BLOCKCHAIN

LA GUIDA DEFINITIVA PER CONOSCERE BLOCKCHAIN, BITCOIN, CRIPTOVALUTE, CONTRATTI SMART E IL FUTURO DEL DENARO.

Scritto da Mark Gates

Blockchain:

La guida definitiva per conoscere blockchain, Bitcoin, criptovalute, contratti smart e il futuro del denaro.

Scritto da Mark Gates

Le informazioni contenute in questo volume sono solo per scopi istruttivi e di informazione generale. Il contenuto di questo volume non dovrebbe essere considerato un consiglio o una raccomandazione.

Il lettore dovrà considerare gli aspetti legali, finanziari e di tassazione nel valutare in che modo le informazioni contenute in questo volume si adattino alle sue personali circostanze.

Sebbene sia stata presa ogni precauzione nella preparazione di questo volume, l'editore non assume alcuna

responsabilità per errori, omissioni o danni risultanti dall'uso delle informazioni qui contenute.

L'autore e l'editore non sono responsabili per alcuna perdita causata, sia a causa di negligenza che altro, risultante dall'uso, o dall'affidamento alle informazioni fornite, direttamente o indirettamente, da questo libro.

Blockchain: la guida definitiva per conoscere blockchain, Bitcoin, criptovalute, contratti smart e il futuro del denaro.

Prima edizione. 1 giugno, 2017

Scritto da Mark Gates.

Errori e Feedback

Contattateci se trovate degli errori

Sebbene sia stato effettuato ogni sforzo possibile per assicurare la qualità e la correttezza di questo libro, talvolta nelle prime edizioni di una pubblicazione rimangono degli errori di ortografia e grammatica.

Apprezzeremmo molto se, avendo notato degli errori in questo libro, ci contattaste prima di intraprendere

qualsiasi altra azione. Ciò ci permetterà di risolvere rapidamente questi errori prima che abbiano un'influenza negativa sull'autore.

Se troverete dei problemi o degli errori all'interno del libro, contattateci e li correggeremo prima possibile.

I lettori che ci segnaleranno degli errori saranno invitati a ricevere in anticipo copie dei libri che pubblicheremo in futuro.

Errori: errors@wisefoxpub.com

Feedback

Per ogni feedback generale riguardo al libro, potete contattarci all'indirizzo e-mail qui sotto:_

Feedback: contact@wisefoxpub.com

Indice

Guida Bonus alle Risorse

Ottieni gratis la Guida alle risorse blockchain.

La guida include delle risorse per imparare di più sulla blockchain, su Bitcoin, Ethereum e gli ICO.

Include anche una rapida guida di riferimento per

comprendere gli aspetti importanti della blockchain e delle criptovalute.

Attualmente, questa guida è disponibile solo in inglese.

Clicca qui per ottenere la Guida Bonus alle Risorse

Recensioni

Le recensioni ci aiutano a migliorare il libro e aiutano l'autore.

Se questo libro vi è piaciuto, apprezzeremmo molto se poteste impiegare qualche minuto per condividere la vostra opinione e pubblicare una recensione su Amazon.

Introduzione

"Su Internet, nessuno sa che sei un cane." - Peter Steiner

"Nella blockchain, nessuno sa che sei un frigorifero." - Richard Gendal Brown

La tecnologia Blockchain è stata chiamata la più grande innovazione dall'avvento di internet.
I sostenitori della tecnologia ritengono che nel giro di qualche decennio danneggerà ogni industria attualmente esistente, e che avrà un impatto sulla vita di quasi tutti gli abitanti del

pianeta.

La tecnologia blockchain è davvero una delle più grandi rivoluzioni tecnologiche nella storia, o è solo una moda?

La tecnologia blockchain porterà i governi e le banche a cambiare il modo in cui processano le informazioni, o non succederà nulla?

I sostenitori delle aziende che si occupano di tecnologia blockchain sono troppo eccitati, e stanno creando un'altra bolla di sapone per quella che è semplicemente solo un nuovo modo di creare un database?

In questo libro scopriremo le risposte a tutte queste domande, e affronteremo i due lati della questione, i pro e i contro della tecnologia blockchain.

Questo libro spiegherà cos'è la tecnologia blockchain, come funziona, quali sono i suoi usi potenziali e qual è l'impatto di questa tecnologia.

Sebbene parleremo di molte delle potenziali applicazioni e dei benefici, questo libro non intende proporre la tecnologia blockchain come risposta a tutti i problemi dei sistemi di governo, delle banche e delle industrie.

Lo scopo di questo libro è quello di fornire una comprensione equilibrata della tecnologia blockchain, combinando i benefici e i potenziali usi con i rischi e gli svantaggi, e smontando alcune delle esagerazioni che la riguardano.

Questo libro è scritto per le persone che si affacciano per la prima volta alla tecnologia blockchain, e che cercano una spiegazione non tecnica di questa tecnologia.

Quando ho conosciuto per la prima volta la tecnologia blockchain, ho visto che c'erano moltissime informazioni tecniche

sulla blockchain, sebbene distribuite e mal strutturate, ma nessuna guida che partisse da una base non tecnica.

Ho scritto questo libro pensando al libro che avrei voluto leggere quando ho cercato di imparare e comprendere per la prima volta la blockchain.

Spero che questo libro vi piacerà e che lo troverete utile, istruttivo e arguto per imparare a comprendere la tecnologia blockchain.

Una nota sui punti chiave:

- Alla fine di ogni capitolo ci sono dei punti chiave, che ripeteranno le informazioni contenute nel capitolo in una breve lista puntata. La lista è pensata per le persone che preferiscono una sintesi delle informazioni dei punti chiave.

- Se un capitolo non vi piace o se non avete tempo per leggerlo, potrete passare ai punti chiave per comprendere le informazioni principali del capitolo.

- I punti chiave vi aiuteranno inoltre a prendere appunti, a ripassare il materiale o a trovare rapidamente dei riferimenti senza dover rileggere nuovamente il capitolo.

- Se avete letto l'intero capitolo, potete saltare i punti chiave, perché potrebbero sembrarvi una ripetizione del materiale già letto.

Capitolo Uno: Cos'è una blockchain?

Per spiegare in modo semplice, una blockchain è come un database, è un modo per registrare dei valori e delle transazioni.

Sfortunatamente, questa semplice definizione non è abbastanza eccitante per molte persone, e farà loro pensare "E quindi? Tutto questo rumore per un nuovo tipo di database?"

Tuttavia, chiamare una blockchain un nuovo tipo di database equivarrebbe a

dire che l'e-mail è un nuovo modo per spedire delle lettere. Sebbene la blockchain sia un database, tale definizione non spiega la vera innovazione del modo in cui la blockchain registra i valori e le transazioni.

Nel passato, quando un valore o una transazione veniva salvato in un database, le persone si affidavano a una terza parte come una banca, un governo o un'azienda affinché registrasse tale informazione. Tutti confidano nel fatto che le banche non rubino il loro denaro perché sono regolate dal governo, e nel caso in cui una banca fallisca confidano nel fatto che il governo verifichi che il

loro denaro sia al sicuro.

Quando trasferiscono del denaro o pagano beni e servizi, tutti confidano nel fatto che le banche e le aziende di carte di credito prelevino l'importo corretto dal loro conto corrente e lo depositino nel conto del venditore. Il venditore, a sua volta, confida nel fatto che la società della carta di credito lo pagherà, e che ogni eventuale disputa o frode sulla transazione verrà gestita dalla società stessa.

Se una persona paga in contanti in un negozio, il negoziante confida nel fatto che potrà portare quel pezzo di carta con

stampato un numero, garantito dal governo, in un altro negozio, e che potrà scambiarlo per ottenere altri beni e servizi. Il negoziante sa anche che, se porterà la banconota in banca, potrà essere aggiunta al saldo digitale del suo conto corrente e utilizzata per effettuare pagamenti con carte di credito e transazioni online.

Tutti confidano nel fatto che queste istituzioni esterne si prenderanno cura del loro denaro e delle loro informazioni. Tutti confidano nel fatto che le banche e le società finanziarie manterranno i dati delle loro carte di credito riservati e al sicuro. Confidano nel fatto che le banche e le società

finanziarie abbiano dei database con i dati dei loro saldi e delle loro transazioni, e che questi database siano aggiornati accuratamente. Le banche, a loro volta, confidano nel fatto che i governi abbiano database ed elenchi delle banconote stampate.

La fiducia nelle istituzioni non è soltanto finanziaria, ma si estende a ogni aspetto della nostra vita. Se avete mai preso in prestito un libro da una biblioteca, sapete che la biblioteca ha un database che contiene tutti i libri in suo possesso. La biblioteca ha anche un database dei membri, di tutti i libri in prestito, della data di scadenza di ciascun prestito e di

tutti i libri oltre la scadenza.

La biblioteca ha anche un database centrale con i vostri dati personali, l'indirizzo di casa e altre informazioni. Se non restituite un libro che avete preso in prestito, può imporre una multa e, eventualmente, procedere legalmente contro di voi per furto.

Queste informazioni sui database, che riguardano i vostri dati personali, i libri che avete preso in prestito, le vostre abitudini di lettura, sono informazioni private e mantenute dalla biblioteca; confidate nel fatto che non le condividano con altre persone.

In queste istituzioni le informazioni sono centralizzate, e ognuna di esse tiene in esercizio il proprio sistema, con i propri dati.

Il tema comune a tutte queste transazioni quotidiane è la fiducia che riponiamo nelle istituzioni e nei database centralizzati che tengono in esercizio per mantenere un archivio dettagliato delle nostre vite.

Un altro tema sottostante molto comune è il fatto che non ci fidiamo l'uno dell'altro.

Provate a immaginare gli scenari sopra

presentati, ma senza che le istituzioni centralizzate a cui date fiducia siano coinvolte nelle transazioni.

Immaginate di possedere un negozio, e che qualcuno vi dia un pezzo di carta con scritto sopra "Ti devo 100 €", con la loro firma. Immaginate che vi dicano che, se porterete quel pezzo di carta in un altro negozio, potrete usarlo per comprare beni e servizi per 100 € da quel negozio.

Vi fidereste?

La risposta è probabilmente no, ma è esattamente quello che tutti fanno ogni giorno con la valuta cartacea. Una

banconota da 100 € è soltanto un pezzo di carta con un "Ti devo 100 €" firmato dal governo. Usiamo e accettiamo queste banconote praticamente ogni giorno, confidando nel fatto che i negozi le accetteranno, e i negozianti a loro volta confidano che i loro fornitori le accetteranno e così via.

La situazione in cui la blockchain offre il potenziale più significativo è quella dei paesi in cui la gente non si fida delle banche, delle istituzioni, dei governi, delle valute né di ciascun altro.

Anche negli Stati Uniti, uno dei paesi più sviluppati e con un sistema

finanziario più regolato al mondo, diverse grandi istituzioni finanziarie hanno dichiarato fallimento durante la Grande Crisi Finanziaria. Delle società finanziarie che esistevano da centinaia di anni sono fallite da un giorno all'altro, portando con sé i risparmi di una vita di moltissime persone.

Nel 2015 in Grecia, un paese sviluppato dell'Eurozona, le banche hanno congelato tutti i conti correnti e consentito ai correntisti di prelevare dai bancomat soltanto 70€ al giorno.

Quale alternative avevano i risparmiatori, se non affidare il proprio denaro a quelle che credevano essere

banche e società degne di fiducia? Prendere tutti i loro soldi e nasconderli sotto il materasso? Se qualcuno scoprisse che tenete i vostri risparmi in casa rischiereste un furto, e se ci fosse un incendio potreste perdere tutto il vostro denaro.

Se le banche possono collassare, e i governi possono congelare i prelievi negli Stati Uniti e in Europa, come possono coloro che vivono in paesi meno sviluppati e regolati fidarsi delle loro banche e dei loro governi?

La risposta è semplice: non possono.

La questione della fiducia e della blockchain

Ci sono miliardi di persone nel mondo che vivono in nazioni governate da dittature militari, in cui i governi controllano le banche e rubano o sequestrano il denaro dai conti, in cui la valuta locale non viene accettata nei negozi, il crimine è altissimo e non ci sono sistemi legali per proteggere i cittadini e i loro beni.

Ci sono molti paesi in cui, anche se le banche non rubano il denaro dei cittadini o rischiano di collassare, le transazioni sono monitorate attentamente dal

governo, che può arrestare, imprigionare o giustiziare i cittadini in base alle loro transazioni.

Prendiamo l'esempio della biblioteca, un database centrale apparentemente innocuo, con cui non dovreste temere di condividere delle informazioni. Potreste prendere in prestito un libro malvisto dal governo del vostro paese, come "Guida per principianti al rovesciamento di una dittatura militare", o 1984 di George Orwell. Il governo potrebbe segnalare le vostre abitudini di lettura come potenzialmente pericolose, e ciò potrebbe portare a un'investigazione della vostra vita personale, e in certi paesi all'arresto, o

anche peggio.

In queste nazioni, in cui c'è una mancanza di fiducia nelle società e nel governo, le transazioni sono rischiose e pericolose. Se le persone mettono del denaro in banca, rischiano che la banca o il governo lo rubino. Se devono fare un acquisto importante, come ad esempio una casa, sono costrette a tenere il denaro in contanti, oro, gemme o metalli per risparmiare per l'acquisto, rischiando così che il denaro venga rubato o distrutto in un incendio.

Anche nonostante tutto questo rischio, se riescono a risparmiare abbastanza

denaro per l'acquisto di una casa, rischiano comunque che il venditore rubi il loro denaro e non trasferisca loro la proprietà della casa. Non c'è un sistema legale stabile per contestare la proprietà o denunciare il furto. Se l'acquisto è stato fatto in denaro o in oro, e non con una transizione elettronica, non c'è nemmeno una prova che la transazione abbia avuto luogo.

I database centralizzati e le istituzioni funzionano quando c'è fiducia nella legge, nelle regole, nel governo, nella finanza e nelle persone. Anche quando in un paese c'è fiducia relativamente a tutti questi fattori, a volte la fiducia viene tradita e le persone perdono il loro

denaro e i loro beni.

Un database decentralizzato costruito sulla blockchain elimina la necessità di istituzioni e database centralizzati. Tutti sulla blockchain possono visualizzare e validare le transazioni, creando trasparenza e fiducia.

La fiducia è il cuore della blockchain; fornisce un sistema di fiducia tra le persone, senza che sia necessario coinvolgere un intermediario nella transazione.

La blockchain permette alle persone di effettuare transizioni l'una con l'altra,

scambiandosi beni di qualsiasi valore. Nell'esempio fornito si tratta di libri, ma può essere usata anche per proprietà, azioni, denaro, file digitali e molto altro.

Differenze tra la blockchain e i Bitcoin

Il primo riferimento alla blockchain si trova nel codice sorgente di Bitcoin. Essenzialmente, la prima blockchain è stata creata nel momento in cui Bitcoin è stato creato. Nel prossimo capitolo parleremo della storia di Bitcoin e della blockchain, quindi adesso non andremo molto nel dettaglio.

La Blockchain è una delle tecnologie sottostanti di Bitcoin. A volte si ritiene, erroneamente, che la blockchain sia la sola tecnologia che sta dietro Bitcoin, ma in realtà Bitcoin è stato creato utilizzando una vasta gamma di altre tecnologie crittografiche, combinate con la blockchain.

Bitcoin è una valuta digitale, principalmente utilizzata per i pagamenti. Rappresenta uno dei modi in cui la tecnologia blockchain può essere utilizzata; tuttavia la blockchain può essere utilizzata per archiviare e trasferire qualsiasi cosa che abbia valore, non solo transazioni finanziare.

I sistemi basati sulla blockchain vengono utilizzati per una vasta gamma di applicazioni in diverse industrie, come le identità digitali, i social network, il voto, l'archiviazione cloud, le applicazioni distribuite e molto altro di cui parleremo più in là nel libro. Le aziende private e i governi stanno attualmente sviluppando altri sistemi basati sulle blockchain, le cui possibilità sono praticamente infinite.

I Bitcoin, invece, vengono utilizzati soltanto come pagamento digitale. Sebbene Bitcoin stia crescendo in popolarità, e il suo prezzo stia salendo

continuamente, è pensato principalmente come metodo di pagamento.

Nel prossimo capitolo parleremo nel dettaglio di come funziona la blockchain, e forniremo degli esempi.

Punti chiave:

- La blockchain è come un database, è un modo per registrare dei valori e delle transazioni. Su una blockchain è possibile salvare praticamente ogni cosa.

- La maggior parte delle transazioni che avvengono tra le persone richiedono un intermediario che fornisca fiducia, sicurezza e che faciliti le transazioni, ad esempio banche o istituzioni finanziarie.

- La tecnologia blockchain elimina la

necessità di un intermediario, permettendo alle persone di effettuare transazioni direttamente l'una con l'altra.

- Miliardi di persone al mondo vivono in paesi dove non è possibile fidarsi degli intermediari come banche, governi e sistemi legali per le transazioni o l'archiviazione dei propri dati. Le blockchain sono particolarmente utili in queste circostanze, perché aiutano a fornire fiducia e assicurazioni alle persone quando effettuano transazioni l'una con l'altra.

- Bitcoin è un sistema basato sulle

blockchain. Le blockchain non sono un sistema basato su Bitcoin.

- Bitcoin è usato principalmente per i pagamenti. I sistemi basati sulle blockchain hanno un'ampia gamma di applicazioni, e possono essere usate per trasferire qualsiasi cosa abbia valore.

Capitolo Due: Come funziona la Blockchain

Nota: questo capitolo è una guida generale e non tecnica sul funzionamento della blockchain. La sezione Risorse contiene dei link che vi aiuteranno a esplorare ulteriormente gli aspetti tecnici della tecnologia blockchain.

Il capitolo precedente vi ha presentato la tecnologia blockchain con un breve accenno a come può essere usata per sostituire gli intermediari nelle transazioni. In questo capitolo parleremo nel dettaglio di come funziona la

blockchain, e forniremo degli esempi.

Tornando all'esempio della biblioteca del capitolo precedente, possiamo dire che la biblioteca sia un intermediario che mantiene in esercizio in database centralizzato delle persone che richiedono in prestito i libri.

Se qualcuno ha già preso in prestito un libro che vi interessa, potete chiedere che la biblioteca vi notifichi quando il libro sarà restituito, ma la biblioteca non vi rilascerà i dettagli della persona che ha preso in prestito il libro.

La persona che ha il libro potrebbe essere il vostro vicino di casa, più vicino di quanto la biblioteca non sia

per entrambi, ma non potrete andare a casa sua e chiedere di prendere in prestito il libro da lui. La biblioteca mantiene il database centrale con tutte le informazioni sui libri presi in prestito, e non le condivide con i membri.

Adesso, immaginate una biblioteca condivisa in cui ognuno contribuisce con i suoi libri, e permette agli altri di prenderli in prestito. Probabilmente avete moltissimi libri che le altre persone vorrebbero prendere in prestito da voi, e allo stesso modo ci sono molte altre persone che hanno libri che voi vorreste prendere in prestito e leggere.

Nell'esempio della biblioteca condivisa,

tutti possono unirsi, possono prendere in prestito i libri e anche prestarli ad altre persone, senza doverli riportare alla biblioteca o al proprietario originale.

Come manterreste i dati su chi ha preso in prestito i libri, che libro hanno, e chi è il proprietario originale di ciascun libro?

Non dovreste mantenere un archivio relativo solo ai vostri libri, ma ai libri di tutti coloro che fanno parte della biblioteca condivisa. Dovrete mantenere un archivio di tutti i libri che si trovano attualmente nella biblioteca, dei proprietari originali, dei libri presi in prestito, e di tutte le altre persone a cui

sono stati prestati dei libri.

Potreste assegnare a una persona del gruppo il compito di registrare i dati, ma significherebbe tornare al modello originale della biblioteca con database centralizzato.

Tutto ciò può sembrare complicato, e probabilmente vi starete chiedendo, perché sono entrato in questa biblioteca condivisa quando potrei comprare tutti questi libri in formato Kindle?

Questa è una situazione in cui è davvero possibile apprezzare i benefici della tecnologia blockchain rispetto ai

database tradizionali.

La blockchain fornisce un database distribuito e decentralizzato di tutti i dati dei libri della biblioteca.

Con un database decentralizzato, tutti nella biblioteca hanno accesso ai dati. Possono vedere tutti i libri della biblioteca, i proprietari originali, chi ha preso in prestito ciascun libro, e se poi hanno prestato quel libro a qualcun altro.

Ogni volta che un libro viene preso in prestito dalla biblioteca condivisa, tutti i dati sui libri, a cui tutti hanno accesso, vengono aggiornati. Non c'è un database

centrale e non serve un'istituzione che gestisca il sistema, perché tutti contribuiscono nel mantenere in esercizio il database.

Potete gestire una biblioteca senza avere necessità di un database centrale e di un'istituzione esterna che la gestisca.

Perché si chiama blockchain?

Nell'esempio della biblioteca, ogni volta che viene preso in prestito un libro si crea una transazione. Ci sono moltissime transazioni che avvengono nello stesso momento, quindi queste transazioni vengono raggruppate e aggiunte a un nuovo blocco.

Il nuovo blocco viene aggiunto "sopra" il blocco precedente con un riferimento al blocco che viene prima, collegando così i due blocchi.

Ad esempio:

Il blocco 10 è collegato al blocco 9
Il blocco 9 è collegato al blocco 8
Il blocco 8 è collegato al blocco 7
Etc.

Collegando insieme questi blocchi, si crea una catena ("chain") di blocchi ("block"), da cui il nome "blockchain". Ogni nuovo blocco ha un riferimento al

blocco precedente, quel blocco ha un riferimento a quello prima ancora e così via fino all'inizio.

Nell'esempio della biblioteca, tutti potrebbero andare al blocco più recente della catena. Potrebbero vedere tutti i libri che sono stati presi in prestito, e da chi. Potrebbero poi vedere le transazioni nel blocco precedente, per vedere chi aveva i libri prima di loro, e andare indietro fino all'inizio per vedere il proprietario originale.

Non c'è alcun database o autorità centrale; se una persona sostiene di essere il proprietario originale di un libro, per scoprire se è vero è possibile

tracciare dall'ultimo blocco di transazioni fino al primo blocco, noto come "blocco genesi".

Cambiare le transazioni e i blocchi dopo che sono stati aggiunti

I blocchi aggiunti alla blockchain non possono essere modificati o cambiati; sono permanentemente aggiunti alla blockchain. Dal momento che ogni blocco fa riferimento al precedente, se qualcuno vuole commettere una truffa cambiando una transazione, dovrà cambiare tutti i blocchi prima e dopo quel blocco.

Il network Bitcoin ha stimato che, dopo un'aggiunta di 6 blocchi sopra un determinato blocco, diventa impossibile cambiare le transazioni in quel blocco perché la potenza di calcolo richiesta rende il cambiamento impossibile.

Se la transazione avviene nel blocco numero 10, quando la blockchain raggiunge il blocco 16 diventa impossibile tornare a cambiare le transazioni nel blocco 10.

I blocchi in cima a una transazione possono essere chiamati anche conferme; alcune aziende aspettano di avere 6 conferme prima di accettare un pagamento, come assicurazione del fatto

che la transazione non verrà cambiata nella blockchain.

Spesa Doppia

Per comprendere un altro problema che viene risolto dalla blockchain, prendiamo un esempio in cui qualcuno vuole trarre profitto dal sistema della libreria condivisa, rubando dei libri.

Ogni volta che un libro viene preso in prestito si crea una transazione pendente; questa transazione viene mandata a tutti coloro che sono nel network per essere validata e aggiunta alla blockchain. La persona che la raggruppa con altre transazioni pendenti

e aggiunge un blocco valido di transazioni alla blockchain ottiene una ricompensa.
Il nuovo blocco di transazioni viene aggiunto alla blockchain, e il database di tutti viene aggiornato con una registrazione della transazione.

Tutti coloro che si trovano nel network possono vedere chi ha ciascun libro, e da chi l'ha preso in prestito. Dal momento che tutti sanno chi ha ciascun libro, l'intero network può vedere se qualcuno non restituisce un libro, e qual è il suo status in ogni momento.

Scambio di valore nella blockchain

Aggiungiamo un altro fattore alla biblioteca condivisa; ogni volta che qualcuno prende in prestito un libro, paga alla persona da cui ha preso in prestito il libro un gettone chiamato "bookcoin".

Supponendo che una persona possa fare un profitto soltanto prestando i libri ad altre persone, dovrebbe pagare 1 bookcoin per prendere in presto un libro e riceverebbe 1 bookcoin quando qualcuno prende in prestito un libro da lui. Per fare un profitto, quindi, dovrebbe prestare più libri di quanti ne prende in prestito.

Lorenzo Losco si unisce alla biblioteca condivisa. Gli altri membri, però, sospettano che voglia fare qualcosa di losco.

Ciò nonostante, Lorenzo Losco contribuisce alla biblioteca con il libro "Romeo e Giulietta", qualcuno lo prende in prestito e lui ottiene 1 bookcoin.

Essendo un tipo losco, pensa a un piano per provare a prendere in prestito più libri di quelli che potrebbe permettersi con il suo saldo in bookcoin.

Lorenzo Losco prende in prestito "1984" da Davide.

Lorenzo Losco poi va velocemente a prendere in prestito "Amleto" da Susanna.

Entrambe le operazioni creano delle transazioni sul network. La prima transazione viene mandata a tutti i presenti sul network affinché approvino il prestito del libro "1984", e il fatto che Lorenzo Losco debba pagare a Davide 1 bookcoin per il prestito del libro.

Questa transazione viene dichiarata valida da tutti i presenti sul network, che la aggiungono a un nuovo blocco, il quale viene aggiunto alla blockchain: Lorenzo Losco prende in prestito "1984"

da Davide.
Lorenzo Losco paga 1 bookcoin a Davide.

Dopo che questa transazione viene eseguita, il network riceve la seguente transazione da approvare:
Lorenzo Losco prende in prestito "Amleto" da Susanna.
Lorenzo Losco paga 1 bookcoin a Susanna.

Il network controlla il saldo dei libri di Lorenzo Losco e vede che aveva solo 1 bookcoin, e che sta cercando di creare delle copie dei bookcoin per provare a imbrogliare il network.

Dal momento che il network è aperto e tutti hanno una copia dei dati, possono tracciare le transazioni fino all'inizio. Possono vedere che Lorenzo Losco aveva ricevuto 1 bookcoin per avere dato in prestito il libro, dandogli un saldo di 1 bookcoin.

Non ha 2 bookcoin da spendere, e tutti sul network possono vederlo. La maggioranza delle persone nel network concorda sul fatto che la transazione sia invalida. Non gli permettono di prendere in prestito un secondo libro, e il pagamento viene considerato invalido. La transazione viene rifiutata, e non viene aggiunta alla blockchain.

Consenso distribuito

In questo esempio è stato menzionato come la maggioranza delle persone in un network debbano concordare che una transazione sia valida affinché essa avvenga; ciò è noto come consenso distribuito.

Non è possibile che tutti coloro che si trovano su un network siano sempre d'accordo, perché ci saranno sempre persone che proveranno a imbrogliare il sistema, cercando di approvare transazioni false come valide.

Con molte blockchain, la soglia del consenso è del 50%; se più del 50% delle persone sul network concordano sulla validità di una transizione, la transizione viene accettata come valida.

Questo è il metodo in cui in genere le blockchain decentralizzate funzionano per approvare le transazioni e gestire il network. Invece di avere una sola entità che approva le transazioni e mantiene il database accurato, questa responsabilità viene condivisa in tutto il network. Tutti coloro che sono collegati a un network hanno diritto di parola sull'accettare o meno una transazione all'interno della blockchain.

Più avanti nel libro discuteremo i potenziali rischi e i pericoli che si verificano nel caso in cui più del 50% di un network accetti una transazione invalida.

Minare

Potreste avere sentito la parola "minare" quando si parla di Bitcoin e criptovalute.

Le richieste di transazioni vengono inviate a tutti i computer del network, affinché vengano validate e incluse nella blockchain.

Per validare una transazione e aggiungerla a una blockchain, i computer sul network devono risolvere un puzzle collegato al blocco successivo da aggiungere alla blockchain.

Il computer che risolve correttamente il puzzle per primo può aggiungere le transazioni in un blocco, e poi aggiungere il blocco di transazioni in una blockchain.

Chi riceve il puzzle per primo riceve una ricompensa, generalmente pagata nella criptovaluta o token utilizzato su quel network.

Questo processo viene chiamato "minare", perché è come minare piccole quantità di materiale da un blocco.

Prova del lavoro

I minatori che risolvono i puzzle e aggiungono blocchi validi al network vengono ricompensati per aver fornito potenza di calcolo, elettricità e risorse al network, perché ciò permette al network di mantenersi in esercizio.

Il puzzle che risolvono viene chiamato prova di lavoro. Si tratta di un puzzle matematico molto difficile da risolvere, ma la cui risposta è facile da verificare

una volta trovata.

Si può pensare ad esso come a un lucchetto con combinazione. Per aggiungere un nuovo blocco alla blockchain e ricevere una ricompensa, dovete trovare la combinazione di un lucchetto.

Potete trovare la combinazione del lucchetto soltanto provando a indovinare i numeri. Tutti coloro che si trovano sul network provano a indovinare i numeri della combinazione in modo casuale. La persona che trova per prima la combinazione ottiene una ricompensa e può aggiungere un blocco alla blockchain.

Una volta trovata la combinazione del lucchetto, tutti coloro che si trovano sul network possono inserire facilmente i numeri nel lucchetto per verificare che la combinazione sia giusta.

Risolvere il puzzle significa potere provare di avere contribuito con potenza di calcolo, elettricità, tempo e risorse al network. La ricompensa è un pagamento per il costo della contribuzione di queste risorse alla blockchain.

La prova di lavoro richiede una grande potenza di calcolo; ci sono altri metodi che possono essere utilizzati per gestire

una blockchain, e ne parleremo più avanti.

Riassunto di come funziona la blockchain

Abbiamo parlato di come un network di blockchain possa essere utilizzato per creare un database che sostituisca la biblioteca come istituzione centralizzata.

Per molte persone, sostituire il database di una biblioteca non è particolarmente importante al giorno d'oggi, quando tutto è centralizzato. Tuttavia, al posto dei libri possiamo pensare a qualsiasi cosa che abbia un valore.

Se sostituiamo i libri con dei titoli di

proprietà, ad esempio, possiamo vedere come la proprietà di un determinato bene possa essere trasferita o gestita via blockchain.

Quando la proprietà di un bene viene trasferita, tutti coloro che si trovano sul network ricevono una notifica del trasferimento di proprietà; la maggioranza del network approva il trasferimento, ed esso viene aggiungo alla blockchain come un dato visibile da tutti.

Se il proprietario del titolo prova a vendere la sua proprietà a due persone differenti, tutti sul network vedranno il

doppione del trasferimento, e una delle due transazioni verrà rifiutata dal network.

Come detto nel capitolo precedente, i luoghi in cui i network di blockchain possono avere il potenziale maggiore sono i paesi in cui non è possibile fidarsi delle società, delle banche e dei governi, e in cui gli archivi sono manuali o poco affidabili. La possibilità di sostituire i database e le istituzioni centralizzate con un network di blockchain per i documenti sulle proprietà potrebbe avere grandi benefici per coloro che vivono in questi paesi.

Abbiamo parlato principalmente di

come funziona la tecnologia blockchain a livello generale, e abbiamo parlato di alcuni esempi in cui può essere usata. Più avanti nel libro faremo altri esempi di applicazioni in cui i network di blockchain potrebbero sostituire le tecnologie e le istituzioni esistenti.

Punti chiave:

- Affinché una transazione sia processata e considerata valida, viene raggruppata insieme ad altre transazioni e aggiunta a un nuovo blocco.
- Il nuovo blocco viene aggiunto "sopra" il blocco precedente della blockchain. Ogni blocco fa riferimento al blocco precedente, collegandoli insieme come in una catena, da cui il nome "blockchain".
- La catena di blocchi nella blockchain si ricollega fino al primo blocco della catena, chiamato "blocco

genesi".

- Con una blockchain decentralizzata, ogni blocco di transazioni nella blockchain viene validato dal network. Tutti coloro che si trovano sul network ricevono informazioni sulle transazioni sul network; non c'è il controllo di un database centralizzato, posseduto da una sola azienda o istituzione.
- Quando un blocco di transazioni viene aggiunto alla blockchain, è difficile eliminarlo. Ogni blocco aggiunto al di sopra è una conferma del fatto che la transazione non verrà cancellata. Più blocchi ci sono al di sopra, più difficile è cancellarla,

finché non diventa impossibile. Nel network Bitcoin, il numero di blocchi accettato come conferma del fatto che una transazione non sarà cancellata è 6.

- Con il consenso distribuito, la maggior parte dei computer nel network devono essere concordi sul fatto che una transazione sia valida prima che venga accettata nella blockchain.
- La doppia spesa è quello che accade quando qualcuno sul network cerca di duplicare una transazione. Ciò viene generalmente fatto inviando transazioni più di una volta, prima che una di esse venga confermata e

accettata nella blockchain.

- Un attacco di doppia spesa accade quando un utente controlla più del 50% dei computer nel network. Ciò permette all'utente di duplicare le transazioni, controllando quali vengono accettate e rifiutate.
- "Minare" è ciò che si fa per validare transazioni e aggiungere nuovi blocchi alla blockchain. Per ogni blocco aggiunto alla blockchain viene data una piccola ricompensa, come un minatore che mini una piccola quantità di oro da un blocco.
- La prova di lavoro consiste nel risolvere un puzzle informatico per aggiungere un nuovo blocco alla

blockchain. È difficile da risolvere ma facile da provare, come la combinazione di un lucchetto. Fornisce una prova del fatto che si sono usate potenza di calcolo e risorse per contribuire al network.

Capitolo Tre: Storia della Blockchain e dei Bitcoin

"Credo che il fatto che all'interno dell'universo Bitcoin un algoritmo sostituisca la funzione del [governo] ... sia molto interessante. Sono un grande fan di Bitcoin"

-- Al Gore, 45esimo Vicepresidente degli Stati Uniti

La blockchain è stata nominata per la prima volta nel codice originale di Bitcoin. Sebbene adesso ci sia una

separazione tra la tecnologia blockchain e Bitcoin, la storia della blockchain è legata alla storia di Bitcoin, e questo capitolo parlerà della loro storia comune.

La crittografia è un fondamento chiave della blockchain. La crittografia ha una lunga storia come mezzo per proteggere segreti e messaggi, che risale a migliaia di anni fa. Un famoso esempio di crittografia nel mondo antico era il "Cifrario di Cesare", utilizzato da Giulio Cesare quando le informazioni scritte che mandava contenevano informazioni sensibili.

Il Cifrario di Cesare consisteva nel

sostituire ogni lettera del messaggio con una lettera diversa dell'alfabeto, a una distanza di un determinato numero di lettere. Per esempio, si possono spostare tutte le lettere di 3 lettere in avanti, facendo diventare ogni A una D, ogni B una E, ogni C una F e così via fino a sostituire ogni lettera del messaggio. Solo chi conosceva il numero di cui ogni lettera era stata spostata era in grado di leggere facilmente il messaggio.

Ai tempi l'alfabetizzazione era scarsa e c'erano moltissime lingue diverse che venivano parlate nel mondo, quindi i nemici che avessero intercettato il messaggio non sarebbero riusciti a leggerlo, o avrebbero pensato che le

lettere venissero scritte in una lingua straniera. Si tratta di un metodo semplice che oggi è facile da decifrare, ma che all'epoca era abbastanza efficiente da nascondere le comunicazioni, rendendole difficili da intercettare.

La crittografia moderna ha fatto molta strada dalle sue origini, ma le fondamenta di base rimangono le stesse. I messaggi o i dati vengono nascosti sostituendo le lettere e i numeri in modo da rendere impossibile leggere il messaggio senza avere il codice segreto o il metodo da utilizzare per decifrarlo.

Tornando alla crittografia sulla quale si

basa la tecnologia blockchain, tra gli anni '80 e '90 sono stati pubblicati diversi articoli che proponevano di cifrare i dati collegandoli in modo sicuro in delle catene, e vi erano anche delle proposte per delle valute digitali.

Nel 1982, David Chaum scrisse un articolo intitolato "Blind signatures per pagamenti non tracciabili". A causa di questo articolo, David Chaum viene riconosciuto come l'inventore del denaro digitale e delle blind signatures. Le blind signatures (firme cieche) nascondono il contenuto di un messaggio prima che esso sia firmato. La firma digitale può essere confrontata con l'originale, ma i contenuti rimangono

nascosti. Si tratta di una versione primitiva della firma crittografica utilizzata dalle criptovalute.

Questo e i successivi articoli pubblicati da David Chaum proponevano la possibilità che gli utenti potessero ottenere e spendere una valuta digitale in modo non tracciabile da banche o altre istituzioni. David Chaum, insieme ad Amos Fiat e a Moni Naor ha inoltre proposto delle transazioni online in grado di capire se il denaro era stato precedentemente speso, una possibile soluzione al problema della doppia spesa.

Nel 1990, David ha fondato DigiCash

per creare una valuta digitale basata sulle idee espresse nei suoi articoli, e nel 1994 è stato inviato il primo pagamento elettronico con DigiCash. L'inizio del comunicato stampa Digi-Cash del 1994 è qui sotto:

"Il primo sistema di pagamento elettronico del mondo su una rete di computer. (Data di Rilascio: 27 maggio 1994)

Il denaro elettronico ha la privacy del denaro fisico, e allo stesso tempo fornisce l'elevata sicurezza richiesta per gli ambienti di reti elettroniche esclusivamente grazie alle innovazioni nella crittografia a chiave pubblica."

La conferenza stampa era 14 anni in anticipo rispetto alla creazione di Bitcoin, e nonostante ciò se avessimo sostituito le parole "denaro elettronico" con Bitcoin, lo stesso comunicato stampa potrebbe essere utilizzato oggi per Bitcoin.

DigiCash aveva creato il primo sistema di denaro elettronico non tracciabile dalle banche, dai governi o dalle altre istituzioni. Utilizzava la crittografia, con chiavi pubbliche e private e firme per nascondere il contenuto dei messaggi nello stesso modo in cui le criptovalute lo fanno oggi.

DigiCash era forse troppo all'avanguardia per il suo tempo, perché nel 1994 la maggior parte delle persone non aveva neanche sentito parlare di internet. DigiCash dichiarò il fallimento nel 1998 e i suoi beni vennero acquistati da eCash technologies, un'altra azienda che si focalizzava sulle valute digitali.

All'inizio di Internet, lo spam via e-mail era un problema per cui ancora non esisteva una soluzione. Nel 1997, Adam Back propose un sistema per limitare lo spam via e-mail con degli attacchi denial-of-service, utilizzando un algoritmo prova di lavoro noto come hashcash.

Questo algoritmo prova di lavoro richiedeva che il mittente dell'e-mail risolvesse un puzzle informatico, e che mettesse la risposta nell'header dell'e-mail. Ciò implicava che il mittente dovesse utilizzare risorse e potenza di calcolo per mandare e-mail, rendendo più difficile mandare e-mail di spam in blocco. Il puzzle era difficile da risolvere per il mittente, ma verificare che la risposta fosse corretta era semplice per il destinatario dell'e-mail, rendendo così facile filtrare le e-mail spam che non avevano completato la prova di lavoro.

Nel 1998 Nick Szabo propose una valuta digitale decentralizzata chiamata

"bit gold"(oro bit). Nella sua proposta per il bit gold, gli utenti avrebbero allocato risorse e potenza di calcolo per risolvere puzzle crittografici. La maggioranza della rete avrebbe dovuto accettare la risposta come valida prima di passare al puzzle successivo. Una volta risolto e accettato dalla rete, il puzzle sarebbe diventato parte del successivo puzzle che la rete avrebbe dovuto risolvere. Ai puzzle erano associate data e ora, e ogni risposta diventava parte del puzzle successivo legandoli insieme come in una catena.

Nick Szabo dichiarò che, fino a quel momento, le valute digitali erano state vulnerabili al problema della doppia

spesa, perché potevano essere copiate e incollate a meno di dare il controllo a una banca o autorità centrale. Il suo lavoro sul bit gold era un tentativo di risolvere il problema della doppia spesa, combinandolo con una valuta digitale decentralizzata.

Bit gold non fu mai una valuta reale; la sua esistenza fu soltanto teorica, ma si ritiene che abbia gettato le fondamenta sulle quali furono successivamente costruiti Bitcoin e la tecnologia blockchain.

Nel 1998, Wei Dai pubblicò un articolo intitolato: "B-money: un sistema di denaro elettronico anonimo e

distribuito." L'articolo delineò le fondamenta per le criptovalute, come Bitcoin, e infatti è citato nell'articolo su Bitcoin di Satoshi Nakamoto.

Nell'articolo di Wei Dai, viene teorizzato che un sistema di denaro elettronico abbia bisogno dei seguenti elementi per funzionare:

- Una certa quantità di potere di calcolo e prova di quel lavoro.
- Ricompense allocate per il lavoro computazionale completato.
- Un registro collettivo di gruppo, verificato e aggiornato da tutti i membri.
- Trasferimenti di fondi completati sul registro collettivo di gruppo, e

verificati con gli hash crittografici.
- Tutte le transazioni sono firmate con delle firme digitali, utilizzando la crittografia a chiave pubblica, e vengono verificate dalla rete.

Nel 2000, Stefan Konst pubblicò un articolo che forniva soluzione pratiche per implementare catene crittografiche sicure.

Il lavoro compiuto tra gli anni '80 e il primo decennio del 2000, insieme agli articoli accademici pubblicati, ha posto le fondamenta per Bitcoin e la blockchain.
Nel 2008, Satoshi Nakamoto (il cui

nome è largamente ritenuto uno pseudonimo) ha pubblicato un articolo su internet intitolato "*Bitcoin: Un sistema di denaro elettronico Peer-To-Peer"*. Questo articolo delinea la creazione di Bitcoin e dei blocchi di transazioni legati come catene. L'articolo non usa mai la parola "blockchain" per riferirsi a questo metodo.

Nel 2009, quando Satoshi Nakamoto ha creato la rete Bitcoin e il primo blockchain, Bitcoin è diventato più di un'idea in un articolo accademico. Il primo riferimento alla blockchain vedeva in realtà le due parole separate, ovvero "block chain", nel codice

sorgente originale di Bitcoin.

Questa prima blockchain era una caratteristica chiave di Bitcoin, in quanto impediva la doppia spesa e agiva come un registro pubblico distribuito per tutte le transazioni sulla rete Bitcoin.

A Nakamoto va il credito per aver minato il primo blocco della rete Bitcoin, chiamato "blocco genesi".

Nel "Blocco Genesi", Satoshi Nakamoto ha lasciato il messaggio:
"The Times 03/Gen/2009 Il cancelliere sulla soglia di un secondo salvataggio delle banche"

Questo messaggio potrebbe essere stato lasciato come prova del fatto che il blocco era stato creato il 3 gennaio o dopo, ed era inoltre un commento indicativo del fallimento della struttura attuale delle banche e dei mercati finanziari. Dal momento che la frase è il titolo di un articolo apparso in un quotidiano britannico, è possibile che in quel periodo Satoshi vivesse nel Regno Unito.

Le parole "block" e "chain" erano usate separatamente all'interno di Bitcoin, anche quando ottenne un successo più ampio. Passarono alcuni anni prima che diventasse una sola parola: blockchain.

La blockchain originale di Bitcoin non era priva di errori. Come nella maggior parte delle imprese tecnologiche o di business, ci furono problemi lungo la loro strada. Ad agosto del 2010 fu scoperto il primo grave problema del protocollo Bitcoin. Erano state trovate delle transazioni che erano state alterate prima di essere registrate nella blockchain, manomettendo così le transazioni ufficiali. In qualche modo, gli utenti stavano bypassando le restrizioni costruite all'interno di Bitcoin e stavano creando un numero infinito, manomettendo le transazioni originali e facendo poi la cresta.

La vulnerabilità del sistema venne

sfruttata, e più di 184 milioni di Bitcoin vennero generati con una singola transazione e mandati a due soli indirizzi nella rete. Nel giro di poche ore la transazione venne scoperta, e successivamente cancellata dalla blockchain. La rete Bitcoin subì un grosso aggiornamento, e da allora a oggi non si è più verificato un problema del genere.

Nel 2011 venne lanciato il mercato nero virtuale "Silk Road". Si trattava di un sito di acquisti come eBay, ma che permetteva agli utenti di comprare e vendere droghe online. Bitcoin era la principale forma di pagamento utilizzata su Silk Road e, sebbene ciò portò a un

aumento nell'uso di Bitcoin, contribuì anche ad associare Bitcoin con lo spaccio di droga e altre attività illegali.

Bitcoin continuò a diventare sempre più popolare e famoso; nel 2013 il Bitcoin raggiunse il picco di circa 1000 dollari, e nonostante le critiche dalle autorità e dal governo sembrava impossibile da fermare.

Poi, nel 2013, Silk Road venne chiuso dell'FBI e tutti i sui beni vennero congelati, mentre il suo creatore venne arrestato rischiando l'ergastolo. All'incirca nel periodo in cui il Bitcoin era più forte Mt. Gox, che gestiva il

70% delle transazioni in Bitcoin, ricevette mandati, multe e si trovò a fronteggiare problemi di regolamentazione da vari dipartimenti governativi statunitensi. Alla fine del 2013, Mt.Gox aveva sospeso i prelievi in dollari statunitensi, e dichiarò fallimento all'inizio del 2014.

Nel frattempo, stavano nascendo altre criptovalute basate sul codice sorgente di Bitcoin, che utilizzavano blockchain diverse. Litecoin si era separata dalla blockchain originale Bitcoin come una biforcazione nella blockchain; diventò una criptovaluta separata la cui blockchain richiedeva un tempo minore per l'aggiunta dei blocchi, e vi furono

altri cambiamenti. Per aggiungere un blocco alla blockchain di Bitcoin ci vogliono 10 minuti, per aggiungerlo alla blockchain di Litecoin ne servono solo 2 e mezzo.

Dopo la chiusura e il fallimento di Silk Road e Mt. Gox, il valore del Bitcoin scese da un picco di 1000$ a circa 200$. Venivano create nuova criptovalute, e molti dichiararono pubblicamente che Bitcoin era arrivato alla fine.

Tuttavia, Bitcoin non era ancora morto. Al contrario, con la chiusura di Silk Road, Bitcoin iniziò ad essere meno

associato con lo spaccio di droga e il crimine, e le aziende iniziarono a interessarsi alla tecnologia dietro Bitcoin.

Era ancora difficile per le grandi aziende, le banche e le aziende finanziarie prendere sul serio Bitcoin, perché era difficile dimenticare il fallimento di Mt.Gox, la droga e gli omicidi pagati con Bitcoin. Anche senza il crimine che vi era associato, molti consideravano ancora Bitcoin come una moneta finta, una moda, una bolla pronta a scoppiare o una truffa.

La parola Bitcoin aveva ancora moltissime connotazioni negative, ma la

parola "blockchain" era una parola rispettabile da utilizzare per discuterne la tecnologia. Utilizzare la parola blockchain separava la tecnologia dalla valuta o dalla rete Bitcoin. Gli investitori e le istituzioni finanziarie non erano interessati a Bitcoin, ma iniziarono a mostrare interesse nella tecnologia blockchain.

Il prezzo dei Bitcoin, così come il livello di interesse nella valuta era basso nel 2014, ma l'interesse nella blockchain stava crescendo. Il termine "blockchain" stava iniziando a essere utilizzato come riferimento per registri e database distribuiti, invece che per le valute. La gente proponeva che i registri

manuali e ormai superati per registrare dati fossero sostituiti dalle blockchain.

Nel 2015 venne lanciata la blockchain live di Ethereum. Questo lancio portò le possibilità della tecnologia Bitcoin a un altro livello. La rete Ethereum permette alle applicazioni decentralizzate di essere eseguite su una blockchain insieme ai contratti smart. I contratti smart e le app decentralizzate sono visti da molti come la direzione futura della tecnologia blockchain, e spesso vengono definiti come Blockchain 2.0.

La maggior parte delle banche e dei servizi finanziari nel mondo stanno sviluppando dei sistemi basati sulle

blockchain per sostituire i database e le reti esistenti. Grazie alla sua facilità di accesso, unita alle funzionalità che la combinazione di app decentralizzate e contratti smart fornisce, la tecnologia blockchain si è aperta a quasi tutti i settori. I programmatori possono scrivere programmi da eseguire sulle blockchain, senza avere bisogno di creare la loro blockchain.

Nel 2017, il giornale Harvard Business Review ha dichiarato che la blockchain potrebbe potenzialmente creare delle nuove fondamenta nei sistemi economici e sociali. Questa dichiarazione è indicativa del modo in cui si sta

sviluppando la tecnologia blockchain, e ricorda l'infanzia di internet, con un potenziale senza limiti che stiamo soltanto adesso iniziando a realizzare. Le grandi aziende, le startup, i capitalisti di rischio, i governi e i programmatori stanno tutti lavorando su sistemi, database e applicazioni decentralizzate basate sulla blockchain.

Adesso dovreste avere una comprensione di base sulle blockchain, la loro storia e il loro sviluppo. Nei prossimi capitoli parleremo dei vantaggi, svantaggi, pericoli e del potenziale futuro della tecnologia blockchain.

Punti chiave:

- La crittografia è un fondamento chiave della blockchain. La crittografia risale a migliaia di anni fa, quando i messaggi erano scritti in codice per proteggerli dai nemici.

- Durante gli anni '80 e '90 sono stati pubblicati diversi articoli che teorizzavano l'uso della crittografia, insieme alle catene sicure di dati, per la creazione di valute digitali.

- 1982 - David Chaum scrive un articolo intitolato "blind signatures per pagamenti non tracciabili".

David Chaum viene riconosciuto come l'inventore del denaro digitale e delle blind signatures.

- 1990 - David fonda DigiCash, che crea una valuta digitale non tracciabile utilizzando la crittografia, chiavi pubbliche e private e firme. DigiCash dichiara bancarotta nel 1998, e i suoi beni vengono venduti a eCash tecnologies.

- 1997 - Adam Back crea un algoritmo di prova di lavoro per limitare lo spam via e-mail, noto come hashcash. Richiede al mittente di un’e-mail di provare di avere risolto un puzzle informativo prima di

mandare un'e-mail. Ciò usa potenza di calcolo e risorse, rendendo più costoso mandare e-mail spam in blocco.

- 1998 - Nick Szabo propone una valuta digitale decentralizzata chiamata "bit gold"(oro bit). Incorpora la prova di lavoro insieme a una rete di computer che accetta la prova di lavoro come valida, e la unisce al puzzle successivo come un timestamp. Bit gold non è mai stato creato come una reale valuta, ma è esistito solo a livello teorico.

- 1998 - Wei Dai pubblica un altro articolo intitolato: "B-money: un

sistema di denaro elettronico anonimo e distribuito." L'articolo delineò le fondamenta per le criptovalute, come Bitcoin, e infatti è citato nell'articolo su Bitcoin di Satoshi Nakamoto.

- Il lavoro compiuto tra gli anni '80 e il primo decennio del 2000, insieme agli articoli accademici pubblicati, ha posto le fondamenta per Bitcoin e la blockchain.

- 2008 - Satoshi Nakamoto (il cui nome è largamente ritenuto uno pseudonimo) pubblica un articolo su internet intitolato "*Bitcoin: Un sistema di denaro elettronico Peer-*

To-Peer". Questo articolo delinea la creazione di Bitcoin e dei blocchi di transazioni legati come catene. L'articolo non usa mai la parola "blockchain" per riferirsi a questo metodo.

- 2009 - Quando Satoshi Nakamoto crea la rete Bitcoin e il primo blockchain, Bitcoin diventa più di un'idea in un articolo accademico. Il primo riferimento alla blockchain vedeva in realtà le due parole separate, ovvero "block chain", nel codice sorgente originale di Bitcoin.

- Questa prima blockchain era una caratteristica chiave di Bitcoin, in

quanto impediva la doppia spesa e agiva come un registro pubblico distribuito per tutte le transazioni sulla rete Bitcoin.

- A Nakamoto va il credito per aver minato il primo blocco della rete Bitcoin, chiamato "blocco genesi". "The Times 03/Gen/2009 Il cancelliere sulla soglia di un secondo salvataggio delle banche"

  Questo messaggio potrebbe essere stato lasciato come prova del fatto che il blocco era stato creato il 3 gennaio o dopo, ed era inoltre un commento indicativo del fallimento della struttura attuale delle banche e

dei mercati finanziari.

- Il creatore di Bitcoin e della blockchain, Satoshi Nakamoto, è ancora ignoto. Molti sospettano che Nick Szabo o Wei Dei siano i creatori di Bitcoin, ma entrambi negano.

- 2015 - Viene lanciata la blockchain Ethereum, che permette alle applicazioni decentralizzate e ai contratti smart di essere eseguiti sulla blockchain. Ciò migliora la funzionalità della tecnologia blockchain, ed è nota come Blockchain 2.0.

Capitolo Quattro: Benefici della tecnologia Blockchain

"La tecnologia blockchain ha la capacità di ottimizzare l'infrastruttura globale per affrontare i problemi globali in questo spazio, in modo molto più efficiente dei sistemi attuali."
- Marwn Forzley, fondatore di Align Commerce

In questi primi capitoli abbiamo parlato di cos'è una blockchain, come funziona e abbiamo fatto qualche esempio dei potenziali usi. Alcuni dei benefici sono

stati brevemente menzionati nei capitoli precedenti, ma in questo capitolo andremo maggiormente nel dettaglio sui benefici della tecnologia blockchain.

Trasparenza

I sistemi basati sulle blockchain offrono una trasparenza migliore rispetto ai registri e ai sistemi attuali. I cambiamenti al registro sono visibili a tutti gli utenti sulla rete, e una volta che le transazioni entrano nella blockchain non possono essere alterate o cancellate.

Con i database esistenti, è possibile per una persona alterare il database e nascondere il cambio dagli altri utenti.

Ci sono stati moltissimi esempi in cui evidenti casi di frode non sono stati scoperti perché i registri non erano trasparenti. Questa mancanza di trasparenza ha permesso alle persone di alterare o manipolare i dati senza che gli altri sapessero dei cambiamenti.

La tecnologia blockchain fornisce trasparenza a tutti gli utenti sulla rete, e le transazioni sono visibili a tutti i computer collegati. La maggioranza dei computer collegati alla blockchain deve approvare le transazioni o i cambi alla blockchain, impedendo che le transazioni vengano nascosta o manipolate.

Tutte le modifiche sono praticamente in tempo reale; il processo avviene quando le transazioni vengono approvate e aggiunte alla blockchain. Lo scenario di una persona in un'organizzazione che ruba denaro o nasconde le perdite dell'azienda manipolando le informazioni sui registri è molto più improbabile nel caso di un registro distribuito basato su una blockchain.

Implementare una blockchain porterà trasparenza in molteplici campi, in una vasta gamma di aree. Con una transazione finanziaria, è possibile guardare lo status del trasferimento sulla blockchain in tempo reale, al posto di

non conoscere lo stato di una transazione finché non viene completata, il che è spesso il caso con i sistemi di oggi.

La stessa trasparenza può essere applicata a qualsiasi cosa di valore sia registrata sulla blockchain. Nei capitoli successivi parleremo dei diversi settori in cui la tecnologia blockchain è in corso di sviluppo, e della trasparenza che fornisce a clienti e aziende rispetto ai sistemi esistenti.

Eliminazione degli intermediari

Come discusso all'inizio del libro, molte transazioni che avvengono oggi tra le

persone hanno bisogno di intermediari come le banche per garantire la sicurezza e la fiducia delle transazioni.

Un vantaggio della tecnologia blockchain rispetto ai sistemi esistenti è l'abilità di eliminare gli intermediari, permettendo che le transazioni avvengano direttamente tra le parti invece di coinvolgere una terza parte.

Ciò è di enorme beneficio per i miliardi di persone nel mondo che vivono in paesi in cui non possono fidarsi degli intermediari di terza parte a causa di governi corrotti, alti tassi di crimine, cattiva regolazione delle aziende, presenza di registri manuali e limitate

opzioni legali per la risoluzione delle controversie.

Le blockchain sono particolarmente utili in questi casi in cui non c'è fiducia negli intermediari e svolgere transazioni direttamente tra le persone è difficile o rischioso.

La blockchain fornisce fiducia e trasparenza riducendo i rischi coinvolti nelle transazioni, senza la necessità di una terza parte che faccia da intermediario.

Decentralizzazione

La decentralizzazione di un database

blockchain è una componente chiave del modo in cui è possibile eliminare gli intermediari, aumentando allo stesso tempo la trasparenza e la fiducia. Le blockchain sono mantenute su un singolo registro condiviso, invece di registri multipli gestiti privatamente da diverse istituzioni. Utilizzando la blockchain, i privati e le aziende non devono lasciare il controllo a una singola istituzione. Ciò rende la collaborazione tra le parti più veloce e facile da gestire.

Per usare l'esempio di un gruppo di banche che trasferiscano denaro tra di loro, con le strutture e i sistemi attuali ogni banca manterrebbe i propri registri e i propri dati sulle transazioni

separatamente. Utilizzando un registro basato su una blockchain, avrebbero bisogno soltanto di sincronizzare le transazioni in un registro condiviso al quale tutte le banche avrebbero accesso, e concordare sulla correttezza della registrazione delle transazioni.

La struttura decentralizzata della blockchain è un vantaggio per le aziende che, pur essendo concorrenti, lavorano insieme come parte di un gruppo industriale o un consorzio. Un'azienda potrebbe essere titubante nel mandare dati o nel collaborare su un database gestito da un concorrente. Quando due concorrenti lavorano insieme ma una

sola delle parti possiede tutti i dati, sono necessari complessi contratti legali e accordi di confidenzialità per proteggere la privacy e l'accesso ai dati. Invece, con un sistema basato sulle blockchain, i concorrenti possono lavorare insieme su un database condiviso al quale tutti hanno accesso e controllo.

I database centralizzati sono sensibili all'hacking, alla perdita di dati e alla corruzione. La blockchain non ha un database centrale che possa portare a un fallimento, a una manipolazione o corruzione dei dati. Tutti i computer sulla rete della blockchain hanno una copia della blockchain, riducendo il rischio di perdita dei dati. Per

manipolare i dati su una blockchain sarebbe necessario hackerare più del 50% dei computer sulla rete allo stesso tempo, il che è praticamente impossibile.

Fiducia

Come indicato precedentemente nel libro, i metodi attuali per le transazioni tra parti richiedono la fiducia in un intermediario che faciliti il processo.

La blockchain permette di eliminare gli intermediari e allo stesso tempo di mantenere la fiducia e la sicurezza tra le parti coinvolte nella transazione.

La fiducia viene riposta nella rete

blockchain invece che in una terza parte. Le reti blockchain sono generalmente decentralizzate, e tutti gli utenti connessi alla rete hanno accesso alla blockchain.

Abbiamo già parlato dell'eliminazione degli intermediari, della trasparenza migliorata e della struttura decentralizzata della blockchain. L'aumento della fiducia tra le parti in una transazione è un beneficio importante e intangibile di questi cambiamenti.

Sicurezza

I dati inseriti in una blockchain sono

immutabili, e ciò significa che non possono essere alterati o cambiati. Ogni blocco di dati nella blockchain può essere tracciato all'indietro fino al "blocco genesi".

L'immutabilità dei dati inseriti in blocchi combinati, che possono essere tracciati all'indietro fino al primo blocco della blockchain, crea un percorso facile da seguire che ricostruisce tutte le transazioni della blockchain.

Nella storia ci sono stati moltissimi casi di frode e di manipolazione dei dati. Spesso, quando viene commessa una frode, il percorso che porta

all'occorrenza della frode è alterato, rendendo difficile e lungo investigare. A volte il percorso dei dati è così tanto alterato da rendere impossibile il tracciamento delle transazioni e della frode.

Con un sistema basato sulla blockchain, le transazioni passate non possono essere alterate, lasciando una traccia chiara di ciò che è accaduto nella blockchain. Come menzionato nella sezione sulla decentralizzazione della blockchain, alterare una transazione esistente richiederebbe il controllo contemporaneo di più del 50% dei computer sulla rete, il che è

praticamente impossibile. Se anche questo accadesse, sarebbe rapidamente scoperto dagli altri computer appartenenti alla rete.

La sicurezza della blockchain non è perfetta, ma i sistemi attualmente esistenti si sono già dimostrati più volte poco sicuri. La blockchain risolve molti dei problemi di sicurezza dei sistemi convenzionali. Sebbene sia impossibile eliminare completamente le frodi, la blockchain fornisce una traccia chiara fino all'inizio, permettendo di identificare facilmente i tentativi di frode.

Ampia gamma di utilizzi potenziali

Tutto ciò che ha un valore può essere registrato sulla blockchain; la frase "ha un valore" non deve però essere intesa in senso esclusivamente finanziario. Nel primo capitolo abbiamo fatto l'esempio di un libro, ma si potrebbe parlare di atti di proprietà, identità digitali, licenze di copyright, file digitali o tutto ciò che può attualmente essere registrato in un database.

Nell'esempio delle licenze di copyright, si tratta di beni di valore, anche se le licenze sono solo dati o numeri salvati in un database. Il valore viene dal fatto che queste licenze proteggono la proprietà e il reddito che deriva da ciò

che il copyright protegge.

ci sono organizzazioni e associazioni che controllano e gestiscono le licenze di copyright in un database centralizzato. Queste licenze sono beni di valore, che possono essere conservati in una blockchain eliminando la necessità delle organizzazioni che controllano le licenze. I beni di valore come le criptovalute, le licenze e altri beni digitali possono esistere solamente sulla blockchain come asset nativi della blockchain, rendendoli più facili da gestire rispetto agli attuali atti di proprietà.

La tecnologia blockchain è una

tecnologia nuova e facilmente accessibile, specialmente grazie alle recenti innovazioni come la piattaforma Ethereum e i contratti smart. Ciò permette a tutti di sviluppare applicazioni che utilizzino la tecnologia blockchain.

La blockchain può potenzialmente cambiare ogni settore nel mondo. I progetti in corso d'opera mostrano l'impatto che la tecnologia blockchain potrebbe avere sulla vita di tutti, e molte aziende stanno già sviluppando i loro sistemi proprietari basati sulle blockchain.

Più avanti nel libro, andremo

maggiormente nel dettaglio sulle diverse industrie e i diversi usi per la tecnologia blockchain, con alcuni esempi di progetti attualmente in sviluppo.

Costi ridotti

La tecnologia blockchain potrebbe ridurre significativamente i costi in molte industrie, rimuovendo gli intermediari coinvolti nel processo di registrazione e trasferimento di beni. Ogni intermediario o livello coinvolto in una transazione aggiunge un costo per la registrazione e il trasferimento dei beni.

Nei sistemi attuali, quando trasferiamo o registriamo beni, ci sono spesso diversi

registri e database mantenuti da ciascuna organizzazione. Un registro distribuito permette alle parti di trasferire beni su un registro condiviso, riducendo i costi legati al mantenimento di diversi registri in ogni organizzazione.

Mantenere registri o database è costoso, e spesso si tratta di un processo manuale che coinvolge molte persone che verificano l'integrità di ciascun registro. I registri distribuiti basati sulle blockchain riducono i costi, sostituendo i registri individuali con un registro condiviso, il che fornisce la possibilità di accordi e verifiche in tempo reale da parte di tutti coloro che sono connessi

alla rete al momento della transazione

Aumento della velocità di transazione
I sistemi basati sulle blockchain non solo riducono i costi coinvolti nelle transazioni, ma ne aumentano la velocità in modo sostanziale. Eliminando gli intermediari e registrando le transazioni su un registro distribuito condiviso, i registri basati sulle blockchain possono registrare le transazioni in modo praticamente istantaneo.

Se avete mai fatto un bonifico, sicuramente avrete notato che il denaro viene rimosso dal vostro conto immediatamente, ma non viene ricevuto dall'altro conto prima di alcuni giorni.

Allo stesso modo, con gli acquisti con carta di credito, le transazioni possono rimanere in attesa di conferma per diversi giorni. Per quanto riguarda i negozianti, ad esempio, forniscono dei beni al cliente ma non ricevono i pagamenti per alcuni giorni, finché l'azienda della carta di credito non completa la transazione.

Negli esempi qui sopra, sono in sviluppo sistemi basati su blockchain per aumentare la velocità di queste transazioni. Tuttavia, non bisogna limitarsi solo a questi esempi; qualsiasi tipo di transazione o trasferimento di

valuta può potenzialmente utilizzare la tecnologia blockchain per aumentare la velocità delle transazioni.

Più avanti nel libro, parleremo di esempi nel mondo reale di aziende che stanno sviluppando sistemi basati sulle blockchain per aumentare la velocità delle transazioni nella finanza e in altri settori.

Note finali

Molte delle informazioni pubblicate riguardo alla tecnologia blockchain riguardano i benefici, i vantaggi e la promozione del suo potenziale. Sebbene questo capitolo abbia parlato di molti benefici nell'uso dei sistemi basati su

blockchain, ciò non significa che siano privi di problemi o che siano la risposta a tutti i problemi all'interno di un settore.

Nel prossimo capitolo parleremo di alcuni degli svantaggi e dei problemi dell'uso di sistemi basati sulle blockchain.

Punti chiave:

- **Trasparenza -** La blockchain offre miglioramenti significativi nella trasparenza rispetto agli attuali sistemi di registrazione dati e ai registri in uso in molti settori.
- **Eliminazione degli intermediari -** I sistemi basati sulle blockchain permettono di eliminare gli intermediari coinvolti nella registrazione e nel trasferimento di beni,
- **Decentralizzazione -** I sistemi basati sulle blockchain possono essere eseguiti su una rete decentralizzata di

computer, riducendo il rischio di hacking, downtime del server e perdita di dati.

- **Fiducia -** I sistemi basati sulle blockchain aumentano la fiducia tra le parti coinvolte in una transazione grazie al miglioramento della trasparenza e alle reti decentralizzate, insieme all'eliminazione degli intermediari di terza parte in nazioni dove la fiducia negli intermediari non esiste.
- **Sicurezza -** I dati inseriti in una blockchain sono immutabili, impedendo di manipolare le transazioni e lo storico dei dati e prevenendo così le frodi. Le

transazioni inserite nella blockchain forniscono una traccia chiara dall'inizio della blockchain, permettendo a ogni transazione di essere facilmente investigata e verificata.

- **Ampia gamma di utilizzi -** Quasi tutto ciò che ha un valore può essere registrato su una blockchain, e ci sono molte aziende e settori che stanno già sviluppando sistemi basati sulla blockchain. Questi esempi saranno affrontati più avanti nel libro.
- **Tecnologia facilmente accessibile -** Oltre alle sue vaste possibilità di utilizzo, la tecnologia blockchain

rende semplice creare applicazioni senza un significativo investimento nell'infrastruttura, grazie a recenti innovazioni come la piattaforma Ethereum. Parleremo delle app decentralizzate, dei contratti smart e della piattaforma Ethereum più avanti nel libro.

- **Riduzione dei Costi -** I registri basati sulla blockchain permettono di eliminare gli intermediari e i livelli di conferma coinvolti nelle transazioni. Le transazioni che normalmente richiederebbero più registri individuali possono essere registrate su un solo registro condiviso, riducendo i costi legati

alla validazione, la conferma e la verifica di ciascuna transazione su più organizzazioni.

- **Aumento della velocità di transazione -** L'eliminazione degli intermediari e la registrazione su registri distribuiti permette di aumentare in modo sensibile la velocità della transazione, rispetto a un'ampia gamma di sistemi esistenti.
- **Svantaggi -** Ci sono molte ottime ragioni per passare dai sistemi esistenti a quelli basati sulle blockchain. Tuttavia, ci sono anche svantaggi e rischi che non dovrebbero essere ignorati.

Capitolo Cinque: Svantaggi / Pericoli della tecnologia Blockchain

La blockchain è stata ideata in modo specifico con un obiettivo: prevenire la "doppia spesa" del denaro elettronico, senza ricorrere a un'autorità centrale. Tuttavia, pochi dei casi teorizzati sono vulnerabili alla doppia spesa o a problemi simili. Di contro, la blockchain non risponde a molti importanti obiettivi di sicurezza.

Per questo, le blockchain non sono né necessarie né sufficienti per molte delle loro applicazioni ideali; nella pratica sono incredibilmente sovra-ingegnerizzate, incomplete, o entrambe le cose.

-- Steve Wilson, Oltre l'hype: comprendere gli anelli deboli nelle blockchain

La tecnologia blockchain sembra spesso essere presentata come la soluzione a tutti i problemi delle industrie e del mondo.

Ci sono nuove start-up che si occupano

di blockchain e criptovalute che vengono lanciate ogni giorno, e che promettono di fare di tutto, dal distruggere i sistemi bancari all'eliminare la povertà del mondo.

Molte di queste affermazioni ricordano ciò che si diceva di Internet al suo inizio. Anche se Internet ha cambiato il mondo, molte delle affermazioni erano eccessive, le tempistiche erano poco realistiche e molte start-up delle quali si prevedeva il successo sono andate in bancarotta.

In questo capitolo, parleremo di alcuni dei problemi e degli svantaggi della tecnologia blockchain.

Mancanza di Privacy

Le blockchain decentralizzate mancano di privacy, e ciò rende difficile la loro piena accettazione. Non solo le informazioni non sono private, ma sono facilmente accessibili in ogni momento a tutti coloro che usano il sistema.

Scoprire l'identità di un account sulla blockchain Bitcoin, dopo aver ricevuto un pagamento da quella persona, è relativamente semplice.

Se andaste in un negozio fisico e faceste un pagamento, il negoziante sarebbe in grado di vedere la transazione sulla blockchain. Le informazioni sulla

transazione mostrerebbero il portafoglio da cui sono stati inviati i fondi, controllerebbero quell'account e potrebbero visualizzare il suo saldo e tutte le transazioni in ingresso e in uscita dall'account.

L'idea che una blockchain decentralizzata possa davvero pubblicare ogni singola transazione su una rete pubblica è preoccupante per molte persone, specialmente nel caso di acquisti fisici, dove è possibile collegare un'identità a un account e a delle transazioni.

Ciò è preoccupante anche perché bisogna considerare che i computer su

cui viene eseguita buona parte della rete blockchain si trovano in paesi come la Russia o la Cina, in cui i crimini informatici sono frequenti e le informazioni personali potrebbero essere usate contro le persone che vivono o che viaggiano in quei paesi.

Ci sono blockchain decentralizzate che forniscono una maggiore privacy nelle transazioni, o che restringono il numero di persone che hanno accesso alle informazioni. Tuttavia, Bitcoin, Ethereum e molte delle altre grandi criptovalute basate sulla blockchain non operano in questo modo, e attualmente non hanno in programma di implementare una maggiore privacy per

le transazioni o gli account.

Problemi di Sicurezza

I beni basati sulla blockchain sono come il denaro contante; se il denaro viene rubato o scivola via dal tuo portafoglio, è perso per sempre. I sistemi basati sulla blockchain usano un sistema di criptografia e criptazione avanzata, più sicuro rispetto a una password standard di internet o un codice d'accesso. Tuttavia, una maggiore sicurezza a volte può rendere un sistema meno sicuro.

Con le criptovalute è accaduto spesso che alcune persone perdessero le proprie chiavi di accesso e non avessero

accesso al proprio denaro. Basta guardare i forum su internet, in cui gli utenti avvertono gli altri di non perdere la propria chiave, raccontando come abbiano perso la loro chiave e adesso non possano accedere al denaro nel proprio portafoglio.

Ciò accade spesso quando qualcuno compra una particolare criptovaluta a un basso prezzo e non le presta molta attenzione. Dopo qualche tempo, scopre che il valore della criptovaluta si è alzato moltissimo e che il piccolo investimento iniziale ora vale migliaia di dollari, e prova nuovamente ad accedere.

Acquistando 50$ in Bitcoin nel 2009 una persona oggi avrebbe più di un milione di dollari, quindi è facile capire come ciò potrebbe accadere, con degli aumenti di prezzo così grandi su quantità di denaro inizialmente piccole. Un caso molto pubblicizzato è quello di James Howells nel Regno Unito, che ha buttato via il suo portatile con al suo interno 7500 bitcoin. Al prezzo di oggi, varrebbero oltre 15 milioni di dollari.

A causa della trasparenza nella blockchain, avendo la propria chiave pubblica è possibile vedere il proprio saldo e il valore, ma non è possibile accedervi. Questo è l'equivalente di una

banca in grado di dirvi il saldo del vostro conto corrente, senza che abbiate la possibilità di accedervi.

Con i conti correnti tradizionali, se perdete la password per l'internet banking, le carte di credito o dimenticate il numero del conto, potete andare fisicamente in banca e provare la vostra identità per ottenere nuovamente l'accesso. Questo non è ciò che succede con le criptovalute decentralizzate e basate sulla blockchain come Bitcoin. Negli ultimi anni miliardi di dollari in criptovalute sono stati rubati attraverso hacking, truffe o problemi di sicurezza.

Se qualcuno dovesse ottenere accesso

alla vostra carta di credito e prelevare del denaro, potreste chiamare la banca e cancellare la carta in modo da impedire ulteriori prelievi. La banca avrà probabilmente delle protezioni contro la frode e sarà in grado di annullare la transazione e tracciare il pagamento.

Con i sistemi basati sulla blockchain, le transazioni non possono essere alterate o annullate, e non c'è alcun intermediario che possa assistervi in caso di truffa sul vostro conto. Se mandate del denaro all'account (portafoglio) sbagliato della blockchain, quel denaro è perduto. Se qualcuno ottiene accesso alla vostra chiave privata, può prelevare tutto il

denaro sul conto, senza che vi sia alcun modo di annullare la transazione o chiedere un rimborso.

La prima domanda o una delle domande chieste più frequentemente sulle pagine di sistemi basati sulla blockchain è "come resetto la password se la dimentico o la perdo?" e la risposta è "non puoi". Il consiglio che viene dato a chi imposta una chiave privata sulla blockchain è di "scriverlo da qualche parte". L'avanzata crittografia e l'elevatissima sicurezza si scontrano con le persone che scrivono le loro chiavi private e le tengono a casa o sul computer, riducendo la sicurezza rispetto ai metodi tradizionali.

Quando si parla di implementazione su larga scala dei sistemi basati sulle blockchain, l'elevata sicurezza ne rende più difficile l'adozione da parte del grande pubblico. I portafogli web basati sulle blockchain, in cui è possibile salvare criptovalute affidandosi a un'azienda di terza parte, sono molto popolari. Utilizzando portafogli web di terza parte, le persone sacrificano i benefici di sicurezza della blockchain - come le chiavi private - in favore di password tradizionali che possono essere resettate in caso di perdita.

Nessun controllo centralizzato

"Nei mercati finanziari c'è sempre un meccanismo per correggere un attacco. In una blockchain non c'è un meccanismo per correggerlo - le persone devono accettarlo."
- Robert Sams, fondatore e amministratore delegato di Clearmatics, basato su Londra

I sistemi basati sulla blockchain sono pensati per sostituire gli intermediari di terza parte, riportando la responsabilità e il controllo agli individui coinvolti nelle transazioni.
Il controllo viene dato in mano alla maggioranza delle persone sulla rete, e

ciò rende problematico il controllo della blockchain.

La natura decentralizzata di molte blockchain significa che la rete deve mettersi d'accordo e decidere la direzione futura della rete e della blockchain. Con una rete e un software tradizionale, se un'organizzazione vuole implementare un cambiamento, può farlo solo dopo aver ottenuto l'approvazione dei dipartimenti rilevanti dell'organizzazione. Con un network di blockchain decentralizzato come Bitcoin, i cambiamenti devono essere accettati da una maggioranza del network. Ciò può andare dal 50% +1 fino al 70% o anche l'80% della rete.

Un esempio recente è stata la divisione sulla rete Bitcoin riguardo alla scelta tra l'implementazione di SegWit (Segregated Witness) o Bitcoin Unlimited. Diverse parti della rete supportano cambiamenti diversi per la rete Bitcoin, e nessuna delle due parti è riuscita a ottenere la maggioranza necessaria per attuare il cambiamento.

Questo disaccordo ha permesso ad altre criptovalute e reti di blockchain di superare Bitcoin in termini di avanzamento tecnologico. Questo disaccordo ha inoltre fatto sì che la rete Bitcoin diventasse stagnante, con rallentamenti dei tempi di transazioni e

conferme, e problemi di scalabilità tutt'oggi presenti.

La tecnologia, come il software, cambia costantemente nel tempo. Le reti decentralizzate di blockchain possono risultare in una divisione riguardo alla direzione dei cambiamenti, specialmente quando non si riesce a raggiungere la maggioranza con un accordo. Se anche si raggiunge la maggioranza con un accordo, ci sarà sempre un ampio numero di persone nella rete che saranno in disaccordo con i cambiamenti fatti.

Ciò rende le reti decentralizzate rischiose per le organizzazioni. Un'azienda potrebbe costruire

un'impresa o un software centrato su una rete sulla quale non ha controllo, i cui cambiamenti potrebbero avere un impatto drammatico sul suo software o la sua impresa.

Rischio di attacco 51%

Ricollegandoci al problema del controllo, se qualcuno è in grado di controllare più del 50% dei computer su una rete blockchain, potrà controllare le transazioni nella blockchain. La presenza di un utente malintenzionato che controlla più del 50% dei computer su una rete blockchain è noto come "attacco 51%".

Facendo leva su questo controllo su una rete di criptovalute, sarebbe teoricamente in grado di bloccare la conferma delle nuove transazioni, annullare le transazioni e permettere la temuta "doppia spesa" del denaro.

Un attacco 51% su una rete blockchain è teorico, perché sarebbe difficile controllare una tale quantità della rete, ma ci sono grandissime farm di mining in Cina, in Russia e in altre parti del mondo, che controllano una larga parte della potenza di calcolo delle reti di blockchain. Se queste grandi farm collaborassero, potrebbero potenzialmente prendere il comando

delle reti blockchain e manipolarle per il loro beneficio.

Anche senza controllare il 51% della rete, possono comunque manipolare la rete allocando la loro potenza di calcolo in modo da influenzare lo sviluppo futuro della rete. Questo è ciò che è successo con la divisione della rete Bitcoin di cui parlavamo prima.

Tecnologia nuova e non ancora provata

I sistemi basati sulle blockchain sono una tecnologia nuova e non ancora provata, applicata principalmente alle criptovalute. Mancano però applicazioni nel mondo reale, che esistano attualmente e possano provare l'efficacia

della tecnologia.

La tecnologia è nuova e ha moltissimo potenziale, ma molte delle potenziali applicazioni sono solo teoriche. Il detto "Costruisci una trappola per topi migliore, e il mondo farà la fila alla tua porta" è una comune falsa credenza nel mondo degli affari. Solo perché la tecnologia potrebbe essere migliore dei sistemi esistenti in molti modi, non significa che le persone la preferiranno alle opzioni esistenti.

Come detto prima, la sicurezza crittografica è superiore ai sistemi di sicurezza esistenti, ma in molti sistemi basati sulla blockchain è impossibile

recuperare una chiave privata persa. Molti preferiscono scrivere le loro chiavi private su carta, o salvarle sul computer per non dimenticarle, eliminando così i benefici dati dall'elevata sicurezza e rendendo il sistema potenzialmente meno sicuro.

Un altro beneficio delle reti di blockchain consiste nell'eliminare gli intermediari di terza parte. Collegarsi a una rete di blockchain, mandare transazioni e impostare le chiavi private è, per molte persone, complicato e rischioso. Molti preferiscono dare accesso alle loro chiavi private a intermediari di terze parti, con

portafogli o software simili che eliminano un altro principale beneficio delle reti blockchain.

Costo

L'algoritmo prova di lavoro utilizzato da molte reti blockchain richiede, prima di aggiungere un blocco alla rete, una prova del fatto che si sia dato un contributo alla rete con risorse e potenza di calcolo. Di norma, la prova è la risposta a un puzzle allegato al blocco, la cui correttezza viene verificata dalla rete.
Risolvere questo puzzle richiede un'enorme quantità di elettricità e potenza di calcolo.

Il professore John Quiggin dell'Università di Queensland ha calcolato che la rete Bitcoin utilizza in mezz'ora la stessa quantità di elettricità che una casa media statunitense consuma in un intero anno.

Una casa media statunitense usa 10-12 000 kWh di elettricità ogni anno, circa la stessa energia necessaria per generare quattro Bitcoin dal valore di circa 1000$.

A causa degli alti costi dell'elettricità necessari per fare girare i computer sulle reti blockchain utilizzando questo algoritmo prova di lavoro, i

paesi in cui l'elettricità costa poco o le organizzazioni che hanno accordi speciali con i fornitori di energia elettrica sono in vantaggio.

Quando la difficoltà dei puzzle nella blockchain di Bitcoin cresce, così fa il consumo di elettricità, rendendo ancora più costoso e difficile eseguire su larga scala una blockchain con algoritmo prova di lavoro.

Mancanza di scalabilità

Al tasso attuale di consumo di energia, il costo dell'elettricità necessaria per l’esecuzione di una blockchain che

utilizza l'algoritmo prova di lavoro rende impossibile gestire il numero di transazioni delle grandi compagnie di carte di credito, come Visa e Mastercard. Questo è uno dei fattori che attualmente influenza la scalabilità delle reti di blockchain.

Nella blockchain di Bitcoin viene aggiunto un blocco ogni 10 minuti; ogni blocco attualmente contiene circa 2000 transazioni, e ciò significa che la rete Bitcoin processa circa 3 transazioni al secondo.

A causa dei limiti sulla dimensione dei blocchi, la rete Bitcoin è in grado di gestire circa 7 transazioni al secondo.

La Visa ha condotto dei test con l'IBM, e ha concluso che la rete Visa è in grado di gestire più di 20.000 transazioni al secondo.

Se andate in un negozio e utilizzate la carta di credito, ma non avete abbastanza denaro per effettuare l'acquisto, la transazione verrà rifiutata. La rete Bitcoin non ha in atto nessun meccanismo del genere.

Una transazione sulla blockchain di Bitcoin richiede un minimo di 10 minuti per essere aggiunta alla blockchain; le aziende potrebbero volere attendere l'aggiunta di diversi altri blocchi prima

di accettare la transazione, per assicurarsi che non venga annullata.

Mettendo a confronto i due metodi, possiamo dire che se andassimo in un negozio e volessimo pagare in Bitcoin, il negoziante dovrebbe aspettare un'ora per assicurarsi che la transazione venga confermata, e che diversi altri blocchi vengano aggiunti alla blockchain sopra al blocco che contiene la transazione.

Ci sono reti di blockchain molto più veloci di quella Bitcoin, ma nessuna ha lo stesso livello di popolarità o accettazione come forma di pagamento che ha Bitcoin. Anche le blockchain e le criptovalute che hanno tempi di

conferma delle transazioni più rapidi riescono a scalare al livello delle reti di pagamento finanziario esistenti, come Visa o Mastercard.

A causa di questi problemi di scalabilità, molti ritengono che l'implementazione su larga scala della tecnologia blockchain non sarà niente di più di un registro ufficiale con data e ora delle transazioni.

Fiducia, Reputazione e Comprensione delle Blockchain

Molte persone non conoscono ancora il funzionamento della blockchain, la cui reputazione è ancora macchiata dal

collegamento a Bitcoin.

Bitcoin è l'utilizzo più comune e noto della blockchain, e molti associano fortemente i Bitcoin al crimine. Sebbene Bitcoin stia diventando un metodo di pagamento legittimo più comunemente accettato, i terroristi e i criminali informatici hanno recentemente riportato alla ribalta il collegamento con Bitcoin.

Un esempio recente è quello della rete informatica del National Health Service in Gran Bretagna. Un virus aveva bloccato i computer del NHS, impedendo l'accesso e richiedendo il pagamento di un riscatto in Bitcoin. Ciò ha riportato Bitcoin sui giornali

britannici, che lo collegavano ai crimini informatici anonimi, agli hacker e ai terroristi. Gli ospedali non riuscivano ad accedere alle cartelle cliniche dei pazienti, minacciando potenzialmente le vite delle persone che durante la crisi avevano bisogno di cure.

La blockchain sostiene di poter creare fiducia tra le persone, senza la necessità di fidarsi di un intermediario di terza parte per le transazioni. Però, le persone devono comunque fidarsi della rete blockchain e dei computer anonimi sulla quale viene eseguita. Per le persone è difficile fidarsi di un sistema utilizzato apertamente dai criminali, specialmente

considerando che molti dei computer sulla rete si trovano in paesi stranieri poco regolati e controllati dal governo.

I crimini collegati a Bitcoin fanno parte delle ragioni per cui le aziende che sviluppano sistemi basati sulle blockchain stanno cercando di distanziare il collegamento tra Bitcoin e la blockchain. Il termine "registro distribuito" è recentemente diventato sempre più popolare, per aumentare ulteriormente la distanza tra Bitcoin e le nuove tecnologie basate sulla blockchain.

I benefici dei sistemi basati sulla blockchain sono spesso difficili da

capire. Come detto prima, molte persone scelgono già intermediari di terze parti per accedere alla blockchain, e usano password standard per accedere a un sito web, eliminando i principali benefici della tecnologia blockchain. Molte persone non amano che gli altri possano vedere il loro saldo, o le transazioni, o altri aspetti della blockchain e preferiscono i sistemi esistenti.

La comprensione del pubblico, la fiducia e la percezione delle reti blockchain sarà importante per l'accettazione su larga scala della tecnologia. Potrebbe volerci molto

tempo prima che il grande pubblico inizi a fidarsi delle reti di blockchain e a utilizzarle tranquillamente per effettuare transazioni.

Regolazione e Integrazione

"i più grandi analisti e operatori finanziari del mondo sono eccitati per un'invenzione diventata famosa in parte per aver promesso di distruggerli." - Mike Gault

I beni basati su blockchain dovranno aspettarsi un lungo processo di regolazione e problemi di integrazione con i sistemi esistenti. I governi e le

banche sono restii ai cambiamenti, a causa della scala e del costo necessario per sostituire i sistemi esistenti.

A meno che i sistemi basati sulle blockchain non riescano a fornire un risparmio significativo o altri benefici che giustificheranno la sostituzione dei sistemi esistenti, è improbabile che le grandi istituzioni come i sistemi o le banche decideranno di usarli.

Il governo dell'Estonia sta testando dei sistemi basati sulla blockchain, ma l'Estonia ha una popolazione di meno di 1.5 milioni. Ci sono città negli Stati Uniti, in Cina e in altri paesi che

hanno 10 volte questo numero di abitanti. Anche se i sistemi basati sulle blockchain potrebbero funzionare su una piccola scala, non è facile integrarli sulla scala necessaria per governi come quello degli Stati Uniti o per le grandi banche.

Il consorzio R3 e Ripple sono esempi di registri distribuiti o basati sulle blockchain che stanno venendo integrati con molte aziende finanziarie in diversi paesi.
Ci sono aziende finanziarie che stanno rifiutando la transizione verso un registro basato sulle blockchain a causa della scala "piccola" con cui le

blockchain sono state testate.

Se un ampio numero di istituzioni finanziarie si muove verso una nuova tecnologia non testata, e la sta utilizzando nel momento in cui vengono scoperti dei problemi, possono verificarsi dei rischi molto significativi nei confronti dei mercati finanziari e dei dati dei clienti.

Il Financial Stability Oversight Counsel (FSOC, Consiglio di Controllo della Stabilità Finanziaria) teme inoltre che alcuni sistemi basati sulle blockchain possano essere più vulnerabili alla frode di quanto sia possibile capire con un test su piccola

scala.

Un altro problema che riguarda l'adozione, da parte delle diverse istituzioni finanziarie, di un registro distribuito o un sistema condiviso basato sulle blockchain consiste nell'area in cui lavorano i regolatori. Un sistema basato sulle blockchain può teoricamente coinvolgere diverse giurisdizioni di regolazione e confini nazionali, confondendo ulteriormente le acque tra gli enti regolatori e le giurisdizioni da cui una transazione dovrebbe essere gestita.

Le grandi istituzioni finanziarie sono caute nel passare a un sistema in cui la

regolamentazione governative è poco chiara. Se i governi non hanno regole chiare su come trattare i beni basati su blockchain, i rischi finanziari e d'impresa sono semplicemente troppo alti. I problemi con la regolazione, il costo dell'integrazione e la mancanza di applicazioni su larga scala per i sistemi basati su blockchain porteranno a una lenta adozione della tecnologia da parte delle grandi istituzioni finanziarie e dei governi.

Entusiasmo

Moltissimo di ciò che viene scritto sulla tecnologia blockchain potrebbe essere descritto come evangelico o

troppo entusiastico, affermando ad esempio che le tecnologie basate sulla blockchain cambieranno il mondo, distruggeranno i governi, elimineranno le banche, risolveranno la povertà del mondo e magari vi daranno anche degli addominali da paura senza andare in palestra.

L'ultima affermazione sugli addominali non è vera, ma visto tutto l'hype che circonda le blockchain non mi sorprenderebbe se ci fosse una start-up nella Silicon Valley che in questo momento sta sottoponendo questa idea alle imprese di capitale.

È facile lasciarsi prendere

dall'entusiasmo per una nuova tecnologia, è successo anche con internet. Era una tecnologia rivoluzionaria che ha cambiato il mondo, ma molte delle precisioni fatte nel primo periodo di internet sono state "esuberanza irrazionale".

Le tempistiche stimate sull'impatto delle nuove tecnologie variano grandemente, e sono spesso sottostimate. Come detto nel capitolo sulla storia della blockchain, DigiCash e le altre tecnologie di denaro digitale basate sulla crittografia sono nate decenni prima di Bitcoin, ma erano troppo avanti nelle

loro previsioni sull'adozione da parte del mercato della tecnologia.

Anche se molte delle previsioni sull'impatto della tecnologia blockchain si sono rivelate accurate, non avranno un impatto su larga scala sulla società ancora per molti anni. Le start-up che oggi sono pioniere della tecnologia potrebbero non sopravvivere abbastanza per vedere la loro tecnologia raggiungere un mercato di massa.

Come detto prima nel capitolo, anche quando le persone vogliono utilizzare Bitcoin e i sistemi basati sulla blockchain, molti preferiscono ancora

i metodi che le blockchain vorrebbero sostituire. Ciò elimina la necessità dei sistemi basati su blockchain, perché le persone preferiscono i sistemi esistenti ai supposti benefici della blockchain.

La tecnologia blockchain è solo un nuovo modo per conservare e gestire i dati. Non è la soluzione a tutti i problemi del mondo, quindi non credete a tutto l'entusiasmo.

Punti chiave:

- **Mancanza di Privacy -** Molte blockchain decentralizzate non sono private. I saldi degli account e le transazioni sono visibili a tutti coloro che si trovano sulla rete.
- **Problemi di Sicurezza -** I beni basati sulla blockchain sono come il contante; se perdi il denaro nel tuo portafoglio o se viene rubato, è andato per sempre. Molti dei metodi di sicurezza utilizzati nella blockchain renderanno l'adozione su larga scala più difficile e forse meno sicura rispetto ai metodi esistenti,

perché le persone scrivono e salvano le loro chiavi private per non dimenticarle.

- **Nessun Controllo Centralizzato -** Con un network di blockchain decentralizzato come Bitcoin, i cambiamenti devono essere accettati da una maggioranza del network. Ciò può andare dal 50% +1 fino al 70% o anche l'80% della rete. Nessuna organizzazione avrebbe il controllo sui cambiamenti o sulla direzione delle blockchain decentralizzate, rendendole rischiose per le aziende perché non potrebbero controllare alcun cambiamento al sistema.
- **Rischio dell'attacco 51% -** Molti dei

computer su cui vengono eseguite le blockchain si trovano in paesi con cui le persone si sentono a disagio per ragioni storiche come il crimine, i sistemi legali o la mancanza di regolazioni. I bassi costi di elettricità e hardware in questi paesi hanno portato alla nascita di grandi centri in cui si minano blocchi delle blockchain. Se questi data center collaborassero, potrebbero potenzialmente controllare più del 50% di una rete e prenderne il controllo.

- **Tecnologia nuova e non provata -** La tecnologia blockchain è una tecnologia nuova e non provata, che

fino a ora è stata applicata principalmente alle criptovalute. I software e aziende nel mondo reale che usano la tecnologia blockchain sono ancora troppo pochi per provarne i benefici rispetto ai sistemi esistenti.

- **Costo -** Necessita di una considerevole quantità di energia per funzionare. È stato stimato che la rete Bitcoin utilizzi in mezz'ora la stessa quantità di elettricità che si consuma in una casa media americana in un intero anno.

  Nota: i calcoli sul consumo di elettricità sono basati sul consumo medio domestico negli Stati Uniti, di

10-12000 KWh di elettricità. Questo è l'equivalente della quantità di elettricità necessaria per generare quattro blocchi sulla blockchain di Bitcoin.

- **Problemi di Scalabilità -** Non è ancora stato possibile scalare in modo efficiente le reti di blockchain, allo stesso livello dei sistemi esistenti. La rete Bitcoin è capace di gestire circa 7 transazioni al secondo, mentre la rete Visa è in grado di gestire circa 20.000 transazioni al secondo.
- **Reputazione e Fiducia -** Bitcoin è l'uso più comunemente noto della blockchain, e ha un forte

collegamento con il terrorismo, lo spaccio di droga e il crimine. Le persone devono fidarsi della rete blockchain che stanno utilizzando, specialmente se essa sostituisce un intermediario in cui si ha fiducia. Molte persone esitano nel fidarsi di reti blockchain associate ad attività criminali.

- **Mancanza di comprensione della tecnologia blockchain** - Per molte persone è difficile capire come funziona la blockchain e quali sono i suoi benefici. Alcune persone sono inoltre preoccupate su alcuni aspetti delle reti blockchain, come i loro saldi e le loro transazioni che

verrebbero resi pubblici. Anche comprendendo i benefici, molti preferiscono i sistemi esistenti.

- **Regolazione e integrazione -** I sistemi basati sulla blockchain dovranno fare i conti con dei problemi di regolazione, nonché con problemi di integrazione con i sistemi esistenti, costosi e che richiederanno molto tempo. I governi e le banche sono restii ai cambiamenti, a causa della scala e del costo necessario per sostituire i sistemi esistenti.
- **Entusiasmo -** C'è moltissimo hype che circonda ciò di cui sono capaci i sistemi basati sulle blockchain. La

blockchain è solo un nuovo tipo di database, non è la soluzione magica che spesso viene pensata essere. È inoltre ancora non provata su larga scala e non ha applicazioni pratiche al di là delle criptovalute.

Capitolo Sei: Blockchain e l'Industria Finanziaria

"La tecnologia Blockchain continua a ridefinire non solo il modo in cui opera il settore del mercato azionario, ma l'economia finanziaria globale nella sua interezza."

- Bob Greifeld, Amministratore Delegato di NASDAQ

Bitcoin è stato il primo uso stabile a livello mondiale della tecnologia

blockchain, e ha rapidamente catturato l'attenzione dell'industria finanziaria. Molte aziende di servizi finanziari non hanno visto un grande potenziale in Bitcoin, finché non l'hanno esaminato attentamente e hanno compreso la tecnologia blockchain su cui è basato. Una volta compreso ciò che la tecnologia blockchain era in grado di fare, hanno investito milioni di dollari nella ricerca, sviluppo e acquisizione per sviluppare le loro blockchain.

Utilizzare una tecnologia basata sulla blockchain nel mercato della finanza ha molti vantaggi. L'abilità della blockchain di processare velocemente le informazioni, eliminando gli

intermediari, ha il potenziale di far scendere i costi aumentando la velocità. Ciò può essere applicato ai trasferimenti di valuta, trading azionario, pagamenti, accordi e molte attività che formano il nucleo delle operazioni delle istituzioni finanziarie.

Trasferire un valore è un processo lento, rispetto alla lunghezza media delle transazioni finanziarie. A volte possono servire settimane per trasferire denaro in certi paesi in cui il tasso di cambio è spesso incerto al momento del trasferimento. Un registro basato su blockchain non solo più abbassare i costi insiti nel trasferimento, ma può

velocizzare significativamente il processo grazie alla rimozione dei canali intermediari attraverso cui le informazioni devono passare per validare la transazione.

Per le banche, la tecnologia blockchain offre un'aumentata velocità delle transazioni e sostituisce i livelli di autenticazione con la trasparenza nelle transazioni.
Le banche registrano gli accordi su dei registri interni, e ciò può essere fatto in momenti diversi per ciascuna banca. Ciò spesso nel fatto che, durante un trasferimento, i fondi vengano rimossi dal registro di una banca ma non appaiano su quello di un'altra banca per

diversi giorni.

Nei paesi in via di sviluppo il processo, in larga parte manuale, può essere molto lungo e prono agli errori. Sostituire questo processo con una blockchain permetterebbe alle banche di risolvere una transazione su un registro distribuito, permettendo a tutti coloro che sono sulla rete di vedere la transazione.

Il trading di azioni funziona più o meno nello stesso modo. Le blockchain possono essere utilizzate per abbassare il tempo necessario per la transazione e per aumentare l'accuratezza dei trade. Infatti, il NASDAQ ha già creato una

blockchain per il trading di azioni.

Attualmente la blockchain che il NASDAQ esegue viene utilizzata per i trade azionari pre-IPO, che trasferiscono la proprietà delle azioni di aziende private tra gli investitori prima che vengano elencate sul mercato azionario. La blockchain NASDAQ è già operativa, e ciò dimostra quanto molti settori siano vicini all'adozione di tecnologie blockchain.

Dopo la prima transazione che ha trasferito la proprietà di azioni tra investitori, Bob Greifeld ha dichiarato che si trattava di un momento determinante nell'applicazione della

tecnologia blockchain, e un enorme avanzamento nel settore finanziario globale.

Indipendentemente da quanto siano grandi i potenziali benefici della tecnologia blockchain, però, le istituzioni finanziarie sono pronte a implementarla?

Sono pronte ad affidare milioni e potenzialmente miliardi di dollari in transazioni, affinché siano processati utilizzando la tecnologia blockchain?

Per farla breve, sì.

L'industria dei servizi finanziari è una delle prime industrie ad aver accettato

positivamente i benefici che vengono dall'utilizzo della tecnologia blockchain.

Molte aziende stanno già utilizzando la tecnologia blockchain, come nell'esempio del NASDAQ fatto prima. Quasi tutte le maggiori istituzioni finanziarie del mondo sono attualmente coinvolte nella ricerca del campo della blockchain, attraverso uno sviluppo interno o iniziative congiunte con altre aziende.

Nasdaq, Visa, Citibank, Capital One hanno investito più di 30 milioni di dollari su chain.com per costruire registri distribuiti per le transazioni tra istituzioni finanziarie.

Ripple è una rete di pagamento che può essere utilizzata per trasferire diverse valute, commodities o tutto ciò che ha un valore utilizzando registri distribuiti.

La rete di pagamento Ripple è attualmente utilizzata dalle principali banche e istituzioni finanziarie nel mondo come una rete per accordi, che permette alle banche di inviare pagamenti internazionali in tempo reale a un costo molto più basso rispetto ai metodi esistenti.

Ad oggi, 15 delle 50 maggiori banche del mondo stanno lavorando con Ripple per sviluppare la piattaforma blockchain.

Paolo Cederle, di Unicredit, ha detto: "La blockchain e le tecnologie collegate rappresentano un cambiamento di paradigma dallo status quo, e un'innovazione sulla quale ci focalizziamo sempre di più.

Attraverso la nostra partnership con Ripple, stiamo ottimizzando i nostri pagamenti globali e siamo una delle prima grandi banche a implementare una tecnologia finanziaria distribuita in un ambiente commerciale."

L'azienda tecnologia R3 lavora con 25 grandi banche tra cui Wells Fargo, JP Morgan e Citibank. Le aziende coinvolte in questo progetto sono note come il

consorzio R3. R3 è una tecnologia di database distribuito che conta su diversi sviluppatori di alto profilo provenienti da Bitcoin, crittografia e l'industria tecnologica. Il registro distribuito che hanno creato è diverso da una blockchain, ma ne condivide molte caratteristiche. Undici banche nel consorzio R3 sono già collegate al registro distribuito R3.

Un altro nome importante che sta sviluppando tecnologia blockchain è la Bank of England. La banca ha dichiarato di volersi impegnare a rovesciare le fondamenta dei suoi database e implementare una blockchain. La Bank of England ha una squadra dedicata alla

blockchain, e sostiene che si tratti di un'innovazione tecnologica chiave.

La Bank of England spera di utilizzare la tecnologia come difesa contro un numero crescente di cyber attacchi, aiutando i sistemi e permettendo ai pagamenti extra bancari di arrivare più velocemente, rendendoli maggiormente compatibili con la tecnologia sempre in movimento.

La Bank of England conta inizialmente di utilizzare il sistema in modo interno, ma ha promesso di aprire la tecnologia a un numero maggiore di imprese dal 2020. Se manterranno la parola, la tecnologia basata sulla blockchain sarà testata su sistemi di accordi lordi in

tempo reale, gestendo centinaia di miliardi di transazioni bancarie ogni giorno.

L'Estonia è un'altra nazione che sta implementando la tecnologia blockchain. Il governo estone è un pioniere della tecnologia digitale e sta sviluppando blockchain per l'identificazione e le cartelle cliniche, e potenzialmente progetta di espandersi ad altre zone come la tassazione e il voto, da costruire sulle basi delle prime.

La tecnologia blockchain sta rapidamente venendo adottata dall'industria finanziaria e dalle banche centrali, ma sta diventando sempre più popolare anche con istituzioni lontane

dalla finanza. Il prossimo capitolo esaminerà le aziende al di fuori della finanza che utilizzano questa nuova tecnologia per trasformare altre industrie.

Punti chiave:

- Trasferire valori tra aziende e nazioni è attualmente un processo lento. La tecnologia blockchain offre un'aumentata velocità di transazione, con la potenzialità di trasferimenti istantanei in tempo reale.
- La tecnologia blockchain può sostituire i livelli di autenticazione

con la trasparenza nelle transazioni.

- Molte banche, banche centrali, governi e aziende finanziarie stanno già utilizzando la tecnologia blockchain, o stanno attualmente facendo ricerca e sviluppo al riguardo.
- Il trading di azioni implica un trasferimento di proprietà tra le persone. Le blockchain possono essere utilizzate per sostituire gli intermediari e processare i trade; il NASDAQ implementa già una blockchain funzionante.
- Molte funzioni finanziarie e amministrative svolte dalle istituzioni finanziarie sono obsolete e manuali.

Queste funzioni potrebbero potenzialmente essere rimpiazzate dalle blockchain e dai registri distribuiti.

Capitolo Sette: Blockchain e le altre industrie non finanziarie

"La blockchain e le tecnologie correlate rappresentano un cambiamento di paradigma rispetto allo status quo, e sono per noi un focus sempre maggiore di innovazione."

Paolo Cederle, AD di UniCredit Business Integrated Solutions

Nel capitolo precedente abbiamo visto in che modo il mondo della finanza stia

rapidamente adottando la tecnologia blockchain. Sebbene la blockchain abbia una forte associazione con i pagamenti e le transazioni, in larga parte a causa del suo inizio con Bitcoin, il potenziale della tecnologia blockchain è potenzialmente molto più grande rispetto ai pagamenti e al settore finanziario.

La blockchain può potenzialmente cambiare ogni settore nel mondo. I progetti in corso di sviluppo mostrano l'impatto che la tecnologia blockchain potrebbe avere sulla vita di tutti i giorni. In questo capitolo parleremo dei potenziali usi della blockchain, facendo esempi di aziende che stanno attualmente sviluppando sistemi basati sulle

blockchain.

Gestione delle identità e identità digitali

La gestione delle identità tramite blockchain è un'innovazione chiave, che potrebbe spianare la via alla fondazione e alla sicurezza di altri settori. Se possiamo fidarci del fatto che qualcuno sia chi dice di essere, possiamo utilizzare questa fiducia per un'ampia gamma di altre applicazioni.

La tecnologia blockchain risolve molti problemi che oggi esistono con le identità digitali. Adesso è abbastanza facile creare delle false identità, o

rubare l'identità di qualcuno online. Le password non sono sicure, e i database centralizzati sono vulnerabili agli attacchi. Quando un database centralizzato viene attaccato, può fornire accesso a tutti i dati dei clienti salvati nel sistema.

I sistemi di identificazione basati sulla blockchain forniscono delle firme digitali usando la crittografia. Sono uniche, sicure, inoppugnabili e praticamente impossibili da duplicare o da accedere senza autorizzazione.

L'identificazione basata sulla blockchain è una possibilità reale per il futuro; il governo dell'Estonia e alcune aziende

come ShoCard stanno già sviluppando sistemi di identificazione sulla blockchain.

In futuro, ciò potrebbe essere usato per identità digitali, passaporti, patenti di guida, permessi di residenza, certificati di nascita, certificati di matrimonio e altre forme di identificazione.

Voto Digitale

Dopo aver sviluppato una tecnologia che permetta le identità e le firme digitali, diventa semplice autenticare l'identità di qualcuno per una serie di altre transazioni e azioni online.

Il voto digitale è una tecnologia la cui applicazione nei vari paesi è fallita a causa di rischi sulla sicurezza e dubbi sulla privacy.

L'Estonia, la Danimarca e la Norvegia hanno fatto delle sperimentazioni riguardanti il voto digitale, ma solo l'Estonia è riuscita a organizzare con successo un voto digitale su larga scala.

La Danimarca ha utilizzato la tecnologia blockchain su piccola scala per il voto all'interno dell'Alleanza Liberale, un partito politico danese che nel 2014 ha usato un sistema di voto basato sulla blockchain.

Utilizzando un sistema di voto basato sulla blockchain un elettore potrebbe controllare l'effettiva ricezione del suo voto, pur mantenendo la sua privacy e nascondendo la sua identità. Renderebbe inoltre il voto più accessibile per molte persone, potenzialmente aumentando la partecipazione al voto nelle elezioni.

Sanità e Cartelle Cliniche

Una blockchain fornisce un registro distribuito nel quale tutti i cambiamenti fatti su una copia del registro vengono aggiornati immediatamente sulle altre copie. Ciò permette di assicurarsi che tutti abbiano i dati più recenti e validi, e che corrispondano a tutte le altre copie

sulla rete.

Ciò ha un enorme potenziale di applicazione nel settore della sanità. Se siete mai stati da più di un medico o in più di un ospedale, certamente sapete che ogni volta che vi recate da un nuovo medico o in un nuovo ospedale dovete compilare moltissimi moduli e scartoffie che riguardano la vostra storia clinica, le vostre allergie e molte altre domande a cui avete già risposto molte volte in altri luoghi.

Salvare queste informazioni in un database condiviso di cartelle cliniche permetterebbe ai medici, agli ospedali, ai chirurghi, agli infermieri e agli

operatori sanitari di avere accesso ai dati condivisi su un paziente. Avrebbero a disposizione tutti i dettagli delle cartelle cliniche, risparmiando tempo e permettendo loro di fare decisioni più informate nel trattamento di un paziente.

Nel caso di un paziente operato d'urgenza, ciò potrebbe anche salvare delle vite. Le informazioni su eventuali malattie preesistenti, gruppo sanguigno, allergie a certi farmaci, contatti di emergenza, farmaci presi o altri dettagli sarebbero immediatamente disponibili all'occorrenza.

I dettagli della storia clinica di un paziente potrebbero anche aiutare a

completare il puzzle e capire cosa sta causando i sintomi di un paziente. Una visita da un medico per un certo sintomo potrebbe non far pensare a un allarme, ma se combinata a una visita a un altro medico od operatore sanitario per una condizione apparentemente non correlata, potrebbe indicare la presenza di una malattia non ancora diagnosticata. Ogni operatore sanitario potrebbe avere avuto a disposizione solo una parte dei sintomi del paziente, dando così una visione parziale, ma avendo più informazioni sarebbe possibile riuscire a fare una diagnosi migliore.

Se avessero accesso a questo database,

anche le assicurazioni sanitarie risparmierebbero una quantità significativa di tempo e denaro. Quando si richiede un preventivo per un'assicurazione sanitaria, vengono fatte moltissime domande e molti esami medici che possono essere invasivi, lunghi e spiacevoli. Dando all'assicuratore accesso alle proprie cartelle cliniche, l'assicurazione avrebbe una visione completa della nostra storia clinica e sarebbe in grado di prendere decisioni sull'assicurazione basandosi su tali informazioni, senza avere bisogno di esami o domande.

Attualmente, aziende come Gem, Tieroim e Philips Healthcare stanno

lavorando su delle blockchain per delle cartelle cliniche. Anche in questo caso, l'Estonia è tra le nazioni più all'avanguardia. L'autorità eHealth dell'Estonia sta lavorando con l'azienda di tecnologie blockchain Guardtime per inserire i dati medici dei cittadini in un database sicuro basato su blockchain.

La motorizzazione dell'Estonia riceve già da tempo certificati medici digitali per assicurarsi che le persone che richiedono il rinnovo della patente abbiano i requisiti fisici per la guida. In passato questo era un processo manuale per i cittadini, ma oggi è digitalizzato e automatizzato. In futuro, le cartelle

cliniche sulla blockchain potranno essere aggiornate con queste informazioni, come ad esempio la presenza o assenza di requisiti fisici per la guida. La pubblica amministrazione avrà accesso a queste informazioni, e i sistemi potranno fornire automaticamente i rinnovi in base alle informazioni contenute nelle cartelle cliniche sulla blockchain.

Una blockchain di cartelle cliniche offre dei vantaggi sia per i pazienti che per gli operatori sanitari. I pazienti avranno una visione più trasparente e accurata delle loro cartelle cliniche e dei dati sulla salute. Nessun governo o azienda potrà cambiare tali informazioni senza che il

paziente, insieme a tutti gli altri utenti della rete, ne sia a conoscenza.

L'Estonia ha creato un portale per i pazienti, che permette ai cittadini di avere pieno accesso alla propria storia clinica, alle prescrizioni, alle visite specialistiche e alle informazioni sull'assicurazione. Nel portale è inoltre possibile dichiarare la volontà di donare gli organi e prendere decisioni sui trattamenti da ricevere durante un'operazione chirurgica.

Nel futuro, questo database potrebbe essere tutto su una blockchain. Sebbene l'Estonia si stia rapidamente portando in testa, tra pochi anni tutto ciò potrebbe

essere una realtà.

Certificati Accademici

La Holbertson School in California ha intenzione di utilizzare la tecnologia blockchain per autenticare i suoi certificati accademici. La falsificazione di transcript e certificati accademici è una pratica comune, nella quale gli studenti millantano qualificazioni che non hanno realmente ottenuto.

La blockchain permetterebbe una maggiore trasparenza sulla storia accademica e le qualifiche degli studenti. Permetterebbe di verificarle facilmente, eliminando le frodi e

risparmiando il tempo e il denaro necessari per i controlli manuali delle certificazioni.

Musica

Il settore della musica sta già sviluppando delle tecnologie basate sulla blockchain, da utilizzare in una vasta gamma di applicazioni. Ci sono diverse aziende che stanno sviluppando app basate sulla blockchain per cambiare il modo in cui la musica viene distribuita, condivisa e acquistata, e il modo in cui le royalty per le vendite vengono pagate agli artisti.

Peertracks, Uio Music e Mycelia sono alcune delle start-up che stanno

lavorando su piattaforme basate sulla blockchain per permettere agli artisti di vendere la loro musica direttamente ai fan, senza bisogno di intermediari o case discografiche.

Spotify ha recentemente acquisito Mediachain, che ha sviluppato un sistema basato su blockchain che permette agli artisti di creare record digitali per le canzoni sulla blockchain di Bitcoin e sull'InterPlanetary File System. Spotify si propone di utilizzare la piattaforma blockchain sviluppata da Mediachain per fornire agli artisti pagamenti più giusti e trasparenti per la loro musica.

Archiviazione Cloud

Le aziende di archiviazione Cloud come Google Drive, Dropbox e Microsoft OneDrive sono diventate lo standard per l'archiviazione di dati e file. Moltissime persone utilizzano l'archiviazione cloud per salvare ogni tipo di dati personali e professionali.

Attualmente, l'archiviazione cloud richiede una grandissima fiducia in aziende di terza parte. Spesso le persone salvano tutti i loro dati in un solo posto, con una sola azienda di archiviazione cloud che richiede una password a basso livello di sicurezza per accedere. I sistemi di archiviazione cloud

centralizzati sono vulnerabili agli attacchi, e le password possono facilmente essere ottenute con un semplice hacking o una truffa

Ci sono diverse start-up che forniscono un'alternativa, unendo l'archiviazione cloud alla tecnologia blockchain.

Aziende come Storj hanno creato sistemi di archiviazione cloud decentralizzati, meno vulnerabili agli attacchi e agli hacking. Lo spazio di archiviazione cloud è distribuito tra gli spazi di archiviazione non utilizzati dei computer collegati alla rete, è criptato e soltanto il proprietario può accedervi.

Siacoin e Filecoin sono delle start-up che stanno anch'esse lavorando sull'unione di archiviazione cloud e blockchain, come Storj.

Leasing e Noleggio Auto

Il settore automobilistico è un altro settore che potrebbe essere trasformato dalla tecnologia blockchain. Visa e DocuSign hanno già avviato una collaborazione per sviluppare una tecnologia basata sulla blockchain per il leasing di automobili.

Ciò taglierebbe di molto la modulistica e la presenza di intermediari coinvolti nel leasing. Il cliente sceglierebbe la

macchina da prendere in leasing; la sua identità digitale conterebbe già informazioni finanziarie e sulla sua patente; accetterebbe una polizza assicurativa per il leasing, e la blockchain verrebbe aggiornata con le nuove informazioni sul leasing.

I noleggi auto negli aeroporti si stanno già muovendo verso un sistema più automatico, eliminando la necessità delle lunghe scartoffie prima del noleggio di una macchina. La tecnologia in corso di sviluppo per i leasing e le identità digitali potrebbe essere applicata anche al noleggio auto.

Le cartelle cliniche di molti cittadini in

Estonia sono già state digitalizzate, e passate alla motorizzazione per il rinnovo automatico delle patenti. Il collegamento delle informazioni sulla blockchain e delle identità digitali potrebbe essere utilizzato, in futuro, anche per approvare automaticamente i noleggi auto.

Ride-Sharing

Le app di Ride-Sharing come Uber hanno sconvolto l'industria dei taxi, e hanno cambiato le modalità di trasporto di milioni di persone intorno al mondo. Le aziende di taxi hanno avuto per molto tempo il monopolio sui trasporti automobilistici in molte città del mondo,

con una sola azienda che controllava tutte le licenze di taxi di una città.

Sebbene Uber e le altre app di ride-sharing forniscano un'alternativa ai taxi, si tratta comunque di database centralizzati, di sistemi tutti controllati da una sola azienda.

Il ride sharing riguarda il conducente e il passeggero; tuttavia con le attuali piattaforme di ride sharing c'è sempre un intermediario in tutte le interazioni e transazioni.

La tecnologia blockchain renderebbe possibile eliminare tutti gli intermediari e creare app di ride sharing

decentralizzate.

Una start-up di nome La'zooz sta attualmente lavorando su una piattaforma di ride sharing decentralizzata e basata sulla blockchain.

Quello del ride sharing è un settore in cui sostituire le piattaforme esistenti con una blockchain sarebbe facile.

La sicurezza dei conducenti potrebbe essere un problema; tuttavia, se le identità digitali venissero collegate alla blockchain della motorizzazione o se le blockchain per il noleggio e il leasing delle auto fossero comuni, il ride

sharing si integrerebbe bene con queste blockchain.

Immobili

Il settore immobiliare è uno di quelli che ad oggi richiede moltissime scartoffie, moduli e intermediari per facilitare le transazioni. Gli atti notarili necessitano di documenti spesso difficili da ottenere, soggetti agli errori o addirittura persi, con un processo lentissimo.

Gli atti di proprietà e le transazioni basati sulla blockchain potrebbero aumentare enormemente la velocità e la trasparenza degli atti di compravendita immobiliare, riducendo il costo delle

transazioni.

Le piattaforme immobiliari basate sulla blockchain potrebbero salvare gli atti di proprietà, le compravendite, i permessi edilizi o le varie documentazioni, e qualsiasi altro documento attualmente salvato dalle aziende o dalle pubbliche amministrazioni.

Ubitquity è una start-up che sta attualmente sviluppando una piattaforma immobiliare basata sulla blockchain per le banche, istituzioni finanziarie, per le finanziarie e per tutti coloro che vogliono cercare documenti relativi alle compravendite immobiliari.

Affitti a breve termine

AirBnB è un altro esempio di una piattaforma come Uber, che ha sconvolto un intero settore creando una piattaforma che ha permesso alle persone di affittare i propri appartamenti ad altre persone, in tutte le città del mondo.

Airbnb ha eliminato gli intermediari come hotel e agenti di viaggio, portando le persone a effettuare transazioni l'una con l'altra. Sebbene sia un passo avanti nella direzione dell'eliminazione degli intermediari, ha soltanto sostituito gli intermediari con un'altra piattaforma che facilita le transazioni sulle persone.

Le piattaforme di affitto a breve termine e hotel basate sulla blockchain potrebbero operare come Airbnb, ma senza un intermediario che faciliti tutte le transazioni e le prenotazioni. Queste sarebbero svolte direttamente dalle persone sulla blockchain.

Settore dei Viaggi

Anche le piattaforme di prenotazione hotel più tradizionali potrebbero essere sostituite da sistemi di prenotazione basati sulla blockchain.

John Guscic, il direttore generale di Webjet, ha dichiarato che *"Nelle transazioni che riguardano le prenotazioni di hotel in tutto il mondo,*

in 1 transazione di 25 qualcuno si trova a fornire un servizio senza essere pagato"

Ciò accade a causa del numero di intermediari coinvolti nel settore delle prenotazioni di hotel e viaggi, in cui le prenotazioni vengono perse o pagate in modo errato. Un sistema di prenotazioni basato sulla blockchain permetterebbe un sistema di prenotazione più trasparente e meno soggetto agli errori.

Attualmente, Webjet sta lavorando con la Microsoft per sviluppare un sistema basato sulla blockchain per il settore dei viaggi, ma non c'è attualmente una data prevista per il suo rilascio.

Programmi di Fedeltà / Raccolta Punti

I programmi di Fedeltà / Raccolta punti sono comuni in molti settori, dalla pasticceria di quartiere alle compagnie aeree più grandi. Tuttavia, i programmi di fedeltà sono spesso costosi da mantenere, soggetti alle frodi e spesso i clienti non sono soddisfatti dei premi ricevuti, oppure pensano che il processo necessario per controllare il saldo dei punti e ottenere i premi sia troppo complicato.

La tecnologia blockchain offre una soluzione a molti problemi esistenti che riguardano i programmi di fedeltà e raccolta punti. L'azienda di servizi

finanziari Deloitte ha pubblicato un articolo intitolato "Realizzare una blockchain per i programmi di fedeltà clienti", che ha esaminato il modo in cui i programmi di fedeltà basai sulla blockchain potrebbero fornire benefici ad aziende e clienti.

L'articolo sostiene che gli attuali programmi di fedeltà soffrano a causa della scarsa partecipazione dei clienti, i tempi di lavorazione lunghi, le frodi e gli elevati costi per il mantenimento. Un sistema di fedeltà basato sulla blockchain sarebbe più trasparente, ridurrebbe in modo significativo i tempi di lavorazione e i costi, e aumenterebbe la sicurezza.

I punti ottenuti dai clienti in seguito alle transazioni verrebbero aggiornati in tempo reale, tagliando i lunghi tempi di lavorazione che oggi sono necessari per aggiornare i saldi dei clienti. Le aziende potrebbero integrare i programmi fedeltà in modo più semplice, aggiungendo valore e opportunità per i clienti e creando potenziali opportunità commerciali condividendo i programmi con altre aziende amiche.

Una start-up chiamata Loyyal sta lavorando con altre aziende nel settore tecnologico e commerciale per sviluppare un programma di fedeltà

basato sulla blockchain. Con la trasparenza, i costi ridotti e l'aumentata velocità saranno possibili programmi di fedeltà e raccolta punti migliori, sia per le aziende che per i clienti.

Predizioni e Gioco d'azzardo

Il settore del gioco d'azzardo cambierà in modo significativo a causa della nascita delle start-up che si occupano di blockchain. Non saranno solo le scommesse sugli eventi sportivi a cambiare ma l'intero settore delle predizioni, includendo le previsioni del tempo e le previsioni sui mercati finanziari.

Una delle criptovalute in più rapida crescita è Augur, che sta sviluppando un mercato di predizioni in cui gli utenti possono fare predizioni e trarre profitto dal risultato di un evento.

Augur sarà una piattaforma decentralizzata per prevedere la probabilità che un qualsiasi evento si verifichi. Il sistema si basa su una ricerca che mostra che i mercati di predizione sono, sul lungo periodo, più accurati dei singoli analisti, degli esperti, dei sondaggi o delle interviste.

Nei sondaggi, molto spesso le persone rispondono con quello che sperano sia il risultato di un evento, non quello che

credono accadrà. Questo è il motivo per cui gli exit poll possono essere del tutto inaccurati, con risultati che cambiano in modo sensibile rispetto al risultato effettivo delle elezioni. I mercati di predizione chiedono alle persone di "scommetterci", e rischiare del denaro in base al risultato di un evento; ciò porta a risultati nel tempo più accurati.

Contratti Smart

Gli esempi nel capitolo mostrano che la tecnologia blockchain potrebbe essere la prossima grande innovazione in moltissimi settori. In termini di ciò di cui è capace la tecnologia blockchain,

questi esempi sono solo la punta dell'iceberg. Molte delle applicazioni della tecnologia blockchain potranno essere gestite utilizzando i contratti smart.

Nei prossimi capitoli parleremo di contratti smart, app decentralizzate, della piattaforma Ethereum e di altri esempi di ciò di cui è capace la tecnologia blockchain.

Punti chiave:

- Non sono solo le aziende di servizi finanziari a implementare sistemi basati sulla blockchain. La tecnologia blockchain ha un'ampia gamma di usi in diversi settori.
- La tecnologia basata sulla blockchain può essere utilizzata per trasferire e salvare tutto ciò che ha un valore.
- Molte aziende stanno già sviluppando i loro sistemi di blockchain, e altri sistemi sono già disponibili e in attività.
- Nel futuro, intermediari e piattaforme potrebbero essere sostituiti da

piattaforme blockchain.

- La tecnologia blockchain è una realtà molto più vicina di ciò che credono molte persone. È probabile che nei prossimi anni ci saranno moltissimi settori che implementeranno tecnologie blockchain.

Capitolo Otto: Ethereum, i Contratti Smart e le Applicazioni Decentralizzate

"Dare agli utenti un accesso facile a molti diversi tipi di beni digitali sulla blockchain, specialmente token collegati a beni nel mondo reale, è cruciale per permettere all'adozione della tecnologia blockchain di raggiungere il prossimo livello..."
Vitalik Buterim, Scienziato Capo,

Ethereum

Introduzione a Ethereum

Ethereum è il prossimo passo nel futuro della tecnologia blockchain. Costruito sulle stesse fondamenta della tecnologia blockchain di Bitcoin, porta però le possibilità della tecnologia blockchain a un altro livello.

Ethereum è una blockchain con un linguaggio di programmazione che permette ad applicazioni e contratti smart di essere eseguiti sulla blockchain sottostante.

Ciò permette agli sviluppatori di creare

programmi che vengono eseguiti su una blockchain e usano la potenza di calcolo di migliaia di computer collegati alla rete della blockchain.

Quasi tutte le applicazioni che oggi vengono eseguite su un computer potrebbero potenzialmente essere eseguite su una blockchain. Utilizzando la rete Ethereum, gli sviluppatori possono creare applicazioni in modo rapido e semplice, senza dover creare la loro blockchain o la loro criptovaluta. La rete Ethereum usa la criptovaluta "Ether", che agisce come valuta sulla rete. Gli Ether vengono scambiati come pagamento per aver eseguito app decentralizzate sulla rete.

La criptovaluta Ether è la seconda criptovaluta più grande del mercato dopo Bitcoin, con una capitalizzazione di mercato superiore a 10 miliardi di dollari.

Differenze tra Ethereum e Bitcoin

La differenza principale tra Bitcoin ed Ethereum sta nel fatto che Bitcoin viene utilizzato principalmente come registro distribuito per transazioni finanziarie, mentre Ethereum è pensato per essere usato come piattaforma di calcolo distribuito per eseguire applicazioni.

I Bitcoin possono essere usati per pagare beni e servizi in ogni luogo in cui siano accettati, mentre la valuta della

rete Ethereum, l'Ether, è pensato per essere usato dagli sviluppatori, che pagano per la potenza di calcolo sul network eseguono applicazioni decentralizzate.

Sia Bitcoin che Ethereum hanno delle valute digitali, ma nel complesso hanno uno scopo diverso. L'Ether non vuole essere un sistema di pagamento alternativo, ma serve a incoraggiare gli sviluppatori a creare ed eseguire applicazioni su Ethereum.

Per dirla semplicemente: Bitcoin è principalmente una valuta per transazioni finanziarie. Ethereum ha molte facce, ha una sua criptovaluta

("Ether"), ma non è tutto ciò che ha. La valuta è solo una piccola parte della rete, ed Ethereum ha un'intera piattaforma di calcolo costruita sulla blockchain.

Benefici di Ethereum

Dal momento che la blockchain di Ethereum viene eseguita da migliaia di computer in tutto il mondo, le applicazioni possono essere eseguite utilizzando la potenza di calcolo di un enorme network globale di computer.

Uno dei problemi con la rete Bitcoin consiste nel fatto che, pur essendo più potente dei più grandi supercomputer

del mondo messi insieme, il suo potere di calcolo viene sprecato generando numeri casuali per aggiungere blocchi alla blockchain.

Ethereum usa in modo migliore i computer collegati alla rete e la loro potenza di calcolo, permettendo agli sviluppatori di creare applicazioni da eseguire utilizzando la potenza di calcolo combinata della rete, insieme alla tecnologia blockchain.

Gli sviluppatori non devono creare la loro blockchain o convincere dei computer a connettersi ad essa. Ethereum ha già una rete consolidata di computer sulla blockchain Ethereum.

La piattaforma Ethereum ha anche l'Ethereum Virtual Machine e il linguaggio di programmazione Solidity. Solidity può essere utilizzato per creare applicazioni decentralizzate o contratti smart, che vengono poi compilati dall'Ethereum Virtual Machine ed eseguiti sulla blockchain.

Applicazioni Decentralizzate (dApp)
Le applicazioni decentralizzate sono applicazioni open source, che non vengono controllate da una sola persona o entità e che vengono eseguite su una blockchain distribuita o una rete di computer.

Le dApp non hanno un server centrale; gli utenti si connettono l'uno con l'altro attraverso connessioni peer to peer.

Con le applicazioni standard, le app vengono controllate da una sola entità, e vengono eseguite su un server centralizzato vulnerabile all'hacking o al downtime a causa della possibilità che il server vada offline.

Un'app decentralizzata non ha un singolo server o entità che la controlla. Viene eseguita su una rete di computer, e i cambiamenti vengono decisi dagli utenti.

Non c'è un punto centrale in cui il server possa crashare o essere hackerato. Se un

computer sulla rete va offline, l'applicazione non viene influenzata perché ci sono migliaia di altri computer su cui l'applicazione viene contemporaneamente eseguita.

Anche se un computer sulla rete viene hackerato, non può fare cambiamenti non autorizzati all'applicazione, perché la maggioranza della rete deve accettare i cambiamenti.

Contratti Smart

I contratti smart sono contratti scritti utilizzando un codice sorgente, e operano su una blockchain o un registro distribuito.
Verificano, eseguono ed applicano il

contratto in base ai termini scritti nel sorgente. I contratti smart possono essere parzialmente o totalmente auto-eseguibili e auto-applicabili.

I contratti smart possono essere utilizzati per scambiare qualsiasi cosa abbia un valore; come detto nel capitolo sui potenziali usi della blockchain, molti settori che utilizzano la tecnologia blockchain inizieranno a usare contratti smart.

Quando un contratto smart viene eseguito sulla blockchain, opera in modo automatico. Se le condizioni di un contratto vengono rispettate, il pagamento o il valore viene scambiato

in base ai termini del contratto. Allo stesso modo, se le condizioni nel contratto non sono rispettate, i pagamenti possono essere trattenuti, se ciò è specificato nel contratto smart.

I contratti smart vengono eseguiti nel modo in cui sono programmati, su una rete decentralizzata di computer sulla blockchain, ed eliminano il rischio di cambiamenti non autorizzati, frodi, avaria del server o mancato rispetto dei termini del contratto. I contratti vengono eseguiti automaticamente, scambiando valore e pagamenti tra le persone senza che sia necessario avere avvocati o tribunali che li facciano applicare.

A ogni voce sulla blockchain sono associate data e ora, e non possono essere alterate. Ciò rende la blockchain una piattaforma ideale per i contratti, perché a ogni cambiamento nei contratti verrebbe associata data e ora, e le versioni precedenti verrebbero mantenute sulla blockchain.

I contratti possono essere salvati, e nuove versioni possono essere create mantenendo le copie precedenti (e i timestamp accurati di ogni modifica e revisione). Ciò non solo permette di seguire il processo avvenuto in modo più accurato, ma rende tutte le parti coinvolte nella transazione più oneste,

perché il registro non può essere alterato. La rete blockchain elimina la necessità di intermediari di terza parte che gestiscano i contratti.

Usi dei contratti smart

Un rischio con il network Bitcoin consiste nel fatto che, se acquisti un oggetto pagando in Bitcoin, dopo aver fatto il pagamento non c'è garanzia di ricevere i beni acquistati. L'altra persona coinvolta potrebbe decidere di non spedire la merce, o dichiarare di non aver ricevuto il pagamento.

Dal momento che non ci sono

intermediari di terza parte per le transazioni sulla rete Bitcoin, non è possibile un corso d'azione tradizionale come la disputa della transazione, la richiesta di un rimborso o il contatto di un intermediario.

I portafogli Bitcoin sono anonimi, quindi è possibile non avere alcuna informazione su dove sia finita la transazione. Se una transazione viene mandata all'indirizzo sbagliato, è andata per sempre e il denaro viene perso.

I contratti smart risolvono molti dei rischi associati alle transazioni sulla rete blockchain. I contratti smart possono essere utilizzati per tutto ciò

che ha un valore e può essere scambiato, e ci sono molte aziende che stanno sviluppando applicazioni decentralizzate e basate sulla blockchain, che utilizzano i contratti smart.

Ascribe è una start-up nel settore dell'arte, che permette a molti artisti di rivendicare la proprietà del proprio lavoro e di realizzare stampe in edizione limitata. La realizzazione di arte digitale numerata utilizza una blockchain per tracciare all'indietro tutte le creazioni e le transazioni originali riguardo a tali creazioni. Ascribe ha un mercato in cui gli artisti possono farsi pubblicizzare, e le persone possono comprare e vendere

arte attraverso il sito web.

UProov, un'azienda legale e di media, fornisce timbri verificabili e in tempo reale su tutti i video e le immagini scattate da dispositivi elettroniche. Le immagini e i video dotati di timestamp non possono essere alterati, e sono dunque prove più affidabili in tribunale.

BitProof, un'altra azienda che usa una blockchain per creare dei timestamp, ha un'app facilmente scaricabile su un telefono. Ciò permette di applicare dei timestamp verificabili a ogni pezzo di documentazione sottoposto all'app. Può essere tracciato all'indietro fino alla sua creazione, su una blockchain che non

può essere modificata. Questa tecnologia potrebbe potenzialmente eliminare, in futuro, la necessità dei notai.

Warranteer è un'altra azienda che ha già dei legami con GoPro e LG. Utilizza contratti smart per spostare le garanzie dei prodotti su una blockchain in modo da renderle facilmente accessibili, trasferibili e conservabili. Tutte le tracce di modifiche, cambiamenti, aggiornamenti e spostamenti vengono registrate su una blockchain alla quale sia chi richiede che chi offre la garanzia può accedere in qualsiasi momento.

Peertracks, Mycelia e Ujo Music sono

aziende separate, ma tutte si focalizzano sull'uso della tecnologia blockchain all'interno del settore della musica. Tutte e tre le aziende utilizzano contratti smart in modi diversi, con gli obiettivi di eliminare gli intermediari come le case discografiche, rendendo più semplice per i musicisti vendere direttamente ai fan e farsi pagare per la propria musica.

Il microcredito è il prestito di piccole somme di denaro, principalmente nei paesi poveri del mondo. La quantità di denaro è piccola per una banca ma significativa per chi la richiede, perché permette di avviare un'azienda, ottenere un reddito e supportare la propria famiglia.

Il microcredito ha fatto uscire dalla povertà milioni di persone in tutto il mondo, con l'aiuto di Mohamed Yunus, che ha vinto il Premio Nobel per il suo lavoro con il microcredito. Prima della modernizzazione del microcredito da parte di Mohamed Yunus, la maggior parte delle banche non volevano finanziare prestiti piccoli, perché la burocrazia costava di più del profitto ottenuto sul prestito.

La micro-assicurazione è un settore che non ha visto un cambiamento drammatico come il microcredito. La start-up Stratumn si propone di cambiare

il mondo della micro-assicurazione, lavorando con Lemonway sulla creazione di un sistema di micro-assicurazione basato sulla blockchain, chiamato "LenderBot". LenderBot farà uso dei contratti smart e di una blockchain per creare e gestire contratti di micro-assicurazione.

Quando si parla del futuro della blockchain, il termine "Blockchain 2.0" viene comunemente utilizzato per descrivere il passo successivo nell'evoluzione della tecnologia blockchain. Le app decentralizzate e i contratti smart portano le capacità della tecnologia blockchain a nuovi ed eccitanti livelli. Il futuro della

blockchain girerà intorno ai contratti smart e alle dApp. La blockchain 2.0 potrebbe potenzialmente avere un impatto sul mondo esponenzialmente più grande dell'impatto avuto da Bitcoin e dalla tecnologia blockchain originale.

Punti chiave:

- Ethereum è una piattaforma costruita su una blockchain con un linguaggio di programmazione, che permette agli sviluppatori di creare ed eseguire applicazioni decentralizzate e contratti smart su una piattaforma di calcolo potente e distribuita, e sulla blockchain sottostante alla piattaforma Ethereum.
- La valuta Bitcoin e la sua rete sono usate principalmente per le transazioni finanziarie. Ethereum ha una valuta, "Ether", ma è pensata per essere scambiata esclusivamente in

cambio di potenza di calcolo, non per transazioni finanziarie al di fuori della rete Ethereum.

- Le app decentralizzate (dApp) non hanno un singolo server o un'entità che le controlla, ma vengono eseguite su una rete di computer.
- I contratti smart sono contratti scritti utilizzando un codice sorgente, e operano su una blockchain o un registro distribuito.

I contratti smart verificano, eseguono ed applicano automaticamente il contratto in base ai termini scritti nel codice, senza che sia necessario avere intermediari di terza parte

come avvocati o tribunali che li facciano eseguire.

- Tutto ciò che ha un valore può essere scambiato utilizzando i contratti smart, non si riferiscono solo ai contratti legali. I contratti smart riducono i rischi associati alle transazioni sulla rete blockchain, perché le transazioni e i pagamenti vengono gestiti automaticamente dalla rete.
- Ci sono molte aziende che stanno già sviluppando applicazioni decentralizzate basate sulla blockchain e contratti smart sulla piattaforma Ethereum.
- La piattaforma Ethereum è il

prossimo passo nel futuro della tecnologia blockchain, che include contratti smart e app decentralizzate, a cui ci riferiamo come "Blockchain 2.0".

Capitolo Nove: Il Futuro della Blockchain

"Nel futuro vedo una blockchain pubblica - che sia quella di Bitcoin o un'altra che aprirà nel futuro, come modo per registrare la proprietà di ogni tipo di bene e come modo per trasferire la proprietà di un bene in un singolo sistema, che possa essere letta da tutte le persone giuste e da nessuna delle persone sbagliate.

Per me diventerà semplice scambiare i

miei dollari per le tue azioni IBM, o le tue sterline per la mia casa. Ogni bene al quale diamo un valore, e della cui proprietà vogliamo essere certi potrà essere registrato utilizzando questa tecnologia."

- James Smith, AD di Elliptic

Come discusso nel libro, la tecnologia blockchain ha il potenziale di raggiungere ogni stato, settore e persona sul pianeta nelle prossime decadi. Molte delle predizioni sul futuro della blockchain sono supposizioni, ma non si tratta di supposizioni del tipo "in futuro ci saranno macchine volanti". Ci sono molti sistemi basati sulla blockchain che

sono già in sviluppo nelle varie industrie.

Il momento ottenuto dalla tecnologia blockchain negli ultimi anni, in termini di investimenti in progetti pubblici e privati, rende molto realistica la previsione di un futuro in cui la tecnologia blockchain è incorporata nella nostra vita quotidiana.

Se guardiamo i sistemi basati sulla blockchain attualmente in sviluppo, i settori in cui vengono utilizzati e i trend che si stanno creando, possiamo espandere quei trend nel futuro per farci un'idea della direzione futura dei sistemi basati sulla blockchain.

Open source decentralizzato vs Closed source centralizzato

Un'attuale divisione nello sviluppo della blockchain riguarda il conflitto tra l'idea che le blockchain dovrebbero essere decentralizzate e con il codice sorgente disponibile al pubblico (open source) o centralizzate con il codice sorgente privato in mano a un'organizzazione o a un gruppo di collaboratori (closed source).

I componenti originali della tecnologia blockchain ritengono che le blockchain dovrebbero essere open source e decentralizzate. Le aziende e i governi vedono le tecnologie blockchain open

source e decentralizzate e pensano che siano una splendida idea, ma le vorrebbero senza gli aspetti decentralizzati e open source.

È un po' come nei primi tempi di diffusione dei computer, in cui la maggior parte dei programmatori ritenevano che il software dovesse essere open source e gratuito per tutti. Bill Gates ricevette molte critiche per essere andato contro questa mentalità, rendendo il software qualcosa di commerciale, sui cui applicare e vendere licenze. Sebbene il software open source sia ancora popolare, al giorno d'oggi la maggior parte delle aziende di software non condividono

apertamente il loro codice.

Ripple è uno dei progetti di blockchain più noti, ed è attualmente la terza criptovaluta più grande in base alla capitalizzazione del mercato. Ripple è closed source e centralizzato, è distribuito tra un numero selezionato di istituzioni finanziarie come un registro distribuito per gestire transazioni tra di loro.

Ripple ha ricevuto moltissime critiche da parte della comunità open source, che non vuole che il futuro della tecnologia blockchain sia rappresentato da blockchain chiuse e centralizzate, possedute da grandi istituzioni

finanziarie.

Ethereum è la seconda criptovaluta più grande per capitalizzazione del mercato, ed è una delle più grandi reti di blockchain. Ethereum è open source e decentralizzata. Fornisce agli sviluppatori una piattaforma per sviluppare applicazioni decentralizzate con dei token sulla blockchain, che usa la piattaforma Ethereum.

Non sembra che ci sia un chiaro vincitore in questo conflitto, e non sappiamo in che direzione si muoveranno le blockchain tra open source decentralizzate e closed source distribuite/centralizzate. C'è un

significativo lavoro di sviluppo e un importante finanziamento per entrambi i metodi, perché entrambi hanno dei benefici e si adattano a comunità, organizzazioni e requisiti differenti.

Con ogni probabilità la tecnologia blockchain continuerà a muoversi simultaneamente in entrambe le direzioni. I governi e le grandi aziende sceglieranno un metodo mentre i singoli programmatori, i progetti su piccola scala e le start-up ne sceglieranno un altro.

Registri distribuiti

Il consorzio R3 delle più grandi

istituzioni finanziarie è un'altra delle direzioni prese dalle aziende. Il consorzio stava in origine sviluppando una blockchain, ma è passato a un registro distribuito. Sebbene il registro distribuito del consorzio R3 abbia molti dei benefici di una blockchain, non è una blockchain.

Oggi i registri distribuiti sono fortemente associati alle blockchain, e si assume che tutti i registri distribuiti si basino sulle blockchain. Tuttavia, i registri distribuiti possono operare senza usare le blockchain.

La maggior parte del lavoro di sviluppo e delle start-up si basa sulle blockchain,

ma i registri distribuiti non basati sulle blockchain potrebbero essere un trend che emergerà in futuro.

Meno criptovalute

All'inizio dello sviluppo di ogni settore ci sono molte aziende, ma quando il settore e il mercato si sviluppano il numero si riduce, finché non ci rimangono solo alcune grandi aziende o compagnie.

All'inizio del '900, quando le automobili erano una nuova tecnologia, c'erano migliaia di case automobilistiche negli Stati Uniti; oggi sono solo poche grandi aziende.

Il tasso di riduzione nelle case automobilistiche è un caso comune in

molti settori, e probabilmente sarà il trend tra le criptovalute nel futuro. Attualmente ci sono migliaia di criptovalute, e ogni giorno ne vengono create di nuove. È probabile che in futuro rimarranno soltanto poche grandi criptovalute, che saranno accettate in tutto il mondo come forma di pagamento.

Questo trend è già in atto, e i nuovi progetti di blockchain vengono lanciati utilizzando token su blockchain esistenti come Ethereum, invece di creare le proprie criptovalute.

Più token blockchain

Anche se probabilmente ci sarà una

riduzione nel numero delle criptovalute, il numero di token sulle piattaforme blockchain aumenterà.

I token sono simili alle criptovalute, e vengono scambiati sulla blockchain per pagare degli acquisti. La differenza sta nel fatto che esistono su una blockchain già esistente, e che il token rappresenta un valore relativo alla valuta di un'altra blockchain.

Ethereum è la blockchain più popolare che si adatta a questo concetto. La blockchain di Ethereum usa una valuta nativa chiamata "Ether". Chiunque può creare token che stiano sulla blockchain Ethereum; i token rappresentano un

valore e vengono usati per gli scambi, ma utilizzano la blockchain esistente di Ethereum e l'Ether.

I token permettono agli sviluppatori e alle organizzazioni di creare applicazioni che vengono eseguite su una blockchain, senza dovere creare la propria blockchain o criptovaluta.

Blockchain 2.0 - App decentralizzate (dApp) e Contratti Smart

Blockchain 2.0 è il termine utilizzato per descrivere le nuove funzionalità delle blockchain che esistono oggi, rispetto al codice sorgente originale.

La piattaforma Ethereum ha reso possibile creare ed eseguire app decentralizzate e contratti smart su una blockchain. Abbiamo parlato nel dettaglio delle dApp, dei Contratti Smart e della piattaforma Ethereum in precedenza.

Le dApp e i Contratti Smart costruiti sulla rete Ethereum o su altre blockchain esistenti, che usano token al posto di criptovalute, rappresentano un trend in rapida crescita, che non dà segno di volersi fermare.

Una maggiore regolazione e accettazione

Ci sono ancora molte critiche e dubbi riguardo alla tecnologia blockchain. Bitcoin ne è un esempio: i governi ritengono che le transazioni siano troppo private, rendendo facile utilizzarlo per attività criminali, riciclaggio del denaro ed evasione fiscale. Guardando l'altro lato della medaglia, altri ritengono che un database centralizzato come Bitcoin, con la sua trasparenza, la possibilità di vedere i portafogli, il saldo e le transazioni di tutti gli utenti sia troppo aperto e non abbastanza privato.

Molte delle critiche sono dovute al fatto che Bitcoin è la tecnologia blockchain più nota, conosciuta e utilizzata a livello mondiale. Le blockchain sono ancora

all'inizio, sono pesantemente associate con Bitcoin e le criptovalute, e ci sono centinaia di criptovalute open source che vengono create ogni mese.

Inizialmente, i governi avevano bollato Bitcoin come utilizzato solo dai criminali e per il riciclaggio del denaro. Adesso la tecnologia blockchain è stata compresa meglio, e le istituzioni finanziarie hanno iniziato a integrarla nei mercati finanziari; di conseguenza, questa visione sta iniziando a cambiare. I governi stanno incoraggiando le aziende di tecnologie finanziarie (FinTech) a entrare in affari nei loro paesi, ad accettare le criptovalute come forma di pagamento e ad assicurarsi che

siano correttamente regolate all'interno del loro paese.

Il Giappone ha recentemente legalizzato Bitcoin come forma di pagamento, l'Australia ha eliminato le tasse sulle criptovalute e ha iniziato a incoraggiare le aziende che operano nel mondo delle tecnologie basate su blockchain a stabilirsi in Australia.

I governi continueranno a provare ad attrarre le start-up dell'ambito FinTech per lavorare con banche, aziende e istituzioni finanziarie per creare lavori, promuovere il commercio e far crescere l'economia attraverso le nuove

tecnologie basate sulla blockchain.

Le blockchain nella vita quotidiana

Sia che le applicazioni decentralizzate open source vengano costruite sulle blockchain esistenti, sia che vengano creati nuovi consorzi privati di blockchain, ci sarà un aumento nel numero di blockchain utilizzate in ogni parte della nostra vita.

Molti database aziendali e governativi, che usano fogli di calcolo o registri manuali, saranno sostituiti dalle blockchain. Le principali banche del mondo stanno già sviluppando le proprie blockchain per gestire transazioni, voci di registro, scambi di valuta e così via.

L'utilizzazione della tecnologia blockchain potrebbe continuare a crescere, finché non sarà comune come oggi lo sono i database utilizzati da aziende e governi. Ci sarà anche un trend di alternative basate sulla blockchain per tutti i settori che utilizziamo nella vita quotidiana.

Un esempio che mostra il trend delle alternative basate su blockchain, che coesistono con le opzioni attuali, è l'archiviazione cloud. Le aziende Storj e Siacoin stanno creando sistemi di archiviazione decentralizzata cloud basati sulle blockchain. Sebbene sia improbabile che riescano a sostituire

Google Drive o Dropbox in breve tempo, forniscono un'opzione alternativa per chi desidera archiviare i propri file in cloud.

L'idea che i sistemi basati su blockchain possano sconvolgere le industrie esistenti e sostituire le aziende di oggi potrebbe non realizzarsi nel breve termine, ma c'è un chiaro trend che mostra che in molti settori le alternative basate su blockchain coesisteranno con quelle tradizionali.

La tecnologia blockchain potrebbe non sostituire gli intermediari esistenti come le banche, o le aziende come Google o Uber, come qualcuno ha previsto,

specialmente non sul breve termine. Tuttavia, anche se gli intermediari non vengono eliminati, nel tempo troveremo le tecnologie blockchain al lavoro, attraverso i registri decentralizzati basati su blockchain, i contratti smart, le applicazioni decentralizzate, o semplicemente saremo in grado di scegliere alternative basate sulla blockchain ai sistemi esistenti in molti campi della nostra vita.

Punti chiave:

- **Open source decentralizzata vs closed source centralizzata -** Non c'è ancora un vincitore chiaro per quanto riguarda la direzione futura dello sviluppo. Le blockchain open source decentralizzate verranno sviluppate insieme a quelle closed source centralizzate/in consorzi per adattarsi a requisiti diversi.

- **Registri distribuiti:** i registri distribuiti che non usano una blockchain, ma hanno molti dei benefici delle blockchain,

rappresentano un trend che in futuro potrebbe competere con i registri basati sulla blockchain.

- **Meno criptovalute e più token blockchain:** un trend attualmente in atto è quello delle aziende che usano token sulla piattaforma Ethereum al posto delle loro blockchain e criptovalute. Questo trend continuerà, perché la funzionalità della piattaforma Ethereum permette lo sviluppo di app decentralizzate e contratti smart.

- **Blockchain 2.0:** la tecnologia Blockchain adesso ha aumentato le sue funzionalità in modo

significativo, con app decentralizzate (dApp) e contratti smart che non facevano parte del codice sorgente originale della blockchain. Si usa il termine blockchain 2.0 per riferirsi al futuro della tecnologia blockchain, che include questi miglioramenti, per separarlo dalle capacità originali della blockchain.

- **Più regolazioni e accettazione:** i governi e le aziende stanno iniziando ad accettare le criptovalute come forme legittime di pagamento, e stanno investendo pesantemente nell'infrastruttura e nella tecnologia blockchain.

- **Blockchain nella vita quotidiana:** anche se la tecnologia basata su blockchain non è rivoluzionaria come era stato previsto, diventerà con ogni probabilità parte della vita quotidiana attraverso i registri distribuiti, le opzioni di pagamento o le alternative software alle opzioni esistenti.

Se ti è piaciuto questo libro, hai trovato degli errori o vuoi contattarci:

Se hai apprezzato le informazioni contenute in questo libro, ti preghiamo di condividere le tue opinioni, inserire una recensione su Amazon e dare un'occhiata agli altri libri che troverai al link qui sotto:

www.wisefoxbooks.com/block

Se pensi che questo libro sia stato utile, ti sarò grato per il tuo supporto.

Se vuoi darmi un feedback, hai trovato

degli errori o vuoi semplicemente contattarmi per salutarmi, mandami un'e-mail a: mark@wisefoxpub.com

Grazie per aver letto questo libro. Spero che le informazioni siano state utili, e che ti aiutino a farti conoscere la tecnologia blockchain.

Ci vediamo sulla blockchain!

Guida Bonus alle Risorse

Ottieni gratis la Guida alle risorse blockchain.

La guida include delle risorse per imparare di più sulla blockchain, su Bitcoin, Ethereum e gli ICO.

Include anche una rapida guida di riferimento per

comprendere gli aspetti importanti della blockchain e delle criptovalute.

Attualmente, questa guida è disponibile solo in inglese.

Clicca qui per ottenere la Guida Bonus alle Risorse

Recensioni

Le recensioni ci aiutano a migliorare il libro e aiutano l'autore.

Se questo libro vi è piaciuto, apprezzeremmo molto se poteste impiegare qualche minuto per condividere la vostra opinione e pubblicare una recensione su Amazon.

Link per valutare questo libro:

Per la vostra convenienza, qui sotto troverete un link breve al libro:

www.wisefoxbooks.com/block

L'Autore

Mark Gates è cresciuto in California e si muove sulla scena tecnologica da più di 10 anni.

Ha iniziato a progettare siti web alle superiori, utilizzando l'HTML e un normale editor di testo prima dell'avvento degli editor più avanzati. All'epoca del boom di Internet, più di 15 anni fa, Mark ha iniziato un'azienda di web design mentre faceva l'università.

Ha poi espanso la sua azienda nei settori del digital marketing, SEO e social media. Dopo avere venduto la sua attività, adesso vive la sua vita

viaggiando per il mondo e guadagnando con il suo portatile.

Sebbene all'inizio fosse scettico riguardo alle criptovalute, Mark è diventato un forte sostenitore delle tecnologie basate sulla blockchain e delle criptovalute.

Mark ritiene che il miglior modo di imparare sia l'esperienza diretta. Ama tuffarsi in tutto ciò che riguarda la tecnologia, ottenere un'esperienza diretta e insegnare agli altri a fare lo stesso.

Sia che tu stia lanciando un sito, migliorando un business esistente, facendo trading in criptovalute,

imparando a programmare o cercando di ottenere capacità vere per trovare un buon lavoro, Mark scrive i suoi libri con un linguaggio semplice ed esercizi pratici per aiutarti a raggiungere il tuo obiettivo.

Anche se non hai esperienza, i libri di Mark ti porteranno da principiante a esperto in pochissimo tempo.

Su Amazon potrete trovare gli altri libri di Mark Gates, sotto il profilo dell'autore, al seguente link:

www.wisefoxpub.com/markga