentPaymentEvent {
              amount: 15000000,
              receiver: 2d07dd9865fc406720b1cb68fac16dd2c4
              1b476e6c65394a8e6361712a307d15, metadata: [] }
              }

ContractEvent { key: 00000000000000002d07dd9865fc406720b1cb68
              fac16dd2c41b476e6c65394a8e6361712a307d15,
              index: 2,
              type: Struct(StructTag { address: 000000000000
              0000000000000000000000000000000000000000,
              module: Identifier("LibraAccount"),
              name: Identifier("ReceivedPaymentEvent"),
              type_params: [] }),
              event_data: ReceivedPaymentEvent {
              amount: 15000000,
              sender: 32342a442c63b622f91dd488ce40de17af3
              3a55c295b15965d07f22c10139828, metadata: [] } }
```

E' interessante vedere tutti i parametri in formato Json contenuti nella transazione. E' presente tutto quello che è stato descritto nella sezione precedente: "Struttura di una transazione". Inizialmente vengono mostrati l'indirizzo del mittente, il numero di sequenza, il payload che contiene l'indirizzo del destinatario e il quantitativo di denaro spostato espresso in microlibra, il gas price e il massimo quantitativo di gas disposti a pagare. In seguito viene mostrata la public key e la firma digitale con la quale è stata firmata la transazione. Infine vengono lanciati due eventi relativi alla transazione: *SentPayementEvent* e *RecievedPayementEvent*.

Purtroppo allo stadio attuale del testnet, non è possibile effettuare ulteriori prove per vedere il funzionamento della blockchain. Il protocollo è ancora in fase di sviluppo e solo al lancio del sistema sarà possibile effettuare tutti i test del caso. Sarà interessante vedere quali migliorie saranno apportate prima della data di lancio del network.

Il prossimo capitolo andrà ad analizzare i possibili scenari futuri di Libra e proporrà un'analisi economica che mostrerà il possibile impatto sul mercato. Inoltre verranno estrapolate le critiche che sono state avanzate in questi mesi nei confronti del progetto al fine di comprendere al meglio i punti di forza e debolezza di questa criptomoneta.

Capitolo 4

Scenari futuri di Libra nel mondo

Una delle principali domande che ci si pone è: Quanto successo può ottenere questa moneta globale? Anche se non è possibile predire il futuro, si possono osservare le statistiche attuali delle criptovalute per formulare un'idea su che tipo di successo Libra potrebbe avere.

Per esempio è stato appurato che le transazioni effettuate con le criptovalute, specialmente Ethereum e Bitcoin, stanno raggiungendo quelle con sistemi di pagamento tradizionali. Secondo una ricerca condotta dalla rivista *News Logical*[32], le transazioni giornaliere di Bitcoin negli Stati Uniti hanno raggiunto quota 6 miliardi di dollari. Un risultato sorprendente se si pensa che i circuiti di pagamento convenzionali, come Visa e MasterCard, arrivano rispettivamente a 30 miliardi e 16 miliardi di dollari di transazioni giornaliere (vedi tabella 4.1).

Un altro esempio importante è il numero di utenti che possiedono portafogli (*wallet*) in criptovalute. Secondo uno studio del sito *Statista.com*, il numero di utilizzatori di Blockchain wallet a livello globale è passato da 10 milioni del 2016 ad oltre 42 milioni del terzo trimestre del 2019 [33].
A questi due scenari c'è da aggiungere il fatto che Facebook, il promotore principale del progetto, ha all'attivo oltre 2 miliardi di utenti, escludendo le

Circuito	Volume (mld $)
VISA	30.3
MasterCard	16.2
Bitcoin	6.3
American Express	3.2
Square	0.2

Tabella 4.1: Transazioni giornaliere dei principali circuiti di pagamento

altre piattaforme in suo possesso come Instagram e WhatsApp (vedi figura 4.1). Anche se questo non significa che tutti i suoi utenti sosterranno Libra, ne aumenta drasticamente i numeri e le potenzialità.

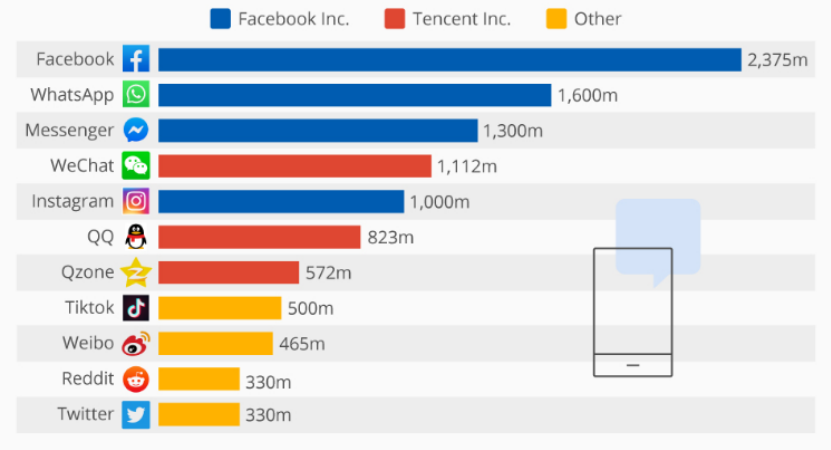

Figura 4.1: Utenti attivi dei principali social network. Fonte: *Statista.com*

L'azienda *Wikistrat*, che si occupa di crowdsourcing analysis e di consulenza, ha condotto uno studio [34] nel quale è stato chiesto ad esperti di 16 nazioni diverse di analizzare quattro scenari differenti per il futuro di Libra e della sua governance. Chiaramente queste previsioni non rappresentano tutti i possibili sviluppi di Libra, ma possono fornire un'indicazione preliminare sui diversi percorsi che può intraprendere questo progetto.

Primo Scenario: La vecchia guardia prevale

In questo scenario, i governi autorizzano l'uso di Libra solamente sotto strette regolamentazioni nazionali. Negli Stati dove Libra non partecipa e non collabora con i governi, il suo uso potrebbe essere sanzionato, ostacolato o addirittura divenire illegale. In questo scenario Libra fallisce nel suo più ambizioso intento di rompere le barriere, sopratutto monetarie, che vi sono tra le nazioni.

Vi sono diverse ragioni per cui questa situazione potrebbe divenire realtà:

- E' probabile che Libra Association sia intenzionata inizialmente a prendere accordi con i governi per espandere e diffondere la sua criptovaluta.
- Gli stati non accetteranno facilmente Libra poichè vista come una minaccia alla loro sovranità e metteranno a punto delle linee guida per contenere e ridurne l'uso sui loro territori.
- Probabilmente la Libra Association firmerà degli accordi con i diversi governi, troverà modi per conformarsi alle regolamentazioni imposte, creando allo stesso tempo un framework uniforme da poter adottare a livello internazionale.

Gli esperti enfatizzano che questo scenario potrebbe essere solo uno stadio intermedio prima che Libra raggiunga il suo potenziale globale. Una volta raggiunta la massima espansione, potrebbe essere più semplice per la Libra Association rimodellare e ridefinire le regolamentazioni nazionali per adattarle alle sue necessità.

Esistono però diverse contromisure che i governi possono adottare per assicurarsi che Libra si conformi alle loro richieste. Oltre al renderla semplicemente illegale, possono imporle regolamentazioni bancarie dichiarando la Libra Association come un'azienda che si occupa di servizi finanziari e quindi soggiogandola alle norme bancarie internazionali. Potrebbero inoltre limitarne l'uso alle piccole transazioni, escludendo la possibilità di acquistare case,

terreni e immobili di alto valore. Un'ultima soluzione sarebbe quella di rendere Libra poco interessante agli utenti imponendo, ad esempio, tassazioni alle aziende che usano e commerciano Libra.

Secondo Scenario: Il potere in mano a pochi

In questo scenario Libra lavora a stretto contatto con i governi, condividendo dati ed informazioni degli utenti di Libra con ogni nazione. Libra diventa una piattaforma globale ma operante solamente sotto leggi e regolamentazioni imposte dai vari governi. Di seguito le ragioni per il quale questo scenario risulta possibile:

- La Libra Association è stata creata essenzialmente per lavorare e collaborare con gli enti governativi

- Vi sono diverse parti interessate che possono beneficiare dall'adozione di Libra per rimanere al passo coi tempi in una economia digitale.

- Anche se i governi rigettassero l'uso di Libra, gli utenti potrebbero adottare forzatamente questo sistema di pagamento e trasferimento di denaro. In questo caso gli enti governativi sarebbero costretti a permettere l'uso di Libra, con le dovute restrizioni e regolamentazioni.

Vi sono diversi rischi che accompagnano questo scenario. Il più pericoloso riguarda sicuramente la privacy, che potrebbe essere minata dai governi che mancano di solide leggi sulla privacy e di trattamento dei dati personali. Alcuni enti governativi potrebbero utilizzare Libra per rintracciare i propri cittadini e recuperare preziose informazioni. Per ovviare a ciò, possono essere implementate diverse soluzioni: leggi sulla privacy, usare delle organizzazioni non governative per combattere gli illeciti (sempre se le informazioni degli utenti di Libra non vengono condivise con i governi), stabilire dei protocolli legali di condivisione di dati finanziari, ecc.

Terzo scenario: Un nuovo ordine mondiale

In questo scenario Libra diventa una piattaforma di successo mondiale e i governi riscontrano numerose difficoltà nel regolamentarla. La Libra Association rigetta ogni tipo di regolamentazione e, come risultato, i confini economici nazionali cominciano a dissolversi permettendo a Libra di diventare, a tutti gli effetti, una *cloud nation*, che raggruppa decine di nazioni di tutto il mondo. Sebbene questo scenario sia piuttosto irrealistico, gli esperti forniscono 3 importanti ragioni:

- L'enorme quantià di utenti (potenzialmente 2.3 miliardi) possono assicurare sufficiente potere contrattuale per Libra, che sarebbe utilizzato per rafforzare le sue policies a discapito di quelle governative.
- In molte nazioni con economie deboli, gli enti normativi avrebbero serie difficoltà nel fermare i propri cittadini nell'utilizzare Libra.
- La Libra Association potrebbe coinvolgere ed incoraggiare i governi ad abbracciare la sua visione, così da limitare potenziali regolamentazioni che ne ostacolerebbero l'espansione.

Se Libra diventasse una moneta globale al di fuori del controllo governativo, cosa potrebbe succedere? Nonostante sarebbe lo scenario più interessante non è esente da controindicazioni. Anche qui ritornerebbe il problema della privacy: Chi definisce i termini e diritti degli utenti? Come si possono prevenire breccie nella privacy se non ci sono regolamentazioni a cui far riferimento? Chi potrebbe prevenire gli atti illeciti come riciclaggio di denaro, acquisto di armi illegali, traffico di essere umani e supporto di attività terroristiche? Se la Libra Association diventasse più ricca e forte di un singolo paese, che influenza avrebbero i suoi utenti sulle decisioni dell'associazione?

Queste sono solo alcune delle domande che si pongono gli esperti. In questo scenario, il successo di Libra sarebbe alle spese dei singoli governi e delle loro economie. Le aziende che si trovano in nazioni dove Libra non è adottata potrebbero decidere di trasferirsi in paesi *Libra-friendly*. Nel lungo

periodo queste azioni potrebbero erodere le economie nazionali, rafforzando Libra e la sua economia digitale.

Quarto scenario: Il potere alle persone

In questo scenario (il più improbabile), i governi non riescono a regolamentare la piattaforma, ma la Libra Association decide di non esercitare alcun potere decisionale sui suoi utenti. Come risultato, la piattaforma è orientata al servizio del grande pubblico: gli utenti hanno la possibilità di decidere come vengono gestiti i propri dati personali.

Nonostante le possibilità che questo scenario si trasformi in realtà siano remote, vi sono diverse ragioni per le quali è stato formulato:

- Se Libra vuole essere una piattaforma di successo, Libra Association deve lavorare per costruire e poi preservare la fiducia dei suoi utenti in merito a privacy e alla protezione dei dati personali.

- Organizzazioni private di controllo possono collaborare con Libra per garantire la privacy dei suoi utenti. In questo modo, gli enti governativi sarebbero allontanati da qualsiasi forma di interferenza e di controllo.

- Gli utenti diventano consapevoli del modo in cui vengono trattati i propri dati e decidono di evitare i servizi basati su Libra che non rispettano i requisiti minimi di sicurezza. Libra sarebbe dunque costretta a definire delle policies che rispecchino le richieste degli utenti, allontanando definitivamente i governi dalla piattaforma.

In questo scenario improbabile, ne i governi ne la Libra Association controlla Libra e non vi è alcuna censura sulle transazioni che vengono effettutate sulla piattaforma. Il risultato più evidente sarebbe che le organizzazioni criminali ne trarrebbero vantaggio ad usare la criptovaluta per i loro scopi, sapendo di non essere controllati da nessuno. In ogni caso, la probabilità che questo scenario si trasformi in realtà, sono molto basse. Il primo motivo sta

nel fatto che lanciare Libra senza alcun tipo di consenso e/o collaborazione da parte degli enti governativi potrebbe danneggiare la reputazione dei diversi membri della Libra Association. Secondariamente, questo scenario richiede un sistema più decentralizzato e distribuito di quello che Libra sta pianificando di lanciare e, poichè il passaggio da un sistema all'altro richiede tempo e ingenti investimenti, è improbabile che accada nei primi anni di vita della criptovaluta.

Inoltre, secondo quanto riportato sul white paper ufficiale, ci si aspetta che Libra sarà un ecosistema aperto per gli sviluppatori. Ciò significa che gli utenti saranno in grado di creare servizi ad hoc per i loro business. Potenzialmente si potrà formare un'economia parallela, dove per esempio vengono affittati gli appartamenti oppure vengono effettuati servizi di trasporto/car sharing solamente per utenti di Libra. Ancora più importante, gli utenti sarebbero in grado di creare sistemi di governance basati su Libra per convogliare idee e richieste alla Libra Association.

In conclusione possiamo dire che tutti questi possibili scenari futuri per Libra non sono certi e potranno essere soggetti a cambi di direzione che porteranno Libra verso tutt'altra strada. Quello che sappiamo per certo sono solo le interviste e le parole di Mark Zuckemberg riportate da The Verge [35]:

> *"... And we have this bigger, or at least more exotic, project around Libra, which is to try to stand up a new kind of digital money that can work globally, [and] that will be stable ... But it's a big idea, and it's a new type of system, especially to be implemented by big companies. We're not the only ones doing this. We've led that the thinking and development on it so far, but the idea is to do this as an independent association, which is what we announced with about 27 other companies. By the time it launches, we expect we'll have 100 or more companies as part of it. But part of what we're trying to do overall on these big projects now that touch very socially important aspects of society is have a more consultative approach. So not just show up and say, "Alright, here we're launching this. here's a product, your app got*

updated, now you can start buying Libras and sending them around." We want to make sure. We get that there are real issues. Finance is a very heavily regulated space. There's a lot of important issues that need to be dealt with in preventing money laundering, preventing financing of terrorists and people who the different governments say you can't do business with. There are a lot of requirements on knowing who your customers are. We already focus a lot on real identity, across especially Facebook, so there's even more that we need to do in order to have this kind of a product. And we're committed to doing that well, and part of doing that well is not just building the internal tools and showing up and saying, "Hey, we think we've solved this," but addressing and meeting with all the regulators up front, hearing their concerns, hearing what they think we should be doing, making sure other folks in the consortium are handling this appropriately. ..."

4.1 La necessità di regolamentare

Il focus della Libra Association è stato fin da subito quello di aprire un diaologo con i legislatori. Come ben sappiamo, le criptovalute sono state frenate dalle autorità centrali in quanto non vi sono regolamentazioni sufficienti a riguardo. Libra si vuole porre come apripista verso gli enti governativi, così da permettere la globalizzazione e la diffusione delle tecnologie basate su blockchain e delle relative criptovalute. Il progetto è ambizioso e ha già trovato le prime opposizioni.

Il ministro della finanza francese Bruno Le Maire e la controparte tedesca Olaf Scholz hanno già annunciato che potrebbero bloccare Libra in Europa, poichè "potenzialmente dannosa per il settore finanziario". Hanno anche aggiunto che Libra "potrebbe essere una minaccia per la sovranità monetaria dei paesi dell'Unione Europea".

"France and Germany consider that the Libra project, as set out in Facebook's blueprint, fails to convince that those risks will be properly addressed."

La Banca Centrale Europea ha aggiunto che il progetto di Libra è stata una "wake-up call" per l'Europa nello sviluppare una propria criptovaluta.

La situazione attuale

L'Unione Europea non ha ancora fornito nessun tipo di specifica su come devono essere trattate le criptovalute. Sono state però evidenziate delle linee guida su come agire a livello fiscale. Le transazioni effettuate con criptovalute per l'acquisto di beni e/o servizi, come dichiarato dalla UE, non sono esenti dalle tradizionali tassazioni, come VAT/GST e tasse sul reddito. A Dicembre 2016, la corte di giustizia dell'Unione Europea ha constatato che *"The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT"* e che *"Member States must exempt, inter alia, transactions relating to 'currency, bank notes and coins used as legal tender'"* [36].

Secondo la Banca Centrale Europa, le regolamentazioni in vigore per il settore finanziario non sono applicabili alle criptovalute in quanto "non coinvolgono gli stessi attori del sistema finanziario tradizionale"[31]. Alcuni Stati, tuttavia, hanno espresso il proprio disappunto chiedendo che le norme venissero estese anche per le criptovalute. Sempre la BCE classifica le criptomonete, con particolar riferimento al Bitcoin, come "una valuta digitale convertibile e decentralizzata"[37].

Per quanto riguarda gli Stati Uniti, sono nate delle definizioni contrastanti in merito alla classificazione delle criptomonete. Il dipartimento del tesoro, così come la BCE, le classifica come "valute digitali convertibili e decentralizzate". La *Commodity Futures Trading Commission* le identifica come semplici commodity.

A differenza della UE, gli Stati Uniti si sono espressi chiaramente in merito alle società che trattano criptovalute, come per esempio gli exchange e i servizi di trasferimento di criptomonete. Queste attività devono rispettare 3 punti:

- Registrarsi alla FinCEC, *Financial Crimes Enforcement Netork*, come attività di servizi monetari.
- Elaborare programmi e software per combattere il riciclaggio di denaro.
- Mantenere un appropriato resoconto delle transazioni e fornire report periodici alla FinCEC, tra cui "Suspicious Activity Reports (SARs)" e "Currency Transaction Reports (CTRs)".

In Cina la situazione è completamente diversa rispetto alla maggior parte dei paesi occidentali. Da Settembre 2017, la Cina ha chiuso totalmente le porte alle criptovalute, nonostante l'interesse nei confronti dei progetti blockchain. Il primo passo è stato quello di vietare il trading delle criptomonete e le *ICO (Initial Coin Offering)*. Successivamente sono stati chiusi gli exchange e, a inizio 2018, sono state adottate misure restrittive nel confronto del mining e vietato l'accesso agli investitori cinesi agli exchange internazionali.

Nonostante ciò negli ultimi mesi c'è stato un cambio di rotta da parte delle autorità cinesi. L'1 Gennaio 2020 è entrata in vigore una legge[38] che mira ad istituire degli standard per l'applicazione della crittografia e la gestione delle password. Sebbene le criptovalute non vengano menzionate, la legge sta costruendo le basi per l'imminente criptomoneta di stato. In merito a ciò, anche Mark Zuckerberg si è espresso durante l'evento al Congresso degli Stati Uniti del 23 Ottobre 2019:

> *"China is moving quickly to launch a similar idea in the coming months. We can't sit here and assume that because America is today the leader that it will always get to be the leader if we don't innovate. Libra will be backed mostly by dollars and I believe it will extend America's financial leadership as well as our democratic values and oversight around the world. If America doesn't innovate, our financial leadership is not guaranteed."*

Quindi, come possiamo constatare, la situazione normativa varia drasticamente da stato a stato ed è costantenemente in continua evoluzione, pertanto

non è possibile fornire un resoconto preciso per ognuno di essi. L'infografica 4.2 riassume lo stato legale delle criptomonete per ogni paese.

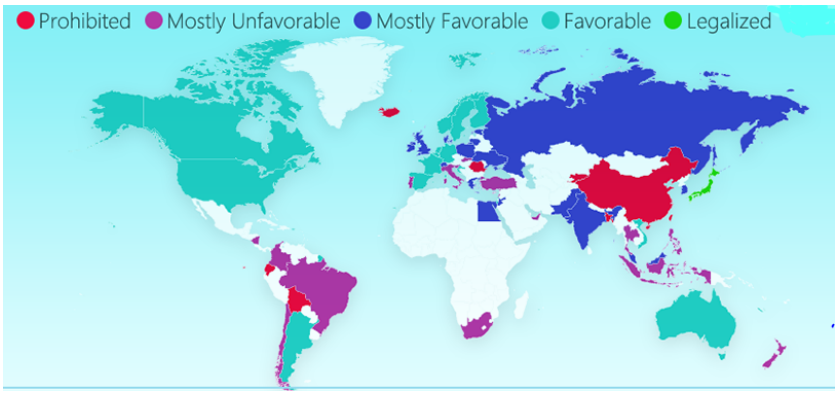

Figura 4.2: Situazione legale delle criptovalute nel mondo. Fonte: *Knoema.com*

4.2 Le critiche rivolte al progetto

Da quando Facebook ha formalmente annunciato il progetto Libra il 18 Giugno 2019, l'accoglienza da parte delle autorità centrali, banche e gli enti regolatori è stata tutt'altro che positiva.

I legislatori americani, nei mesi scorsi, hanno chiesto a Facebook di esaminare il protocollo di Libra e il presidente della Federal Reserve, Jerome Powell, ha espresso diverse preoccupazioni in merito al progetto. Pertanto, dato l'intensificarsi delle ricerche e degli scrutini nei confronti di Libra, Facebook ha rilasciato una dichiarazione dove assicura che "Libra won't launch until regulators satisfied".

In un joint statement di Agosto 2019 [39], i rappresentanti della protezione dati di diversi paesi (UK, USA, UE) hanno espresso i loro dubbi e preoccupazioni sui rischi per la privacy del progetto Libra e della sua infrastruttura. In particolar modo le preoccupazioni fanno riferimento a precedenti episodi nei quali Facebook non ha gestito correttamente le informazioni dei pro-

pri utenti (vedi scandalo Facebook-Cambridge Analytica). Come scritto sul documento:

> *"...We are supportive of the economic and social benefits that new technologies can bring, but this must not be at the expense of people's privacy. In today's digital age, it is critical that organisations are transparent and accountable for their personal information handling practices. Good privacy governance and privacy by design are key enablers for innovation and protecting data – they are not mutually exclusive...."*

I regolatori hanno anche aggiunto che sono stati "sorpresi" riguardo alla mancanza di informazioni che Facebook e la sua sussidiaria Calibra, che ricordiamo sarà un portafoglio digitale per facilitare i pagamenti con Libra, hanno fornito in merito alla protezione dei dati degli utenti.

Ulteriori preoccupazioni sono state avanzate dal segretario del tesoro statunitense Steven Mnuchin per il potenziale uso illecito che si potrebbe fare di Libra. Come lui stesso ha detto: *"Cryptocurrencies such as bitcoin have been exploited to support billions of dollars of illicit activity like cyber crime, tax evasion, extortion, ransomware, illicit drugs and human trafficking"*, Libra potrebbe essere utilizzata per finaziare attività terroristiche e il riclaggio di denaro.

Altre dubbi sono scaturiti in merito al grande potere che Facebook può esercitare sul mercato: Maxime Waters, membro del Comitato americano per i Servizi Finanziari, ha richiesto l'interruzione dello sviluppo di Libra. In particolare, Waters ha dichiarato che "Considerando il passato travagliato della compagnia, richiedo che Facebook accetti la sospensione di ogni sviluppo della criptovaluta, fino a che il Congresso e gli organi di regolamentazioni non avranno avuto l'opportunità di esaminare potenziali problematiche e prendere una decisione a riguardo". Ha aggiunto inoltre che "l'espansione incontrollata di Facebook e l'influenza che ha sulla vita dei suoi utenti, con l'introduzione di Libra, deve essere vista come una minaccia per la privacy e la sicurezza nazionale".

Il deputato Patrick McHenry, anch'egli facente parte del Comitato per i Servizi Finanziari, ha poi aggiunto che "In quanto responsabili delle politiche, è nostro compito comprendere Project Libra. Dobbiamo andare oltre le voci e le speculazioni, e aprire al più presto un dibattito per valutare il progetto e il suo potenziale impatto senza precedenti sul sistema finanziario globale".

Esperti provenienti dalla Germania, come Gerhard Schick, presidente e cofondatore del *Finanzwende*, un movimento associato ai *Green*, ha dichiarato che "Facebook sta usando la sua posizione di mercato dominante nel settore dei social media per ottenere potere in un'altra area come quella dei pagamenti, così da accrescere il suo potere e la sua influenza verso gli enti governativi." Schick aggiunge inoltre che "non ci si può fidare delle promesse in merito alla salvaguardia della privacy proposte da Facebook. Le transazioni potrebbero essere anche controllate sistemicamente, aumentando enormemente le attuali già grandi capacità di *monitoring* di Facebook."

Markus ferber, un europarlamentare, ha detto che Facebook potrebbe diventare, testuali parole, una "shadow bank con 2 miliardi di utenti".

Il ministro francese Le Maire, che come detto in precedenza non ha visto di buon occhio il progetto Libra tanto da volerlo bloccare in Europa, ha sottolineato il pericolo che Libra possa costituire per la sovranità monetaria dei paesi.

Tutte queste affermazioni allarmiste e preoccupanti provenienti dall'elitè governativa mondiale dimostrano che la "moneta di Facebook" sia qualcosa di completamente diverso rispetto a Bitcoin e le altre criptovalute. Il motivo principale sta nel fatto che Libra è centralizzata, governata e gestita dalla Libra Association. E poichè è centralizzata, i governi possono decidere di avere voce in capitolo nel controllo e nella gestione della criptovaluta. Nel caso dei Bitcoin, per esempio, non è possibile aver nessun tipo di controllo e supervisione poichè, semplicemente, è totalmente decentralizzata. Libra è diversa e i governi possono intervenire, ed è proprio quello che hanno intenzione di fare.

Facebook sembra però aver già considerato tutto ciò. Lo sviluppo della

criptovaluta è dato dal fatto che Facebook ha riscontrato difficoltà nell'ottenere le licenze per creare una piattaforma ordinaria di servizi finanziari. Libra è nata dunque per aggirare la supervisione e i limiti imposti dai governi. Poichè la criptovaluta sarà gestita da svariati membri della Libra Association, imporre dei limiti e delle regolamentazioni a Facebook non sarà sufficiente per controllare Libra in quanto Facebook non ha potere decisionale sui membri dell'organizzazione. Questa struttura societaria, dunque, rende estremamente complicato per i governi avere alcun tipo di controllo su Libra. In questo modo Libra Association avrebbe il tempo sufficiente per decentralizzare Libra, così da rendere infinitesimale l'influenza stessa dei membri dell'associazione.

Un report recente pubblicato dal quotidiano *The Information* il 3 marzo 2020, afferma che Facebook sta alterando i suoi piani per la criptomoneta a causa del forte *push-back* governativo e delle grosse pressioni regolatorie. In particolare è stato posticipato il lancio del Libra token in favore di un supporto delle valute nazionali sulla piattaforma (come Euro e Dollaro). Anche il wallet Calibra, che inizialmente doveva favorire lo sviluppo e l'espansione di Libra, supporterà diverse valute nazionali e non. Questo è una grossa battuta d'arresto per Facebook e la Libra Association in quanto c'è il rischio concreto che, se il sistema supportasse tutte le valute nazionali, il potenziale esplosivo del Libra coin vada ad affievolirsi nel tempo e a finire nel dimenticatoio. In ogni caso Facebook ha dichiarato che è *fully-committed* nel progetto e che quindi, per ora, l'obiettivo finale non cambia.

Libra perde il supporto di alcune aziende

Paypal è stata la prima azienda a lasciare la Libra Association il 4 Ottobre 2019 a causa delle forti pressioni dei governi sul progetto. PayPal ha dichiarato:

> *"PayPal has made the decision to forgo further participation in the Libra association at this time and to continue to focus on advancing our existing mission and business priorities as we strive to democratise*

Figura 4.3: Partner della Libra Association che si sono allontanati

> *access to financial services for underserved populations... We remain supportive of Libra's aspirations and look forward to continued dialogue on ways to work together in the future. Facebook has been a long-standing and valued strategic partner to PayPal and we will continue to partner with and support Facebook in various capacities."*

Il CEO di PayPal, Dan Schulman, ha affermato successivamente che la ragione principale del divorzio dalla Libra Association è stata di natura ideologica. Il focus dell'azienda sarà quindi di concentrarsi su progetti autonomi legati alla sfera delle criptomonete al di fuori di Libra.

In seguito alla notizia dell'uscita di PayPal dal gruppo, altre aziende di grosse dimensioni hanno preso la stessa decisione. Qualche giorno dopo altri 4 dei 28 fondatori iniziali decide di abbandonare il progetto: eBay, Stripe, Mastercard e Visa. Quest'ultima ha dichiarato che non ha ancora intenzione

di far parte della Libra Association finchè tutti i requisiti di regolamentazione che verranno imposti dai governi non verranno rispettati.

In risposta a questo esodo, il portavoce delle politiche e delle comunicazioni di Libra Association, Dante Disparte, ha dichiarato:

> *"Building a modern, low-friction, high-security payment network that can empower billions of financially underserved people is a journey, not a destination. This journey to build a generational payment network like the Libra project is not an easy path...We recognize that change is hard, and that each organization that started this journey will have to make its own assessment of risks and rewards of being committed to seeing through the change that Libra promises..."*

Qualche giorno fa, il 23 Gennaio 2020, anche Vodafone decide di abbandonare il progetto, giustificando il ritiro con l'intenzione di dedicare le risorse previste per Libra al suo sistema digitale di Pagamento *M-Pesa*.

Questo gruppo di aziende che ha lasciato Libra, ad eccezione di Ebay e Vodafone, sono tutte operanti nel settore dei pagamenti elettronici. Questo significa che devono rispettare rigide regolamentazioni governative per gestire frodi, riciclaggio, ecc. D'altro canto i governi stanno riscontrando diverse difficoltà nel trovare le regolamentazioni necessarie per Libra. Questa situazione di stallo può portare dunque dei danni considerevoli ai core business delle aziende di pagamento, specialmente se Libra non riesce a trovare accordi regolamentatori con i governi. Tutti questi dubbi e perplessità verso il progetto hanno quindi causato una fuga di massa estremamente controproducente per la Libra Association e la sua reputazione.

4.3 Sintesi delle principali differenze con le altre criptovalute

La principale differenza con le maggiori criptovalute che governano il mercato, come Bitcoin ed Ethereum, risiede nel fatto che Libra, come è stato detto in precedenza, è una permissioned blockchain. Il vantaggio di avere una criptomoneta permissioned è da identificare nel maggiore *throughput* di transazioni. In poche parole, avendo meno nodi validatori, in quanto solo i membri della Libra Association possono esserlo, il processo di validazione di una transazione è decisamente più rapido (vedi capitolo 3 maggiori dettagli). Per fare un esempio pratico, la blockchain di Bitcoin, allo stadio attuale, processa solamente 7 blocchi al secondo. Anche Ethereum, come denotato dal cofondatore Vitalik Buterin, ha una capacità massima di 15 transazioni al secondo. Perciò trasferire Bitcoin richiede approssimativamente un ora, mentre Ethereum può richiedere fino a 6 minuti. Queste cifre sono innammissibili per un sistema di pagamento globale come può essere Libra.

I circuiti di pagamento tradizionali, come ad esempio Visa, hanno un TPS (Transactions per Second) di circa 1700, una cifra molto distante dalle criptovalute sopracitate e ciò permette trasferimenti di denaro pressochè istantanei. Perciò la struttura permissioned di Libra potrebbe tranquillamente permettere di raggiungere un TPS di 1000 transazioni, il che la renderebbe estremamente competitiva sia verso le altre criptovalute che verso i metodi di pagamento tradizionali.

Un'altra differenza sostanziale risiede nel protocollo di consenso utilizzato da Libra, il LibraBFT. Questo protollo, che sarà discusso alla fine del terzo capitolo, è di natura completamente differente rispetto alla Pow di Bitcoin o alla PoS di Ethereum. Tutti sanno che la PoW di Bitcoin, e delle altre criptomonete che la utilizzano, è assolutamente dannosa per l'ambiente, per via del grosso consumo di elettricità necessario al suo funzionamento. D'altro canto la Pos di Ethereum è sì più eco-friendly, poichè rimuove il processo laborioso di calcolo, ma è molto più complicato e difficile da rendere sicuro.

Il protocollo di consenso di Libra, che è una variante del protocollo HotStuff, è estremamente più veloce, sicuro, scalabile ed eco-friendly rispetto ai due sopracitati. Questi vantaggi derivano anche dal fatto che è un protocollo per blockchain permissioned e non permissionless, dove quindi coloro che gestiscono i nodi validatori sono conosciuti e selezionati in precedenza, e che quindi il concetto di trust è ancora parzialmente presente.

Un'altra differenza da tenere presente è la bassa volatilità dei prezzi che Libra avrà rispetto alle normali criptomonete presenti sul mercato (vedi tabella 4.2). Una caratteristica tipica delle criptovalute è infatti quella di avere degli sbalzi notevoli, anche giornalieri, nelle quotazioni. Libra invece, dato che sarà coperta da asset reali a bassa volatità, non avrà questa proprietà, il che non farà di certo sorridere gli speculatori, ma al contrario sarà un ottimo incentivo come metodo di pagamento tradizionale per gli utenti finali.

Coin	**Valore Attuale ($)**	**+- % 1 Giorno**	**+- % 7 Giorni**
BTC	8663.48	-1.8%	-9.7%
ETH	224.43	-1.4%	-12.7%
LTC	59.77	-3.1%	-13.9%
Ripple	0.24	+1%	-11.5%
ETC	7.45	-3.6%	-16.1%
DASH	89.2	+0.1%	-14.9%
ZEC	51.05	-3.2%	-15.9%
XMR	68.32	-2.9%	-10.4%
BCH	313.05	-3.4%	-15.8%

Tabella 4.2: Andamento criptovalute in data 28/02/2020

Alla luce di queste considerazioni e delle analisi effettuate in merito agli sviluppi futuri del progetto, Libra si attesta ad essere una criptovaluta con potenzialità illimitate, ma che tutt'ora non è stata in grado di convincere a pieno le autorità. Purtroppo le informazioni che ora sappiamo sul progetto

sono limitate e non ci possono fornire ulteriori dettagli sul futuro di questa misteriosa criptovaluta. Sappiamo però che, da quando è stata annunciata, l'interesse verso il mondo delle criptomonete e delle tecnologie associate ad esso è cresciuto enormemente; governi e istituti finanziari hanno capito che il futuro delle valute e dei sistemi di pagamento sta cambiando e la necessità di stare al passo coi tempi è più attuale che mai.

Conclusioni

Le criptovalute sono una delle tante trasformazioni naturali dell'evoluzione della moneta che si sono susseguite nel corso della storia. Come per ogni nuova tecnologia che si rispetti, Libra sarà accolta inizialmente con perplessità e diffidenza, ma porterà sempre avanti l'obiettivo di rivoluzionare il futuro delle criptomonete e del mondo finanziario.

Libra ha un vantaggio che tutte le altre criptovalute che sono nate dopo il successo del Bitcoin non posso neanche sognare: la potenziale user base vicina ai 3 miliardi di utenti le permette di essere una minaccia anche per il Bitcoin che detiene il 68% del mercato. Le immense fluttuazioni delle comuni criptovalute e la scarsa regolamentazione che ruota attorno ad esse non ha permesso la diffusione e l'adozione globale di questi sistemi. Libra si pone in una posizione di vantaggio, cercando contatto con i legislatori e garantendo fiducia e trasparenza all'utente inesperto del mondo delle criptomonete.

Le blockchain e i sistemi decentralizzati sono innovazioni rivoluzionarie che possono stravolgere il mondo delle banche tradizionali e dei pagamenti online e non solo. Facebook promuove Libra come una valuta digitale stabile, dove il suo valore non è derivato da aspettative o speculazioni di mercato, ma bensì è speculare all'andamento di asset reali. Questa caratteristica intrinseca della moneta sarà di sicuro un punto a favore per coloro che vorranno adottarla come metodo di pagamento e per coloro che non possono accedere alle banche tradizionali.

C'è ancora tempo prima della data di lancio di Libra prevista per metà 2020, ma il tempo corre veloce e Facebook deve prima rispondere alle critiche

dei governi e degli investitori e chiarire i dubbi che ruotano attorno a questo ambizioso progetto. Il passato travagliato di Facebook in merito alla privacy e alla sicurezza dei dati personali non possono essere dimenticati, ma almeno c'è la certezza che le informazioni degli utilizzatori di Libra non saranno condivise con Facebook senza previo consenso. Nonostante i piani di diventare una blockchain permissionless nel prossimo futuro, Libra sarà inizialmente un network permissioned per supportare le miliardi di transazioni che il sistema potrebbe dover gestire.

Le differenze con le altre criptovalute sono tante, così come i dubbi e le perplessità che ruotano attorno a questo progetto. Solo il tempo ci dirà se Libra sarà un fallimento o una rivoluzione globale.

Bibliografia

[1] S.Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, pag 1

[2] R.C. Merkle, *Protocols for public key cryptosystems*, In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pagine 122-133, Aprile 1980

[3] S. Haber, W.S. Stornetta, *How to time-stamp a digital document*, In Journal of Cryptology, vol 3, n 2, pagine 99-111, 1991

[4] A. Back, *Hashcash - a denial of service counter-measure*, 2002.

[5] D. Chaum, *Blind Signatures for Untraceable Payments*, 1983

[6] E-Cash disponibile a https://www.chaum.com/ecash/

[7] W. Dai, *B-Money, an Anonymous, Distributed Electronic Cash System*, 1998

[8] T. May, "The Crypto Anarchist Manifesto", 1992

[9] N. Szabo, *Trusted Third Parties Are Security Holes*, pagine 5-6, 1995

[10] https://www.economist.com/printedition/2015-10-31

[11] https://cointelegraph.com/news/jamie-dimon-calls-bitcoin-fraud-despite-clear-conflict-of-interest

[12] Michael J. de la Merced e Nathaniel Popper, *JPMorgan Chase Moves to Be First Big U.S. Bank With Its Own Cryptocurrency*, New York Times, Feb 14 2019

[13] *Deloitte's 2019 Global Blockchain Survey*, https://www2.deloitte.com/content/dam/Deloitte/se/Documents/risk/DI_2019-global-blockchain-survey.pdf

[14] *Fintech 2.0: Rebooting Financial Services*, https://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

[15] Ito J., Narula N., Ali R., *The Blockchain Will Do to the Financial System What the Internet Did to media*, 2017

[16] *Banking on Blockchain*, https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/consulting/accenture-banking-on-blockchain.pdf

[17] *Blockchain: an opportunity for energy producers and consumers?*, https://www.pwc.com/gx/en/industries/assets/pwc-blockchain-opportunity-for-energy-producers-and-consumers.pdf

[18] Grech A., Camilleri A. F., *Blockchain in Education*, 2017

[19] https://it.wikipedia.org/wiki/Firma_digitale

[20] *Bitcoin Block Reward Halving Countdown*, https://www.bitcoinblockhalf.com/

[21] M. Cavicchioli, *Ethereum: arriva la Proof of Stake sulla blockchain*, The Cryptonomist, 3 Maggio 2019

[22] N. McCarthy, *Bitcoin Devours More Electricity Than Switzerland*, Forbes, 8 Luglio 2019

[23] https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake/

[24] *An Introduction to Libra*, https://libra.org/en-US/white-paper/#introduction

[25] *Counting the World's Unbanked*, McKinsey, https://www.mckinsey.com/industries/financial-services/our-insights/counting-the-worlds-unbanked

[26] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," http://gavwoo d.com/paper.pdf, 2016.

[27] L. Lamport, R. Shostak, M. Pease *The Byzantine Generals Problem*, SRI International

[28] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, I.Abraham *HotStuff: BFT Consensus in the Lens of Blockchain*, Cornell University

[29] M. Castro, B. Liskov, *Practical Byzantine Fault Tolerance*, Massachusetts Institute of Technology

[30] C. Dwork, N. Lynch, *Consensus in the Presence of Partial Synchrony*, Massachusetts Institute of Technology

[31] S. Micali, M. Rabin, S. Vadhan, *Verifiable Random Functions*

[32] *Bitcoin Accrues Over $6 Billion Daily Transactions, Targets Mastercard's Record*, NewsLogical, https://newslogical.com/bitcoin-accrues-over-6-billion-daily-transactions-targets-mastercards-record/

[33] *Number of Blockchain wallet users worldwide from 3rd quarter 2016 to 3rd quarter 2019* , https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

[34] R. Tzezana, M. Perry, *The Future of Libra: A New World Order?*, Settembre 2019

[35] https://www.theverge.com/2019/10/1/20892354/mark-zuckerberg-full-transcript-leaked-facebook-meetings

[36] *The exchange of traditional currencies for units of the 'bitcoin' virtual currency is exempt from VAT*, Corte di Giustizia dell'Unione Europea, 6 Dicembre 2016

[37] *Virtual Currency Schemes*, Banca Centrale Europea, 5 Marzo 2015

[38] https://www.insideprivacy.com/data-security/china-enacts-encryption-law/

[39] *Joint statement of global privacy expectations of the Libra network*, https://ico.org.uk/media/about-the-ico/documents/2615521/libra-network-joint-statement-20190802.pdf