ETHEREUM

La guida definitiva che vi farà conoscere
Ethereum, Blockchain, Contratti Smart,
ICO e App decentralizzate.

SCRITTO DA MARK GATES

Ethereum

La guida definitiva che vi farà conoscere Ethereum, Blockchain, Contratti Smart, ICO e App decentralizzate.

Include delle guide su come comprare Ether, criptovalute e investire in ICO.

Scritto da Mark Gates

Le informazioni contenute in questo volume sono da considerarsi esclusivamente a 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.

Ethereum: la guida definitiva che vi farà conoscere Ethereum, Blockchain, Contratti Smart, ICO e App decentralizzate.

Prima edizione. 25 novembre 2017.

Scritto da Mark Gates.

Errori

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, grammatica o altro.

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

I lettori che ci segnaleranno errori

saranno invitati a ricevere copie anticipate dei futuri libri che pubblicheremo.

Errori: errors@wisefoxpub.com

INDICE

GUIDA BONUS ALLE RISORSE

INTRODUZIONE A ETHEREUM

CAPITOLO 1: COS'È ETHEREUM?

CAPITOLO 2: COMPRENDERE LA TECNOLOGIA BLOCKCHAIN

CAPITOLO 3: STORIA DI ETHEREUM

CAPITOLO 4: DIFFERENZE TRA ETHEREUM, ETHEREUM CLASSIC E BITCOIN

CAPITOLO 5: APP DECENTRALIZZATE (DAPP)

CAPITOLO 6: CONTRATTI SMART

CAPITOLO 7: BENEFICI DI ETHEREUM

CAPITOLO 8: SVANTAGGI E RISCHI DI ETHEREUM

CAPITOLO 9: APRIRE UN PORTAFOGLIO ETHEREUM

CAPITOLO 10: COMPRARE, MANDARE, RICEVERE E FARE TRADING CON GLI ETHER

CAPITOLO 11: ICO E TOKEN ETHEREUM

CAPITOLO 12: IL FUTURO DI ETHEREUM

Guida Bonus alle Risorse

Ottieni gratuitamente la guida alle risorse Ethereum e Blockchain.

La guida include delle risorse per scoprire di più su Ethereum, ICO e la tecnologia Blockchain.

È inclusa anche una breve guida ai riferimenti per comprendere gli aspetti importanti di Ethereum, bitcoin e blockchain.

Attualmente, questa guida è disponibile solo in inglese.

Potete ottenere la Guida Bonus alle Risorse al link qui sotto:

www.wisefoxbooks.com/ethbonus

Recensioni e Feedback

Recensioni

Se questo libro ti è piaciuto, apprezzeremmo molto se potessi impiegare qualche minuto per condividere la tua opinione e pubblicare una recensione su Amazon dopo aver finito di leggerlo.

Anche poche parole e un voto possono aiutarci molto.

Feedback

Se il libro non ti è piaciuto o se hai un

feedback da darci, facci sapere cosa non ti è piaciuto mandando un'e-mail a contact@wisefoxpub.com

Apprezziamo tutti i commenti, perché ci aiutano a migliorare il libro in base al feedback dei lettori.

Introduzione a Ethereum

"Quando ho avuto l'idea di Ethereum, il mio primo pensiero è stato, ok questa cosa è troppo bella per essere vera. Alla fine, l'idea di base di Ethereum si è rivelata buona, solida, in modo completo e viscerale." - - Vitalik Buterin, Creatore di Ethereum

Quando Bitcoin è stato creato, nel 2009, all'inizio non ha goduto di grande considerazione, ed era ritenuto solo un modo per permettere a criminali e informatici di trasferire soldi "finti" l'un l'altro. In meno di 8 anni, è passato dall'essere considerato una truffa all'essere visto come una tecnologia che

potrebbe rivoluzionare la finanza, le banche, il mercato delle valute e potenzialmente creare una valuta globale valida in tutto il mondo.

Questo cambiamento nella percezione è dovuto in larga parte alla realizzazione del potenziale della tecnologia blockchain sulla quale è basato Bitcoin. La tecnologia Blockchain è ancora più rivoluzionaria di Bitcoin, e molti prevedono che avrà un impatto sul mondo paragonabile a quello dell'avvento di Internet.

Sebbene molti abbiano sentito parlare di Bitcoin, a far conoscere al mondo il potenziale della tecnologia blockchain è stato il meno noto Ethereum. Bitcoin

utilizza la tecnologia blockchain principalmente per i pagament e i trasferimenti di valuta digitale, mentre la creazione di Ethereum ha portato le possibilità della blockchain da una tecnologia usata principalmente per i pagamenti finanziari a una tecnologia che potrebbe rivoluzionare e sostituire i sistemi e le aziende in quasi tutti i settori del mondo.

La tecnologia blockchain originale creata da Bitcoin è nota come Blockchain 1.0. Le nuove funzionalità che con Ethereum sono state aggiunte alla tecnologia blockchain prendono il nome di Blockchain 2.0.

Ethereum è considerato, da molti

governi e aziende, una tecnologia di molto superiore rispetto a Bitcoin. Diverse grandi aziende come Microsoft, MasterCard, UBS, ING, Intel, BP, Deloitte, J.P Morgan e altre si sono unite in un'alleanza per lavorare insieme nello sviluppo, nella costruzione e nell'integrazione di applicazioni su larga scala basate su Ethereum.

Ethereum non è soltanto un'idea che potrebbe avere un impatto in futuro. La piattaforma Ethereum ha già mostrato di avere un'ampia gamma di applicazioni nel mondo reale, in una varietà di settori diversi.

Sebbene Ethereum sia stato rilasciato soltanto nel 2015, in questo breve tempo

ci sono state migliaia di aziende e applicazioni create appoggiandosi a Ethereum.

Grazie all'uso delle rivoluzionarie capacità di Ethereum, aziende e sviluppatori hanno guadagnato in pochi anni miliardi di dollari. Su Ethereum è già stato creato tutto: dalle identità digitali, alla condivisione di file, all'archiviazione in cloud alle app di messaging istantaneo.

Ethereum è ancora una tecnologia nuova, ma si prepara a cambiare il mondo. Capire Ethereum in questo stato iniziale potrebbe rendervi all'avanguardia in una tecnologia che in futuro potrebbe essere

parte della vita quotidiana.

Anche se non avete esperienza di Bitcoin, Ethereum o altre criptovalute, alla fine di questo libro saprete in modo chiaro cos'è Ethereum, cosa funziona e perché è così rivoluzionario.

Partiamo dal primo capitolo, che spiegherà esattamente cos'è Ethereum.

Capitolo 1: Cos'è Ethereum?

Per capire Ethereum, bisogna prima sapere qualcosa di Bitcoin e della decentralizzazione.

La centralizzazione

Quasi tutti i siti web che visitate, le applicazioni che utilizzate e le transazioni finanziarie che effettuate hanno alle loro spalle un'azienda o istituzione centralizzata.

Quando caricate una foto su Instagram, l'app si collega ai server centralizzati di Instagram. La foto viene inviata ai server, dove viene salvata.

Quando un'altra persona apre l'app di Instagram, si connette ai server centralizzati di Instagram e accede alla foto direttamente da lì.

Nella maggior parte dei casi, le applicazioni centralizzate come Instagram funzionano bene per la maggioranza delle persone. Tuttavia, hanno rischi e svantaggi significativi.

I server centralizzati sono suscettibili all'hacking. Se qualcuno riuscisse ad hackerare un server centralizzato come quello di Instagram, potrebbero potenzialmente ottenere i dati degli utenti, le loro foto e i loro messaggi. Se un server centralizzato venisse attaccato, o se ci fosse un problema col server, il

server e le applicazioni risulterebbero non disponibili per tutti gli utenti.

I siti web centralizzati, le applicazioni e i server possono inoltre essere bloccati dai governi. La Cina ha bloccato molti siti web famosi come Google, Facebook, Twitter e YouTube, e molti altri siti web che non si adeguano alle regole del governo cinese sulla censura e sulla condivisone dei dati dei loro utenti con il governo.

L'hacking, la censura e i downtime dei server sono rischi comunemente associati ai server e alle applicazioni centralizzate.

La Decentralizzazione

Parlando di Ethereum, la decentralizzazione distribuisce i server e la potenza di calcolo su una rete di computer. Questi computer sono tutti collegati e lavorano insieme come un grande supercomputer. Tuttavia, ogni computer lavora anche in modo indipendente, e la rete non si affida a ogni singolo computer per funzionare.

Se un server va offline, gli altri server continueranno a funzionare senza problemi. I benefici di un sistema decentralizzato su più server sono stati spiegati in modo semplice da Vitalik Buterin, quando ha spiegato che è più probabile per un singolo server andare down, piuttosto che per 5 server su 10.

In un sistema decentralizzato, se un hacker volesse accedere al sistema dovrebbe ottenere accesso alla maggioranza dei computer sulla rete nello stesso momento. Sebbene ogni computer lavori separatamente, tutti insieme lavorano come un solo supercomputer. Non è possibile controllare l'intero supercomputer, a meno che non vengano controllati nello stesso momento la maggior parte dei computer.

Ci sono migliaia di computer sulla rete Ethereum, quindi il sistema potrebbe essere hackerato solo se migliaia di computer fossero hackerati nello stesso momento, il che è quasi impossibile.

Più avanti nel libro, andremo maggiormente nel dettaglio su come funziona la decentralizzazione della rete Ethereum.

La rete decentralizzata di Bitcoin

Bitcoin ha una rete decentralizzata di computer che lavorano insieme. Bitcoin ha più computer di Ethereum, e la rete esiste da più tempo. Il potere di calcolo della rete Bitcoin è più grande di quello dei 500 supercomputer più potenti messi insieme.

Sembrerebbe che Bitcoin abbia tutti i vantaggi di una rete decentralizzata che ha Ethereum, quindi perché Ethereum viene visto come superiore a Bitcoin?

I computer collegati alla rete Bitcoin processano transazioni finanziarie, e possono portare a termine un numero limitato di operazioni. Sebbene la rete Bitcoin abbia un'incredibile potenza di calcolo, la maggior parte di questa potenza di calcolo viene utilizzata per validare e aggiungere transazioni al registro Bitcoin. La rete Bitcoin non è in grado di fare girare applicazioni complesse, o di utilizzare la potenza di calcolo per altri scopi.

La Macchina Virtuale Ethereum

La rete Ethereum ha la Macchina Virtuale Ethereum, sulla quale possono girare applicazioni per computer.

In passato, quando uno sviluppatore voleva scrivere un programma per computer, lo scriveva in un linguaggio di programmazione standard e poi lo faceva girare su un computer o un server centralizzato.

La tecnologia blockchain sulla quale si basa Bitcoin offre un grande potenziale; tuttavia, per utilizzarla, gli sviluppatori devono creare una loro blockchain e una rete di computer che la utilizzino.

Costruire una rete distribuita di persone disposte a contribuire a una nuova blockchain con potenza di calcolo e risorse è complesso, specialmente perché ogni giorno vengono creati nuovi sistemi basati su blockchain.

Creare un'applicazione significativa della tecnologia blockchain richiede un impegno significativo in termini di costi, risorse e tempo. Per molte persone e aziende, ciò è proibitivo.

La Macchina Virtuale Ethereum permette agli sviluppatori di eseguire programmi per computer su una blockchain. I programmi possono essere scritti in un codice simile ai normali linguaggi di programmazione che gli sviluppatori usano già. Inoltre, Ethereum ha una rete di computer esistente, collegati tra loro e pronti ad eseguire applicazioni.

Il Supercomputer Ethereum

Una delle ragioni per cui Ethereum è

così potente è il fatto che permette agli sviluppatori di creare applicazioni nei linguaggi di programmazione che già conoscono. Possono eseguire questi programmi su un potente supercomputer realizzato con una rete decentralizzata di computer.

Le applicazioni che vengono eseguito su una rete decentralizzata di computer hanno una probabilità molto minore di andare offline o di essere hackerate. Inoltre, la potenza di calcolo della rete è molto superiore a quella dei server centralizzati o dei singoli computer.

Con Ethereum, gli sviluppatori e le aziende possono utilizzare la tecnologia blockchain nelle loro applicazioni senza

dovere creare la loro blockchain o costruire una rete di computer per eseguirle.

Note di Fine Capitolo su Ethereum

Adesso dovreste avere un'idea di cosa sia Ethereum. Nei capitoli successivi, parleremo di come funzionano Ethereum e la tecnologia blockchain, delle applicazioni decentralizzate e dei contratti Smart.

Capitolo 2: Comprendere la Tecnologia Blockchain

La tecnologia Blockchain è una delle tecnologie chiave su cui si basa Ethereum. In questo capitolo, parleremo nel dettaglio di cos'è la tecnologia blockchain e di come funziona.

Cos'è una blockchain?

La prima blockchain è stata creata con Bitcoin; il codice sorgente di Bitcoin include dei commenti che descrivono i gruppi di transazioni come blocchi legati insieme in una catena.

In Bitcoin, le transazioni finanziarie sono raggruppate insieme in "blocchi" di

transazioni. I blocchi di transazioni agiscono come un registro digitale di tutte le transazioni avvenute sulla rete Bitcoin.

Ogni 10 minuti, un nuovo blocco di transazioni viene aggiunto ai blocchi esistenti. Ogni blocco ha un numero univoco, che aumenta con ogni nuovo blocco. Il primo blocco nella blockchain è il "blocco 0", il blocco successivo è il "blocco 1", seguito dal "blocco 2" e così via. Quando un nuovo blocco viene aggiunto, è collegato al blocco successivo attraverso un riferimento nei dati del blocco.

Il blocco 100 include un riferimento al blocco 99 come blocco precedente.

Il blocco 99 include un riferimento al blocco 98 come blocco precedente.

Ciò continua fino al primo blocco nella blockchain, il blocco 0.

I dati nel blocco sono unici, e anche un minimo cambiamento come il cambiare una lettera da minuscola a maiuscola modificherà i dettagli del blocco. Se i dettagli del blocco vengono cambiati, la catena si rompe. Per hackerare una blockchain e manipolare le transazioni, ogni blocco successivo a quello alterato dovrebbe essere cambiato. Ciò è praticamente impossibile, perché già dopo un'ora dalla transazione in molte blockchain sono già stati aggiunti molti blocchi.

Blockchain decentralizzate

Nei sistemi centralizzati esistenti, una terza parte o un'autorità centrale gestisce le transazioni. Quando trasferite denaro da un conto corrente a un altro conto corrente di un'altra banca, ogni banca ha i suoi registri centralizzati, i suoi controlli, i suoi processi. La prima banca verifica se avete abbastanza denaro nel conto, e se siete autorizzati a trasferire il denaro. Se tutti i controlli sono corretti e validi, manda il denaro all'altra banca. La banca ricevente verifica che i dettagli del conto corrente siano corretti e sincronizza il denaro

ricevuto sui propri registri prima di depositarlo nell'account.

Molte blockchain, come quella di Ethereum, sono decentralizzate. Con una blockchain decentralizzata, tutte le transazioni sono sincronizzate e processate sullo stesso registro. I controlli e i processi sono condotti dai computer sulla rete. Quando viene inviato un trasferimento, i computer sulla rete controllano se il mittente ha abbastanza denaro, e se ha l'autorizzazione a inviare la transazione. Se i computer determinano la validità della transazione, la transazione viene raggruppata in un blocco di transazioni che vengono aggiunte alla blockchain.

Ogni blocco di transazioni che viene aggiunto alla blockchain viene controllato dalla maggioranza dei computer sulla rete. Non è richiesta nessuna autorità centrale che processi le transazioni. Le banche non processano le transazioni quando sono chiuse, o quando nessun impiegato sta lavorando. Tuttavia, con una blockchain decentralizzata, le transazioni vengono processate dai computer della rete 24 ore su 24, 7 giorni su 7.

La Blockchain di Ethereum

Prima di Ethereum, i sistemi basati sulla blockchain venivano creati

principalmente per contenere transazioni finanziarie. C'erano poche applicazioni pratiche della tecnologia blockchain al di fuori delle criptovalute o della finanza.

Sebbene il potenziale della tecnologia blockchain avesse iniziato a realizzarsi prima di Ethereum, ogni nuova idea richiedeva la propria blockchain e la propria rete di computer.

Per applicare la tecnologia blockchain a una nuova idea, bisognava creare una nuova blockchain. Ciò richiedeva la creazione di una criptovaluta, e di una rete di computer che contribuivano con della potenza di calcolo al funzionamento della rete.

La blockchain doveva essere specifica per lo scopo per cui veniva creata. Un sistema basato sulla blockchain per le transazioni finanziarie non poteva processare transazioni che coinvolgevano altri tipi di dati.

La blockchain di Ethereum può contenere contratti, codice sorgente, e praticamente ogni tipo di dati. È possibile costruire applicazioni che vengano eseguite sulla blockchain di Ethereum e che utilizzino la potenza di calcolo esistente della rete Ethereum.

I blocchi di dati non possono essere alterati o annullati, ed è qui che si vede il potere di Ethereum in molti settori. È facile creare un'applicazione sulla

blockchain di Ethereum, e ogni dato registrato sulla blockchain creerà un record permanente di quella informazione.

I dati in un blocco non possono essere alterati o modificati; ogni cambiamento sarà fatto nei blocchi futuri della blockchain, che saranno collegati ai blocchi precedenti. Ciò crea un record permanente e una traccia di controllo di tutte le azioni e i cambiamenti avvenuti fin dal primo dato registrato nella blockchain.

Non c'è confusione su ciò che era stato fatto all'inizio, o sui cambiamenti fatti successivamente. A ogni cambiamento vengono associate data e ora,

permanentemente registrate nel database. Questa immutabile traccia di controllo può essere applicata a ogni applicazione o contratto.

Note di Fine Capitolo sulla Tecnologia Blockchain

La tecnologia blockchain è un'innovazione rivoluzionaria creata nel codice sorgente di Bitcoin, ed è una delle tecnologie di base di Ethereum. È simile a un database, in cui possono essere registrati dati, transazioni e record di valori.

Le transazioni vengono raggruppate in blocchi e collegate ad altri blocchi,

collegandoli insieme in una catena. Questa catena di blocchi, così come le transazioni nei blocchi, non può essere alterata o cancellata - creando così un record permanente di tutte le transazioni avvenute.

Nei sistemi basati su blockchain, le transazioni non richiedono un intermediario come una banca o un'azienda per validare o processare le transazioni. Quando trasferite denaro tra conti correnti, la transazione viene validata dalle banche e dai loro sistemi interni. Una transazione su un sistema basato su blockchain non richiede una banca per essere validata, ma viene controllata e validata dagli altri

computer sulla rete. Se la maggioranza dei computer concordano sulla validità della transazione, questa viene processata.

Non c'è alcuna azienda centralizzata o governo che controlli la blockchain, non si affida ad alcun server od organizzazione centrale per operare.

Prima di Ethereum, la maggior parte delle blockchain venivano utilizzate per le transazioni finanziarie. Ethereum ha reso possibile l'utilizzo della tecnologia blockchain per registrare facilmente tutto quello che ha un valore, in quasi ogni settore nel mondo.

Capitolo 3: Storia di Ethereum

Per capire la storia di Ethereum, bisogna per prima cosa parlare di Bitcoin, dal momento che esiste già da molti anni prima della creazione di Ethereum. Bitcoin ha creato la prima blockchain, e molte delle idee e del codice di Ethereum non sarebbero stati possibili se non fosse stato per Bitcoin.

Il Creatore di Ethereum

Vitalik Buterin è l'inventore e il co-creatore di Ethereum. Nato in Russia nel 1994, si è trasferito in Canada con i suoi genitori nel 2000.

A 19 anni, Vitalik scriveva su Bitcoin per diversi blog, e aveva co-fondato un sito web chiamato "Bitcoin Magazine". Oltre a scrivere su Bitcoin, Vitalik scriveva codice per Bitcoin e altre criptovalute.

Scrivere su Bitcoin e sviluppare codice per le criptovalute lo rese consapevole delle limitazioni e dei problemi di Bitcoin e delle altre criptovalute.

Ogni nuova criptovaluta richiedeva una nuova rete di computer, nuovi sviluppatori, codice e hardware per funzionare. Tutte le criptovalute operavano in modo indipendente, senza interagire o collegarsi.

Alla fine del 2013, Vitalik pubblicò un white paper su Ethereum. Vitalik non sapeva che genere di accoglienza avrebbe ricevuto il suo white paper. Temeva di non avere notato un errore ovvio, gli sembrava impossibile. Aveva detto, *"Quando ho avuto l'idea di Ethereum, il mio primo pensiero è stato, ok questa cosa è troppo bella per essere vera...e alla fine, l'idea di base di Ethereum era buona, solida, in modo completo e viscerale.*

A chi gli aveva chiesto da dove avesse preso il nome, Vitalik aveva risposto di aver scoperto il nome cercando degli elementi di fantascienza online. Gli piaceva come suonava, oltre al fatto che

conteneva la parola "Ether", ovvero un "ipotetico mezzo invisibile che permea l'universo e permette alla luce di viaggiare".

Alla fine del 2014, Vitalik iniziò a lavorare su Ethereum con Gavin Wood e Jeffrey Wilke. Pubblicarono quindi lo "Yellow Paper" di Ethereum. che delineava i dettagli tecnici di come Ethereum avrebbe funzionato.

Per creare Ethereum, però, era necessario un enorme lavoro di sviluppo e moltissimo denaro. Fu dunque creata una campagna di crowfunding per raccogliere i fondi necessari a sviluppare la piattaforma Ethereum. Vennero raccolti 18 milioni di dollari in

poco più di un mese, in cambio di criptovaluta Ether da consegnare dopo la creazione della piattaforma.

Dopo 18 mesi di sviluppo, Ethereum fu rilasciato al pubblico a metà del 2015.

Il DAO

Circa un anno dopo il rilascio di Ethereum, alcuni sviluppatori crearono dei contratti smart sulla piattaforma Ethereum, chiamati "Il DAO".

DAO è un acronimo che sta per decentralized autonomous organization, organizzazione autonoma decentralizzata. Opera in modo simile alla struttura di un'azienda o di un'organizzazione, ma tutte le decisioni

vengono prese in base ai voti dei detentori dei token DAO.

Il DAO era pensato per essere simile a un fondo speculativo per le app decentralizzate sulla piattaforma Ethereum. Gli sviluppatori potevano presentare le loro idee per le dApp, e i membri del DAO avrebbero votato per decidere se finanziare o meno la dApp.

Ci fu una campagna di crowfunding anche per il DAO, che raccolse più di 150 milioni di dollari in meno di un mese. Alla fine della campagna di crowfunding, conteneva quasi il 15% di tutti gli Ether in circolazione.

L'attacco al DAO

Alcune persone avevano espresso delle preoccupazioni riguardo alla sicurezza del DAO, ed in particolare le vulnerabilità riguardo ai prelievi.

Nel codice di un programma, le istruzioni vengono eseguite nell'ordine in cui sono scritte. Il codice scritto alla fine sarà eseguito solo dopo l'esecuzione di tutto il codice precedente.

La funzione di prelievo nel DAO aggiornava il saldo solo dopo il prelievo. Ciò aveva senso, perché se scritto correttamente, il codice avrebbe funzionato nel modo seguente:

- L'utente manda al DAO una richiesta di prelievo per $100.
- Il codice controlla se l'utente ha un saldo di almeno $100.
- Se l'utente ha un saldo di almeno $100, consegna $100 all'utente.
- Rimuove $100 dal saldo dell'utente dopo il prelievo.

Il problema del codice del DAO stava nel fatto che era possibile attaccarlo mandando richieste multiple di prelievo prima dell'aggiornamento del saldo.

Supponete di avere solo $100 nel vostro conto corrente. Immaginate di andare in banca e chiedere al cassiere di

prelevare $100 dal vostro conto. Il cassiere controlla se avete un saldo di almeno $100, e poi va nel caveau a prendere il denaro.

Mentre il primo cassiere sta prendendo il denaro dal caveau, andate dal secondo cassiere e gli chiedete di prelevare $100 dal vostro conto. Il secondo cassiere controlla il vostro saldo. Dal momento che il vostro saldo non è ancora stato aggiornato con il primo prelievo, va nel caveau a prendere $100 per voi.

Il primo cassiere ritorna, vi dà i $100 e aggiorna il vostro saldo a $0, perché avete prelevato tutto il vostro denaro. Anche il secondo cassiere torna, e aggiorna il vostro saldo a $0. In

entrambi i casi, le transazioni risultavano valide perché, al momento del controllo, avevate il denaro sul vostro conto. Il saldo non era stato aggiornato.

Adesso avete $200 in contanti; andate in banca e depositate i $200. Ripetete poi il processo di prelievo, richiedendo un prelievo di $200 dal primo cassiere e di $200 dal secondo cassiere. Potete continuare così finché non avrete prelevato tutto il denaro nel caveau della banca.

Questo è più o meno ciò che è accaduto con il DAO. Venivano fatti dei depositi, e successivamente dei prelievi multipli, fino ad arrivare a prelevare 50 milioni

di dollari dal DAO.

L’attacco sul DAO, e l'errore causato dal codice sorgente scritto male, non rappresentavano una vulnerabilità nella piattaforma Ethereum. Il DAO era un'applicazione scritta sulla piattaforma Ethereum, così come un sito web viene eseguito su internet.

Gavin Wood, il cofondatore di Ethereum, ha dichiarato che dire che Ethereum sia stato hackerato solo perché lo è stato il DAO sarebbe come dire che Internet è rotto perché un sito web non funziona.

Capitolo 4: Differenze tra Ethereum, Ethereum Classic e Bitcoin

A questo punto, dovreste avere una buona infarinatura su cosa sia Ethereum e su come funzioni. In questo capitolo, parleremo di come Ethereum differisca da Bitcoin e da Ethereum Classic.

Bitcoin vs Ethereum

Come enunciato precedentemente nel libro, Ethereum è dotato di una piattaforma informatica e di un linguaggio di programmazione che permette agli sviluppatori di creare contratti Smart e applicazioni

decentralizzate (dApp). Gli sviluppatori possono utilizzare la potenza di calcolo di una rete globale e decentralizzata di computer, sulla piattaforma Ethereum, per eseguire questi contratti Smart e dApp.

Bitcoin ha anch'esso una rete globale e decentralizzata di computer; tuttavia, la potenza di calcolo viene utilizzata principalmente per processare le transazioni. Bitcoin non ha un linguaggio di programmazione o una piattaforma di calcolo, come Ethereum.

Bitcoin ed Ethereum hanno le loro blockchain per registrare i dati. Bitcoin aggiunge un nuovo blocco alla blockchain di Bitcoin all'incirca ogni

dieci minuti. Ethereum aggiunge un nuovo blocco alla blockchain di Ethereum all'incirca ogni 30 secondi.

La valuta di Bitcoin vs la valuta di Ethereum

Considerate le funzionalità addizionali che Ethereum ha rispetto a Bitcoin, si potrebbe sembrare che Ethereum sia superiore, e che sostituirà Bitcoin come criptovaluta dominante.

Tuttavia, Ethereum non è stato pensato come un sostituto di Bitcoin. Ethereum e Bitcoin sono stati ideati per motivi diversi, e non sono in competizione l'uno con l'altro.

Bitcoin è stata la prima criptovaluta, e la prima rete di blockchain. La valuta sulla rete Bitcoin, anch'essa chiamata "bitcoin", è stata ideata per le transazioni finanziarie. Bitcoin è una valuta globale, che esiste al di fuori del controllo deli governi e delle istituzioni finanziarie.

La valuta della rete Ethereum, chiamata "Ether", era stata pensata per essere utilizzata come pagamento in cambio di potenza di calcolo sulla piattaforma Ethereum. Quando uno sviluppatore vuole eseguire un'applicazione sulla piattaforma Ethereum, compra la potenza di calcolo in Ether.

Anche l'Ether esiste al di fuori del

controllo dei governi e delle istituzioni finanziarie; tuttavia, è pensato per essere una valuta locale utilizzata sulla piattaforma Ethereum.

I Bitcoin sono in numero fisso, con un numero fissato di 21 milioni di bitcoin. Ciò serve a evitare di svalutare il prezzo del bitcoin creando un'offerta eccessiva. Ethereum non pone limiti sul numero di Ether che possano essere creati, e ciò significa che il prezzo dell'Ether potrebbe diminuire all'aumento dell'offerta.

Ci sono molti siti web e negozi in tutti il mondo che accettano Bitcoin come forma di pagamento. All’aumentare della sua popolarità, Bitcoin sarà

sempre più accettato come metodo di pagamento insieme alle carte di credito, PayPal e il denaro contante. È possibile utilizzare i Bitcoin per pagare merci e servizi, sia online che nei negozi fisici.

Ethereum non è pensato per essere utilizzato nei negozi e nei siti web come forma di pagamento. All'aumentare della sua popolarità, Ethereum sarà sempre più accettato come piattaforma per lo sviluppo di applicazioni in linguaggi di programmazione che competeranno tra loro, sistemi operativi e server informatici. Gli sviluppatori e le aziende compreranno Ether per utilizzarlo come pagamento per la

potenza di calcolo che utilizzeranno sulla rete Ethereum.

Ethereum vs Ethereum Classic

Sebbene Bitcoin ed Ethereum siano stati pensati per scopi differenti, Ethereum ed Ethereum Classic vengono dallo stesso codice e sono simili tra loro. Ci sono però delle importanti differenze, di cui parleremo in questo paragrafo. Abbiamo precedentemente parlato del disaccordo nella comunità di Ethereum, che ha portato alla creazione delle due blockchain di Ethereum.

All'inizio c'era solo una piattaforma e una valuta Ethereum; tuttavia, a causa di

un errore nel codice di un contratto Smart, noto come il DAO, la comunità si è spaccata in due blockchain e valute separate.

Il DAO è stato uno dei progetti più grandi che siano mai stati finanziati con il crowdfunding. Il DAO possedeva più di 150 milioni di dollari in Ether, il 15% delle intere riserve di Ether.

L'errore nel codice del contratto Smart non era una vulnerabilità o un problema di Ethereum. Non c'era nulla che non andasse con la piattaforma Ethereum; il contratto Smart aveva un errore che era stato sfruttato, portando al furto di 50 milioni di dollari in Ether.

L'errore nel contratto Smart del DAO era essenzialmente come un contratto con una clausola scritta male, che permetteva a una parte di sfruttare il contratto. Se ciò accadesse con un contratto, ci si rivolgerebbe a un tribunale e a degli avvocati, che discuterebbero il vero spirito della clausola.

Con un contratto Smart, non ci sono avvocati o tribunali; il codice del contratto è la legge. Il codice era corretto; tuttavia era scritto male, come potrebbe esserlo un contratto legale.

Gli "hacker" riuscirono a rubare 50 milioni di dollari in Ether fruttando il pezzo di codice scritto male. Non

hackerarono il sistema; si limitarono a trovare una parte del codice che permetteva loro di trasferire fondi tra di loro, all'interno dei termini del contratto Smart.

La comunità di Ethereum votò per annullare il contratto, perché quella non era l'intenzione del codice. Una parte della comunità sosteneva che non si trattasse di un hack; il contratto Smart era valido. Annullando le transazioni, la comunità avrebbe agito essenzialmente come giudice e tribunale, decidendo quali contratti e transazioni fossero valide.

Annullando le transazioni, avrebbe agito come un intermediario di terza parte,

decidendo un cambiamento ai contratti eseguiti sulla piattaforma. Questo andava contro alle intenzioni originali della piattaforma Ethereum, che voleva essere decentralizzata, libera dall'interferenza di ogni governo, azienda o terza parte. Se i termini di un contratto Smart sono validi, non dovrebbe essere annullato; il codice del contratto Smart dovrebbe essere la legge.

A causa della quantità di denaro rubato, la comunità votò per annullare le transazioni, e il denaro fu restituito. Ciò equivaleva al permettere a una delle parti coinvolte in un contratto di agire come giudice sulla validità del contratto.

Molte delle persone che avevano votato avevano perso del denaro, quindi avevano votato non necessariamente in base a ciò che era giusto, ma per riavere indietro il loro denaro.

Per annullare le transazioni, la blockchain fu sostanzialmente resettata allo stato che aveva prima che il denaro venisse rubato. Tale operazione aveva il supporto della maggioranza degli utenti, inclusi i creatori originali di Ethereum.

Una parte della comunità vide questa decisione come una chiara violazione dell'ideologia e del design della rete Ethereum, e così continuò a utilizzare la piattaforma e la blockchain Ethereum senza annullare la transazione.

C'erano quindi due blockchain di Ethereum e due valute in uso, e ciò creava confusione. La blockchain originale prese il nome di Ethereum Classic, e la sua valuta di Ether Classic.

Ethereum Classic era costruito su principi di immutabilità, neutralità, decentralizzazione, e sull'ideologia secondo la quale il codice è la legge. La comunità crede nello sviluppare la piattaforma, rimanendo neutrale riguardo al modo in cui viene utilizzata e senza interferire con i contratti o le transazioni della rete.

Ethereum Classic ha tutte le funzionalità di Ethereum; tuttavia, ha una comunità

molto più piccola e una minore potenza di calcolo che la supporta. Ad oggi, Ethereum Classic è una versione simile a Ethereum ma meno supportata.

L'attuale prezzo dell'Ether è di 300 dollari statunitensi, con una capitalizzazione sul mercato di 28 miliardi di dollari. L'attuale prezzo dell'Ether Classic è di 15 dollari statunitensi, con una capitalizzazione sul mercato di 1.5 miliardi di dollari.

Ethereum Classic mira a differenziarsi; tuttavia, non c'è la certezza che avrà abbastanza supporto per sopravvivere contro Ethereum. La piattaforma principale di Ethereum ha un supporto significativo dagli sviluppatori, insieme

all'interesse da parte di governi e grandi aziende.

Capitolo 5: App Decentralizzate (dApp)

A questo punto, dovreste avere già familiarità con alcune delle differenze tra la centralizzazione e la decentralizzazione. In questo capitolo, entreremo più nel dettaglio su una delle maggiori innovazioni introdotte da Ethereum: le app decentralizzate eseguite su una blockchain.

Cosa sono le app decentralizzate (dApp)?

Le app decentralizzate (dApp in breve) sono applicazioni che, a differenza delle applicazioni tradizionali, non hanno un

server centrale. Vengono eseguite su una rete distribuita di computer e non hanno bisogno, per funzionare, di un server centrale o un'azienda che le controlli.

Gli utenti delle dApp si collegano direttamente l'uno all'altro, invece di utilizzare un server o un'azienda centrale. Sebbene un'azienda o uno sviluppatore possa creare una dApp, dopo il suo rilascio la stessa verrà controllata dalla maggioranza degli utenti. Il creatore della dApp non può censurare o avere un controllo centrale sull'app.

Come funzionano le dApp

Per comprendere meglio come funzionino le dApp, parliamo della differenza tra le app standard e le dApp.

Differenza tra le dApp e le app centralizzate standard:

App centralizzate:

Le app centralizzate sono installate e vengono eseguite su un server centrale. Quando accedete a un sito web, state accedendo a quel sito web dallo stesso server che utilizzano tutti gli altri. Tutti i dati vengono inviati dal server centrale a tutti gli utenti che accedono.

Come detto precedentemente nel libro, alcuni dei rischi delle applicazioni

centralizzate sono:

- Hacking: se il server principale viene attaccato, tutti i dati degli utenti potrebbero essere vulnerabili, e gli hacker possono controllare l'applicazione.
- Guasto del server: se il server principale va offline, l'intera applicazione va offline.
- Censura: i siti web centralizzati, le applicazioni e i server possono inoltre essere bloccati dai governi.
- Potenza di calcolo: più utenti sono collegati al server, più lento è il server, a meno che il potere di calcolo non venga continuamente

aumentato.

Una dApp non è installata su un server centrale ma su numerosi computer degli utenti, che contribuiscono all'app con la loro potenza di calcolo.

Se pensiamo al modo in cui le e-mail vengono attualmente inviate usando Gmail, possiamo mettere a confronto le differenze tra i server centralizzati e le dApp.

Attualmente, quando mandate un’e-mail con Gmail, fate il login all'applicazione sul vostro telefono, computer o sul sito web, e vi collegate ai server centrali di Gmail. Tutte le vostre e-mail vengono

conservate e gestite dal server centrale. L'abilità di mandare e-mail viene gestita dal server. Quando l'e-mail viene mandata, viene passata al server di Gmail, che la manda al destinatario.

Se il server di Gmail va giù, non potete mandare o ricevere e-mail. La vostra connessione a Internet può funzionare perfettamente, ma se il server non funziona, non potete accedere alle vostre e-mail. Se il server di Gmail venisse hackerato, l'hacker potrebbe ottenere accesso a tutti gli account e le e-mail degli utenti.

Con un'app decentralizzata per le e-mail, potreste contribuire con la vostra potenza di calcolo al sistema, e il vostro

computer funzionerebbe come un server. Quando accedereste alle vostre e-mail, le trovereste direttamente sul vostro computer - non dovreste preoccuparvi di collegarvi a un server centralizzato. Se mandaste un'e-mail, verrebbe mandata direttamente dal vostro computer al destinatario. Non passerebbe attraverso un server centralizzato di terza parte.

Non dovreste necessariamente contribuire al sistema con la vostra potenza di calcolo - potreste anche limitarvi ad utilizzare l'app. Gli altri utenti contribuirebbero con la loro potenza di calcolo, agendo come server multipli in tutto il mondo. Accedendo alle vostre e-mail, vi collegherete a uno

di questi server. Ogni server manterrebbe una copia di tutte le informazioni nell'app. Se uno dei server andasse down, potreste collegarvi a un altro e accedere così alle vostre e-mail. Gli utenti si collegherebbero direttamente l'uno all'altro, senza avere bisogno di un intermediario di terza parte o di un server centralizzato per eseguire l'app o registrare email e dati.

Condivisione di file centralizzata

Probabilmente avete usato un qualche tipo di condivisione di file centralizzata, come Google Drive o Dropbox. Anche scaricare un file da un sito è una forma

di condivisione di file centralizzata.

Quando condividete un file utilizzando un server centralizzato, il file viene caricato su un server centrale. Tutti gli utenti che scaricheranno quel file scaricheranno lo stesso file dallo stesso server. Più persone scaricheranno il file nello stesso momento, più il server e la velocità di download rallenteranno, a meno che la potenza di calcolo del server non venga aumentata.

Se il server fosse offline, il file non sarebbe disponibile e nessuno potrebbe scaricarlo. Se il governo o l'azienda che possiede il server non approvasse il file da condividere, potrebbe bloccare il file o il server, impedendo così l'accesso al

file.

Se un hacker riuscisse ad hackerare il server, potrebbe sostituire il file con una versione diversa dello stesso, con un virus. Tutti coloro che provassero a scaricare il file scaricherebbero quindi la versione del file che contiene il virus.

Condivisione di file decentralizzata

Se siete abbastanza vecchi da ricordare Napster, o se avete familiarità con un'applicazione di condivisione file più recente come BitTorrent, allora avete già utilizzato la condivisione di file decentralizzata.

Con BitTorrent, ogni utente ha una copia

dell'applicazione sul proprio computer. Salva sul proprio computer tutti i file che vuole condividere.

Quando cercate un file su BitTorrent, vengono cercati tutti gli utenti che hanno una copia di quel file; il risultato potrebbe mostrare che ci sono 100 persone che stanno condividendo quel file. Quando scegliete di scaricare quel file, non vi state connettendo né lo state scaricando da un server centrale. Al contrario, vi state collegando direttamente ai computer di tutti gli utenti che hanno una copia di quel file.

Ogni computer agisce come un server, con una copia esatta del file che volete scaricare. Se uno dei server va offline,

non vi sono conseguenze per il vostro download, perché potete semplicemente collegarvi a un altro computer che condivide quel file, e continuare a scaricarlo da esso.

Se molti utenti stanno scaricando il file nello stesso momento, si collegheranno all'utente con il file che ha la connessione più veloce rispetto a loro. Non si connettono tutti a un server centralizzato, quindi un utente dall'Europa può collegarsi a un altro utente europeo che condivide il file, mentre un utente dagli Stati Uniti si collegherà ad un altro utente statunitense.

Quando gli utenti finiscono di scaricare

il file, possono scegliere di condividerlo, facendo diventare anche il loro computer come un server. Gli altri utenti si collegheranno direttamente ai loro computer per accedere e scaricare il file. Più sono gli utenti a utilizzare BitTorrent e a scaricare file, più veloci saranno i tempi di download, perché ci saranno più server che condivideranno il file.

Se uno dei computer che condivide il file viene hackerato, l'hacker non ottiene accesso a tutti i file e dati della rete. L'hacker potrebbe riuscire a manipolare il file su quel computer; tuttavia, con BitTorrent, un file per essere accettato come valido deve essere una copia

esatta di tutti gli altri file sulla rete.

Se un hacker ottiene accesso a un computer e prova a inserire un virus in uno dei file che vengono condivisi, il file non sarà una copia esatta degli altri file. Quando proverete a scaricare lo stesso file, vedrete che ci sono 99 utenti che condividono un file e un solo utente che condivide una versione diversa del file. Dal momento che la maggior parte degli utenti concordano sulla validità del primo file, la maggior parte delle persone che scaricheranno il file si fideranno dei file condiviso da 99 utenti, e non della versione differente.

Per riuscire ad aggirare il sistema, un hacker dovrebbe riuscire ad hackerare i

computer della maggior parte degli utenti nello stesso momento, e inserire un virus in tutti i file. Così, se una persona provasse a scaricare il file, verrebbe mostrato che la maggior parte degli utenti stanno condividendo il file infetto. La persona che vuole scaricare il file si fiderebbe della maggioranza, e scaricherebbe il file corrotto con il virus.

Se un governo o un'azienda disapprovasse la condivisione del file, dovrebbero bloccare ogni singola persona che condivide il file. Dal momento che le persone che condividono il file si trovano probabilmente in paesi diversi in tutto il

mondo, sarebbe difficile bloccarli tutti, a meno che il file non sia illegale in tutti i paesi in cui viene condiviso.

dApp sulla piattaforma Ethereum

Sebbene BitTorrent sia un esempio facile da comprendere di come funzioni un sistema decentralizzato, non si tratta di una dApp e non viene eseguita sulla piattaforma Ethereum.

Le dApp sulla piattaforma Ethereum operano in modo simile a BitTorrent; tuttavia, ci sono delle sostanziali differenze.

Open Source

Le dApp sono open source, e ciò significa che chiunque può vedere il codice sorgente e creare la propria versione dell'applicazione.

Le applicazioni come BitTorrent non devono necessariamente essere open source, e gli sviluppatori dell'applicazione sono le uniche persone a poter visualizzare il codice sorgente.

Le dApp vengono e seguite su una blockchain

Sulla rete Ethereum, le dApp vengono eseguite su una blockchain, il che permette delle funzionalità che non sono possibili per le applicazioni standard.

Abbiamo parlato della tecnologia blockchain precedentemente nel libro.

Le dApp hanno una valuta o token in-app

La piattaforma Ethereum richiede agli sviluppatori di pagare la potenza di calcolo in Ether, in modo da rendere le app redditizie e coprire i costi della potenza di calcolo. Le dApp che vengono eseguite su Ethereum possono creare i loro token in-app, che gli utenti potranno acquistare e utilizzare per pagare ulteriori funzionalità nell'applicazione.

Per esempio, mandare un messaggio in un'app di messaggistica potrebbe costare

1 token. Il token potrebbe costare solo una frazione di un centesimo, quindi mandare un messaggio potrebbe non costare molto. Tuttavia, non sarebbe gratuito come nelle attuali app di messaggistica.

Cambiamenti decentralizzati all'app

Sebbene vi siano sviluppatori che creano le dApp, una volta che esse vengono rilasciate, i cambiamenti all'app e le decisioni sull'app vengono presi dalla maggioranza degli utenti.

Questo è un pericolo delle dApp e delle reti decentralizzate; il controllo dell'app o della rete è nelle mani della maggioranza della rete.

Chiunque può modificare il codice di un'applicazione open source e rilasciare la propria versione. Se la maggior parte degli utenti sceglie di eseguire quella versione dell'applicazione, essa diventa la versione dell'app.

Note di Fine Capitolo sulle dApp

Adesso dovreste conoscere cosa sono le dApp e come funzionano. Nel prossimo capitolo, parleremo dei contratti Smart su Ethereum.

Capitolo 6: Contratti Smart

Contratti Smart

I contratti Smart che operano su una blockchain sono un'altra delle principali innovazioni introdotte da Ethereum. I contratti Smart basati sulle blockchain sono stati esaltati come un concetto rivoluzionario, che potrebbe avere un forte impatto sulla finanza, sui contratti, e su quasi ogni settore del mondo a livello globale.

Cosa sono i contratti Smart?

I contratti Smart sono contratti applicabili in modo molto simile ai

contratti legali; tuttavia, invece di essere scritti da avvocati e applicati da un tribunale, sono scritti in un linguaggio di programmazione e sono in grado di applicarsi da soli.

Contratti tradizionali

I contratti tradizionali vengono in genere scritti da avvocati, e contengono diverse pagine di termini e condizioni di un accordo tra due parti. Contengono i dettagli di ciò che è stato stabilito, insieme ad eventuali risarcimenti e conseguenze per aver rotto i termini del contratto.

Se una delle parti del contratto non

rispetta la sua parte del contratto, l'altra parte può assumere un avvocato e fare causa per ottenere un risarcimento.

I termini del contratto possono essere ambigui, e la grammatica ha un ruolo nell'interpretazione di un contratto. Ci sono stati casi in cui una semplice virgola ha cambiato il significato di una frase in un contratto.

Un recente esempio di ciò è stato il caso di Oxhurst Dairy, in cui l'azienda è stata portata in tribunale per 10 milioni di dollari di straordinari non pagati, a causa di un disaccordo su una frase in cui una virgola mancante cambiava il significato.

Le cause civili sono lunghe e costose, e anche in caso di vincita, non c'è garanzia di ricevere un risarcimento. In ogni caso, l'intero processo richiederà molto tempo e denaro prima di essere risolto.

Come funzionano i contratti Smart:

I contratti Smart vengono scritti in codice sorgente utilizzando il linguaggio di programmazione Solidity; non c'è ambiguità nei termini di un codice sorgente. I contratti Smart vengono eseguiti sulla macchina virtuale di Ethereum e sulla blockchain di Ethereum, collegati alla criptovaluta di Ethereum, l'Ether.

I termini di un contratto possono contenere dei pagamenti e dei risarcimenti in caso non si rispettino i termini del contratto, tutto scritto utilizzando il codice sorgente.

Nel caso di un contratto per la vendita di un'azienda, il contratto Smart conterrebbe la proprietà delle azioni dell'azienda e i diritti di proprietà. Il pagamento verrebbe inviato al contratto Smart, non direttamente al venditore. Alla ricezione del pagamento, il contratto Smart trasferirebbe la proprietà dell'azienda al compratore e l'importo di vendita al venditore.

Se il compratore non pagasse l'intera somma, o se il pagamento non venisse

ricevuto prima della data di scadenza, il contratto start trasferirebbe le azioni e la proprietà nuovamente al venditore, cancellerebbe il contratto e rifiuterebbe i futuri pagamenti.

Vantaggi dei contratti Smart:

- I contratti legali esistenti possono essere ambigui, secondo le parole e la grammatica utilizzata. I contratti Smart sono scritti in codice sorgente, in modo da prevenire i fraintendimenti sulle frasi e i termini.

- Non servono avvocati o tribunali per applicare il contratto. Se i termini del contratto vengono rispettati, il contratto viene eseguito. Se i termini del contratto non vengono rispettati, allora vengono automaticamente eseguiti i termini del caso di rottura del contratto, e viene pagato un risarcimento.

- I contratti Smart vengono eseguiti sulla rete Ethereum decentralizzata. Come detto prima, ciò riduce i rischi di hacking, frode, avaria del server e accesso non autorizzato ai contratti.

- È possibile determinare il livello di

autonomia del contratto. I contratti smart possono essere parzialmente o totalmente auto-eseguibili e auto-applicabili.

- Tutti i cambiamenti e le modifiche a un contratto Smart vengono registrati nella blockchain. Ciò crea un record permanente di tutte le modifiche e azioni avvenute al contratto Smart.

- I contratti Smart hanno una vasta gamma di utilizzi. Molte aziende stanno sviluppando contratti Smart che potrebbero migliorare il modo in cui le industrie e i processi esistenti vengono portati a termine.

Svantaggi/Rischi dei contratti Smart:

- Gli avvocati vengono sostituiti dai programmatori. Sebbene chiunque possa creare un contratto Smart, poche persone hanno le capacità necessarie per scriverne uno. A scriverli dovranno essere gli sviluppatori invece degli avvocati.

- Gli errori del codice sorgente possono essere molto più pericolosi di una frase ambigua in un contratto. Se ci sono frasi ambigue in un contratto, è possibile discuterne,

modificarle, dibattere o andare in tribunale. Se c'è un errore nel codice sorgente di un contratto, il contratto eseguirà il codice con l'errore, e non potrà essere annullato o portato in tribunale. Questo è stato il caso del DAO, in cui una cattiva formulazione del contratto Smart ha causato la perdita di 50 milioni di dollari.

- Non si può discutere con un contratto Smart. Il contratto applicherà i termini in base al codice. Non c'è alcun giudice che possa determinare se i termini sono giusti, né è possibile fare appello in

tribunale per contestare una decisione. Se una parte ritiene che il contratto sia ingiusto, o sia stato eseguito in modo errato a causa di un errore o un fraintendimento dei termini, non c'è alcun modo per modificare il contratto. Ciò è accaduto anche con il DAO, nel cui caso per annullare il contratto Smart è stata necessaria una biforcazione e una nuova versione di Ethereum.

- C'è un limite ai tipi di contratti che possono essere creati. È possibile determinare la proprietà digitale dei beni; tuttavia, ciò è più difficile per i beni del mondo reale. Per i

contratti Smart può inoltre essere difficile determinare se la qualità di un lavoro è stata conforme agli standard attesi. È possibile programmare dei requisiti sì/no di base, ad esempio: "E' stata completata un'ora di lavoro?" Tuttavia, non è possibile determinare la qualità di quel lavoro.

- I problemi software possono causare errori nei contratti Smart. I contratti Smart vengono eseguiti su Ethereum, che si appoggia a una rete di computer e programmi per operare. Eventuali problemi nel software o

nella rete potrebbero causare errori nei contratti Smart.

- La giurisdizione per l'applicazione di un contratto Smart potrebbe essere poco chiara. I contratti Smart sono codice sorgente che esiste al di fuori della giurisdizione legale di uno stato o nazione. Se si verifica una violazione del contratto o una disputa sui termini del contratto, per il contratto Smart potrebbe non esserci alcuna giurisdizione legale se non la blockchain. È stata avanzata la possibilità che ogni eventuale arbitrato possa avvenire in un tribunale di arbitrato sulla

blockchain, gestito da codice sorgente, come proposto dall'azienda CodeLegit.

- Si tratta di un metodo non testato per creare e applicare contratti. I contratti legali sono in uso da centinaia di anni; magari non sono perfetti, ma sono sopravvissuti alla prova del tempo. I contratti Smart sono nuovi, e non sono stati provati su un lungo periodo di tempo. Utilizzare i contratti Smart in questa fase primitiva potrebbe esporre le aziende a rischi inaspettati, associati a una nuova tecnologia.

Note di Fine Capitolo sui Contratti

Smart

I contratti Smart offrono molti vantaggi rispetto ai contratti esistenti; tuttavia, vi sono anche degli svantaggi significativi a loro associati. I contratti Smart sono ancora un concetto nuovo, quindi le implicazioni e i problemi del loro uso non sono ancora del tutto chiari.

Capitolo 7: Benefici di Ethereum

Supercomputer Gigante Mondiale

Uno dei più grandi vantaggi di Ethereum sta nel fatto che tutti i singoli computer collegati in rete agiscono come un supercomputer gigante a livello mondiale.

Sebbene anche la rete Bitcoin sia connessa come un supercomputer, la potenza di calcolo della rete Bitcoin viene utilizzata soltanto per processare le transazioni.

La potenza di calcolo della rete Ethereum può essere utilizzata nella

Macchina Virtuale Ethereum. Ciò permette di eseguire delle applicazioni, utilizzando il potere di uno dei più potenti supercomputer al mondo.

La Macchina Virtuale Ethereum

La tecnologia blockchain è rivoluzionaria; tuttavia, prima di Ethereum, le blockchain avevano funzionalità limitate ed erano utilizzate principalmente per registrare transazioni.

Una delle più importanti innovazioni offerte da Ethereum rispetto alle tecnologie blockchain esistente è la Macchina Virtuale Ethereum (Ethereum

Virtual Machine, EVM).

La Macchina Virtuale Ethereum permette agli sviluppatori di creare applicazioni utilizzando linguaggi di programmazione simili a quelli a cui sono abituati. Queste applicazioni possono essere sofisticate come qualsiasi altra applicazione che possa essere creata su altre piattaforme informatiche. Vengono eseguite sulla Macchina Virtuale Ethereum, che permette a queste applicazioni decentralizzate di utilizzare la tecnologia blockchain in modo più semplice e con costi minori rispetto a quelli possibili in passato.

Facilità di Sviluppo

Creare una rete di blockchain è costoso, complesso e richiede molto tempo, perché richiede la presenza di molte persone che contribuiscano alla nuova rete blockchain con la loro potenza di calcolo.

Gli sviluppatori devono creare una nuova blockchain e costruire una rete di computer e utenti che la supportino.

Ethereum permette agli sviluppatori di utilizzare la blockchain esistente di Ethereum e la sua rete di computer. La Macchina Virtuale Ethereum permette inoltre agli sviluppatori di creare applicazioni sulla tecnologia

blockchain, senza che abbiano bisogno di creare la loro rete di blockchain.

Sviluppare applicazioni che vengano eseguire sulla blockchain di Ethereum e sulla EVM è relativamente semplice. Il linguaggio di programmazione è simile a quelli più comunemente usati, come JavaScript. Dal momento che il linguaggio di programmazione è simile a quelli esistenti, gli sviluppatori possono creare facilmente programmi, dovendo imparare poche nozioni nuove.

Decentralizzazione

Possiamo credere di avere il controllo sulle nostre foto su Facebook, sui file

che teniamo in cloud, o sui messaggi nel nostro programma di chat. In realtà, però, tutti questi file vengono controllati da sistemi e aziende centralizzate.

Quando caricate delle foto su Facebook, tutte le immagini vengono salvate su un server centrale di proprietà di Facebook. Lo stesso vale per i file che caricate su Google Drive o su altri sistemi di archiviazione cloud.

Quando mandate un messaggio utilizzando un programma di chat, il messaggio viene inviato ai server centrali dell'azienda, che poi lo manda dal server centrale al destinatario. Il server tiene una traccia di tutti i messaggi. Quando accedete alla vostra

cronologia della chat, accedete da quei server.

Ethereum permette la decentralizzazione di applicazioni e dati, e ciò significa che non c'è un server centrale o un'azienda che controlla tutti i vostri dati. Le applicazioni decentralizzate vengono eseguite su una rete di computer; se un computer va offline, è comunque possibile accedere ai dati dagli altri computer sui quali viene eseguita l'applicazione.

Sono in corso di sviluppo versioni decentralizzate sulla rete Ethereum di molte delle app e dei programmi che utilizziamo quotidianamente, come programmi di archiviazione cloud

decentralizzata, app di messaggistica, social network e molto altro.

Nessuna Censura

La struttura decentralizzata della rete Ethereum fa sì che i governi e le aziende non possano censurare siti web o applicazioni.

Se un governo volesse censurare un sito web, potrebbe bloccare l'accesso al sito o chiudere il server su cui viene eseguito il sito web. Se volesse censurare un'applicazione decentralizzata, dovrebbe chiudere ogni computer e server su cui l'applicazione venga eseguita.

I computer che eseguono le dApp sono distribuiti in tutto il mondo, rendendo impossibile per un governo chiuderli tutti quanti.

Se un utente posta un'immagine su Twitter, Facebook o Instagram e l'azienda la disapprova, può rimuovere l'immagine e bannare l'utente. Ciò può non essere un problema per la maggior parte delle persone, che non postano nulla che vada contro le regole di questi siti. Tuttavia, queste aziende devono rispettare le leggi delle nazioni in cui operano. La maggior parte delle piattaforme di social media sono proibite in Cina, perché le aziende straniere non rispettano la dura censura

del governo cinese.

In Cina, gli utenti che postano contenuti che riguardano il Tibet, il massacro di Piazza Tiananmen o qualsiasi altro contenuto che sia critico del governo cinese vedranno il loro post rimosso, e potrebbero inoltre essere oggetto di investigazione da parte del governo cinese per il loro post. Le aziende che operano in Cina devono vietare i contenuti che il governo non approva, e fornire al governo i dati degli utenti.

Con delle reti e delle applicazioni decentralizzate, i governi e le aziende non possono censurare contenuti, proibire applicazioni od ottenere i dati degli utenti. Ciò fornisce una maggiore

libertà di parola e rimette il controllo nelle mani degli utenti delle applicazioni che vengono eseguite su Ethereum.

Sicurezza

Molti dei rischi che corrono i sistemi centralizzati esistenti vengono fortemente ridotti dalle applicazioni decentralizzate.

Facebook, PayPal, le banche e molte altre aziende hanno server centralizzati. Se questi server venissero hackerati, gli hacker potrebbero ottenere tutti i vostri dati personali salvati su quei server. Se i server centrali crashassero o andassero offline, tutti i dati diventerebbero

inaccessibili.

I server decentralizzati non sono altrettanto vulnerabili all'hacking o all'avaria. Per hackerare un sistema decentralizzato, l'hacker dovrebbe controllare la maggioranza della potenza di calcolo sulla rete. Dal momento che la rete Ethereum è composta da centinaia di migliaia di computer in tutto il mondo, sarebbe praticamente impossibile per una persona riuscire a controllare la maggioranza della rete.

Contratti Smart

I contratti Smart sono contratti scritti in codice sorgente, che vengono eseguiti

automaticamente se i termini del contratto vengono rispettati. Non servono avvocati o tribunali per applicare il contratto.

Sebbene Bitcoin permetta pagamenti su una blockchain, i pagamenti sono manuali, richiedendo ad esempio di scegliere di inviare del denaro a un'altra persona. Ethereum permette di effettuare pagamenti automatici che possono essere attivati quando si verifica un evento, una soglia o una condizione.

Quando prendete un taxi, alla fine della corsa potreste pagare il conducente in contanti. Bitcoin potrebbe sostituire il contante come metodo di pagamento, permettendovi di pagare con Bitcoin

invece che in contanti. Bitcoin si limita a pagamenti e transazioni manuali, come in questo esempio.

Se utilizziamo l'esempio di Uber, i dati della vostra carta di credito sono salvati da Uber. All'inizio di un percorso, contrattate di pagare una certa cifra in base alla distanza percorsa. Alla fine del percorso, il contratto viene eseguito, e sulla carta di credito viene automaticamente addebitato il corso del viaggio.

Ethereum ha creato una piattaforma in cui le app decentralizzate (dApp) possono essere eseguite con dei contratti Smart per sostituire questo processo. Invece dell'app Uber, potreste usare una

dApp che esegua automaticamente dei contratti smart in base alla distanza. Ciò funzionerebbe in modo simile all'esempio di Uber fatto prima, ma opererebbe sulla piattaforma Ethereum utilizzando gli Ether o i token di Ethereum come pagamento.

Questa è una delle potenziali applicazioni di dApp e contratti smart. Ci sono migliaia di dApp in corso di sviluppo, che potrebbero rivoluzionare una vasta gamma di settori.

Nuovi metodi per dare fondi ad aziende e progetti

Ethereum ha aperto nuove possibilità

per permettere ad aziende e sviluppatori di raccogliere fondi per finanziare la propria crescita. Sebbene anche prima di Ethereum esistessero delle Offerte Iniziale di Moneta (Initial Coin Offerings), queste erano legate alla popolarità di una nuova criptovaluta.

Ethereum permette alle aziende di sviluppare applicazioni e vendere token o monete che possono essere usati nell'applicazione. Queste applicazioni vengono eseguite sulla piattaforma Ethereum, e se un'app diventasse popolare, i token utilizzati nell'applicazione dovrebbero teoricamente aumentare di valore.

Le aziende possono raccogliere fondi

per i loro progetti, senza avere bisogno di prestiti o finanziamenti. I finanziatori iniziali dell'applicazione possono inoltre ottenere un profitto nel caso in cui l'app diventi popolare.

Note di Fine Capitolo sui Benefici di Ethereum

Ethereum offre molti altri vantaggi; tuttavia, molti di essi sono relativi alla sottostante tecnologia Blockchain, che non è specifica di Ethereum. Sebbene Ethereum abbia molti vantaggi, ci sono anche molti svantaggi. Nel prossimo capitolo, parleremo di alcuni dei rischi e svantaggi di Ethereum.

Capitolo 8: Svantaggi e Rischi di Ethereum

Sebbene i vantaggi e il potenziale di Ethereum siano notevoli, ci sono anche molti svantaggi e rischi ad esso associati. In questo capitolo, parleremo di alcuni dei rischi e svantaggi di Ethereum.

L'Ether non è pensato per le transazioni nel mondo reale

L'Ether, la criptovaluta utilizzata per i pagamenti sulla rete Ethereum, è utilizzata per pagare la potenza di calcolo necessaria all'esecuzione delle

dApp e dei contratti smart. L'Ether non è progettato per essere utilizzato per pagamenti nei negozi, online, o come alternativa ad altri metodi di pagamento del mondo reale.

Bitcoin, e molte altre criptovalute, sono forme di pagamento molto più pratiche, spesso accettate in negozi e siti web in tutto il mondo. L'utilizzo dell'Ether dipenderà dalla popolarità della piattaforma Ethereum e dal numero di persone che eseguiranno dApp e contratti smart.

L'Ether potrebbe non aumentare in valore

Anche se la piattaforma Ethereum dovesse diventare più popolare, ciò non garantirebbe un aumento del prezzo dell'Ether. Molte delle persone che comprano Ether lo comprano per ottenere un profitto speculativo, e non intendono utilizzarlo per eseguire dApp o contratti smart.

Il prezzo attuale dell'Ether potrebbe essere sopravvalutato da trader e speculatori. Se dovessero vendere, il prezzo dell'Ether potrebbe scendere rapidamente.

Anche se sviluppatori e aziende utilizzassero la piattaforma Ethereum, il prezzo dell'Ether potrebbe non crescere, nel caso in cui ci sia una maggiore

offerta di Ether creato o una diminuzione della domanda da parte dei trader.

Tecnologia nuova e non ancora provata

Ethereum è una tecnologia nuova. Anche se ha un grande potenziale, ci sono ancora molti rischi ignoti, come in qualsiasi nuova tecnologia.

Sebbene molte aziende si siano unite a un'alleanza per sviluppare l'uso di Ethereum all'interno delle loro organizzazioni, sono ancora nella fase di ricerca e studi di fattibilità. Ci sono state poche aziende che hanno implementato Ethereum come sostituto

dei sistemi esistenti. Ci sono anche state poche dApp mainstream che sono diventate popolari.

Molti dei pericoli e dei rischi legati all'uso di Ethereum potrebbero essere ancora sconosciuti, e potrebbero non essere immediatamente visibili finché Ethereum non sarà usato su larga scala.

Problemi con i Contratti Smart

I contratti Smart hanno molti vantaggi; tuttavia, il loro uso può causare pericoli significativi.

Il caso più grande che mostra i problemi dei contratti Smart è l'hack del DAO, come detto prima. Un contratto Smart

scritto male ha permesso a un gruppo di persone di sfruttare il contratto e rubare più di 50 milioni di dollari.

Migliaia di persone avevano visto il codice nel contratto Smart DAO, e non avevano trovato alcun errore. Si è capito di avere un problema col contratto Smart solo dopo che lo stesso era stato sfruttato.

Con un contratto legale standard, se c'è una frase scritta male che consente a qualcuno di sfruttare il contratto, è possibile andare in tribunale. È possibile risolvere il disaccordo sulla formulazione e sull'intenzione di un contratto con un procedimento legale.

Ciò non avviene con i contratti Smart. Quando un contratto Smart viene eseguito, non è possibile discutere o annullarlo. Non ci sono avvocati o tribunali per risolvere le controversie dei contratti Smart.

Pericoli di un Supercomputer Gigante Mondiale

Se avete visto i film di Terminator, sapete che Skynet era una rete di computer a livello mondiale. Quando Skynet venne attivata, individuò l'umanità come una minaccia, e fece guerra agli umani.

La rete Ethereum e i contratti Smart sono

stati paragonati a Skynet. Ethereum è una rete mondiale di computer collegati, che eseguono applicazione e codice sul quale non è possibile discutere.

Nell'hack del DAO, alcune persone hanno sfruttato una vulnerabilità nel codice di un contratto smart per rubare più di 50 milioni di dollari. Anche se ci sono rischi finanziari con i contratti Smart, ci sono rischi di sicurezza ancora più grandi.

Adesso vengono progettati contratti Smart quasi per tutto, inclusi collegamenti a elettrodomestici, macchine, telefoni e altri sistemi elettronici.

Al giorno d'oggi quasi tutti gli eserciti utilizzano sistemi informatici, e alcune delle armi più avanzate si affidano fortemente alle tecnologie informatiche. I governi stanno cercando un modo per implementare le tecnologie basate su blockchain e sostituire i sistemi di database esistenti.

Se ci fosse un errore nel codice o se il codice fosse scritto male, ci sarebbe la possibilità che il contratto Smart non venga eseguito come dovrebbe. Il contratto verrebbe quindi eseguito senza potere essere fermato o alterato, portando a conseguenze potenzialmente disastrose, specialmente nei settori del governo o dei sistemi militari.

La moda delle dApp

Le dApp offrono molti vantaggi rispetto alle applicazioni esistenti. Tuttavia, nella storia ci sono state moltissime tecnologie con vantaggi rispetto alle opzioni esistenti, che non sono però state adottate dal grande pubblico.

Le applicazioni come Instagram o Facebook sono gratuite; usano però le vostre informazioni personali per permettere alle aziende di pubblicità di vendervi prodotti e servizi. Sono gratuite per gli utenti, ma il prodotto che queste aziende vendono alle altre persone sono i vostri dati personali.

Le dApp sono controllate dagli utenti,

non da un'azienda centralizzata. Gli utenti controllano la loro privacy e i loro dati. In cambio di questo controllo, generalmente le dApp sono a pagamento. Caricare una foto, mettere un like a una foto, o fare altre azioni su una dApp di condivisione foto potrebbe costare una certa quantità di denaro per ciascuna azione.

Convincere la gente a pagare per usare una nuova applicazione, simile a una più famosa e gratuita, potrebbe essere difficile. La privacy e gli altri vantaggi della decentralizzazione potrebbero non essere ragioni sufficientemente convincenti per convincere la gente a usare le dApp al posto delle

applicazioni esistente, specialmente se sarà necessario pagare per utilizzarle.

Note di Fine Capitolo su Svantaggi e Rischi di Ethereum

Questi sono solo alcuni dei pericoli e dei rischi della piattaforma Ethereum. Ethereum è ancora nuova, e molti dei pericoli e dei rischi potrebbero essere ancora ignoti. Le dApp e i contratti smart hanno ancora molta strada da fare prima di ottenere l'accettazione del grande pubblico, ed è comunque possibile che ciò non avvenga mai.

Il futuro di Ethereum è ancora incerto, e nel prossimo capitolo parleremo di

alcuni fattori che potrebbero determinarne il futuro.

Capitolo 9: aprire un portafoglio Ethereum

Il primo passo necessario per potere utilizzare la rete Ethereum consiste nell'aprire un portafoglio Ethereum. È possibile aprire diversi tipi di portafogli, ciascuno con differenti vantaggi e svantaggi.

In questo capitolo, parleremo dei diversi tipi di portafogli e di come iniziare a utilizzare Ethereum.

Note e Avvertimenti Importanti

Quando si apre un portafoglio, è importante prestare attenzione al

processo di creazione e registrare tutte le password, frasi, chiavi private e informazioni.

Aprire un portafoglio di criptovaluta è diverso dall'aprire un conto corrente o un account online. Se perdete le vostre password o le frasi di recupero, non c'è modo di recuperarle. Nella maggior parte dei tipi di portafogli, non c'è neanche alcuna azienda da poter contattare per resettare le password dimenticate.

Una delle principali ragioni per cui le persone perdono le loro criptovalute è proprio la perdita delle password o la mancanza di backup delle frasi di

recupero.

È altresì importante salvare le proprie password e frasi di backup su un dispositivo diverso da quello su cui tenete il portafoglio. Se perdete il vostro computer o telefono, e il solo backup delle vostre frasi di recupero è sullo stesso dispositivo, perderete accesso anche al vostro portafoglio.

Questo è un punto molto importante, quindi assicuratevi, se nella creazione di un portafoglio ci sono password o frasi di recupero, di fare un backup e salvarle in un luogo sicuro e diverso dal dispositivo su cui si trova il portafoglio.

Cos'è un portafoglio Ethereum?

Un portafoglio Ethereum consiste di alcune componenti principali:

- Indirizzo Ethereum: questo è simile a un indirizzo e-mail. Darete alle altre persone il vostro indirizzo Ethereum per permettere loro di mandarvi Ether, così come dareste il vostro indirizzo e-mail per permettere di mandarvi e-mail.

- Il vostro indirizzo Ethereum è pubblico. Tutti coloro che si trovano sulla rete Ethereum potranno vedere il vostro saldo e tutte le transazioni

avvenute sul vostro indirizzo.

Un portafoglio Etherem più contenere più indirizzi.

- Chiave Privata: una chiave privata è la password utilizzata per provare la proprietà del vostro indirizzo Ethereum, per accedervi e trasferire Ether da quell'indirizzo.

Nota importante: non date la vostra chiave privata a nessuno. Sarebbe l'equivalente di dare il pin del vostro bancomat. Chiunque abbia la vostra chiave privata avrà autorità sul vostro indirizzo e potrà trasferire Ether dal vostro indirizzo.

- Client / Software: per accedere al vostro portafoglio ed effettuare transazioni, avrete bisogno di un software o di un modo per accedere al vostro portafoglio e comunicare con la rete Ethereum. Ciò è noto come client, e può essere un'app per dispositivi mobili, un sito web, o un programma per computer che si connette alla rete.

Ciò è simile al modo in cui accedete al vostro conto corrente ed effettuate transazioni utilizzando l'app mobile o il sito web della vostra banca.

Token Ethereum e ICO

Parleremo in maggior dettaglio degli ICO e dei Token Ethereum più avanti nel libro; tuttavia, ne parleremo brevemente qui, perché sono un fattore importante nel decidere che portafoglio usare.

ICO sta per "Initial Coin Offering", Offerta Iniziale di Moneta. È ciò che accade quando viene offerta al pubblico una nuova moneta, precedentemente non disponibile per acquisto o scambio. Di solito, queste nuove monete sono token che utilizzano la piattaforma Ethereum.

Token Ethereum

I token Ethereum sono simili alle criptovalute; non hanno però la loro blockchain o la loro rete di computer come le vere criptovalute. Utilizzano la blockchain esistente e la rete di Ethereum e operano su di essa.

In genere, i token Ethereum vengono utilizzati all'interno di un'app decentralizzata eseguita su Ethereum.

Parleremo in maggior dettaglio dei token Ethereum più avanti nel libro; per il momento, è importante sapere che solo alcuni tipi di portafogli vi permettono di tenere token Ethereum e partecipare agli ICO. In questo capitolo descriveremo i portafogli che permettono di tenere token Ethereum.

Metodo per Iniziare Rapidamente

Se non avete mai utilizzato Ethereum e state cercando il modo più semplice per iniziare a comprare Ethereum, qui sotto vi presentiamo un metodo veloce:

- Aprite un portafoglio web ibrido combinato con un mercato, come Coinbase.

- Dopo aver aperto il vostro account Coinbase, potrete acquistare Ether utilizzando i metodi di pagamento

esistenti. Questo è un modo facile e veloce per comprare i vostri primi Ether.

- Coinbase non vi permette di partecipare agli ICO o di avere token Ethereum, quindi dopo aver creato un account Coinbase e aver acquistato Ether, potrete decidere di aprire un altro account per acquistare token.

- Potete scegliere un portafoglio con app mobile o software, che fornisce diverse funzionalità e vantaggi, come MyEtherWallet, Jaxx o Exodus.

- Potrete quindi trasferire gli Ether da Coinbase al vostro nuovo portafoglio.

Tipi di Portafoglio

Ci sono diversi tipi di portafoglio per mantenere ed effettuare transazioni sulla rete Ethereum. Ogni tipo di portafoglio ha diversi vantaggi e svantaggi, di cui parleremo in questa sezione.

Questa lista copre i principali tipi di portafoglio, e alcune opzioni per ciascun tipo. Le opzioni sono le più popolari o le più semplici da usare per ciascuna categoria; tuttavia, esistono molte altri

app, molti programmi e siti web oltre a quelli qui elencati.

Portafoglio Web

Un portafoglio web è un portafoglio al quale si può accedere da un browser web su un computer o un dispositivo mobile. È un processo simile al login nel sito della propria banca, sul browser web nel proprio computer.

I portafogli web possono essere utilizzati sia dai principianti che dagli esperti. Possono essere creati in pochi minuti da un browser web, senza che sia necessario effettuare una verifica con un documento di identità.

I portafogli web non richiedono di installare alcuna applicazione o software. Tutti gli aggiornamenti al portafoglio web vengono effettuati dal sito web sul proprio server, quindi non avrete bisogno di aggiornare o scaricare nuove versioni del portafoglio web.

I portafogli web vi forniscono accesso alle vostre chiavi private. Generalmente non c'è alcun servizio clienti o azienda da contattare in caso di perdita delle chiavi private. Assicuratevi di fare personalmente un backup delle vostre chiavi private e di averne cura; altrimenti, perderete accesso al vostro portafoglio web.

I portafogli web sono simili a ogni altro

sito web. Possono essere bloccati dai governi o dai provider. I truffatori possono creare copie dei siti di portafogli web legittimi, con nomi simili, in modo da indurre gli utenti a fare login nel sito sbagliato e rivelare la propria chiave privata. I siti web possono inoltre essere hackerati, quindi anche se il sito fosse legittimo, potrebbe esserci del codice hackerato inserito nel sito web per rubare le chiavi private.

Non è possibile comprare Ether direttamente attraverso un portafoglio web, quindi avrete bisogno di creare un altro portafoglio per acquistare Ether. Ci sono servizi che permettono di comprare Ether e di trasferirlo nel proprio

portafoglio web; tuttavia, possono anche richiedere una verifica di un documento d'identità. Alcuni portafogli web permettono di tenere token Ethereum e di partecipare agli ICO.

I Portafogli Web Ethereum Più Popolari:

My Ether Wallet: www.myetherwallet.com

My Ether Wallet è il portafoglio Ethereum più popolare e affidabile, permette anche di tenere token Ethereum e di partecipare agli ICO.

Nota: ci sono siti truffa che provano a

copiare My Ether Wallet, quindi controllate attentamente l'indirizzo del sito web e il certificato di sicurezza per assicurarvi di essere sul sito giusto.

Mercati

I mercati sono simili ai mercati azionari o ai mercati valutari. Permettono ai trader di comprare e vendere criptovaluta tra di loro, per trarre profitto dai cambiamenti di prezzo.

All'interno di un mercato, è possibile tenere nello stesso account più criptovalute e scambiarle tra di loro. Sono generalmente regolati, come le istituzioni finanziarie. Possono inoltre

avere altre funzionalità, come un servizio clienti e dei controlli di sicurezza, simili ai tradizionali siti web di online banking.

All'interno di un mercato, non controllate le vostre chiavi private. Sebbene ciò riduca il rischio di perdere le vostre chiavi private, vi apre ad altri rischi, come a un eventuale hackeraggio del mercato o alla bancarotta. Ciò è accaduto con il più grande mercato Bitcoin, Mt. Gox. Sebbene adesso il rischio sia minore, perché i mercati sono più regolati, non è ancora nullo.

I mercati permettono di acquistare criptovalute utilizzando metodi di pagamento tradizionali; tuttavia, hanno

lunghe procedure di verifica. È possibile utilizzare i mercati evitando i lunghi processi di verifica, caricando nei vostri account le criptovalute che avete già.

I Mercati Ethereum Più Popolari:

Poloniex: www.poloniex.com

Kraken www.kraken.com

GDAX: www.gdax.com

Bittrex: www.bittrex.com

Ibrido Portafoglio Web / Mercato

Un ibrido portafoglio web / mercato unisce le caratteristiche di un portafoglio web Ethereum con quelle di

un mercato. Fornisce la possibilità di inviare e ricevere Ether come un portafoglio web, e quella di comprare o vendere Ether ai prezzi di mercato.

Gli ibridi portafogli web / mercati vi permettono di acquistare Ether utilizzando i metodi di pagamento tradizionali, come i conti correnti e le carte di credito. Sono generalmente regolati in modo simile alle altre istituzioni finanziarie, e richiedono la verifica della propria identità prima di poter fare acquisti.

Dal momento che un portafoglio web ibrido è una combinazione tra un portafoglio web e un mercato, non ha le piene funzionalità di nessuno dei due. Le

funzionalità di portafoglio web non sono complete come quelle di altri portafogli web, e le funzionalità di mercato non sono ricche come quelle di altri mercati.

Utilizzando un ibrido portafoglio web / mercato non è possibile tenere token Ethereum o partecipare agli ICO. Inoltre, non si ha il controllo delle proprie chiavi private, e ciò rende importante utilizzare un'azienda regolata e affidabile.

Per chi comincia a utilizzare Ethereum, un ibrido portafoglio web / mercato è spesso l'opzione migliore. Fornisce un'interfaccia user-friendly che non richiede una comprensione delle funzionalità più complicate del

portafoglio o dei mercati azionari. Fornisce inoltre un modo semplice per comprare Ether rapidamente, utilizzando metodi di pagamento esistenti.

I Portafogli Web/Mercati Ethereum Più Popolari:

Coinbase: http://bit.ly/10freebitcoin (10$ gratis in bitcoin utilizzando questo link)

Coinbase è uno dei portafogli web / mercati più grandi ed affidabili. È altamente regolato, come le altre istituzioni finanziarie, e rende l'acquisto di Ether semplice e veloce per i

principianti.

Dal momento che è regolato, come le istituzioni finanziarie standard, richiede una verifica della propria identità prima di poter fare acquisti.

App Mobili

Chiunque abbia uno smartphone ha sicuramente usato un'app mobile. Al giorno d'oggi ci sono app per ogni esigenze, anche app per portafogli Ethereum. Queste app vi permettono di comprare, vendere e ricevere Ether e altre criptovalute dal vostro smartphone.

Le app mobili sono facili da usare e installare, come ogni altra app mobile.

Hanno il vantaggio di permettere accesso al proprio portafoglio di criptovalute dal proprio smartphone, e sono generalmente più sicure delle altre opzioni, perché devono passare i requisiti di sicurezza richiesti dagli app store.

Dal momento che le app devono rispettare certi requisiti imposti dallo store, raramente permettono di tenere token Ethereum o di acquistare Ether all'interno dell'app.

Quando si configura la propria app mobile, è importante ricordarsi di salvare i dati di backup, le chiavi private e le frasi di recupero in un altro dispositivo, non sul proprio telefono.

Salvare tutti i dati di backup e recupero sullo stesso dispositivo del portafoglio è un errore comune. Se il dispositivo viene perso, rubato o si rompe, sia il portafoglio che i dati di recupero vanno perduti.

I Portafogli Mobili Ethereum Più Popolari:

Coinbase - Non permette Token Ethereum

Jaxx - Non permette tutti i Token Ethereum

Software

Sebbene le app mobili e web siano

diventando sempre più popolari rispetto al software per computer, la maggior parte delle persone usano ancora diversi programmi ogni giorno.

I portafogli software vi permettono di installare e gestire un portafoglio Ethereum dal proprio computer. Sono un po' più difficili da installare e configurare; tuttavia, se avete almeno una volta installato un programma per computer, non dovreste avere alcun problema nell'installarli.

I programmi scaricati da Internet possono portare maggiori rischi di sicurezza rispetto a un'app mobile, quindi fate attenzione e controllate il sito da cui state scaricando il programma.

I portafogli software hanno un'interfaccia visualizzata sullo schermo del computer, quindi hanno un design più grande e facile da usare rispetto a uno smartphone. A volte, permettono anche di tenere diverse criptovalute e token all'interno del vostro portafoglio.

È importante proteggere con una password sia il vostro computer che il portafoglio software. È altresì importante salvare le vostre chiavi private e frasi di recupero su un dispositivo differente o su un servizio di archiviazione cloud, in modo che non siano sul vostro computer.

Un grosso rischio dei portafogli software è proprio quello di non salvare

correttamente le password e le frasi di recupero su un altro dispositivo. Se il vostro computer viene rubato, si rompe o viene infettato da un virus, e le vostre sole frasi di recupero sono sullo stesso computer del vostro portafogli, perderete accesso al portafogli.

I Portafogli Software Ethereum Più Popolari:

Exodus: https://www.exodus.io/

Jaxx: https://jaxx.io/

Estensioni Chrome

Le estensioni Chrome sono applicazioni che vengono eseguite all'interno del

browser web Chrome. Possono fare quasi tutto ciò che un sito web o un software può fare, e sono accessibili dalla barra di menu del browser.

Ci sono portafogli Ethereum che sono estensioni Chrome, e che vi permettono di mandare e ricevere Ether dal vostro browser web. Un vantaggio delle estensioni Chrome è il fatto che possono aumentare le funzionalità fornite dai siti web che visitate, ad esempio individuando automaticamente gli indirizzi Ether sulle pagine o collegandosi a web app.

Ci sono però dei significativi rischi di sicurezza connessi alle estensioni Chrome, perché sono semplici da creare

e rilasciare sul Chrome Store. Oltre a fornire funzionalità aumentate alle pagine web, possono anche leggere i dati che inserite nei siti web. Installare estensioni Chrome con problemi di sicurezza o estensioni maligne potrebbe porre a rischio i vostri dati personali e finanziari, quindi assicuratevi di installare solo estensioni affidabili.

Sebbene le estensioni Chrome abbiano la convenienza di essere all'interno del vostro browser, è possibile accedervi solo da quel browser. Non sono come i portafogli web, a cui potete avere accesso da ogni dispositivo con una connessione Internet.

Ciò significa che, se perdete il vostro

computer, se si rompe o viene rubato, e se non avete alcun backup delle vostre password e frasi di recupero su un altro dispositivo, perderete accesso al vostro portafoglio.

Le Estensioni Chrome Ethereum Più Popolari:

MetaMask: https://metamask.io/

Jaxx: https://jaxx.io/

Portafogli Cartacei

Un portafoglio cartaceo è un portafoglio stampato su un pezzo di carta. Il pezzo di carta contiene l'indirizzo pubblico e il codice QR del portafoglio, che può

essere fornito ad altre persone per permettere loro di inviare denaro a quel portafoglio. Quando un portafoglio cartaceo viene stampato, sulla stampa potrebbe anche esserci la chiave privata. Assicuratevi di rimuoverla e di tenerla in un luogo separato.

I portafogli cartacei non sono collegati a un computer, a un sito web o a una rete elettronica, e per questo non sono vulnerabili a molti dei rischi dei portafogli software o web. I portafogli cartacei non possono essere hackerati, e forniscono un'opzione di archiviazione sicura per conservare degli Ether.

Dal momento che non sono collegati alla rete Ethereum, non è possibile mandare

transazioni a meno di non inserire la propria chiave privata in un sito web o software, il che può esporre a rischi di sicurezza.

I portafogli cartacei possono essere rubati, distrutti o persi facilmente; per ridurre questi rischi è opportuno laminarli. Le chiavi private possono essere salvate in modo sicuro in diversi luoghi, separati dalle informazioni pubbliche del portafoglio.

I Portafogli Web Ethereum Più Popolari:

My Ether Wallet: www.myetherwallet.com

My Ether Wallet permette di generare un portafoglio cartaceo. Potrete inviare delle transazioni solo se importerete la chiave privata in un sito web o software.

Nota: ci sono siti truffa che provano a copiare My Ether Wallet, quindi controllate attentamente l'indirizzo del sito web e il certificato di sicurezza per assicurarvi di essere sul sito giusto.

Portafogli Hardware

I portafogli hardware sono dispositivi elettronici su cui vengono salvate le chiavi private per un portafoglio Ethereum o di criptovaluta. Hanno funzionalità di sicurezza simili a un

portafoglio cartaceo, perché non sono connessi alla rete se non quando si invia una transazione, quindi gli Ether rimangono per la maggior parte del tempo conservati al sicuro.

I portafogli hardware devono essere collegati a un computer per inviare transazioni, il che li espone ad alcuni rischi di sicurezza. I portafogli hardware sono in genere progettati in modo da non esporre la chiave privata durante l'invio delle transazioni. Alcuni portafogli hardware permettono inoltre di nascondere i portafogli con un saldo consistente, in caso di furto o in situazioni in cui potreste essere obbligati a esporre il saldo del vostro

portafoglio hardware.

Non è possibile acquistare Ether utilizzando un portafoglio hardware, e non tutti permettono di tenere dei token. È necessario ottenere gli Ether in un altro modo e poi trasferirli sul portafoglio hardware.

I portafogli hardware sono in genere consigliati alle persone che hanno esperienza con Ethereum e le criptovalute.

I Portafogli Hardware Ethereum Più Popolari:

Trezor: www.trezor.io

Ledger: www.ledgerwallet.com

KeepKey: www.keepkey.com

Note di Fine Capitolo sui Portafogli Ethereum

All'inizio, i portafogli Ethereum possono causare confusione; mi auguro che questo capitolo vi abbia aiutato a comprendere le differenze tra i vari tipi di portafogli sul mercato, e vi abbia fornito alcune opzioni per aprirne uno.

Quando aprite un portafoglio Ethereum, ricordate di tenere un backup sicuro della vostra chiave privata e della frase di recupero. Se perderete la vostra chiave privata o la frase di recupero, perderete accesso al portafoglio e ai fondi al suo interno.

Più avanti nel libro, parleremo di come comprare, vendere e utilizzare gli Ether, e di come partecipare correttamente a un ICO.

Capitolo 10: Comprare, Mandare, Ricevere e Fare Trading con gli Ether

Dopo aver aperto un portafoglio Ethereum, sarete pronti a usare la rete Ethereum. In questo capitolo parleremo di come vendere, mandare, ricevere, scambiare e usare gli Ether.

Comprare Ether

Il modo più semplice per iniziare a possedere Ether consiste nel comprarli utilizzando metodi di pagamento tradizionali, come bonifici o carte di

credito.

Ci sono diversi modi in cui è possibile comprare Ether. Creando un account su Coinbase, potrete facilmente comprare Ether. Il processo è semplice, e dopo l'acquisto gli Ether saranno istantaneamente accreditati sul vostro account.

Se invece aprite un account su un mercato, come Kraken, potrete comprare Ether utilizzando una carta di credito o un bonifico in modo tradizionale. Il vostro account Kraken ha un portafoglio dove tenere gli Ether, quindi dopo l'acquisto saranno immediatamente nel vostro account.

Se non avete aperto un portafoglio con Coinbase o Kraken, un'altra opzione per comprare Ether utilizzando una carta di credito è Changelly. Questo sito web permette di scambiare diverse criptovalute e di acquistare criptovalute utilizzando una carta di credito.

Potrete acquistare Ether utilizzando una carta di credito con Changelly su www.changelly.com

Per ricevere Ether con Changelly, avrete bisogno di un portafoglio esistente, e di ciò parleremo nella prossima sezione.

Ricevere Ether

Per ricevere Ether nel vostro

portafoglio, dovrete fornire il vostro indirizzo alla persona o al servizio che vi manderà Ether. È un po' come dare l'IBAN a qualcuno, così che possano farvi un bonifico.

Ci sono due modi principali in cui potrete dare questo indirizzo, sia dando la chiave pubblica (indirizzo pubblico), che è una stringa unica di lettere e numeri, o fornendo il codice QR.

Il vostro indirizzo Ethereum sarà simile a quello qui sotto:

0x3035eE16a1CB8484Af86356D7d9C0

Con un servizio come Changelly, dovrete inserire il vostro indirizzo Ethereum per ricevere Ether. Dopo aver

acquistato gli Ether, verranno inviati al vostro indirizzo.

Nota: non confondete la vostra chiave privata con l'indirizzo pubblico. Possono sembrare molto simili. Assicuratevi di fornire l'indirizzo pubblico corretto quando lo date a qualcun altro, e non date mai a nessuno la vostra chiave privata.

Dare il vostro indirizzo è semplice e sicuro, basta copiare e incollare. Come visto dall'indirizzo mostrato sopra, se l'indirizzo venisse scritto a mano, sarebbe facile fare un errore e mandare Ether all'indirizzo sbagliato. Se non

potete fare copia e incolla, l'opzione migliore potrebbe essere quella di dare il vostro codice QR per assicurarvi di fare arrivare gli Ether al giusto indirizzo.

Un codice QR è un codice Quick Response che funziona come un codice a barre, e contiene informazioni che possono essere scansionate e lette rapidamente da diverse applicazioni. Probabilmente avete visto i quadrati somiglianti a un codice a barre che, venendo scansionati dalla fotocamera dello smartphone, vi mandano a un sito web.

Mandare Ether

Mandare Ether è simile a ricevere Ether. Avrete bisogno dell'indirizzo Ethereum o del codice QR a cui mandare gli Ether.

Nel vostro portafoglio Ethereum, potrete selezionare "Invia", probabilmente premendo il pulsante corrispondente. Vi verrà poi richiesto l'importo in Ether e l'indirizzo a cui mandarlo.

L'importo in Ether potrebbe essere espresso in dollari, ma più comunemente è espresso in unità come 1 Ether, 0.5 Ether e così via.

Potete copiare e incollare l'indirizzo a cui mandare gli Ether, o scansionare il codice QR. È importante controllare

attentamente che l'indirizzo sia corretto, perché se manderete Ether all'indirizzo sbagliato, non ci sarà un modo per annullare la transazione, e potrete perdere i vostri Ether.

Dopo aver verificato che l'importo e l'indirizzo siano corretti, potrete mandare gli Ether al destinatario.

Fare Trading / Scambiare Ether

Dopo aver comprato o ricevuto Ether, potreste volere scambiarli per altre criptovalute.

Potrete fare trading in Ether utilizzando un mercato, come Kraken o Poloniex, come fareste trading di azioni o valute.

Potete utilizzare i vostri Ether per acquistare altre criptovalute, che saranno tenute in un portafoglio per ciascuna criptovaluta sul mercato.

Questo può essere un modo semplice per ottenere e tenere una gamma di diverse criptovalute in un solo account. Fare trading di criptovalute per trarre profitto dalle fluttuazioni di prezzo è altamente speculativo e comporta un grande rischio.

È possibile scambiare Ether per altre criptovalute utilizzando Changelly (www.changelly.com) o Shapeshift (www.shapeshift.io).

Scambiare Ether per altre criptovalute

utilizzando questi servizi implica il mandare Ether a un indirizzo, scegliere la criptovaluta da ricevere in cambio, e l'indirizzo a cui mandare quella criptovaluta.

La maggior parte dei portafogli software e mobili, come Jaxx ed Exodus, includono delle funzionalità di Shapeshift nei loro portafogli. Ciò vi permette di scambiare Ether per altre criptovalute direttamente all'interno del portafogli.

Scambiare Ether per Potenza di Calcolo

È possibile scambiare Ether in cambio

di potenza di calcolo per eseguire applicazioni decentralizzate e contratti smart sulla rete Ethereum. Utilizzare Ether per eseguire dApp e contratti smart è un argomento avanzato, che non verrà trattato in questo libro. Tuttavia, è importante sapere che gli Ether hanno questo utilizzo pratico per molti sviluppatori e aziende.

Note di Fine Capitolo sul Comprare, Mandare, Ricevere e Scambiare Ether

Adesso dovreste aver compreso come configurare un portafoglio e come comprare, inviare e ricevere Ether.

Negli ultimi tempi le Offerte Iniziali di Monete (Initial Coin Offerings, ICO)

sono diventate popolari, e molte persone scambiano Ether per ottenere nuove monete e token di criptovaluta. Più avanti nel libro, parleremo del portafoglio richiesto e di come richiedere gli ICO.

Capitolo 11: ICO e Token Ethereum

Gli ICO sono diventati un metodo molto popolare per permettere ad aziende e sviluppatori di raccogliere fondi per finanziare lo sviluppo di applicazioni e aziende. In questo capitolo parleremo di cosa sono gli ICO, di come funzionano, e dei loro pericoli.

Cos'è un ICO?

ICO è un acronimo che sta per "Initial Coin Offering", Offerta Iniziale di Moneta. Si tratta della situazione in cui gli sviluppatori o l'azienda raccolgono

fondi permettendo di acquistare una nuova moneta o token. Potrebbe trattarsi di una nuova criptovaluta o di un token sulla piattaforma Ethereum, da usare in un'applicazione.

Parleremo di come funzionano gli ICO più avanti in questo capitolo; prima parleremo dei token Ethereum, per capire cosa viene offerto in un ICO.

Token Ethereum

I token Ethereum vengono utilizzati nelle dApp costruite sulla piattaforma Ethereum. Probabilmente avete familiarità con le app e i giochi per iPhone e Android che vi permettono di

accedere a nuovi livelli o acquistare bonus e upgrade all'interno delle applicazioni. In questi casi, comprate le monete e i token dell'app con denaro vero, e ciò vi permette di acquistare oggetti all'interno dell'app. I token sulla piattaforma Ethereum funzionano in modo simile.

Gli sviluppatori creano applicazioni decentralizzate che vengono eseguite su Ethereum. Per acquistare i token da utilizzare in queste applicazioni vengono utilizzati gli Ether. Per esempio, in un'app di messaggistica decentralizzata, è possibile utilizzare gli Ether per acquistare i token dell'app. Questi token saranno poi usati nell'app di

messaggistica per mandare messaggi e accedere ad altre funzionalità.

A differenza dei giochi e delle app mobili, in cui c'è un numero illimitato di crediti disponibili per l'acquisto, il numero di token disponibile per una dApp di Ethereum è limitato. Dal momento che il numero di token è limitato, il prezzo cambierà in base all'uso e alla popolarità di quell'applicazione. Più persone useranno l'applicazione, più token dovranno acquistare dalla riserva esistente di token. L'offerta di token è limitata, quindi all'aumentare della domanda il prezzo dei token aumenterà. Gli utenti che avranno acquistato token

prima dell'aumento godranno di più funzionalità nell'applicazione, e se decideranno di rivendere i loro token ad altri utenti trarranno profitto dall'aumento di prezzo.

Come funzionano gli ICO

Gli ICO funzionano offrendo monete o token agli utenti prima che l'app venga lanciata. Le persone comprano token da utilizzare nell'applicazione pagandoli in Ether o Bitcoin. Gli sviluppatori o l'azienda raccolgono fondi per finanziare lo sviluppo dell'app.

L'idea dietro un ICO è che, se un'azienda sviluppa un'app che diventerà popolare,

i token aumenteranno di valore, e coloro che li hanno acquistati in anticipo trarranno profitto.

Gli sviluppatori possono raccogliere fondi per l'app e pagare gli stipendi, senza vendere le azioni della loro azienda o richiedere un prestito.

Pericoli / Rischi degli ICO

Nel partecipare a un ICO si corrono rischi significativi, di cui parleremo in questa sezione.

Perdita dell'investimento iniziale

Il rischio maggiore è probabilmente la perdita del denaro investito nell'ICO.

Ciò potrebbe accadere a causa di diversi fattori. Anche se sapete che c'è sempre il rischio di perdere il proprio investimento, potreste non essere consapevoli delle ragioni per cui ciò avviene.

Gli sviluppatori non creano l'app

Molti ICO raccolgono fondi per finanziare lo sviluppo di un'applicazione. Non c'è garanzia che l'app verrà effettivamente sviluppata. Sviluppare software è costoso e richiede tempo, e gli sviluppatori potrebbero finire i fondi prima di aver creato alcunché.

L'app non è popolare

Anche se gli sviluppatori creano un'app, non c'è garanzia che sarà popolare o che qualcuno vorrà utilizzarla.

Se poche persone usano l'app, i token non prenderanno valore e potrebbero addirittura perderlo. Nel tempo, i token potrebbero diventare carta straccia, perchè se nessuno usa l'app, nessuno ha bisogno dei token.

I token non salgono di valore

Anche se gli sviluppatori creano l'app e gli utenti la usano, c'è sempre il rischio che i token non salgano di valore.

Potrebbero essere stati venduti molti token durante l'ICO, creando un'offerta eccessiva di token. Anche se gli utenti usassero l'app, la richiesta di token potrebbe non essere sufficiente ad aumentarne il prezzo.

Nessun mercato secondario

Per un'azienda è facile creare un token e offrirlo al pubblico. Una volta comprati i token in un ICO, non c'è garanzia che sia possibile venderli per riavere il proprio denaro.

Se non potrete vendere i vostri token, non potrete riavere il vostro denaro o trarre profitto. Potrete usarli solo

nell'app, e ciò sarà possibile solo se gli sviluppatori creeranno effettivamente un'app.

Rischi legali e di regolazione

La Cina ha recentemente messo fuorilegge gli ICO, e si sta muovendo verso la chiusura dei mercati di criptovalute. Il divieto imposto dalla Cina impedisce inoltre a tutte le aziende che hanno raccolto fondi tramite ICO di restituire il denaro a coloro che hanno acquistato token. □ □

Nella maggior parte dei paesi ci sono regole e linee guida che riguardano la creazione di aziende e l'offerta di azioni

agli investitori, e gli ICO cercano di aggirare queste regole.

Sebbene fino a ora gli ICO siano stati permessi, ciò è dovuto principalmente al fatto che si tratta di una nuova tecnologia, non ancora regolata. La Securities and Exchange Commission (SEC) degli Stati Uniti, insieme agli altri istituti di regolazione finanziaria di altri paesi, stanno esaminando il problema degli ICO e delle aziende che li usano per raccogliere fondi, e probabilmente istituiranno dei regolamenti.

Sebbene ad oggi le aziende possano ancora raccogliere fondi tramite ICO, potrebbero esserci problemi legali e di

regolazione nel futuro. Tali regole potrebbero anche essere applicate retroattivamente, come in Cina, e colpire tutte le aziende che nel passato avessero raccolto fondi tramite ICO. Ciò potrebbe portare le aziende a perdere denaro, e rendere i token per le loro applicazioni privi di valore.

Truffe

Sebbene vi siano molte aziende legittime che raccolgono fondi tramite ICO, vi sono anche moltissime truffe.

Non ci sono regole per le aziende che raccolgono fondi tramite ICO. Ciò ha permesso ai truffatori di creare siti web

e rubare denaro dagli utenti, inconsapevoli della differenza tra un ICO legittimo e una truffa.

I truffatori creano siti web e account di social media che copiano quelli di ICO legittimi. Ciò crea confusione su quale sia la vera azienda, portando molti utenti a mandare denaro all'azienda sbagliata.

Anche gli ICO che sembrano unici e legittimi potrebbero essere stati creati da persone che non hanno la minima intenzione di utilizzare il denaro raccolto per sviluppare applicazioni. Potrebbero semplicemente tenere per sé il denaro raccolto e dire che il progetto o l'azienda è fallito. Dal momento che non ci sono regole, non c'è nulla che

impedisca ai malintenzionati di farlo e non ci sono ramificazioni legali.

Indirizzo o portafoglio sbagliato

Un altro rischio degli ICO consiste nel mandare e ricevere fondi. Se mandate denaro da o verso l'indirizzo sbagliato, lo perderete.

Se il portafoglio o l'indirizzo che indicate per ricevere i token non è del tipo corretto, li perderete.

La maggior parte degli ICO necessitano di un tipo speciale di portafoglio Ethereum che permette di tenere i token al suo interno. Spesso, l'indirizzo da cui mandate il denaro è lo stesso indirizzo a

cui verranno mandati i token. Se si tratta di un indirizzo che non può contenere token, quando i token verranno inviati, verranno persi.

Partecipare a un ICO

Se, dopo aver letto tutti i rischi, volete comunque partecipare a un ICO, dovete fare attenzione a farlo correttamente. In questa sezione parleremo del portafoglio richiesto, e comprenderemo le basi su come partecipare a un ICO.

Portafoglio necessario per partecipare a un ICO.

Per partecipare a un ICO, avrete bisogno

di un portafoglio speciale in grado di tenere token.

I mercati, come Poloniex e Kraken, e i portafogli web ibridi come Coinbase non vi permettono di ricevere token da un ICO. Non mandate Bitcoin o Ether da queste piattaforme, perché perderete il vostro denaro e non riceverete i vostri token.

Per partecipare a un ICO, avrete bisogno di un portafoglio web o software come:

My Ether Wallet - myetherwallet.com

Meta Mask - metamask.io

Questi portafogli vi permettono di inviare Ether e di ricevere e mantenere token. Ci sono altri portafogli che

permettono di mandare Ether e ricevere token; tuttavia, quelli qui sopra sono i più comuni e consigliati sui siti di ICO.

Non mandare denaro prima dell'apertura dell'ICO

Gli ICO hanno generalmente un conto alla rovescia prima dell'inizio dell'ICO. Di solito, non rilasciano l'indirizzo a cui mandare fondi prima dell'inizio dell'ICO.

Talvolta, però, l'indirizzo viene rilasciato qualche ora prima per dare agli utenti il tempo di prepararsi; tuttavia, tutte le richieste mandate prima

dell'orario ufficiale di apertura non verranno accettate, e i fondi potrebbero essere persi.

Mandare Ether a un ICO

Se avete i vostri Ether nei portafogli MyEtherWallet o MetaMask detti prima, potrete ricevere i token allo stesso indirizzo.

Di solito funziona così: all'apertura dell'ICO viene fornito un indirizzo, al quale è possibile mandare Ether.

I token in un ICO di solito sono limitati, e quando tutti vengono venduti, l'ICO è completo. Ciò spesso risulta in un elevato numero di transazioni all'inizio

dell'ICO, causando alcuni ritardi.

Prezzo Gas e Limite GAS

Le richieste di partecipazione a un ICO vengono trattate come transazioni in un contratto Smart. Vengono processate da miner, che ricevono una commissione per aver processato la transazione.

Il prezzo Gas e il limite Gas determinano la commissione che il miner riceve. Più alti sono il prezzo gas e il limite gas impostati in una transazione, più velocemente la stessa sarà processata.

Durante un ICO, le commissioni di transazione pagate sono di solito molto

alte, perché gli utenti vogliono assicurarsi che le loro transazioni siano processate in fretta, così da non perdere l'occasione nel caso in cui l'ICO venga completato velocemente. Di solito, il sito web dell'ICO mostra un Prezzo Gas e un Limite Gas consigliato per l'invio. Potrebbe anche decidere di impostare un limite massimo per creare un'offerta più equa, assicurandosi che nessuno sia costretto a pagare commissioni di transazione elevate per partecipare.

Se una richiesta viene rifiutata, è necessario comunque pagare le commissioni di transazione, quindi fate attenzione a non mandare troppe transazioni o a non impostare le

commissioni al di sopra del limite consigliato dall'ICO.

Mandare Bitcoin o altre Criptovalute a un ICO.

Talvolta, gli ICO permettono di partecipare inviando Bitcoin o altre criptovalute.

Potete ricevere token solo su specifici indirizzi e portafogli Ethereum, come detto prima, quindi se parteciperete con Bitcoin o altre criptovalute, assicuratevi di avere un portafoglio adeguato e inseritene l'indirizzo come indirizzo di ricezione.

Quando inviate Bitcoin o altre criptovalute, potete includere una nota

alla transazione. Questa è la "coinbase" della transazione. L'ICO potrebbe specificare di includere l'indirizzo di ricezione come parte della coinbase della transazione.

Potreste anche includere un indirizzo di rimborso nel caso in cui la transazione sia rifiutata. Non confondete l'indirizzo di rimborso con quello di ricezione. L'indirizzo di rimborso è generalmente l'indirizzo da cui avrete mandato i bitcoin o la criptovaluta. L'indirizzo di ricezione è quello a cui saranno inviati i vostri token. Confonderli potrebbe risultare nella perdita del vostro denaro.

□□

Non tutti i portafogli di criptovaluta vi

permetteranno di includere un messaggio con le vostre transazioni. Partecipare a un ICO con Bitcoin senza includere un indirizzo Ethereum valido che possa ricevere token nella coinbase della transazione porterà alla perdita del vostro denaro.

Ricevere Token

Il momento in cui riceverete token dopo un ICO varia, e dipende dall'ICO. I token potrebbero non essere distribuiti per mesi dopo il completamento dell'ICO. Quando saranno spediti, saranno ricevuti all'indirizzo Ethereum che avete fornito. Per venderli, dovrete

spostarli su un mercato che accetti token.

Fate attenzione nello spostare i token su un indirizzo di mercato, perché potreste perderli nel caso in cui li inviaste all'indirizzo sbagliato.

Note finali sugli ICO

Ci sono molti rischi nel partecipare a un ICO. Adesso avete un'idea dei rischi possibili, e sapete come evitarli. □□

Ricordatevi di seguire tutte le istruzioni nell'ICO. Prendetevi tempo per leggere tutto, e controllate accuratamente che tutti i dettagli siano corretti.□□

Fate attente ricerche su un ICO, assicurandovi specialmente che non si

tratti di una truffa, leggendo le informazioni su reddit e sui social media. □

Capitolo 12: Il Futuro di Ethereum

Le criptovalute esistevano già da diversi anni prima della creazione di Ethereum. Bitcoin è stata la prima; tuttavia, altre criptovalute come Litecoin e Dogecoin avevano un forte seguito e una community prima che arrivasse Ethereum.

Nel momento in cui scrivo, Ethereum ha solo 2 anni, al contrario di Bitcoin che esiste da 8 anni. Ethereum è ancora all'inizio, e sta ancora realizzando il suo potenziale.

Possiamo solo provare a indovinare

cosa porterà il futuro a Ethereum, essendo così nuovo: tuttavia, stanno emergendo alcuni trend, che possiamo utilizzare per provare a predire il potenziale futuro di Ethereum.

Enterprise Ethereum Alliance

La formazione della Enterprise Ethereum Alliance ha portato a un significativo aumento di prezzo e interesse in Ethereum.

La Enterprise Ethereum Alliance ha all'incirca 150 membri. Tra questi ci sono alcune delle più grandi aziende del mondo, che lavorano insieme per sviluppare i framework necessari per

usare Ethereum all'interno delle organizzazioni.

L'alleanza esiste da meno di un anno, e sta ancora svolgendo studi di fattibilità. Non ha ancora fatto alcun annuncio ufficiale sull'uso di Ethereum in una grande organizzazione a livello mondiale.

Questa alleanza vede governi e aziende lavorare insieme, e ha il potenziale di rendere Ethereum una piattaforma utilizzata da aziende e governi in tutto il mondo.

È tuttavia possibile che, dopo aver esaminato Ethereum, aziende e governi decidano di non utilizzarlo. Potrebbero

decidere di creare i propri sistemi basati su blockchain che non si basino sulla piattaforma Ethereum.

Dato il numero di governi e aziende interessati a Ethereum, è ragionevole ipotizzare che Ethereum verrà utilizzato da grandi aziende e governi. Anche se le aziende dell'alleanza non decideranno di usare Ethereum, ci sono migliaia di altre aziende non coinvolge nell'alleanza che contano di utilizzare Ethereum nei loro affari.

Regolazioni e Legislazioni riguardo agli ICO

La Cina ha recentemente vietato gli ICO e i mercati di criptovalute. Ci sono ben

poche regole che riguardano le aziende che raccolgono fondi tramite ICO, e ciò ha portato a truffe e perdite di denaro da parte degli investitori.

Le aziende usano gli ICO come metodo per raccogliere fondi, evitando facilmente i requisiti finanziari e regolatori riguardo all'acquisizione di fondi.

Prima di partecipare a un ICO, gli utenti devono convertire la loro valuta normale in criptovaluta. Inoltre, gli utenti non ricevono azioni dell'azienda, ma token che potranno essere utilizzati nell'applicazione al momento del lancio. Si tratta essenzialmente di scappatoie

che permettono alle aziende di aggirare la legislazione esistente. Dal momento che le aziende ricevono i fondi in criptovaluta, e non in valuta fisica, e dal momento che gli utenti acquistano token e non investono nell'azienda, tutto è legale.

I cambiamenti nelle leggi rimangono sempre indietro rispetto a quelli nella società e nella tecnologia. Prima che una legge venga cambiata sono necessarie lunghe investigazioni, rapporti e cause legali. Molti governi in tutto il mondo stanno valutando gli ICO e come gestirli.

Sebbene gli ICO siano legali nella maggior parte dei paesi, il divieto degli ICO in Cina potrebbe essere la stessa

direzione che prenderanno gli altri governi. Se anche non ci saranno divieti espliciti, ci saranno regole e requisiti crescenti per la raccolta di fondi attraverso ICO.

La competizione dalle altre piattaforme

Ethereum è rivoluzionaria; tuttavia è open source, e ciò significa che chiunque può ottenere il codice sorgente e creare la propria versione. Ethereum Classic è quasi identica a Ethereum, e anche altre aziende o gruppi possono creare la propria versione.

Ethereum Classic è molto meno

popolare di Ethereum, perché i sistemi basati su blockchain e le criptovalute richiedono una grande comunità che contribuisca con potenza di calcolo e supporti la rete. Ethereum ha una grande rete di utenti, ed è supportata da governi e aziende.

Con ogni probabilità Ethereum Classic non rappresenterà una seria concorrenza per Ethereum; tuttavia, la Cina ha le sue startup uniche di blockchain. Ci sono piattaforme, come NEO, che permettono agli sviluppatori di creare app decentralizzate e contratti Smart. La maggior parte dei computer che minano criptovalute si trovano in Cina, e ciò fornisce una potenziale comunità e base

di utenti per NEO.

Anche gli sviluppatori di Bitcoin possono creare una piattaforma simile, che usi la rete di Bitcoin per eseguire dApp e contratti Smart. Se così fosse, ciò potrebbe costituire una concorrenza significativa per Ethereum e fornire un'alternativa per permettere l'utilizzo di Bitcoin per contratti smart e dApp.

La prima azienda a creare una nuova tecnologia non è necessariamente l'azienda che, dopo qualche anno, diventa dominante sul mercato. Ethereum è stata la prima piattaforma basata su blockchain a permettere la creazione di dApp e contratti smart; non è detto che riesca a imporsi sul mercato.

Internet decentralizzato

Tra tutte le potenzialità che Ethereum offre, la più rivoluzionaria potrebbe essere la possibilità di sostituire la struttura di internet con un internet decentralizzato.

Abbiamo parlato dei vantaggi delle app e dei server decentralizzati precedentemente nel libro. Per ricapitolare rapidamente questa informazione, quando accedete a un sito web, lo fate da un server centrale. Tutti i file, le foto e i dati che caricate sono salvati su quel server centrale. Se il server centrale viene hackerato, tutti i

dati su di essi vengono persi. Se il server va offline, il sito e tutti i dati sono inaccesibili.

Ethereum permette a siti web, applicazioni e a qualsiasi altra cosa a cui si possa accedere online di essere decentralizzata. Questi siti web, app e dati vengono salvati e acceduti da una rete di computer decentralizzati in tutto il mondo.

Ciò ha il potenziale di sostituire le aziende di web hosting, di archiviazione dati, e la struttura stessa di internet. Ciò creerebbe un internet decentralizzato controllato dagli individui, non dalle grandi aziende o dai governi.

Accettazione del grande pubblico.

Se i contratti Smart, le dApp e la piattaforma Ethereum diventeranno più popolari dipende in larga parte dall'accettazione del grande pubblico.

Alla maggior parte delle persone non importa di termini come "decentralizzazione" o "a prova di censura". Si preoccupano maggiormente di termini come "sicurezza". Per la maggior parte delle persone non c'è la necessità di usare dApp e contratti smart, e i vantaggi non sono necessariamente attraenti rispetto alle opzioni esistenti.

Per molte persone rimuovere gli intermediari di terza parte non è un vantaggio, perché significa che non c'è un servizio clienti a cui rivolgersi o una sede fisica in cui andare. Sebbene a nessuno piaccia essere messo in attesa quando si chiama la propria banca, è comunque un'opzione migliore rispetto al non avere una banca da chiamare.

Questo è un problema di tutte le dApp, non solo di quelle legate alla finanza. Dire a qualcuno di smettere di usare Instagram e di utilizzare un'app diversa per le foto solo perché è decentralizzata non sarebbe un'argomentazione convincente per gli utenti più fedeli di Instagram.

Se le aziende riusciranno a creare dApp attraenti per un mercato di massa, allora la gente inizierà a usare Ethereum per potere utilizzare quelle dApp. Se non ci saranno dApp che gli utenti vogliano usare, o ragioni sufficientemente convincenti per usarle, allora difficilmente otterranno popolarità o sostituiranno le attuali opzioni.

Ad esempio, se gli utenti potessero guadagnare criptovaluta utilizzando una dApp di condivisione foto, potrebbe essere un buon motivo per usarla. L'uso da parte delle celebrità di dApp otrebbe essere un altro fattore che induca la gente a usare dApp; tuttavia, l'endorsement da parte delle celebrità

dipende più da quanto le si paga che da benefici come la decentralizzazione.

Note di Fine Capitolo sul Futuro di Ethereum

Il futuro di Ethereum è ancora incerto. Non sappiamo ancora se i governi e le grandi aziende sostituiranno i sistemi esistenti con delle soluzioni basate su Ethereum.

Ethereum è ancora nuova, e le applicazioni create su di essa sono molto semplici. All'inizio di internet, la maggior parte dei siti web erano composti da testo e qualche link. Ci sono voluti molti anni prima che i siti

web diventassero avanzati come li conosciamo oggi.

Le capacità attuali di Ethereum potrebbero impallidire a confronto delle possibilità future. Le dApp di oggi si possono paragonare ai siti web fatti di solo testo che esistevano all'inizio di Internet. Per ora, possiamo solo immaginare cosa ci porterà il futuro di Ethereum. Considerando la rapidità con cui la tecnologia avanza, potrebbe superare le nostre più folli aspettative.

Recensioni e Feedback

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 e inserire una recensione su Amazon. Anche poche parole e un voto ci aiuteranno tantissimo.

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

Link per dare un voto al libro:

Per la tua convenienza, qui sotto troverai un link breve al libro:

www.wisefoxbooks.com/ethit

Feedback

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 abbiano aiutato a conoscere Ethereum e la tecnologia blockchain.

Ci vediamo sulla blockchain!

Guida Bonus alle Risorse

Ottiani gratuitamente la guida alle risorse Ethereum e Blockchain

La guida include delle risorse per scoprire di più su Ethereum, ICO e la tecnologia Blockchain.

È inclusa anche una breve guida ai riferimenti per comprendere gli aspetti importanti di Ethereum, bitcoin e blockchain.

Attualmente, questa guida è disponibile solo in inglese.

Potete ottenere la Guida Bonus alle Risorse al link qui sotto:

Errori and 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, grammatica o altro.

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 errori saranno invitati a ricevere copie anticipate dei futuri libri che pubblicheremo.

Errori: errors@wisefoxpub.com

Feedback

Per ogni feedback generale riguardo al libro, sentiti libero di contattarci all'indirizzo e-mail qui sotto:

Feedback: contact@wisefoxpub.com

Altri libri di Mark Gates

Potrete trovare gli altri libri di Mark Gates su Amazon, nel profilo dell'autore al seguente link:

www.wisefoxpub.com/markga