LUISS

Dipartimento
di Impresa e Management

Cattedra di Economia dei Mercati degli Intermediari Finanziari

La Blockchain: come sta cambiando la nostra vita e il nostro futuro.

Prof.Francesco Cerri
RELATORE

Alessio Morgantini
CANDIDATO

Anno Accademico 2020/2021

Alla mia famiglia, ai miei amici, a me stesso.

"A volte si vince, a volte si impara"

Indice

Introduzione

Lo scopo di questa tesi è parlare di una delle tecnologie che più influenzerà il nostro futuro: la Blockchain.

Un viaggio dal concetto di sfiducia verso gli altri, per poter capire a fondo le radici e i motivi della sua esistenza, fino a determinare gli scenari che ci attendono; partendo dalla sua struttura e dalle sue funzioni, per arrivare a comprendere le criptovalute e gli smart contract, che grazie alla decentralizzazione, alla trasparenza, rapidità e convenienza, stravolgeranno interi settori portando benefici tempistici ed economici all'interno del futuro dell'economia mondiale.

I maggiori esperti del settore, infatti, hanno evidenziato la probabilità che, la catena di blocchi, possa essere più influente di internet di ben quindici volte, rivoluzionando il 66% dei lavori che oggi conosciamo. Secondo una *survey* condotta dal World Economic Forum, entro il 2027 il 10% del PIL globale, o il 10% degli scambi monetari, sarà sviluppato o gestito da piattaforme blockchain.

Personalmente, una volta imbattuto in questa "nuova" tecnologia, ne sono rimasto affascinato, soprattutto per lo spazio che sta prendendo all'interno del business (e non solo), dove porterà una nuova visione del mondo che conosciamo, più unito e più *truster*.
Comprendere il suo funzionamento, però, sarà di vitale importanza al fine della determinazione dei processi evolutivi che porteranno al cambiamento delle nostre vite.

Prima di iniziare, però, vorrei citare una frase di Gianluca Comandini, dal suo libro "Da zero alla Luna: quando, come, perché la Blockchain sta cambiando il mondo":

«*Collaborazione* è più forte di *competizione*. Ci vediamo sulla Luna, il razzo è in partenza!»

CAPITOLO I: La nascita della Catena dei Blocchi

I.I La prima Blockchain

Isola di Yap, Micronesia 1400 d.C.

Gli abitanti di quest'isola, gli yapesi, capendo che il baratto non era più equo e conveniente, cercarono di adottare un metodo di pagamento che potesse soddisfare al meglio i loro bisogni: la moneta.

Questi, navigando per Palau, isola distante 400 chilometri, scoprirono delle grosse rocce calcaree circolari con un foro al centro, diametro di 3 metri, peso approssimativo di 4 tonnellate: le pietre Rai.

Decisero di adottare il Rai come valuta per le transizioni economiche ed organizzarono delle spedizioni per portare nella loro isola le loro nuove monete.

Da qui i primi problemi: come si potrebbe immaginare l'eccessivo peso non facilitava il trasporto, provocando morti durante le spedizioni, l'invidia nei confronti di chi possedesse i Rai più belli cresceva a dismisura, sfociando in furti o danneggiamenti, e come se non bastasse, la gente prometteva Rai che non possedeva.

Sfociò il caos.

Capirono dunque che le difficoltà del commercio, riscontrate fino a poco prima, con l'utilizzo del baratto, non risiedevano nel mezzo o nel bene utilizzato per le transazioni ma nelle persone stesse. Si trovavano di fronte ad un problema di *fiducia* nel prossimo.

Come arginarlo? Decisero così di creare un sistema di archivio decentralizzato che sarebbe stato aggiornato giornalmente. Ognuno dei singoli abitanti, infatti, doveva possedere un registro in cui venivano inseriti i nomi di tutti gli yepanesi possessori dei Rai, aggiungendo ogni singola transizione o acquisizione portata a termine. In caso di necessità, discrepanze o litigi, si sarebbero dovuti controllare i libri mastro di ognuno, in modo tale da verificare la correttezza del pagamento e la veritiera appartenenza della moneta. Doveva essere *trasparente*, in modo che ognuno potesse accedervi, e il fatto che tutti avrebbero dovuto aggiornarla, la rendeva anche inalterabile.

Infatti, qualora una persona avesse in mente azioni malevole, avrebbe dovuto modificare la maggior parte dei registri, cosa assai improbabile.

Questo sistema permise agli abitanti di Yap di arginare il problema della fiducia nel commercio, garantendo una pace ed una prosperità economica.

Ci troviamo di fronte alla prima rete blockchain.

I.II Sfiducia nelle Banche

"Chancellor on brink of second bailout for bank" – 3 gennaio 2009, Genesis Block, Satoshi Nakamoto.

Questa è la frase di apertura del primo blocco che ha dato vita al Bitcoin.
Perché?

Dopo la crisi finanziaria del 1929, quella del 2008, è stata la più grande della storia dell'uomo.

In seguito al forte investimento, di privati e non, nel mercato immobiliare statunitense che dal 2000 al 2006 aveva visto schizzare del 15% annuo il tasso di crescita del valore delle case, le banche rilasciarono mutui ad alto rischio, forti del fatto che, qualora fossero andati incontro all'insolvenza, avrebbero guadagnato con la vendita dell'immobile ad un prezzo maggiore.

La brusca discesa del valore immobiliare del 2007, la cartolarizzazione del debito da parte delle banche statunitensi e le agenzie di rating che sottovalutarono il pericolo, promuovendo i titoli come "molto sicuri", portarono ad una rottura insanabile del sistema.

La conseguenza diretta fu la riduzione del valore dei titoli cartolarizzati che, immediatamente, provocò un effetto a catena che portò in crisi di liquidità la maggior parte delle banche del mondo.
La borsa crollò, molte banche fallirono e molti PIL mondiali scesero.

La crisi portò con sé la fine della quarta banca d'affari più grande al mondo: *Lehman Brothers*, la quale dichiarò debiti per oltre 600 miliardi di dollari. Era il 15 settembre 2008.

Il 3 gennaio 2009, qualche tempo dopo il suo fallimento, in seguito al salvataggio di diverse banche con i soldi pubblici, il *Times* titolò: «Chancellor on brink of second bailout for bank» tradotto:
il cancelliere sta per effettuare un secondo salvataggio per le banche.

L'inserimento di questo titolo come capitolo iniziale della vita della Blockchain non era casuale.
Il creatore di Bitcoin, Satoshi Nakamoto, o forse "i creatori", non abbiamo idea di chi possa celarsi dietro questa identità, volle muovere una forte critica nel sistema capitalistico finanziario.

Trovò un modo di poter effettuare transazioni rapide, sicure e veloci senza l'intervento di alcuna istituzione bancaria.

Come sarebbe possibile? Grazie alla Blockchain.

CAPITOLO II: Cos'è la Blockchain

II.I Cos'è la Blockchain

La blockchain (catena di blocchi) facente parte delle Distribuited Ledger Technology (DLT) è un archivio dati decentralizzato, condiviso e criptograficamente immutabile (basato su una rete peer-to-peer) organizzato in blocchi che si generano dopo un meccanismo di consenso. Per "decentralizzato" si intende un network in cui tutte le risorse sono distribuite e replicate all'interno della rete.
Di questi blocchi si ha la possibilità solo di aggiungerne di nuovi mentre la rimozione o la modifica degli stessi non è contemplata.
Possono essere figurativamente immaginati come i mattoni della blockchain, aggiunti in modo sequenziale.
All'interno di ognuno troviamo il codice hash del blocco precedente, le informazioni relative ai file contenuti e l'hash di chiusura del blocco. Il processo attraverso il quale le transazioni vengono validate, aggregate in blocchi e aggiunte alla blockchain si chiama: mining.

II.II Il codice Hash

Il codice hash è l'algoritmo in grado di mappare dati di dimensione arbitraria in stringa di bit.

Questa funzione serve a verificare l'integrità di un messaggio, tramite la ricezione di un input, determinando un output crittografato corrispondente solo e soltanto a quel tipo di input.

Dunque, l'input della funzione può essere qualsiasi cosa: dal testo di un messaggio, un foglio di calcolo oppure una catena di blocchi intera; l'output però, definito come "hash", avrà un numero finito di bit, utile per crittografare il contenuto del blocco unidirezionalmente. Questo vuol dire che, a determinati input, corrisponderanno determinate risposte output; se gli input di diversi blocchi dovessero essere gli stessi allora lo saranno anche gli output (da un punto di vista pratico è quasi impossibile che si verifichi che il contenuto tra due o più blocchi sia esattamente lo stesso).

Non è possibile trovare due messaggi diversi con lo stesso valore di hash.

È una funzione unidirezionale, vale a dire che è facile generarla ma diverrebbe molto complesso calcolare l'input partendo dall'hash (unico modo il brute-force ovvero provando tutte le combinazioni possibili).
Questa permette la connessione tra i blocchi della catena tramite un collegamento matematico indissolubile.

La funzione hash è il mezzo grazie al quale la blockchain diverrebbe impossibile da alterare, poiché all'interno di un blocco già calcolato, basterebbe cambiare la minima cosa (anche una virgola in un testo) e il codice generato muterà radicalmente modificando tutta la stringa di bit del blocco, facendo risultare evidente la manomissione, che verrebbe poi immediatamente segnalata eliminandolo dalla catena. Questo ci fa capire che, per la valutazione di uno stato corretto di un'intera catena di blocchi, basterebbe analizzare solamente il codice dell'ultimo blocco, per poi andare a ritroso fino ad eliminare il "mattone" compromesso.

II.III Il Nodo

Uno degli scopi principali della tecnologia blockchain è quello di permettere a chiunque, in qualsiasi parte del mondo esso si trovi, di effettuare transazioni senza la necessità di affidarsi ad un'istituzione centrale. Per consentire questo servizio ha bisogno di essere distribuita in un network.

Possiamo definire il network come un gruppo di macchine interconnesse che si scambiano informazioni tramite canali di comunicazione, come per esempio internet.

Una macchina connessa ad un network è chiamata nodo.

Il nodo è il punto di connessione fisico o virtuale dove è possibile generare, inviare e ricevere tutti i tipi di dati e informazioni. In poche parole, ogni singola macchina partecipante alla blockchain è un nodo. I nodi funzionano tutti allo stesso modo e sono governati dalle stesse regole del protocollo di consenso stabilito: possono comunicare tra loro trasmettendo e condividendo dati dirigendo tutte le informazioni necessarie al suo funzionamento.
La creazione di nuovi blocchi, la convalida e la conferma delle transazioni.
Ognuno beneficerà della propria conclusione sulla validità di una transazione, indipendentemente dagli altri nodi.

Possiamo distinguere due tipi diversi di nodo: avremo il primo definito come nodo completo; questo è indipendente e non ha bisogno di ricevere fiducia dagli altri nodi. Scaricherà e archivierà copie complete della catena controllando le transazioni. Rappresenta il modo più sicuro per interagire con una rete blockchain ed anche il più scomodo in quanto si dovrebbe scaricare la copia della stessa (basti immaginare che la Blockchain di Bitcoin fino al 15 agosto 2021 raggiunge la dimensione di 350,96 gigabyte, secondo Statista.com)

L'altro nodo conosciuto è il light-node. A differenza del primo, non andrebbe ad effettuare il download dell'intera catena bensì solo del nodo completo, implicando una delega fiduciaria a una terza parte in cambio dell'utilizzo. Viene usata per lo più dagli utenti medi vista la facilità di utilizzo rispetto al nodo completo.

Il concetto della catena di blocchi è comune a quasi tutti i sistemi blockchain, ma tra le varie catene, i blocchi stessi variano di forma e dimensione per consentire il corretto svolgimento delle funzioni richieste.

II.IV La struttura dei Blocchi

Tornando alla composizione della catena, abbiamo visto come i "mattoni" fungono da elementi principali di raccolta. La loro composizione ricorda un cubo che si suddivide in due parti: l'header e il corpo.
Il primo è dove sono conservati una serie di dati del file, il codice hash del blocco corrente e del precedente, la data e l'ora in cui è stato prodotto, i bitcoin totali movimentati nel blocco e la dimensione del contenuto calcolata in kilobyte.
L'altra parte è il corpo del registro in cui sono contenute tutte le transazioni del blocco.

L'aggiunta di un nuovo blocco alla catena viene permesso tramite un protocollo di convalidazione della transazione tra i computer ovvero il mining.

II.V Ledger e Database

Essendo la catena un archivio dati decentralizzato è opportuno definire prima cosa siano i ledger e i database.

Per ledger intendiamo gli strumenti utilizzati per la registrazione delle transazioni. Venivano già usati prima dell'avvento della Blockchain, in quanto parte integrante dei processi commerciali. È possibile unicamente l'aggiunta di nuove informazioni.
Tutto questo è reso possibile grazie alla combinazione di fari fattori come la decentralizzazione, la crittografia, teoria dei giochi e altri sistemi.
Per questo motivo la Blockchain è un ledger digitale.

Con i database, invece, è possibile inserire, cancellare e modificare i dati.

II.VI Tipologie Blockchain

Abbiamo tre tipi diversi di tipologie Blockchain: quelle pubbliche (permissionless), private (permissioned) e ad autorizzazione (a consortium).

Il modello di blockchain pubblica non ha proprietari, è decentralizzata, priva di autorità centrale di riferimento, dunque non censurabili. L'utilità è per ogni tipo di documento che ha la necessità di non mutare nel tempo. Tutti hanno la possibilità di potersi unire alla rete e non si può essere esclusi (resistenza alla censura). È possibile controllare ogni singola transazione effettuata dagli utenti, per questo, quando si parla di blockchcain ci si riferisce alla blockchain permissionless.
Un difetto di queste reti è: per mantenere attivo questo libro mastro pubblico distribuito (DLT) serve un numero elevato di consumo energetico.
Fanno parte di questo tipo di tecnologia: il Bitcoin (criptovaluta) ed Ethereum (smart contract).

La Blockchain Privata è la piattaforma gestita da una o più organizzazioni con regole che vengono condivise ed accettate dagli utenti una volta che vengono autorizzati a far parte della rete. Sono ideale nell'ambito industriale. Nel sistema viene controllato chi riceve il permesso d'accesso al network e la tipologia di diritti e premi nel processo di mining. Le persone, approcciando a questo tipo di tecnologia, sacrificano la decentralizzazione a favore di un controllo sui permessi di accesso e solitamente sulle migliori performance.
Non essendo una rete decentralizzata l'attività di controllo viene redatta da colui che ne è proprietario, avendo il potere decisionale su eventuali censure o transazioni.

La blockchain ad autorizzazione (o a consortium) è quando viene data a tutti la possibilità di poter leggere il registro (anche se è possibile incappare in alcune limitazioni).
Ha alcune peculiarità delle due reti descritte in precedenza. Per questo motivo possono essere definite come: Blockchain appartenenti ad un consorzio ed essere controllate da autorità centrali. A differenza delle reti private, il controllo viene gestito dai partecipanti del network.
Un esempio su chi usa questo tipo di rete è "R3", ovvero un gruppo di ricerca tecnologico di cui fanno parte grandi società finanziarie come Goldman Sachs, Banca d'America, Royal Bank di Canada ed altre prestigiose.

II.VII PoW e PoS

Il primo algoritmo di consenso creato è stato il Proof of Work (PoW), progettato da Satoshi Nakamoto e implementato su Bitcoin, nel 2009, per garantire la Byzantine Fault Tolerance ("Tolleranza degli errori bizantini"), vale a dire la capacità che ha sistema informatico distribuito di resistere ai difetti bizantini (come, fallimenti del consenso, fallimenti di validazione, mancata verifica dei dati o errori nel protocollo di risposta).

La tolleranza degli errori bizantini si basa sul dilemma di come raggiungere il consenso in situazioni dove è presente la possibilità di errori. Questa metafora venne posta nel 1982 dai matematici Leslie Lamport, Marshall Pease e Robert Shostak.

Tre o più generali bizantini, a seguito dell'accerchiamento dell'insediamento nemico, devono compiere una decisione cruciale presa dal comandante superiore per poter vincere: attaccare o ritirarsi. Affinché la scelta risulti vincente è fondamentale che tutti compiano la stessa azione; altrimenti se dovessero dare ordini diversi tra loro, questo comporterebbe la sconfitta in battaglia. Il problema, basandosi sulla fiducia, si trova nel fatto che uno dei generali potrebbe essere un infiltrato, dunque, per far perdere la battaglia cambierebbe l'ordine dato dal comandante.
A sua volta il comandante stesso, accortosi del possibile tradimento, potrebbe dare ordini distorti al fine di far effettuare l'azione corretta al comandante traditore, con il rischio di non coordinare le azioni di tutti quanti i generali provocando, anche in questo caso, la sconfitta.

La risoluzione del dilemma si trova nella comunicazione.

Per recapitare i messaggi di attacco o ritirata devono essere impiegati dei messaggeri che potrebbero tardare la consegna, manipolare il messaggio o smarrirlo.

La chiave risolutiva risiede nel modo di effettuare la Proof of Work la quale prevede che la maggior parte dei partecipanti della rete debbano concordare sullo svolgimento della medesima azione. Una volta deciso il momento dell'attacco esso verrà ritenuto valido per tutti. Essendo il network non istantaneo, il ritardo dell'attacco provocherebbe la sconfitta. Per ovviare a questo, come appunto succede nella PoW, appena ricevuto il messaggio, i generali dovranno risolvere dei problemi estremamente difficili. Colui il quale lo risolverà per primo dovrà annunciare agli altri il risultato. Qualora uno dei generali stesse lavorando ad altri messaggi dovrà sostituirlo con il presente appena validato poiché fa parte della catena corrente che è più lunga, più valida e definitiva. Questo permette ai nodi appartenenti alla stessa catena di lavorare insieme gestendo in maniera efficace e sincronizzata il network.

La Proof of Work ovvero la prova di lavoro, serve per verificare l'autenticità e il corretto rigore con il quale si è svolta una determinata operazione nella blockchain.

Questa varia dalla verifica di uno scambio regolare tra criptovalute, la creazione di nuovi blocchi che si andranno ad aggiungere alla catena e altro. Coloro che andranno ad effettuare questa prova di lavoro sono i così detti miners o validatori che per poter verificare uno svolgimento corretto degli iter finanziari e non, dovranno risolvere ardui problemi matematici.

Questi sono dei veri e propri enigmi che riguardano la scomposizione in fattori primi e il guided tour puzzle protocol che, partendo da una stringa alfanumerica, necessita del calcolo di una funzione hash qualora si dovesse verificare un attacco DoS (ovvero un attacco informatico in cui provano a non farti accedere ai servizi di rete o alle risorse del computer). Questi calcoli matematici aumentano la loro difficoltà proporzionalmente alla crescita della potenza di calcolo della rete.

Ogni miner può scegliere la transazione che vuole basandosi principalmente in quelle più remunerative. Una volta convalidato il blocco, riceverà la sua ricompensa in criptovaluta, verrà inserito all'interno della catena.

La probabilità di essere scelto come miner per risolvere la PoW bisogna fare un rapporto tra potenza di calcolo (denominata hashrate) del miner e l'hashrate del network.

La ricompensa è data dalle commissioni delle transazioni incluse nel blocco più un'eventuale criptovaluta (nel caso del Bitcoin per ogni nuovo blocco venivano dati 12,5 bitcoin. Numero che tende sempre a diminuire in quanto le criptovalute hanno un limite di monete minabili, in questo caso hanno posto il limite di 21 milioni).

Per permettere una pari scalabilità, dunque, la Blockchain pone alla base del mining la possibilità di partire tutti con le stesse armi, indipendentemente dalle elevate quantità di denaro possedute.

Uno dei modi per poter hackerare una rete Blockchain, basata sulla PoW, scartando l'ipotesi del DoS, sarebbe utilizzando l'attacco 51%.

Questo consiste nel dover manomettere il 51% dei nodi della catena, controllando la maggioranza della potenza di un mining di una rete, in modo tale da far credere al restante parte dei server di trovarsi in errore.

Da un punto di vista teorico si tratta di una delle poche manomissioni possibili alla catena che però risulta impossibile nella pratica.

Gli elevati costi energetici, così come l'elevata necessità di potenza di calcolo, lo rende impraticabile ai giorni nostri. Qualora si disponesse di una potenza computazionale simile, il costo energetico sarebbe pari alla somma dei PIL mondiali; senza sottovalutare che la manomissione farebbe crollare il valore delle criptovalute pari allo zero. Dunque, non avrebbe senso pratico effettuare un attacco alla rete blockchain, che risulta così inespugnabile.

Questo però riguarda le reti blockchain decentralizzate. Come prime descritto, le reti con maggior numero di blocchi nella catena sono più difficili da manomettere, vista la robusta presenza di nodi.

Qualora ci trovassimo di fronte ad una blockchain privata, dunque con sistema centralizzato, potrebbe presentare delle falle nella composizione, ed essere più facilmente attaccabile: come già accaduto. Ribadendo: più una catena di blocchi è centralizzata e più è hackerabile.

Un altro svantaggio di questo sistema di verifica è la discriminazione geografica. Poiché è necessario una forte potenza di calcolo, i miner, saranno concentrati in paesi in cui il costo dell'elettricità è inferiore e le temperature sono basse, affinchè si possa risparmiare sugli impianti di raffreddamento.

Nella catena di blocchi il consenso non avviene tramite autorità centrale (in quelle pubbliche si intende) ma tramite il "consenso distribuito" con la prova di lavoro (PoW).

Gli algoritmi di consenso costituiscono, quindi, un elemento cruciale per la blockchain, poiché da questo dipende il principio di trustless della rete

Il Proof of Stake è un algoritmo proposto nel 2011 da un utente del forum Bitcointalk, per la risoluzione dei problemi derivanti dall' utilizzo del PoW.
Entrambi i processi di validazione condividono il medesimo scopo con differenze di processo realizzativo.

Potremmo definirlo, in partenza, come l'alternativa al dispendioso consumo di energia impiegato dall'algoritmo utilizzato per la convalidazione tramite lavoro che offrono una maggiore democraticità, decentralizzazione e scalabilità.
In questo sistema non ci sono miners per la verifica della catena.
Non sarà necessario la risoluzione della scomposizione in fattori primi o della guided tour puzzle protocol, bensì i validatori dovranno confermare la correttezza di un blocco impiegando una loro somma di criptovalute come garanzia o cauzione, definito come stake. Per questo motivo colui che andrà a depositare una somma maggiore avrà più possibiltà di essere scelto. Durante le transazioni si decide, secondo varie metodologie, chi andrà a formare il blocco successivo, come ad esempio: la longevità del deposito, definità come coin age, ovvero il tempo in cui non si viene scelti per la proof of stake, che si azzera una volta che il validatore viene scelto e anche grazie all'ammontare del deposito.
Terminata la creazione del blocco, ci dovrà essere un secondo check da parte degli utenti del network in modo tale da verificare se siano stati aggiunti blocchi fraudolenti. Al raggiungimento della verifica finale da parte degli altri validatori, verrà restituito lo stake assieme ad una ricompensa (commissioni sulle transazioni, dette "fee").

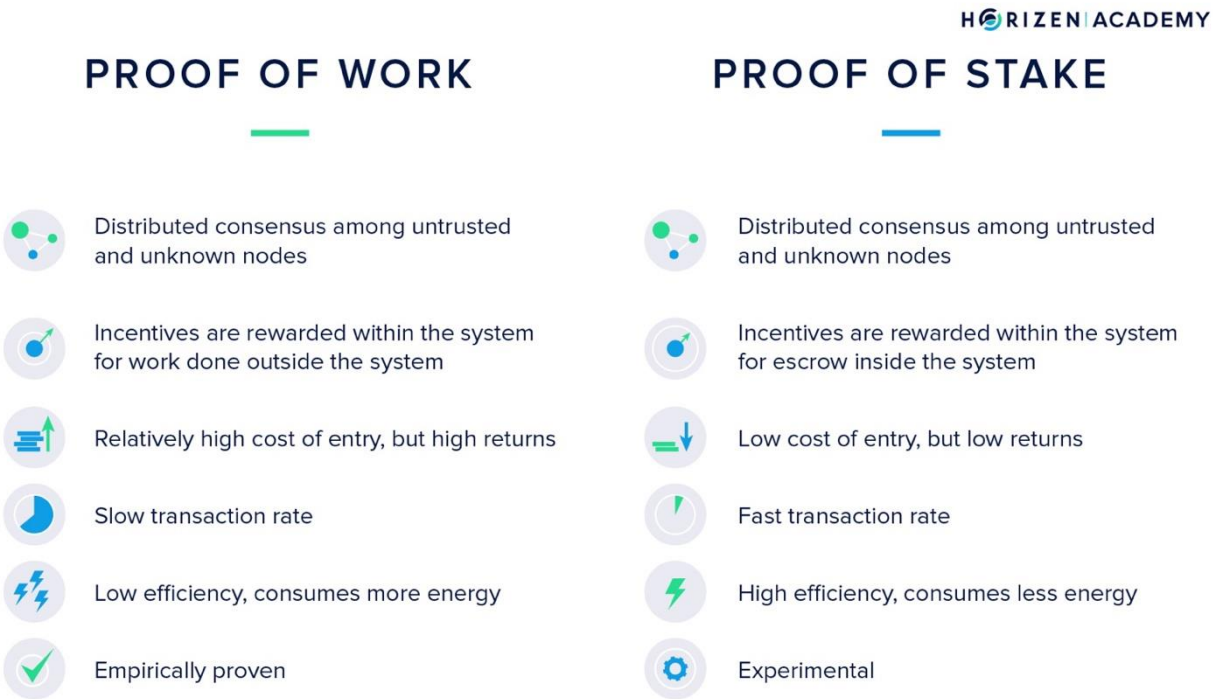
Con questo metodo si va a disincentivare operazioni non lecite, in quanto, la somma posta per cauzione verrebbe revocata e il validatore non potrebbe più essere scelto per la creazione di nuovi blocchi.

Rispetto alla Proof of Work, è molto più efficiente siccome viene accantonata la possibilità di dover eseguire calcoli matematicamente complessi per ogni nuovo blocco.
Gli attacchi da parte di violatori del sistema sono molto più costosi, infatti, grazie alla necessità di dover depositare una somma come garanzia, per la creazione di un nuovo mattone, si dovrebbe possedere almeno il 51% dei token totali della catena (per token si intende una criptovaluta con

funzionalità che vanno oltre il semplice trasferimento di valore, verrà approfondito in seguito). Se ipotizzassimo un'eventuale manovra di manomissione sarebbe assai improbabile e controproducente, in quanto, a seguito del tentativo di acquisizione di una tale somma di criptovalute, il prezzo della stessa salirebbe, ed una volta terminato l'hacking il valore del token scomparirebbe.
Non avendo elevati costi di elettricità, come quelli del processo di mining della PoW, tutti possono permettersi di partecipare alla catena.

Un altro fattore che giova l'uso della Proof of Stake è la lealtà. I miner verrebbero incoraggiati a rimanere nella stessa blockchain poiché un eventuale cambio provocherebbe obbligatoriamente il cambio di token in loro possesso.

Qui di seguito riassunte le differenze tra la Proof of Work e la Proof of Stake



CAPITOLO III: Le criptovalute e gli smart contract

In questo capitolo, andremo ad analizzare due dei concetti chiave che potremmo definire come la punta dell'iceberg della blockchain: criptovalute e smart contract.

III.I Le Criptovalute

Le criptovalute sono delle monete digitali, basate sulla tecnologia blockchain, usate per lo scambio di beni o servizi.
Queste non hanno corso legale e non sono supportate o gestite da alcuna istituzione.

Per far in modo che avvenga un trasferimento di valore, da un partecipante della rete ad un altro, non serve alcuna terza parte che faccia da garante, poiché grazie alla crittografia, non si incorrerebbe nel rischio della controparte. Questo rischio rappresenta il caso in cui la parte coinvolta nello scambio di valore non tenga fede alle condizioni definite nella transazione.

Le criptovalute sono state la prima applicazione a sfruttare le potenzialità della rete blockchain, andando a risolvere il problema del *double spending*.
Durante l'utilizzo della rete Internet, i dati vengono automaticamente duplicati ogni qual volta si effettui un'operazione, comportando la copia dell'oggetto anche infinite volte.
Il *double spending*, appunto, è quando esiste una copia di un qualcosa che dovrebbe essere unico, come il denaro.
Il pagamento tramite rete Internet, che, come detto prima, duplica i dati, potrebbe comportare il rischio di spendere gli stessi soldi per più di una transazione.

Ad oggi le banche riescono ad arginare questo problema grazie al gateway (esempio PayPal) che, gestendo le interazioni con le banche, invia la transazione agli istituti di credito in modo tale che possa essere verificata, impedendo il problema della doppia spesa.

La blockchain è stata la prima tecnologia a risolvere questa difficoltà senza il coinvolgimento di terze parti, poiché il network non lo autorizzerebbe.

L'impossibilità di potere spendere due volte la stessa valuta virtuale crea il concetto di scarsità digitale e permette agli utenti della catena di scambiare le criptovalute direttamente tra loro.

Le caratteristiche delle criptovalute sono quelle di essere: digitali o virtuali, difatti non esiste un equivalente fisico di una "cripto".
Sono globali in quanto non hanno confini fisici o politici; *trustless* perché non appoggiandosi nelle mani di terzi, il consenso è distribuito ai partecipanti della rete che ne controllano la validità e ne garantiscono la sicurezza. Sicurezza, che appunto, ne fa da caratteristica principale grazie alla verifica tramite crittografia.
Immutabile, appena una transazione è confermata e aggiunta al blocco della catena, questa non potrà essere più modificata o rimossa.
La neutralità consente a qualsiasi persona di prenderne possesso senza effettuare distinzioni di nessun genere perché incensurabile, anche nell'oggetto dello scambio stesso.

La politica monetaria delle criptovalute è gestita dal network.

Si possono definire alcuni parametri fondamentali che riguardano il loro tasso di crescita e quantità. Si intende "Total supply" la quantità totale di monete già generate in circolazione.
Di queste, non tutte possono essere spendibili, causa l'eventuale smarrimento di chiavi private di un indirizzo che contiene le cripto, comportando il blocco irreversibile di quella quantità di monete (salvo il ritrovamento della chiave); oppure un eventuale stallo, generato dal creatore della criptomoneta, che poi rilascerà in seguito. Queste monete vanno ad inserirsi nella categoria della quantità spendibile, la "Circulating supply" (nel caso in cui i due eventi di prima non si verificassero, la Total e la Circulating supply coinciderebbero).
La "Max supply" è il totale delle monete che potrà mai esistere per una criptovaluta (per essere beni desiderabili devono avere un limite che viene scelto da colui che le genera), anche se alcune non hanno una fine dichiarata. Ad esempio, la quantità massima di Bitcoin (BTC) è di 21 milioni. Questo numero che ne limita l'estrazione, in seguito al consenso del network, non può essere modificato da nessuno. Dunque, una volta estratto il ventun milionesimo bitcoin, non sarà possibile minarne altri.

È importante definire la quantità di monete non spendibili poiché, queste, non andrebbero ad influenzare la capitalizzazione di mercato della criptovaluta.

La capitalizzazione di mercato è il prodotto tra il valore di tutte le monete in circolazione e il prezzo spendibile per un'unità di moneta.

Il modello di distribuzione delle criptovalute può avvenire tramite due processi: mining o la vendita diretta.
Per alcune monete, però, è possibile scegliere di renderle non minabili.

Ne è esempio Ripple (XRP), dove le valute virtuali, vengono generate al momento della creazione della blockchain per essere vendute direttamente alle persone.

Citando le criptovalute non si può non parlare del Bitcoin.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

1

Questa è la prima pagina del White Paper di Bitcoin in cui Satoshi Nakamoto descrive per la prima volta il suo progetto.

Bitcoin è il protocollo open source diffuso da Satoshi Nakamoto per lo sviluppo della criptovaluta chiamata *bitcoin* (se l'iniziale è minuscola ci rivolgiamo alla criptomoneta, oppure, nel caso fosse maiuscola, ci stiamo riferendo al protocollo open source).

Pur essendo la prima criptovaluta ad essere stata creata, il concetto prese vita nel 1998 nella community Cypherpunks da Wei Dai.
Satoshi Nakamoto stesso, nel 20 luglio 2010, durante una delle sue apparizioni chat, confermò che il bitcoin era l'implementazione del *b-money* di Wei Dai.

Lo scopo era creare una moneta virtuale capace di eliminare l'intervento della polizia o dei governi, consentendo lo pseudonimato, eliminando tentativi di truffe o infrangimento delle regole, con l'allentamento dell'attore malevolo da parte del netwok e, grazie alla struttura crittografica, un elevato sistema di sicurezza che avrebbe facilitato gli scambi fra gli utenti della rete stessa.

La Proof of Work è il protocollo di consenso utilizzato in Bitcoin.
Ogni volta che un nuovo blocco viene creato, il sistema genera una quantità definita di bitcoin che verrà usata come ricompensa per il miner. Questa ricompensa si dimezza ogni 4 anni a causa della quantità massima prestabilita che è di 21 milioni di bitcoin.

Al contrario delle credenze, il Bitcoin, non rende coloro che lo usano anonimi all'interno della catena, infatti grazie alla struttura blockchain, si garanisce lo pseudonimato.
Cerchiamo di fare chiarezza: l'anonimato è la condizione in cui non si riesce a risalire all'identità di colui che effettua una qualsiasi azione all'interno della rete.
Grazie alla crittografia, con l'utilizzo delle chiavi private e pubbliche, vengono impiegati degli pseudonimi durante lo scambio di transazioni fra gli utenti. Questi possono essere dei semplici nickname o direttamente i codici matematici generati della funzione hash, che permettono di capire chi effettua la transazione, senza risalire immediatamente alla vera identità del proprietario, consentendo la privacy.

La crittografia asimmetrica genera contemporaneamente due chiavi, in modo che possano collaborare strettamente tra loro: una pubblica e una privata. Queste serviranno prima per criptare o firmare un contenuto (grazie alla chiave privata), generando numeri e codici, che verranno successivamente decriptati grazie alla chiave pubblica.

Capiamo l'importanza del tenere al sicuro o trascrivere la nostra chiave privata, poiché a seguito di un eventuale smarrimento, non sarà possibile recuperare i bitcoin posseduti.

La chiave privata è un numero casuale compreso tra 1 e 1,158x10^77 mentre quella pubblica si ottiene tramite la correlazione tra la prima chiave e la crittografia a Curva Ellittica.
Il protocollo attuo a conoscere le chiavi è irreversibile ed unidirezionale. Non è possibile, infatti, conoscere la chiave privata, conoscendo solo quella pubblica.

Le chiavi pubbliche e private coprono un ruolo fondamentale all'interno del funzionamento di questa moneta virtuale.

La struttura decentralizzata e la crittografia hanno consentito la nascita del Bitcoin che è riuscito a distinguersi, grazie alle sue caratteristiche, rispetto alle valute attuali.

L'innovatività del sistema della moneta risiede nella sua decentralizzazione, che lo rende libero dall'intervento di stati o banche, ponendo gli utenti in condizione di pagar meno le transazioni indipendenti al fine di poter compiere un pagamento senza l'intervento di terze parti e dunque di m. Grazie alla crittografia e al consenso dello spostamento di denaro virtuale tramite chiave pubblica e chiave privata consente di essere sicuro ed affidabile. Basandosi sulla tecnologia blockchain, inoltre ogni transazione rimane immutabile nella catena, rendendola trasparente.
La velocità con la quale si possono inviare o ricevere bitcoin è notevole, basti pensare che necessitano pochi minuti per l'invio di un bonifico.

Bitcoin è stato criticato per problemi di scalabilità che si sono in parte risolti aggiungendo il SegWit (Segregated Witness) alla struttura stessa dei blocchi.
Essendo il blocco Bitcoin di dimensioni di 1 MB, la velocità nelle transazioni ne risentiva.
Il SegWit è una diramazione leggera del progetto (soft fork) che va ad aumentare lo spazio effettivo da 1 a 4 MB e rende off-chain le transazioni. Questo vuol dire che lo scambio di informazioni o di valore viene aggiornato al termine dell'operazione, senza appesantire la blockchain, rendendo il procedimento ancora più rapido.

III.III Smart Contract

Le criptovalute non sono l'unica tecnologia che ha saputo sfruttare al meglio l'avvento della blockchain.

Nel 1994, Nick Szabo, propose un nuovo metodo capace di porre fine al rischio nella controparte nei contratti. Non sempre la fiducia viene ripagata durante degli accordi, come rimediare?

Szabo introdusse il concetto di smart contract basandosi sulla tecnologia blockchain che compie un ruolo primario in questi contratti intelligenti.
Gli smart contract sono un protocollo di transazione digitale che esegue i termini di un contratto.
Questo tipo di accordo non è vincolato dalla legge, bensì dal consenso e dalla trasparenza del network stesso, in quanto, qualora non giungesse al termine, significherebbe che una delle due parti non ha rispettato il contratto, annullandolo.
Questi tipi di accordi sono già inseriti all'interno del maccanismo, consentendo, a coloro che volessero utilizzarli, di poter scegliere quello che sembra più idoneo alla situazione oppure aggiungendo dei termini o delle condizioni al fine di modificarlo in base alle proprie necessità.
L'autorità che testa la condizione e le decisioni in merito alla valutazione dell'accordo risiede negli utenti del network stesso. Appena le condizioni del contratto vengono soddisfatte questo si concluderà automaticamente tramite azioni specifiche, come ad esempio: il trasferimento di denaro.

III.IV Ethereum

La svolta per i contratti intelligenti avvenne nel 2014 quando il diciannovenne Vitalik Buterin pubblicò il white paper di una nuova piattaforma, basata sulla blockchain, in grado di gestire e sviluppare gli smart contract: Ethereum.

La definizione più vicina a quella dell'Ethereum è definirla come un computer globale, nel quale gli smart contract o i programmi sono eseguiti in modo decentralizzato, continuo e senza censure.

Non può essere definita come una blockchahin specializzata poiché non ha uno scopo preciso, infatti può essere programmata al fine da potersi adattare alle varie situazioni richieste.
È per questo motivo che viene definita come blockchain generica.

Sfrutta la permissioinless della catena, dunque senza autorizzazioni, e si basa, per ora sulla Proof of Work.
L'utilizzo del termine "per ora" non è casuale, in quanto, stanno cercando di adoperare, per la creazione dei blocchi, la Proof of Stake.

Carl Beekhuizen, sviluppatore della Ethereum Foundation, riporta dati secondo cui l'utilizzo di questa metodologia di mining porterebbe ad una riduzione dei consumi di corrente pari al 99,95%. Questo protocollo verrà chiamato "Casper" e trasformerà la piattaforma in "Ethereum 2.0" che dovrebbe essere lanciato in tre fasi, entro il 2022.

La fase 0 sarà caratterizzata dal lancio di una nuova blockchain, chiamata "Beacon Chain", e dall'utilizzo della Proof of Stake. Con questa mossa il consumo energitico, appunto, si abbesserà notevolmente, aumenteranno però le difese del sistema. "Casper", infatti, verrà adoperato come selettore della rete e controllore dei blocchi nella catena. Molti dettagli, per ora, rimangono nascosti in attesa di aggiornamenti.

Ethereum utilizza una propria criptovaluta, denominata Ether (ETH), che, al contrario di Bitcoin, non ha un numero massimo di monete estraibili. Il tasso di inflazione viene regolato limitando il numero di ETH minabili ogni anno. Per capire al meglio lo svolgimento di questo token si potrebbe paragonare al carburante utilizzato da un'automobile per compiere un determinato tragitto.

Con l'Ether viene pagato il *gas* che il nome usato per indicare la quantità di calcolo necessaria per eseguire un'operazione sulla blockchain. È un concetto ad uso esclusivo delle transazioni, infatti non esiste un token *gas* in Ethereum. L'unità di misura del *gas* è il *wei* (1 ETH= 10^18 *wei).* Capiamo dunque che il prezzo del *gas* è il numero di *wei* da pagare per ogni singolo *gas*.

Questo concetto è fondamentale poiché ogni azione ha un suo costo definito, infatti, per determinare la somma tra due numeri o una funzione hash, occorreranno un determinato numero di *gas*.
In Ethereum il concetto delle dimensioni massime dei blocchi della catena non esiste.
Per questo motivo facciamo riferimento ai limiti e ai prezzi di gas di un blocco, che indicano, appunto, la quantità di calcoli necessari per la creazione di ogni blocco (e il loro costo).

Ricapitolando: il mittente di una transazione, ovvero colui che necessita la creazione del blocco della catena con all'interno il file relativo allo scambio monetario virtuale, sceglie e paga un determinato numero di *gas*, con gli Ether (ETH), per poterla inserire in Ethereum.

Il costo di questa transazione, da parte del mittente, è uguale al prodotto fra il limite di gas da impiegare e gli *wei* adoperati per ogni *gas*.

Se per la creazione del blocco contente lo scambio di denaro servissero 10 *gas* e colui che chiede la verifica proponesse il prezzo di 100 *wei* ad unità di *gas*, allora il validatore arriverebbe ad ottenere 1.000 *wei*.
Facile intuire, che la scelta dei *miner*, verterà sulla massimizzazione del profitto.
Il limite dei *gas* impiegato è fondamentale, in quanto, se si richiedessero 15 *gas*, per una funzione, anzi che gli effettivi 18 che ne servono, al raggiungimento del quindicesimo gas di consumo, l'esecuzione del blocco si interromperà.

Capiamo l'importanza di questo meccanismo che andrebbe a porre fine all'eventualità in cui, a causa dell'elevata complessità computazionale degli *smart contract*, si entrerebbe in un ciclo infinito di calcoli che verrebbero interrotti, appunto, dal limite di *gas*.

Definiamo alcuni ambienti interni di Ethereum.

"EVM" è *l'Ethereum Virtual Machine* ed è il luogo in cui viene eseguito lo smart contract. Serve per garantire l'esecuzione in sicurezza del contratto, per questo sono isolati e non permette l'interazione con altri mondi al di fuori della blockchain.

"ERC token" è l'acronimo di Ethereum Request for Comment. Tramite questa funzione possono essere scelte delle funzionalità specifiche all'interno di un contratto intelligente. La creazione dei token su questa piattaforma, ad esempio, è molto vantaggiosa. La presenza di una rete blockchain gestita da Ethereum, porta una maggiore sicurezza e facilità d'uso all'utente che andrebbe solo a personalizzare le applicazioni implementando l'utilizzo degli smart contract.

"Standard ERC 20" è lo standard usato per sviluppare i token nella blockchain di Ethereum. Questi devono contenere al loro interno: la quantità totale di token esistenti, una funzione in grado di

specificare i token posseduti da un indirizzo specifico e la funzione che permetterebbe lo scambio tra i token.

"ERC 721 token" è, come lo Standard ERC 20, la tecnologia con la quale si sviluppano i token, stavolta però, solo quelli unici, non fungibili (NFT).

Per capire meglio cosa si intende è utile prendere da esempio Cryprokitties, gioco popolare che utilizza questa piattaforma con lo scopo di scambiare tra gli utenti dei gatti digitali. Non si può esprimere un valore per lo scambio di un singolo gatto poiché questo è unico. La piattaforma, quindi, mette a disposizione dei gatti virtuali che possono essere comprati e cresciuti. La piattaforma, riconoscendo l'unicità dell'oggetto in questione, assocerà ogni gatto al proprio padrone che deciderà come allevarlo e come scambiarlo, in modo trasparente, al fine di ricevere delle ricompense in Ether.

Come detto in precedenza, per far sì che tutto funzioni, la Proof of Work è il metodo di validità adoperato che però comporta elevati consumi e costi energetici, intaccando la scalabilità di Ethereum. Aspettando il passaggio alla PoS, si è pensato di un ipotetico utilizzo dello *sharding*. Questo consiste nella divisione della catena blockchain in più parti indipendenti, detti *shard*, in modo tale che ogni nodo possa processare solo le transazioni di alcuni *shard*, aumentando così l'efficienza.

Abbiamo visto come, grazie all'EVM, Ethereum non può interagire con il mondo esterno se non con la blockchain. Questo perché gli smart contract, di natura, hanno un comportamento deterministico, ovvero tutti i dati usati dai validatori devono essere verificabili usando solo dati contenuti nella blockchain. Che fare se questi non dovessero essere presenti all'interno della catena? Ne sono esempio le condizioni meteo, le quotazioni azionarie, tassi di cambio e via dicendo. La soluzione, ancora in via di definizione, è il così detto: oracolo. È un servizio progettato per connettere la blockchain al mondo esterno al fine di fornire, ai contratti intelligenti, tutte le informazioni di cui hanno bisogno per una computazione.

CAPITOLO IV: applicazioni della Blockchain nel Business

Dopo tutto questo discorso introduttivo passiamo a capire le applicazioni della blockchain nel business.

IV.I Settore Finanziario

Uno dei settori che sarà maggiormente influenzato dalla catena di blocchi sarà il servizio finanziario. Citando Gianluca Comandini, dal suo libro "Da zero alla Luna", definisce le banche come il settore che basa tutto il suo successo sulla mancanza di fiducia tra gli esseri umani. Eliminando questa sfiducia, avremmo un risultato positivo in termini di costi e sicurezza nella custodia degli asset.

Secondo Harvard Business Review, la blockchain avrà la stessa importanza negli istituti finanziari come quella che ha avuto internet per i media.

La difficoltà di aggiornamento, stando al passo con i tempi, ha portato la nascita di numerose startup di fintech negli ultimi anni.

Per competere in modo efficiente è necessario ottimizzare i costi derivate dalle risorse a disposizione. Esempi possono essere i costi per l'antiriciclaggio, la sicurezza o il trasferimento di fondi internazionale. Studi effettuati da McKinsey & Co hanno sottolineato la possibile perdita di profitto di circa 100 miliardi di dollari, nei prossimi 5 anni, a causa dell'inefficienza di gestione.
Basta pensare al problema esistente dei pagamenti off-border.
Qualora un soggetto, volesse effettuare una transazione dall'Italia al Sudafrica, questa comporterebbe diversi giorni, se non settimane, per motivi burocratici, aggiungendo l'incremento dei costi che supererebbero il 10% della transazione stessa.

L'utilizzo della tecnologia blockchain, secondo un report di Santander, farebbe risparmiare alle banche circa 20 miliardi di dollari ogni anno.

Tra le piattaforme utilizzatrici della catena di mattoni che hanno preso piede in questo campo troviamo Ripple.

A differenza degli altri sistemi, i clienti medi di Ripple sono banche e fornitori di servizi a pagamento, infatti è una società focalizzata sullo sviluppo di soluzioni per il trasferimento globale di denaro.
Il funzionamento si basa sulla trasformazione di qualsiasi asset in token scambiabile all'interno di un ledger distribuito, siglando partnership con Unicredit, Ubs e Santander.

Per la sezione dei prestiti peer-to-peer, quelli da pari a pari, troviamo la *Secured Automated Lending Technology* detta "SALT". Utilizzando Ethereum, consente di adoperare criptovalute come collaterale per un prestito in contanti. L'economicità del trasferimento di valore, immagazzinamento o liquidazione, la rende molto competitiva soprattutto se confrontati con *stock* o proprietà immobiliari.

La creazione di *wallet* mobili, ovvero dei portachiavi virtuali in cui conservare le chiavi private, e di carte di credito fisiche per spendere criptovalute nei negozi, sarà possibile grazie al progetto TenX.
Rendendo questa operazione disponibile anche qualora negozi fisici non accettassero direttamente le monete virtuali. La legislazione, tuttavia, sta rallentando la creazione del progetto, che renderebbe ogni asset su blockchain spendibile istantaneamente.

L'eliminazione degli intermediari finanziari da parte della catena dei valori, istaurandosi come "sorgente di unica verità", citando la nota del libro scritto da Gianluca Chiap, Jacopo Ranalli e Raffaele Bianchi, titolato "Blockchain tecnologia e applicazioni per il business", andrebbe a far risparmiare alle banche dai 50 ai 600 milioni di dollari ogni anno. Tutto questo grazie alla verifica dell'identità basata, ancora una volta, sulla blockchain, che andrebbe a consolidare la sicurezza e la trasparenza, sostituendo le costose metodologie adoperate fino ad oggi come: *Know Your Customer* "KYC" o *Anti Money Laundering* per il riciclaggio di denaro.

Nel mondo della finanza non mancano innovazioni.

Per problemi burocratici, la liquidazione dei titoli azionari, da sempre, rappresenta un rallentamento nel processo del lavoro dei *broker* che impiegherebbero diversi giorni per portare a termine l'operazione. La catena permetterebbe di aumentare la velocità, rendendoli sicuro ed economici.

Questo protocollo viene adoperato da Nasdaq, il secondo più grande *stock exchange* al mondo per *market cap*, sfruttando l'immutabilità della catena, permetterebbe una maggiore efficienza nel processo di liquidazione dei titoli, su una sua piattaforma chiamata "Linq".

Per gli investimenti nel *Digital Asset Array* (DAA) è nata una piattaforma di nome Iconomi. Questa mette in relazioni diversi manager, che possono creare i propri DAA, permettendogli di investire in maniera trasparente tramite smart contract.

IV.II Catena di distribuzione

Nella catena di distribuzione, *supply chain*, l'avvento della blockchain porterebbe numerosi vantaggi in termini di tracciabilità, dunque aumento di fiducia da parte del consumatore.
La globalizzazione del mercato porta un dislocamento non indifferente che vedrebbe, un singolo prodotto, passare da una *location* all'altra, abbassandone la qualità.
Per non parlare dei costi burocratici che gravano sul prezzo del prodotto finale acquistato dal consumatore.

L'esempio per la risoluzione di questo problema, tramite una collaborazione con IBM, lo troviamo in Walmart e Carrefour.
Adoperando la blockchain, con la scanzione di un QRcode è possibile risalire con precisione e trasparenza, a tutte le informazioni di ciascun lotto.
D'altro canto, non presenterebbe un vantaggio solo per il consumatore, bensì il produttore stesso, potrebbe avvalersi dei dati ricevuti al fine di ottimizzare la produzione e la distribuzione.

Ad oggi, negli Stati Uniti, Walmart utilizza questo sistema per tracciare la provenienza di frutta e carne, passando dal tempo necessario di diversi giorni a pochi secondi.

Allo stesso modo Alibaba ha stretto una partnership con Cainiao, che è una sua controllata nel settore logistico, al fine di lanciare un progetto pilota che vede coinvolti 50 Paesi ed oltre trentamila merci.

L'utilizzo dello scanzionamento del codice QR al fine di stabilire le origini e il percorso che ha fatto un determinato prodotto prima di giungere nelle mani di un cliente, è stato adoperato anche dalla "DNV GL".

Questa società di servizi assicurativi e gestione del rischio, utilizza questo sistema per far avere un quadro completo e sicuro dell'unico prodotto inserito nel progetto: il vino.
Risalire alla storia della bottiglia, impiegando specifiche dettagliate e verificabili, sui processi di produzione è l'obiettivo di *My Story*.

Non sempre le società di trasporti e logistica sono efficienti come ci si aspetti.
Integrata nei trasporti e logistica, la A.P: Moller-Maersk, ha dato il via ad una piattaforma con la funzione dell'accelerazione del commercio.
Questa traccerà decine di milioni di container a livello globale rendendo digitale il processo della catena di distribuzione. Trasparenza e semplicità sono alla base del processo.

Anche il settore *luxury* dei diamanti ha consentito l'ingresso della blockchain nei suoi processi di sitribuzione; grazie al gruppo De Beers, che garantisce la tracciabilità dall'estrazione alla vendita dei diamanti. Tramite il registro a blocchi, infatti, non sarà possibile contraffare la rara pietra preziosa, poiché tutta la sua storia sarà ben visibile all'interno della catena.

IV.III Real Estate

Una delle maggiori innovazioni potremmo trovarlo nel settore Real Estate grazie alle *smart home*.
Le case intelligenti, implementate con la tecnologia dei blocchi, potranno raggiungere dimensioni notevoli. Basti pensare alla probabile futura fine dell'occupazione dell'altrui domicilio.
Grazie agli *smart lock*, prenderebbero il posto delle serrature tradizionali, l'ingresso in un'abitazione verrebbe negato qualora non si dovesse adempire ai termini stabiliti dagli *smart contra*ct (locazione affitto, pagamento bollette e via dicendo).

In Svezia sono stati tra i primi a testare la tecnologia blockchain nel real estate.
Gli utenti, grazie alla catena, devono condurre acquisizioni o vendite di immobili nella piattaforma.
Anche se viene adoperata una rete privata e non pubblica, la Lantmateriet, autorità governativa che mappa gli immobili in Svezia, farà risparmiare milioni di dollari di spese al governo svedese.

IV.IV Settore Automobilistico

Anche nel settore automobilistico troveremo notevoli cambiamenti.

Il collegamento della proprietà digitale di un individuo con l'identità digitale dell'autovettura sarà possibile con gli smart property, che semplificheranno le procedure burocratiche come il trasferimento di proprietà o il noleggio.
Oltre a oggetti fisici, come automobili o case, si aggiungono proprietà astratte come le quote di una società o brevetti, che possono essere liquidati o scambiati, senza l'intervento di intermediari.

Qualora dovessimo andare incontro ad un'incidente, l'assicurazione, integrata con la smart property, andrà a verificare le circostanze descritte in maniera trasparente nei parametri dello stato del veicolo (come velocità massima e rispetto della segnaletica) calcolando e rendendo disponibili, immediatamente, i fondi per il risarcimento.

Un brevetto registrato dalla Ford mostra la possibilità di cooperare fra le automobili e coloro che le guidano, decidendo chi ha la priorità a percorrere una strada, grazie alla blockchain.
Motivi diversi portano le persone alla scelta di un tragitto; altrettanti motivi portano il conducente a raggiungere determinate velocità. Qualora un individuo dovesse avere un appuntamento, si metterebbe d'accordo con la rete, pagando coloro che non hanno particolare fretta, al fine di poter arrivare in tempo, sfruttando le corsie di sorpasso o quelle meno trafficate.
Il brevetto si chiama CMMP System: *Cooperatively Managed Merge and Pass System*.
La riduzione del traffico sarebbe significativa grazie all'uso dei *machine learning* per monitorare strade, veicoli ed itinerari.

IV.V Settore Energetico

L'avvento della blockchain nel settore energetico riguarda principalmente le piattaforme di scambio peer-to-peer al fine di comprare o vendere quantità energetiche senza l'intervento di intermediari.

Ne è esempio Power Ledger, basata su Ethereum, capace di vendere e comprare energia rinnovabile, consentendo il salvataggio delle transazioni avvenute e permettendo il raggiungimento dell'autosufficienza energetica.

IV.VI Ambito Governativo e No Profit

Una delle svolte potrebbe basarsi sulle applicazioni in ambito governativo.
La certezza che le elezioni di un Paese avvengano senza alcun errore o tentativo di corruzione con le modifiche delle schede elettorali non è alta.
La catena di blocchi ridurrebbe sensibilmente questi rischi, apportando una votazione trasparente e valida che impedirebbe il rischio della falsificazione o duplicazione dei voti.
Ovviamente le tempistiche di verifica sarebbero immediate garantendo un notevole risparmio economico.

Stesse verifiche potrebbero essere apportate nelle Organizzazioni no-profit.
La sfiducia nelle persone nei confronti di queste organizzazioni verrebbe ricambiata una volta saputo, con chiarezza e trasparenza, l'utilizzo del denaro fornito, aggiornando costantemente il donatore.

Le Nazioni Unite sono riuscite ad aiutare diecimila rifugiati siriani adoperando Ethereum. I fondi, tracciati regolarmente, sono serviti per l'acquisto di beni di prima necessità.

Nasdaq eVoting, in tale proposito, nel 2016 ha sviluppato un progetto per la semplificazione dei processi di voto da parte di compagnie e investitori, andando, ancora una volta ad abbattere i costi di gestione.

IV.VII Settore Sanitario-Farmaceutico

Anche il settore sanitario-farmaceutico potrebbe vedere il processo burocratico snellirsi significativamente con l'uso della tecnologia a blocchi. La gestione delle cartelle cliniche risulterebbe automatica, sicura e condivisibile con Stati esteri in caso di necessità, abbattendo le barriere geografiche.
Non solo, il paziente stesso, potrebbe verificare il contributo che la sua situazione sta apportando alla ricerca.
Come per il settore alimentare, la supply chain farmaceutica incrementerebbe notevolmente il sistema di tracciabilità dei farmaci per verificarne l'autenticità.

IV.VIII Istruzione

"Blockchain in Education" è un report della Comunità Europea, sulle applicazioni della blockchain nell'istruzione, focalizzato sulla possibilità di tracciare in modo digitalizzato le conoscenze degli studenti per crearne un profilo personale unico ed immutabile.
Università prestigiose come MIT e FSMB hanno dato il via a questa iniziativa.

IV.IX Identità Digitale

X-Roard ed E-Residency sono due piattaforme, usate in Estonia, per il l'identità digitale.
La prima, collaborando con infrastrutture pubbliche e private, eroga e traccia servizi come identità digitale, servizi sanitari e istruzione.
La E-Residency, invece, permette a chiunque nel mondo di poter creare un'identità digitale estone. Questa operazione permetterebbe a chiunque di poter aprire una start up da remoto, senza burocrazia. Fino agli ultimi dati troviamo 45mila cittadini digitali, da 167 Paesi diversi che hanno avviato oltre 5mila start up.

IV.X Negozi

I programmi fedeltà ed i codici coupon gestiti dai negozi tramite blockchain permetterebbero al gestore una maggiore sicurezza ed affidabilità per poter tracciare i propri clienti, sbloccando codici sconto al raggiungimento di determinati obiettivi derivanti dall'acquisto di beni.
Stesso discorso per i pagamenti, che quasi annullerebbero le commissioni, le quali in regime ordinario azzererebbero il profitto dei commercianti qualora il bene avesse un importo basso; come nel caso del caffè.

IV.XI Cloud Storage

I robot informatici utilizzati per l'invio dei messaggi hanno causato frodi per oltre 7 miliardi di ollari nel 2017. Determinate pubblicità e tracker rallentano la rete internet dei dispositivi mobili, violando

talvolta la privacy. Queste sono le motivazioni che hanno spinto L'*Interactive Advertising Bureau* (IAB) a rilasciare il suo primo paper sulla tecnologia blockchain per ridurre i costi, eliminare le frodi ed aumentare l'efficienza.

Il Cloud Storage è il processo di archiviazione di piattaforme in grado di gestire grandi spazi in cloud, che dietro pagamento affittano a terzi. Non garantiscono un'elevata sicurezza e privacy nella gestione dei dati personali.
Il supporto della catena la farebbe diventare una commodity scambiabile in maniera centralizzata.

CAPITOLO V: Vantaggi e svantaggi della Blockchain

V.I Svantaggi

Gli svantaggi della blockchain, per ora, risiedono nell'eccessivo consumo energetico riposto nella creazione dei nuovi blocchi o nel processo di verifica (Proof of Work).

Basti pensare che, per alimentare la prova di lavoro nel Bitcoin, l'energia di milioni di computer equivale all'incirca al consumo annuale di elettricità della Danimarca.

I problemi di scalabilità non sono di certo da sottovalutare, infatti, rappresentano uno degli ostacoli maggiori per lo sviluppo della catena. Far sì che un maggior numero di transazioni non risenta delle prestazioni è assai complesso. Il basso volume di transazioni al secondo che si possono effettuare è un grosso ostacolo alla praticità della rete.
Per convalidare un possibile pagamento in criptomonete di un bene comune, come il caffè, ci potrebbero volere alcuni minuti. Questo perché le transazioni al secondo delle criptovalute variano in base alla tipologia e quelle con un alto grado di affidabilità, come Bitcoin, potrebbero vedere la transazione rimandata per alcuni minuti a causa di una congestione della rete.
Il risultato? Niente caffè con pagamento virtuale.
Questo è il prezzo da pagare se si volesse una rete sicura, trasparente e immutabile.
Ed a proposito di prezzo, qualora si dovesse verificare, come detto precedentemente, una congestione della rete, coloro che valideranno le transazioni chiederanno un *feed* più elevato in modo tale da poterla collocare in cima alle loro priorità.

L'altro svantaggio è unicamente quello umano. Nella creazione di reti private è possibile fare numerosi errori rendendo più semplice la via alla manomissione da parte di terzi.

Fortunatamente la rete open sta cercando di porre sostanziali modifiche in modo da poter arginare questi problemi. Uno degli apporti più significativi potrebbe essere quello dell'utilizzo della Proof of Stake a discapito della prova di lavoro.

V.II Vantaggi

Il problema della fiducia è uno dei protagonisti del commercio che, senza dubbio, ne rallenta l'attività. Basti pensare che nel periodo pandemico e post, le attività di e-commerce sono andate incontro ad un'accelerazione notevole, accaparrandosi l'attenzione di esperti e neofiti dell'acquisto online.
Si è potuto notare come, in Italia, la maggior parte delle persone preferissero un pagamento in contrassegno (pagamento alla consegna), piuttosto che pagare con carte di credito o debito, poiché non fiduciosi della corretta portata a termine del contratto.
Nel Sud Italia troviamo il dato maggiore, con una media del 27,27% di persone che avrebbero pagato solo in contrassegno, qualora non fosse possibile avrebbero abbandonato la transazione. La Calabria, con il suo 34,8%, è la regione meno *truster*.
Questo ovviamente ha come effetto il calo delle vendite da parte dei proprietari di negozi online, a meno che non mettano a disposizione il pagamento alla consegna. Questo processo non sarebbe così semplice, poiché, vedrebbe l'acquisto in stock di centinaia o migliaia di prodotti da parte del proprietario dell'e-commerce, se dovesse trattarsi del caso del *dropshipping*, il pagamento di un magazzino per poter porre i beni e la spedizione a dei trasportatori che possano effettuare consegne nelle ventiquattro o quarantotto ore, al fine di essere competitivi con i competitors (Amazon ed altri e-commerce).
Oltre a dover alzare i prezzi, l'imprenditore digitale, si potrebbe trovare di fronte al problema di eventuali furti del denaro contante, da parte dei fornitori, o a valute false date dai clienti.

Tutto questo sarebbe risolvibile grazie all'uso degli smart contract, all'arrivo di un bene si sbloccherebbe la transazione da parte del cliente, e della supply chain gestita dalla blockchain, con trasparenza e costi notevolmente ridotti.

Senza tener conto delle frodi stesse compiute dagli imprenditori digitali che, secondo la stima della Procura delle Repubblica del Tribunale di Pescara, in due anni si aggirerebbe intorno ai 330 milioni di euro.

L'uso della Blockchain nelle transazioni abbatte i costi derivanti dalle commissioni nei confronti degli istituti bancari, che di solito si aggira intorno all'1% e il 3%, e il tempo entro il quale termina la suddetta transazione.
Basti pensare che i giorni che impiegherebbe un trasferimento di denaro fiat internazionale tramite banche richiederebbe dagli uno ai quattro giorni; in blockchain si parla di minuti.

La commissione media sulla blockchain, di bitcoin, è di circa 2,67 $, ovvero 0,000056 BTC.

Lunedì 13 settembre 2021 è stata registrata una transazione di 2 miliardi di dollari in BTC tra due utenti con una commissione pari a 0,00001713 BTC, ovvero: 0,78 $.
La stessa operazione, svoltasi tramite banca, avrebbe portato il prezzo delle commissioni tra i 20 e i 60 milioni di dollari; calcolando anche la minaccia della tutela di privacy che subirebbero le parti coinvolte nella transazione.

Altro punto a favore della catena è la decentralizzazione del sistema che fa calare vertiginosamente la possibilità di poter manomettere il sistema di blocchi. Questo pericolo potrebbe presentarsi solo nel caso in cui questa fosse molto piccola e con pochi utenti.
Per le reti maggiori è quasi impossibile, o non conveniente, a causa dell'eccessivo volume economico ed energetico che richiederebbe. L'eliminazione dell'intervento umano nella fase di verifica, oltretutto, rende questo sistema sicuro ed affidabile, infatti, se uno dei computer dovesse contenere un errore crittografico, questo si troverebbe ad essere l'unico con errore e verrebbe automaticamente escluso dalla catena senza così influenzare gli altri nodi.

V.III Conclusioni

Una volta compresi i possibili svantaggi, che stanno cercando di arginare con vari metodi come l'utilizzo della Proof of Stake per abbattere costi e consumi energetici della Proof of Work, abbiamo potuto notare come la catena di blocchi porterebbe un alleggerimento burocratico ed economico non indifferente nello scambio di beni o servizi. Grazie alla decentralizzazione e all'eliminazione delle terze parti è stato possibile creare un sistema con assenza di sfiducia e con la massima trasparenza (senza violare la privacy).
L'esempio più calzante, come riportato, la conclusione di una transazione regolare fra due individui da due miliardi di dollari (BTC) ha portato il pagamento delle commissioni bitcoin di 0,78$.
Nelle ultime settimane la UE ha deciso di destinare 150 milliardi di euro in blockchain e IoT (*Internet of Things*), vale a dire il 20% dei 750 miliardi di euro per la ripresa economica a seguito della pandemia di Covid-19; si è aperto anche uno spiraglio per la collaborazione tra UE e Stati Uniti per la regolamentazione delle criptovalute della blockchiain.

Questa tesi ha cercato di proporre una visione ampia delle funzioni e delle applicazioni della blockchain, provando a stimolare l'interesse verso questo sistema e far comprendere l'influenza corrente e futura che eserciterà nel mondo venturo, evidenziando i primi piccoli grandi passi verso un futuro che abbraccerà sempre di più la catena di blocchi e le sue potenzialità.

BIBLIOGRAFIA

"Blockchain: tecnologie e applicazioni per il Business"; Gianluca Chiap, Jacopo Ranalli, Raffaele Bianchi; Editore Enrico Hoepli Milano,

"Da Zero alla Luna: quando, come, perché la Blockchain sta cambiando il mondo"; Gianluca Comandini; Dario Flaccovio Editore, prima edizione febbraio 2020

"La blockchain per le imprese: come prepararsi alla nuova Internet del valore; Mauro Bellini; in collaborazione con Maria Teresa Della Mura; tecniche nuove

"Criptovalute & Blockchain 2021: dalla crittografia al Bitcoin"; Henry D. Stone

"Blockchain 2021"; Nathan Real

https://github.com/bitcoinbook/blob/develop/preface.asciidoc

https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf

https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/

https://it.wikipedia.org/wiki/Bitcoin

https://it.investing.com/crypto/bitcoin

https://www.plus500.it/Instruments/BTCUSD/What-Moves-Bitcoins-Price~2

https://www.ilsole24ore.com/art/smart-contract-cosa-sono-e-come-funzionano-clausole-blockchain-ACsDo2P

https://www.altalex.com/documents/news/2020/10/21/blockchain-smart-contract-benefici-limiti

https://www.blockchain4innovation.it/mercati/legal/smart-contract/blockchain-smart-contracts-cosa-funzionano-quali-gli-ambiti-applicativi/

https://www.investopedia.com/terms/s/smart-contracts.asp

https://www.money.it/Smart-Contract-cosa-sono-come-funzionano

https://www.plus500.it/Instruments/ETHUSD/What-is-the-difference-between-Ethereum-and-Bitcoin~2

https://www.cmcmarkets.com/it-it/impara-come-operare-con-criptovalute/cosa-e-ethereum

https://www.ig.com/it-ch/ethereum-trading/cosa-e-ethereum-e-come-funziona

https://www.statista.com/topics/2308/bitcoin/

https://it.cointelegraph.com/news/bitcoin-worth-2-billion-moves-for-just-78-cents

https://www.fortuneita.com/2021/05/08/acquisti-online-il-17-degli-italiani-preferisce-il-contrassegno/

https://www.ilsole24ore.com/art/e-commerce-guardia-finanza-scopre-frodi-fisco-330-milioni-euro-AEzl2fG

https://it.cointelegraph.com/news/german-law-allowing-institutional-funds-to-hold-crypto-comes-into-effect-aug-2

https://it.cointelegraph.com/news/eu-set-to-invest-177b-in-blockchain-and-other-novel-technologies