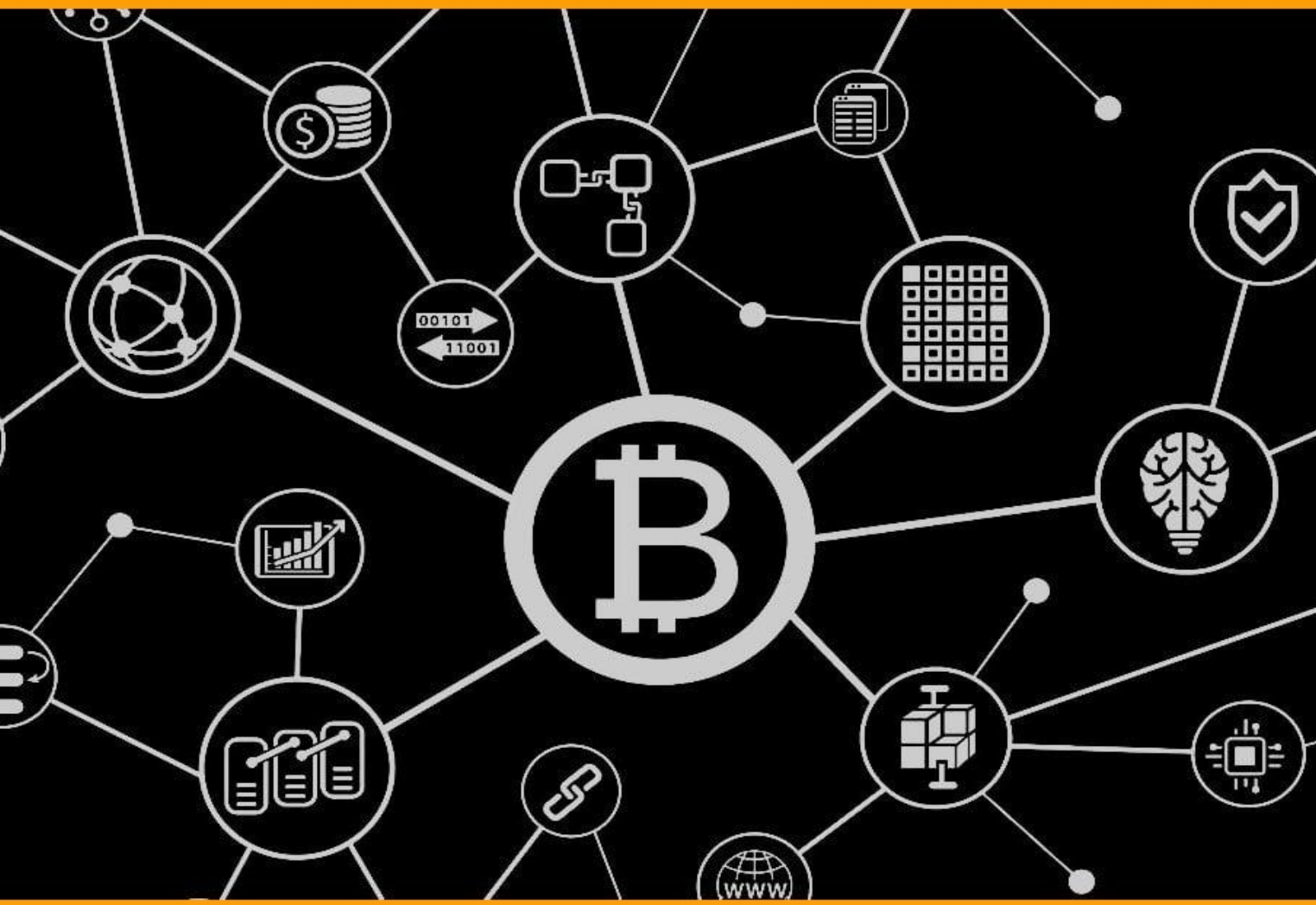
Guida Pratica alla Blockchain e alle Criptovalute

Bitcoin Ethereum Ripple Litecoin



S.Deidda

INTRODUZIONE

Ultimamente le criptovalute stanno vivendo un momento di grande notorietà. Se fino a qualche tempo fà erano impiegate solo dai nerd, dagli smanettoni e nel deep web oggi in molti sono interessati ad utilizzarle sia per

fare transazioni e acquisti, sia per guadagnare soldi speculando. Nell'ultimo anno il valore delle criptovalute è salito alle stelle raggiungendo una capitalizzazione di oltre 700 miliardi di dollari. Nel corso del 2017 sono stati raccolti oltre 2 miliardi tramite le ICO (Initial Coins Offerings), ci sono oltre 70 exchange di valute digitali e flotte di hedge fund che iniziano a interessarsi a questo mondo.

Ma al di là dei rumor e della stampa, la stragrande maggioranza delle persone - anche banchieri, consulenti, scienziati e sviluppatori - ha una conoscenza molto limitata delle criptovalute. Spesso nemmeno i concetti base risultano ben

assimilati. Presumibilmente se avete acquistato questo libro sarete sicuramente interessati a questa nuova realtà, e quindi vi starete chiedendo:

- Cosa sono le criptovalute? E come funzionano?
- Perchè dovrei conoscere le criptovalute?
- E cosa dovrei sapere sulle criptovalute?

Partiamo dal principio, Satoshi Nakamoto è lo pseudonimo utilizzato dall'inventore (o dagli inventori) della criptovaluta più famosa, il Bitcoin nonchè la prima criptomoneta per valore, la prima ad essere conosciuta in

massa e ad essere riconosciuta come forma di pagamento da diversi siti internet e da molti commercianti.

Tutto ha avuto inizio quando nel novembre 2008 Satoshi ha affermato attraverso 'The Cryptography Mailing list' sul sito metzdowd.com di aver sviluppato un sistema di pagamento "Peer-to-Peer".

Il singolo elemento più importante dell'invenzione di Satoshi è stata quella di esser riuscito a creare un sistema di pagamento decentralizzato. La maggioranza delle persone forse non ne è a conoscenza, ma il denaro digitale ebbe un attimo di voga poco prima della bolla tecnologica del 2000. Ci furono

molti tentativi di creare valuta digitale (Flooz, Beenz ecc.), ma con la seguente crisi economica i progetti ebbero vita breve e fallirono.

Satoshi diversamente dagli altri ha avuto l'intuizione di servirsi di una rete Peer-to-Peer come quella utilizzata per la condivisione di file, per realizzare un sitema decentralizzato per scambiare valuta digitale.

Questa decisione è stata fondamentale, ed è la parte vitale delle criptovalute.

L'argomento può risultare un pò tecnico e complesso, ma se lo riuscirai a capire, ne saprai di più sulle

criptovalute rispetto alla maggior parte delle persone.

Quindi, proviamo a renderlo il più semplice possibile:

Per realizzare denaro digitale è necessaria una rete di pagamento con conti, saldi e transazioni.

È facile da capire. Uno dei problemi principali che ogni rete di pagamento deve affrontare è la cosiddetta doppia spesa: per evitare che una entità spenda lo stesso importo due volte. Di solito, questo problema viene risolto da un server centrale che registra i bilanci.

In una rete decentralizzata, non hai

questo server, quindi ogni singola entità della rete deve svolgere questo lavoro. Ogni ‘peer’ della rete deve avere una lista con tutte le transazioni per verificare se quelle future possono essere considerate valide o un tentativo di raddoppiare la spesa.

Come possono queste entità dare un consenso e validare le transazioni? Se un solo ‘peer’ non è d’accordo la transazione non è validata. Hanno bisogno di un consenso assoluto.

Di solito c’è bisogno di un'autorità centrale che dichiari lo stato corretto dei saldi, ma come si può raggiungere un consenso senza un'autorità centrale?

Nessuno lo sapeva fino a quando Satoshi non è emerso dal nulla. In effetti, nessuno credeva che fosse persino possibile, ma Satoshi ha dimostrato che lo era. La sua maggiore innovazione consiste nel raggiungere un consenso senza un'autorità centrale; ed è proprio questa caratteristica che reso le criptovalute elettrizzanti, affascinanti e famose nel mondo. Se volessimo dare una semplice definizione, potremmo considerare il “sistema” ideato da Shatoshi come un database costituito da voci limitate modificabili soltanto soddisfando condizioni specifiche. Questo è esattamente il modo in cui è possibile definire una valuta.

Prendiamo ad esempio i soldi su di un qualsiasi conto bancario:

Di cosa si tratta se non di voci in un database che possono essere modificate solo in condizioni specifiche?

Una criptovaluta è quindi una valuta a tutti gli effetti, decentralizzata e digitale la cui implementazione si basa sui principi della crittografia per convalidare le transazioni e la generazione di moneta in sé.

Le valute digitali si basano su reti p2p (peer-to-peer) i cui nodi (peer) sono computer di utenti disseminati in tutto il mondo. Le transazioni e il rilascio di moneta avvengono

collettivamente in rete, pertanto non c'è una gestione di tipo "centralizzato" che caratterizza le valute tradizionali. Le Criptovalute vengono principalmente utilizzate su internet attraverso circuiti esterni al sistema “centralizzato” dunque si pongono come alternativa ai sistemi di pagamento abituali e di riserva di valore. Sono uno strumento visto spesso con diffidenza dalle autorità e dalle banche centrali per la possibilità di effettuare transazioni con un alto livello di privacy (variabile a seconda del protocollo utilizzato) e anonimato, grazie alla caratteristica di pseudonimia degli utilizzatori.

Per evitare l’iperinflazione ed

imitare la scaristà (e il valore) dei metalli preziosi, la maggior parte delle criptomonete sono state ideate ponendo un limite massimo alla quantità che sarà in circolazione.

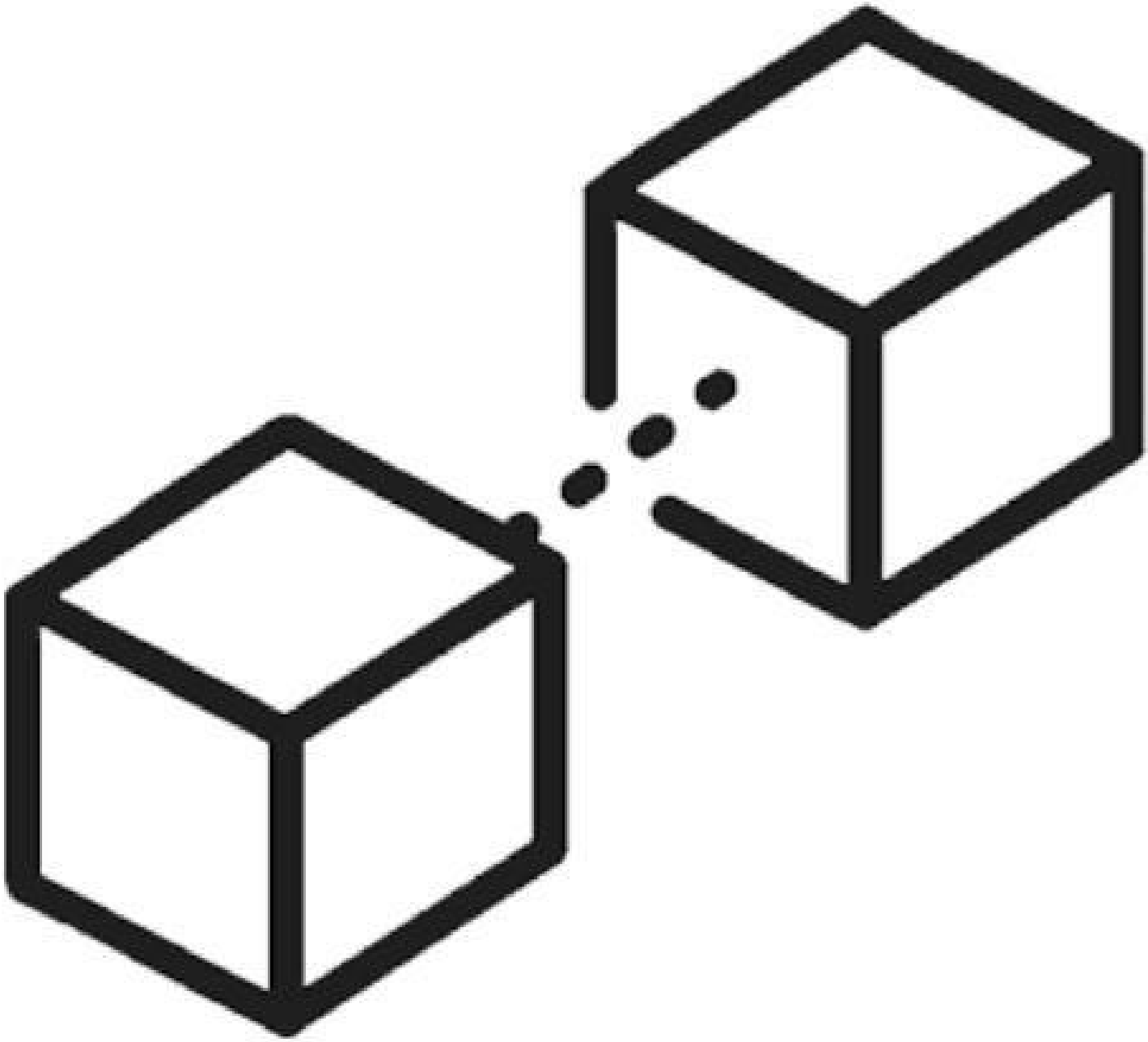
Pur essendo questi sistemi di scambio ancora nelle fasi iniziali di sviluppo, la capitalizzazione di mercato delle criptovalute ha superato i 700 miliardi di dollari a dicembre 2017, un vero e proprio boom che ha catalizzato l'interesse di moltissime persone.

A Gennaio 2018 oltre 1400 criptovalute vengono scambiate sui vari exchange e la maggior parte deriva dal

protocollo utilizzato per i Bitcoin.

Investire in valute digitali è relativamente semplice, ma richiede serietà e disciplina, non bisogna farsi prendere dalla tentazione di giocare i propri soldi alla roulette. Per questo ritengo sia necessario approfondire adeguatamente la materia e conoscere almeno le basi della tecnologia su cui si basano: la Blockchain.

LA BLOCKCHAIN



Cos'è la "Blockchain" ?

Nelle scorse settimane,

probabilmente ne hai sentito sicuramente parlare se hai prestato attenzione alle notizie dal mondo digitale e finanziario.

La tecnologia blockchain è lo strumento utilizzato dalle criptovalute per facilitare transazioni sicure e anonime.

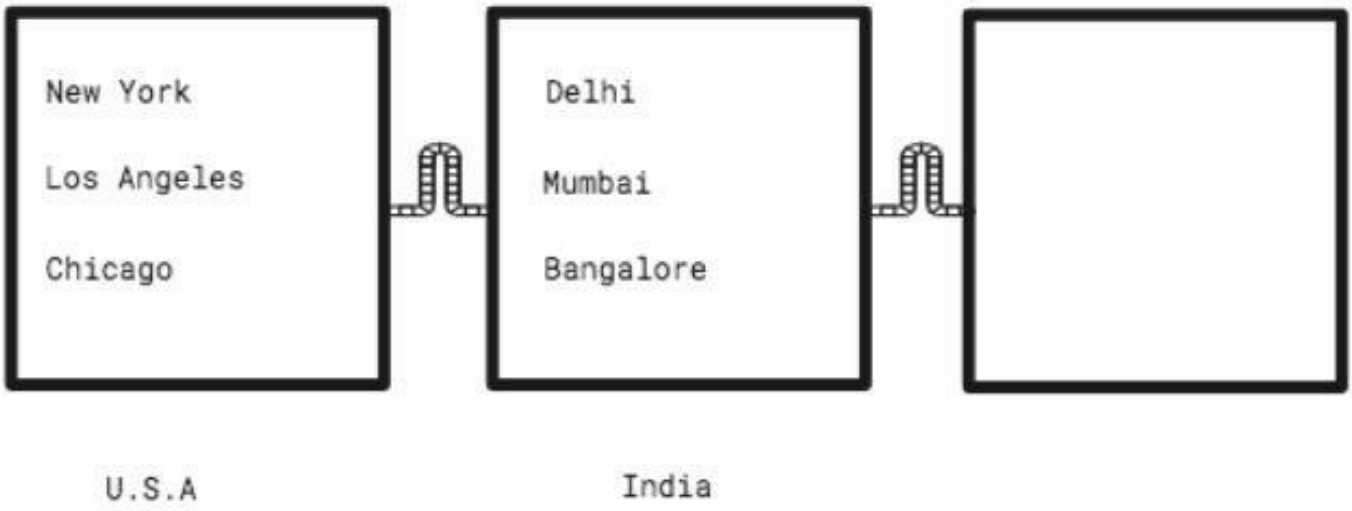
Le origini della blockchain sono un po' "oscure". Come ho già detto, una persona o un gruppo di persone riconosciute dallo pseudonimo Satoshi Nakomoto, ha inventato e rilasciato la tecnologia nel 2009 come un modo per inviare in modo digitale e anonimo pagamenti tra due parti senza la necessità di una terza parte per verificare la transazione. Inizialmente è stato progettato per facilitare,

autorizzare e registrare il trasferimento di bitcoin e altre criptovalute.

La tecnologia blockchain può apparire complessa, ma è in realtà piuttosto semplice da comprendere. Essenzialmente, è un database condiviso popolato da voci che devono essere confermate e crittografate. La tecnologia blockchain offre un modo per creare in modo sicuro ed efficiente un registro di attività sensibili (qualsiasi cosa, dai trasferimenti internazionali di denaro alle registrazioni degli azionisti) a prova di manomissione.

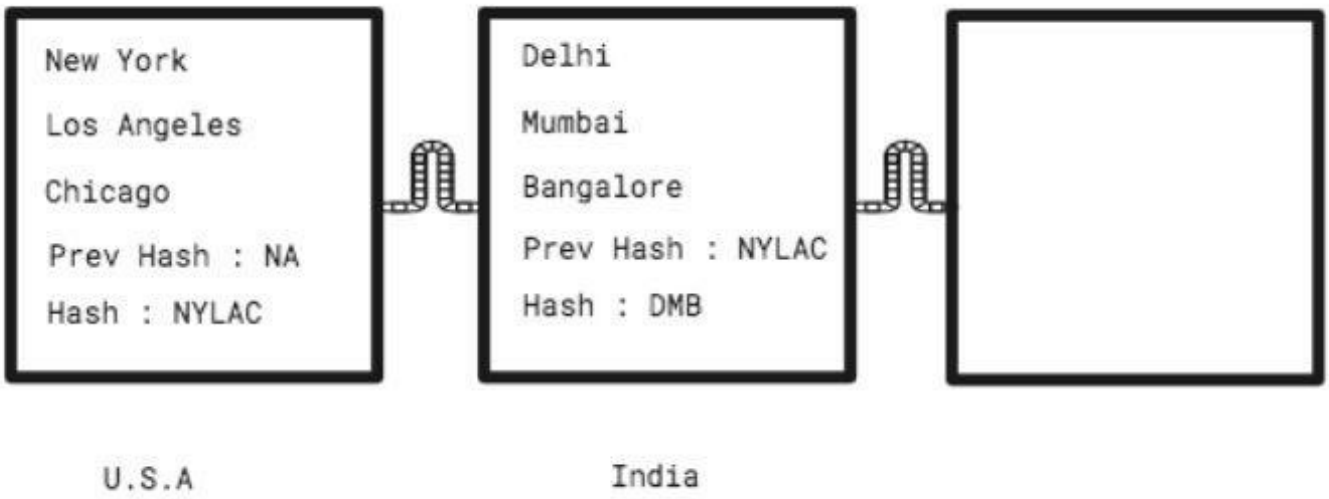
La blockchain è composta solo da due elementi: un blocco e una catena. Nella

Blockchain le informazioni digitali sono divise in blocchi e collegate tra loro. Ad esempio, considera i seguenti blocchi, ognuno rappresenta un paese e ciascuno di essi contiene i nomi delle città del rispettivo paese.



Ognuno di questi blocchi è definito da un codice univoco chiamato hash. Un hash è un insieme di caratteri (ad esempio "1hKs8Hvz7"). L'hash di ogni blocco deriva dalle informazioni

contenute in esso. Il blocco degli Stati Uniti ha le città di New York, Los Angeles e Chicago. Quindi l'hash sarebbe qualcosa come "NYLAC" .



Ogni blocco successivo conterrà l'hash del blocco precedente. Questo è ciò che li lega insieme. Se qualcuno manomette il primo blocco per aggiungere la città di Boston. Il nuovo

hash diventa "NYLACB". Tuttavia, il blocco successivo dell'India ha già memorizzato l'hash come "NYLAC". Questa mancata corrispondenza spezzerà la catena.

Quindi lo scopo dell'hash è assicurarsi che nessuno lo possa compromettere.

Cosa succede se qualcuno cambia il contenuto di un blocco e aggiorna l'hash dei blocchi successivi?

I dati della blockchain non sono conservati soltanto su di un computer, ma sono replicati nei computer di ogni utente facente parte della rete. Se ti unisci a una rete blockchain, il tuo

computer scaricherà questi blocchi. Se qualcuno altera la sua versione, la rete considererà ciò che la maggioranza ritiene sia corretta (rendendo inutile la manomissione). La crittografia inoltre garantisce che gli utenti possano modificare solo le parti della blockchain che "possiedono" avendo a disposizione le chiavi private necessarie per scrivere nel file. Garantisce inoltre che tutte le copie della blockchain distribuita siano mantenute sincronizzate. Nessuno quindi può modificare una blockchain senza avere le chiavi corrispondenti. Le modifiche non verificate da quelle chiavi vengono rifiutate. Naturalmente, le chiavi (come una valuta fisica) potrebbero teoricamente essere rubate,

ma alcune righe di codice possono generalmente essere mantenute sicure a costi molto bassi (rispetto ad esempio alla spesa per immagazzinare una riserva d'oro).

La sicurezza è incorporata nella blockchain, in quanto è stata concepita in modo che funga tramite la rete P2P come un database gestito in modo decentralizzato e autonomo. Ciò rende la blockchain eccellente per la registrazione di dati come ad esempio: cartelle cliniche, transazioni, gestione dell'identità e molto altro. Questo significa che le principali funzioni svolte dalle banche (la verifica delle identità per prevenire le frodi e quindi

la registrazione delle transazioni legittime) possono essere eseguite da una blockchain in modo più rapido e accurato.

Il concetto è stato implementato per la prima volta nel 2009 come parte della valuta digitale bitcoin, la blockchain funge in tal caso da registro pubblico per tutte le transazioni. Usando un sistema blockchain, il bitcoin è stata la prima moneta digitale a risolvere il problema della doppia spesa (a differenza delle monete o delle banconote fisiche, i file elettronici possono essere duplicati e spesi due volte) senza l'uso di un ente autorevole o di un server centrale. Le persone che

mettono a disposizione il loro computer nella rete vengono chiamati ‘miners’ e sono ricompensati in bitcoin.

Perchè la Blockchain è importante?

Al giorno d’oggi siamo tutti abituati a condividere le informazioni attraverso una piattaforma online decentralizzata: internet. Ma quando si tratta di trasferire valore (denaro) siamo costretti a ricorrere a istituzioni finanziarie centralizzate e antiquate come le banche. Anche i metodi di pagamento online che sono nati in contemporanea con internet, come l'esempio più ovvio di PayPal, richiedono l'integrazione con un conto

bancario o una carta di credito per essere utilizzati.

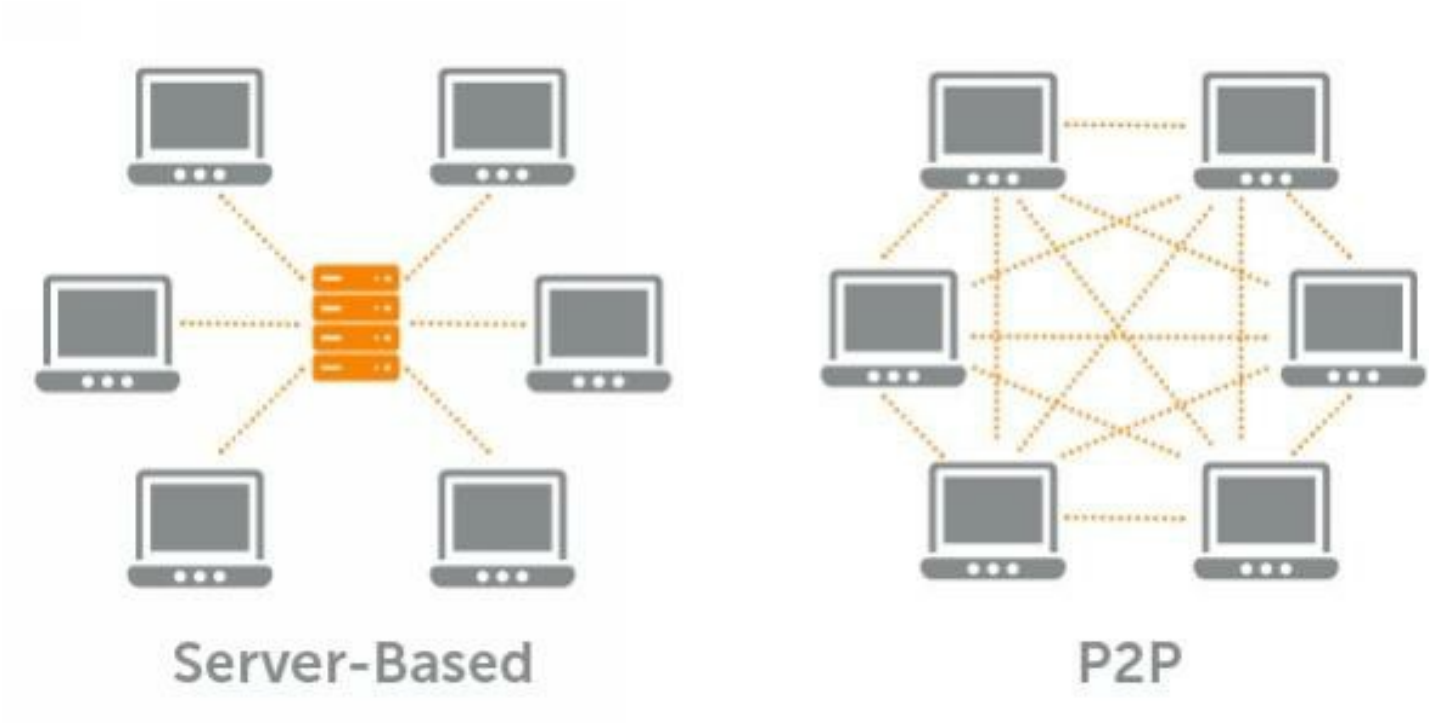
La tecnologia Blockchain offre l'intrigante possibilità di eliminare questo passaggio di mezzo, colmando tre ruoli importanti: registrando transazioni, stabilendo identità e stabilendo contratti tradizionalmente eseguiti dal settore dei servizi finanziari. Ciò potrebbe avere implicazioni enormi perché, a livello mondiale, il mercato dei servizi finanziari è il più grande settore dell'industria per capitalizzazione di mercato. Sostituire anche una minima parte di questo con un sistema blockchain comporterebbe un enorme perdita per il settore dei servizi

finanziari, ma anche un massiccio aumento delle efficienze. Il potenziale che esso offre alle aziende rappresenta un'alternativa digitale sicura ai processi bancari che sono in genere burocratici, dispendiosi in termini di tempo, pesanti e costosi.

Quali sono le differenze tra la Blockchain e le architetture server standard?

Le applicazioni che usufruiscono delle architetture standard, devono configurare i propri server in modo tale

da eseguire il codice in maniera isolata. Se una singola app viene compromessa o va offline, tutti gli utenti e altre app ne sono interessati. Utilizzando una rete blockchain, chiunque può configurare un nodo che possa replicare i dati necessari a tutti i nodi. Ciò consente ai dati degli utenti di rimanere privati e alle app di essere decentralizzate come, agli esordi, si era pensato dovesse funzionare internet.



Le peculiarità della tecnologia Blockchain:

Decentralizzazione e Sicurezza:

L'intero registro degli eventi organizzato in blocchi è distribuito e memorizzato sui diversi nodi della rete, non esiste un unico punto centrale

contenente la totalità delle informazioni, in modo che i malintenzionati non possano sfruttare questa centralizzazione per abbattere l'intero sistema. Ogni utente nel sistema decentralizzato possiede una copia della blockchain. Non esiste nessuna copia ufficiale centralizzata e nessun utente è più credibile di altri, tutti sono allo stesso livello. Inoltre tutti gli eventi possono essere fatti risalire con certezza alle identità digitali che li hanno generati, attraverso l'utilizzo di meccanismi di crittografia a chiave pubblica. La chiave pubblica è un indirizzo sulla rete blockchain. La chiave privata, invece, è come una password che permette soltanto al suo proprietario di accedere

alle proprie risorse digitali oppure di interagire con le varie funzionalità della blockchain.

Incontestabilità:

La decisione riguardante la validità di un'informazione non viene presa unilateralmente, ma attraverso un meccanismo di raccolta del consenso all'interno della rete, rendendo così particolarmente difficile metterne in discussione l'esito.

Inalterabilità:

I dati che sono stati scritti all'interno della Blockchain non possono essere modificati, se non attraverso specifiche

regole del protocollo che definiscono rigorosamente le modalità con cui si possono effettuare cambiamenti.

Tracciabilità:

A tutti gli eventi registrati vengono assegnati un identificativo e una marca temporale che li rende facilmente tracciabili e verificabili.

Programmabilità:

All'interno dei blocchi possono essere incluse istruzioni che facciano scatenare specifiche azioni al verificarsi certe condizioni.

Cosa è un "Hard Fork" ?

Per quanto riguarda la tecnologia blockchain, un hard fork è una modifica radicale del protocollo che rende validi blocchi o transazioni precedentemente invalidi (o viceversa) e richiede che tutti i nodi o gli utenti eseguano l'aggiornamento all'ultima versione del software di protocollo. In altre parole, un Hard Fork è una divergenza permanente rispetto alla versione precedente della blockchain, e i nodi che eseguono ancora la vecchia versione non saranno più accettati da quella più recente. Questo essenzialmente crea una biforcazione nella catena a blocchi, un percorso che segue la nuova blockchain aggiornata e un percorso che continua lungo il vecchio percorso.

Generalmente, dopo un breve periodo di tempo, quelli della vecchia catena si renderanno conto che la loro versione della blockchain è obsoleta o irrilevante e si aggiornano rapidamente alla versione più recente.

Un hard fork può essere implementato per correggere importanti rischi per la sicurezza che si trovano nelle versioni precedenti del software, per aggiungere nuove funzionalità o per invertire le transazioni (es. invertire un hackeraggio).

La rete Blockchain può avere più funzionalità.

La maggior parte di internet è centralizzato. Ad esempio consideriamo Facebook, i suoi dati si trovano sui suoi server. Il computer richiede informazioni dal server di Facebook in base alle necessità dell'utente. Per la blockchain invece non esiste nessun server centrale, essa è costituita da tutti i computer degli utenti che fanno parte della rete.

Sebbene comunemente associato a Bitcoin, la tecnologia blockchain ha molte altre applicazioni che vanno ben oltre le valute digitali. Bitcoin è solo una delle centinaia di applicazioni che utilizzano la tecnologia blockchain oggi. La catena a blocchi quindi può avere più funzionalità, ed essere utilizzata per

qualsiasi cosa, ad esempio per un social network, per una piattaforma di intrattenimento o anche per il commercio. Credo dunque che la blockchain sia un progresso tecnologico che avrà implicazioni di ampia portata che non trasformeranno solo i servizi finanziari. I potenziali usi di questa tecnologia sono enormi, e prevedo che sempre più imprese ed industrie troveranno il modo di utilizzarla nel prossimo futuro. Secondo alcuni autori ha addirittura il potenziale per risolvere il problema della disuguaglianza sociale, cambiando il modo in cui la ricchezza viene redistribuita.

BITCOIN

Il Bitcoin (BTC o XBT) è una valuta digitale creata nel gennaio 2009 , l'obiettivo prefissato era principalmente quello di rendere più semplici, anonimi e sicuri i pagamenti online. Ad oggi è la

prima criptomoneta per valore nonchè la più conosciuta dalle masse. Da molti esperti non è considerata propriamente una valuta in quanto molto volatile e quindi soggetta ad elevate fluttuazioni di valore. Non è riconosciuta nè regolamentata da nessun ente centrale.

No alle Banche centrali!

La struttura della rete Bitcoin rende impossibile a qualunque autorità, governativa o meno, il blocco dei trasferimenti o il sequestro di bitcoin senza il possesso delle relative chiavi. Il Bitcoin si pone quindi in maniera ben precisa, estremamente ostile all'intervento delle banche centrali, un

concetto tornato alla ribalta dopo la crisi del 2008 e gli interventi di quantitative easing ed easy money messi in atto dalla FED e da altre banche centrali in giro per il mondo. Interventi che, con l'immissione di ingente liquidità nel sistema per salvare le banche dalla crisi di liquidità dovuta alla perdita di valore dei titoli in derivati, hanno impopolarmente portato il dollaro a inflazionarsi, con conseguente perdita di valore del risparmio privato.

Ma cos'è realmente il bitcoin?

Il Bitcoin è esploso in un tempo relativamente breve. Grandi ed

importanti società in tutto il mondo hanno iniziato ad accettare la sua valuta ed è oggi possibile acquistare merci e beni tangibili oltre che per servizi online. Per dirla nella modo più semplice possibile è una valuta virtuale che tramite lo scambio di informazioni digitali consente di acquistare o vendere beni e servizi. La transazione garantisce sicurezza e affidabilità tramite la rete Blockchain.

Una forte tendenza deflazionistica

La rete Bitcoin è progettata per generare matematicamente non più di 21 milioni di bitcoin, nel 2013 sono state generate metà delle possibili monete e

nel 2017 siamo arrivati ai tre quarti, in meno di 32 anni verranno generate tutte le monete. É stata progettata per autoregolarsi all'inflazione e nessun ente centrale può ridistribuire la ricchezza tra gli utenti mediante la svlautazione da immissione di nuova moneta. Non è possibile controllarne il valore a causa della natura decentralizzata del metodo di creazione della valuta, quest'ultimo quindi è affidato al libero mercato e precisamente alle forze della domanda e dell'offerta. Se c'è una caratteristica che da sempre ha distinto l'economia del Bitcoin, questo è la forte tendenza deflazionistica, programmata nella valuta stessa.

Da dove vengono i Bitcoin?

Forse avrai sentito parlare di "mining", ma dal terreno non viene estratta nessuna moneta, quindi da dove vengono i bitcoin? Il processo potrebbe essere paragonato all'estrazione dell'oro, in quanto i bitcoin esistono nel progetto del protocollo (proprio come l'oro esiste nel sottosuolo), ma non sono stati ancora portati alla luce (proprio come l'oro non è stato ancora dissotterrato). Il protocollo bitcoin, come ho detto, prevede che a un certo punto esistano 21 milioni di monete. Ciò che fanno i "minatori" è portarli alla luce, pochi alla volta come ricompensa per la creazione e l'inclusione di

blocchi di transazioni convalidate nella blockchain.

Cosa sono i nodi ?

Un nodo è semplicemente un computer che esegue il software bitcoin e aiuta la rete partecipando alla trasmissione e all'elaborazione di informazioni. Chiunque può eseguire un nodo, basta scaricare il software bitcoin (gratuito) e lasciare aperta una determinata porta (l'unico svantaggio è che consuma energia e spazio di archiviazione - la rete al momento della scrittura occupa circa 145 GB). I nodi distribuiscono le transazioni bitcoin sulla rete. Un nodo invierà informazioni ad alcuni nodi che conosce, che trasmetteranno le informazioni ai nodi che conoscono, ecc.

Costi di transazione

Visto che i nodi non hanno l'obbligo di includere le transazioni nei blocchi che generano, chi invia bitcoin potrà volontariamente pagare una tassa di trasferimento. Facendo questo la velocità di trasferimento aumenterà e offrirà un incentivo agli utenti per tenere attivi i nodi, specialmente quando la difficoltà per generare bitcoin aumenterà o se la quantità di premio per blocco decrescerà nel tempo. I nodi collezionano le tasse di transazione associate a tutte le transazioni presenti nel loro blocco dedicato.

Proprietà delle transazioni in

Bitcoin:

I bitcoin possono essere spesi inoltrando una richiesta di trasferimento da un indirizzo Bitcoin nel portafoglio del cliente a un indirizzo Bitcoin nel portafoglio del venditore.

Irreversibile:

Dopo la conferma, una transazione non può essere annullata. Da nessuno e nessuno significa nessuno. Non tu, non la tua banca, non il presidente degli Stati Uniti, non Satoshi. Nessuno può aiutarti, se hai inviato i tuoi fondi a un truffatore o se un hacker li ha rubati dal tuo

computer.

Anonimo:

Né le transazioni né i conti sono collegati alle identità del mondo reale. Ricevi Bitcoin sui cosiddetti indirizzi, che sono stringhe di circa 30 caratteri. Mentre è generalmente possibile analizzare il flusso delle transazioni, non è possibile collegare l'identità del mondo reale degli utenti con tali indirizzi. Per utilizzare i propri bitcoin è neccessario memorizzare i dati su di un computer oppure uno smartphone, sotto forma di portafoglio digitale, o mantenuti presso terze parti che svolgono funzioni simili a una banca.

Veloce e globale:

La transazione viene propagata quasi istantaneamente nella rete e viene confermata in qualche minuto (se la rete non è sovraccarica). Dal momento che avvengono in una rete globale di computer, la tua posizione fisica è completamente ininfluente. Non importa se invii Bitcoin al tuo vicino o a qualcuno dall'altra parte del mondo.

Sicuro:

I fondi in Bitcoin sono bloccati in un sistema di crittografia a chiave pubblica. Solo il proprietario della chiave privata può inviare criptovaluta. La crittografia e la magia dei grandi numeri rendono un

indirizzo Bitcoin più sicuro di Fort Knox.

Senza autorizzazioni:

Non devi chiedere nessun permesso per poter usare Bitcoin. Hai bisogno soltanto di un software. Dopo averlo installato, puoi ricevere e inviare Bitcoin o altre criptovalute e nessuno può impedirtelo.

La tecnologia a cui fà affidamento il Bitcoin consente a due entità di scambiare tra loro fondi in tutta sicurezza, senza la necessità di fare affidamento su di un intermediario. La chiave è la matematica.

Bitcoin utilizza la crittografia a chiave pubblica e un approccio innovativo alla contabilità per ottenere l'autorizzazione, la verifica dell'equilibrio, il divieto di doppia spesa, la consegna dei fondi e l'inalterabilità dei record. E il tutto viene realizzato quasi in tempo reale senza alcun costo.

ETHEREUM

Quando nel 2009 è stato creato il Bitcoin, si è scatenato un movimento sociale e tecnologico.È stata la prima tecnologia che ci ha permesso di inviare denaro in tutta sicurezza su Internet, senza timore di frodi o censure. Tuttavia, diversi pionieri videro alcune potenzialità nella tecnologia sottostante che alimentava il sistema di pagamento sicuro: la blockchain.

Ciò che inizialmente consentiva a molte persone di inviare denaro, aveva anche il potenziale per decentralizzare Internet come lo conosciamo.

Bitcoin non era progettato per inviare grandi quantità di dati per ogni transazione, né era in grado di eseguire

calcoli che non si adattavano al suo limitato linguaggio di progettazione. Il creatore di Bitcoin, riteneva che limitare la funzionalità del sistema avrebbe migliorato significativamente la sicurezza.

Ma Vitalik Buterin un giovane programmatore russo-canadese, il creatore di "Ethereum", ha immaginato le cose in modo differente.

Buterin è rimasto un membro attivo della community Bitcoin fino a quando, nel 2014, a soli 20 anni, rendendosi conto delle potenzialità dei DLT (sistemi distribuiti) e in particolare della Blockchain, ha deciso di sviluppare

Ethereum: una piattaforma attraverso la quale i programmatori possono sviluppare applicazioni decentralizzate (DApp) senza dover "costruire" una nuova blockchain.

Anche se il rilascio del White Paper di Ethereum avviene verso la fine del 2013, il progetto prende concretamente forma nel 2014 quando con gli altri sviluppatori del team Mihai Alisie, Anthony Di Iorio, e Charles Hoskinson, Buterin fonda la società, con sede legale in svizzera, Ethereum Switzerland GmbH. Subito dopo il team darà vita anche ad una organizzazione no-profit: l'Ethereum Foundation.

Grazie ad una ICO lanciata nel luglio

2014, l'Ethereum Foundation raccoglie circa 5000 BTC in poco più di un mese. Grazie a questa cospicua somma il team capitanato da Buterin lancia la piattaforma Ethereum.

Cosa è Ethereum?

Ethereum (ETH) è una piattaforma decentralizzata che gestisce contratti intelligenti: applicazioni che funzionano esattamente come programmato senza alcuna possibilità di inattività, censura, frode o interferenza da parte di terzi.

Queste app utilizzano una blockchain costruita su misura, un'infrastruttura globale condivisa enormemente potente in grado di valorizzare e rappresentare la proprietà dei contenuti.

Ciò consente agli sviluppatori di registrare contratti per debiti o futuri pagamenti, spostare fondi in conformità con le istruzioni impartite in passato (come un testamento o un contratto futures) e molte altre cose che non sono ancora state inventate, tutte senza intermediari o rischio di controparte.

Cosa sono gli Smart Contracts?

Ethereum quindi a differenza di Bitcoin non è una rete utilizzata soltanto come scambio di valore monetario, ma anche per eseguire smart contracts. Un contratto intelligente è un protocollo informatico pensato per facilitare, verificare o imporre in modo digitale la negoziazione o l'esecuzione di un contratto. I contratti intelligenti consentono l'esecuzione di transazioni credibili senza il bisogno di terze parti. Queste transazioni sono tracciabili e irreversibili.

I sostenitori dei contratti intelligenti sostengono che molti tipi di clausole contrattuali possono essere parzialmente o completamente autoeseguiti,

autoaggiustati o entrambi.

L'obiettivo dei contratti intelligenti è fornire una sicurezza superiore al tradizionale diritto contrattuale e ridurre gli altri costi di transazione associati alla contrattazione. Un contratto intelligente in ogni caso non è necessariamente correlato al concetto classico di un contratto, ma può essere qualsiasi tipo di programma per computer.

Varie criptovalute hanno implementato tipi di contratti intelligenti.

L' Ethereum Virtual Machine EVM

Ci sono moltissimi progetti diversi da seguire nel mondo delle criptovalute quindi risulta abbastanza difficile conoscere tutto. L'Ethereum Virtual Machine, anche conosciuta come EVM, è un progetto piuttosto ingegnoso che molte persone ignorano. È importante capire di cosa tratta, in quanto fornisce alcuni vantaggi interessanti allo sviluppo di Ethereum.

L'EVM è il vero elemento innovativo introdotto da Buterin: infatti grazie a questa "macchina virtuale", che nel concreto ha le stesse funzionalità di un computer fisico, gli utenti possono scrivere degli smart-contracts in un ecosistema tutelato e sconnesso

totalmente da inferenze esterne.

Rappresenta di fatto l'ambiente di runtime per lo sviluppo e la gestione di Smart contracts in Ethereum.

EVM opera in modo protetto essendo completamente separato dalla rete.

Il codice gestito dalla Virtual Machine non ha accesso alla rete e gli stessi smart contracts generati sono indipendenti e separati.

Ethereum è un sistema "Turing complete" che permette agli sviluppatori di creare applicazioni che girano sulla EVM utilizzando linguaggi di programmazione che fanno a loro volta

riferimento a piattaforme tradizionali come javascript e python.

Inoltre la macchina virtuale assicura che i nodi, poiché tutti processano implementazioni dell' EVM, si comportino esattamente secondo le "istruzioni" postulate nei codici.

Cosa sono le DApp? E quali sono i possibili usi?

Le applicazioni blockchain bastate su Ethereum sono generalmente definite DApp (decentralized application), poiché si basano sulla EVM decentralizzata e sui suoi contratti

intelligenti.

Molti usi sono stati proposti per la piattaforma Ethereum, le proposte di casi d'uso includono: la finanza, l'internet-of-things (estensione di Internet al mondo degli oggetti), socialmedia, piattaforme di crowfunding, videogames, l'approvvigionamento e il prezzo dell'elettricità, le scommesse sportive ecc.

Ethereum è (a partire dal 2017) la piattaforma blockchain leader per le ICO (Initial Coin offering), con una quota di mercato superiore al 50% .

Ethereum, grazie alla tecnologia

dell'EVM e dei contratti intelligenti, ha dato la possibilità ai programmatori di sviluppare applicazioni decentralizzate gestite in modo completamente democratico dal network.

Ovviamente, come tutte le tecnologie innovative, questa non ha ancora raggiunto il suo pieno potenziale e non è immune da criticità. Proprio per questo motivo gli sviluppatori continuano a lavorare su nuovi protocolli e nuovi aggiornamenti.

Ethereum vs Ethereum Classic

Se hai mai dato un'occhiata alle principali criptovalute ti sarai sicuramente accorto che esistono due diversi tipi di Ethereum: uno è Ethereum (ETH) e l'altro è Ethereum Classic (ETC).

Le due criptomonete non solo condividono lo stesso nome, ma anche una storia interessante che può considerarsi uno degli eventi più cruciali nella storia delle "cripto". La battaglia tra Ethereum e Ethereum Classic è una questione di etica e di ideologia. Un furto da 50 milioni di dollari eseguito da un hacker o da un gruppo di hacker, ha portato alla scissione di Ethereum.

Come è nato Ethereum e come si confronta con Ethereum Classic:

Il momento più cruciale della separazione tra Ethereum e Ethereum Classic ha a che fare con un'organizzazione nota come DAO (Decentralized Autonomous Organization). Il DAO era essenzialmente una sorta di fondo che avrebbe finanziato applicazioni decentralizzate (DAPP) basate sull'ecosistema Ethereum.

DAO era stato ideato in modo tale da consentire ai suoi membri il potere di scegliere quali DAPP finanziare.

Gli investitori avrebbero comprato i token DAO utilizzando Ether come valuta di cambio, i token DAO avrebbero poi integrato i titolari nel sistema dando loro un certo potere di voto.

Il modo in cui le DAPP potevano essere approvate era un processo piuttosto semplice. Se la proposta avesse ottenuto un'approvazione del 20% durante le votazioni una quota dei fondi DAO necessaria per iniziare, sarebbe stata elargita al progetto.

Il meccanismo piuttosto flessibile e il potenziale apparentemente immenso offerto dal DAO aveva attirato fin da subito una grande attenzione, infatti

soltanto ad un mese dalla formazione il DAO aveva già raccolto oltre $ 150 milioni di eterh.

Al suo apice, sebbene il DAO avesse raccolto una cifra ragguardevole con il crowdfunding, ha avuto seri problemi di sicurezza ed il 17 giugno 2016, alcuni hacker sono riusciti a sottrarre circa 50 milioni di dollari.

A quel tempo, il DAO possedeva un'enorme percentuale (circa il 14%) della quantità totale di Ether esistente. Con 50 milioni rubati, circa un terzo dei fondi iniziali del DAO, la comunità Ethereum ha rapidamente iniziato a cercare soluzioni a questo problema.

La maggioranza decretò che Ethereum avesse bisogno di un fork per creare qualcosa di nuovo. Questo "qualcosa di nuovo" è ciò che ora vediamo come Ethereum (ETH) mentre Ethereum Classic (ETC) è, come suggerisce il nome, il primo Ethereum che utilizza ancora la blockchain originale.

La decisione di dividersi naturalmente ha causato molti contrasti e polemiche, e sebbene la maggioranza abbia votato per il fork della blockchain, c'è ancora una piccola ma significativa percentuale (circa il 10%) di persone fedeli alla blockchain originale. La catena Ethereum che ha attuato il fork è stata in grado di recuperare i 50 milioni che

erano stati rubati.

Ethereum (ETH) funziona su una nuovissima blockchain e la stragrande maggioranza di utenti della precedente versione di Ethereum utilizza questa nuova versione.

Comunque sia Ethereum Classic (ETC) esiste ancora, sebbene la sua comunità sia notevolmente inferiore rispetto ad Ethereum (ETH), che d'altra parte, è più simile ad una società di software che vuole crescere e potrebbe subire altri hard-fork in futuro. L'ETH ha principalmente valore a causa dei molteplici casi d’uso e del sostegno della comunità, infatti Ethereum è supportato da aziende prestigiose come

Accenture, JP Morgan, Microsoft e UBS.

Confronto con il Bitcoin

Ethereum è diverso da Bitcoin sotto diversi aspetti:

- Il tempo impiegato per elaborare ogni blocco (block time) è compreso tra 14 e 15 secondi, rispetto ai 10 minuti circa per

bitcoin.

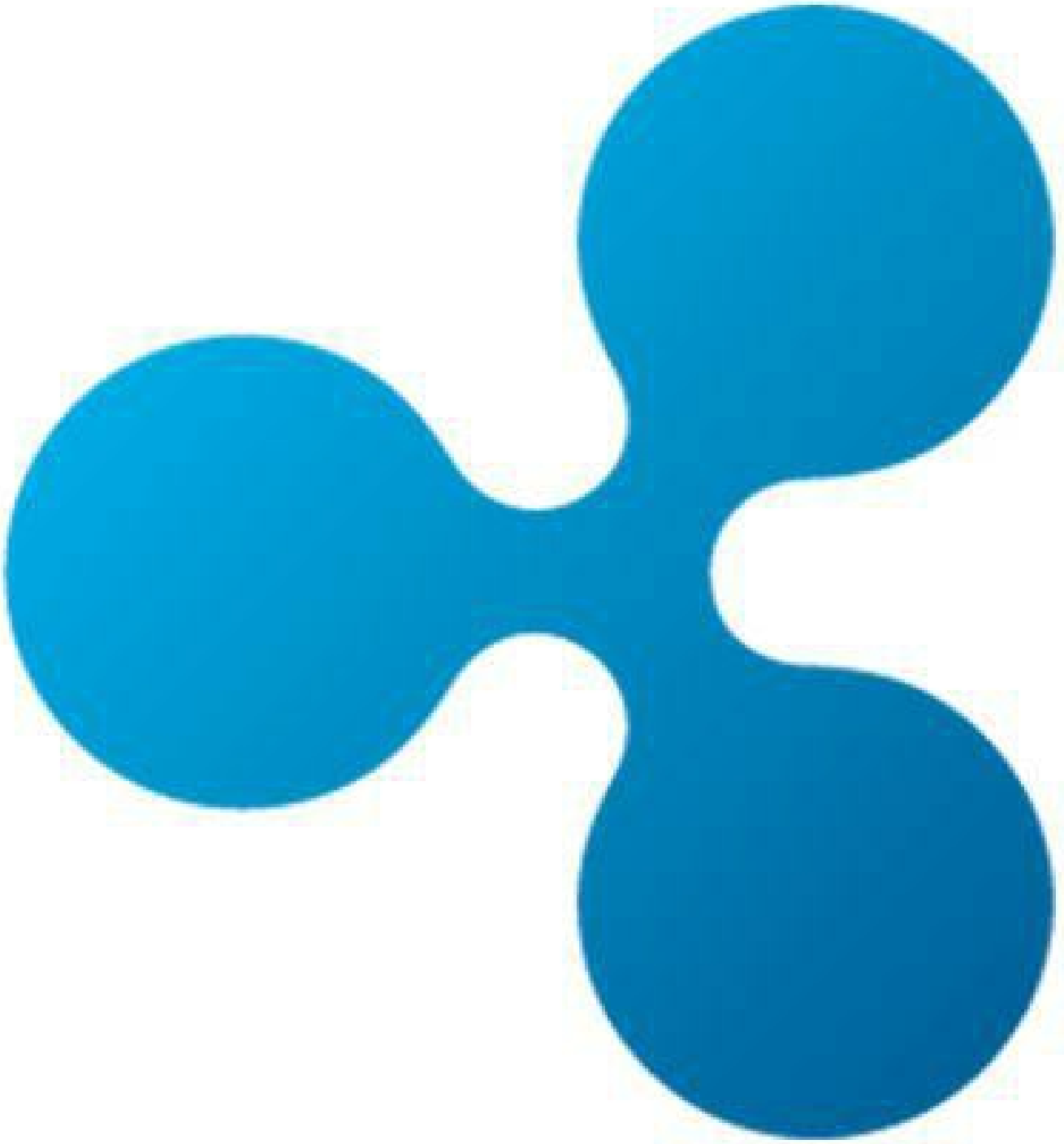
- L'estrazione di ETH genera nuove monete ad un tasso solitamente costante, variando occasionalmente, mentre per il bitcoin il tasso si dimezza ogni 4 anni.

- Le commissioni di transazione in Ether differiscono per complessità computazionale, utilizzo della

larghezza di banda e necessità di archiviazione (un sistema noto come gas), mentre per il trasferimento di Bitcoin si distinguono in base alla dimensione della transazione, in byte .

- Le commissioni di transazione sono generalmente molto più basse per l'Eterh che per il Bitcoin. A dicembre 2017, la commissione media per l'ETH corrispondeva a $ 0,33, mentre per il BTC corrispondeva a $ 23.

RIPPLE



Sebbene il bitcoin sia tuttora il re della criptovalute, ci sono molti pretendenti al trono.

Uno dei più intriganti, che ha fatto parlare molto di sè durante il boom di Dicembre 2017 è Ripple, una criptovaluta molto più centralizzata rispetto alle altre.

Cos'è Ripple?

Ripple opera in modo molto diverso dalle criptovalute concorrenti. Rilasciato nel 2012, Ripple intende abilitare "transazioni finanziarie globali sicure, immediate e quasi gratuite, di qualsiasi dimensione senza chargeback". Il protocollo open source

di Ripple è pensato per facilitare le transazioni tra le istituzioni finanziarie. Ciò consente alle società di servizi finanziari di effettuare pagamenti direttamente tra loro in modo più efficiente rispetto ai metodi tradizionali. Il protocollo consente alle banche e alle società di servizi finanziari non bancari di incorporare il protocollo Ripple nei propri sistemi e quindi permette ai propri clienti di utilizzare il servizio.

Ripple è il nome della piattaforma, il protocollo che gestisce le transazioni in XRP che è la valuta nativa della rete ed esiste solamente in questi sistemi. Come altre criptovalute, Ripple si basa sull'idea di una rete di utenti distribuiti

che richiede di partecipare alla convalida delle transazioni, piuttosto che a qualsiasi singola autorità centralizzata. Ciò facilita le transazioni in tutto il mondo e le tariffe di trasferimento sono molto più economiche di quelle del bitcoin. A differenza di altre criptovalute, i trasferimenti XRP sono effettivamente immediati e non richiedono tempi di conferma tipici.

Ripple è stato originariamente fondato da Ripple Labs,da cui continua ad essere supportato. Ripple non ha una quantità variabile di XRP a differenza dei Bitcoin che hanno un numero in continua crescita con un limite massimo

raggiungibile e Ethereum che teoricamente non ha limiti, Ripple fin dall'inizio ha emesso tutti i suoi 100 miliardi di token XRP. Questo numero viene mantenuto senza attività di mining e la maggior parte dei token è di proprietà e detenuta da Ripple Labs stessa.

Ripple Labs è attualmente in possesso di circa $ 60 miliardi di valore di XRP (il prezzo di Ripple è crollato di recente e potrebbe valere molto meno di $ 60 miliardi mentre leggi). Nel maggio 2017, per alleviare le preoccupazioni relative all'offerta di XRP, Ripple si è impegnata a collocare 55 miliardi (l'88% delle sue partecipazioni in XRP)

in un deposito di garanzia crittografato, che gli consente di vendere fino a un miliardo di dollari al mese, per finanziare nuovi progetti e acquisizioni. La vendita di una tale quantità avrebbe probabilmente un effetto drastico sul valore della criptovaluta e non è qualcosa che Ripple Labs intende fare in qualunque momento.

Servirsi di questa strategia mantenendo “congelati” gli XRP imiterà l'effetto del mining visto in altre valute come il bitcoin e farà sì che la valuta manterrà il suo prezzo in costante crescita. La distribuzione di XRP e il loro movimento possono essere monitorati attraverso il sito Web di Ripple Charts.

Ripple Labs sta cercando di sfruttare la tecnologia dietro XRP per consentire transazioni bancarie più veloci in tutto il mondo. Mentre bitcoin e altre criptovalute si basano sull'idea di separare le transazioni finanziarie dalle organizzazioni finanziarie delle valute tradizionali, Ripple su questo piano si pone praticamente all'opposto.

Ripple è un po' centralizzato

Dato che Ripple Labs detiene circa 61,4 miliardi di token XRP, non è molto difficile capire che Ripple è centralizzato, o almeno molto più della maggior parte delle altre criptovalute. Tuttavia, Brad Garlinghouse (CEO e

fondatore di Ripple), la vede diversamente.

Nel maggio 2017, Ripple ha pubblicato la sua strategia di decentralizzazione; ed inoltre ha annunciato i piani per diversificare i validatori sul registro XRP e li ha espansi fino a 55 nodi di validazione nel luglio 2017. Ripple ha anche condiviso piani per aggiungere nodi di convalida di terze parti, rimuovendo un nodo di convalida gestito da Ripple per ogni due nodi di terze parti , finchè non esisterà nemmeno una singola entità che gestirà la maggioranza dei nodi affidabili.

Ripple si potrebbe quindi definire un pò centralizzato ed un pò

decentralizzato. Essere centralizzati non è necessariamente una cosa negativa, ma dissuade molti ideologi della decentralizzazione all'interno della comunità delle criptovalute.

Sostenuto dalle banche

Sicuramente avrai sentito discutere molti investitori e commentatori finanziari riguardo all'idea di una regolamentazione delle criptovalute. Anche se non penso che questo possa dare qualche preoccupazione significativa, molti sono impauriti dal fatto che le banche possano prendere provvedimenti e inasprire i controlli per

Bitcoin &co.

Questo scenario è molto meno probabile che possa presentarsi con Ripple, poiché è supportato da alcune delle maggiori istituzioni finanziarie del mondo. Santander, UBS, American Express, RBC, Westpac e altre ancora. Queste banche possono anche addebitare le proprie tariffe specifiche per il completamento delle transazioni. Il più grande fattore di differenziazione per Ripple è quindi il controllo .

Confronti con la concorrenza

Sebbene XRP sia la terza criptovaluta per capitalizzazione di mercato, molti esperti hanno descritto

Ripple come un rivale emergente del bitcoin. Ripple è stato descritto come un concorrente significativo, in parte grazie ai suoi trasferimenti internazionali di denaro in tempo reale. Tra i tanti Bill Gates ha supportato questa visione e ha menzionato il sistema Ripple quando ancora nel 2014 gli è stato chiesto del bitcoin, affermando che "ci sono molte cose che Bitcoin o Ripple possono fare per rendere più facile spostare denaro tra paesi e ridurre drasticamente le tasse. Ma bitcoin non sarà il sistema dominante. "

La differenza più importante è che Bitcoin è un sistema decentralizzato che non è di proprietà di alcun governo,

banca o terza parte nonostante sia stato avviato da qualcuno. D'altra parte, Ripple è di proprietà di Ripple Labs.

I BTC invece sono sparsi in tutto il mondo, infatti il portafolgio più ricco contiene solo l'1% di tutti i Bitcoin ed è un exchange. La distirbuzione delle monete risulta quindi essere molto più centralizzata in Ripple, dove Ripple Labs possiede il 60% di XRP.

La rete Ripple presenta diversi vantaggi rispetto al bitcoin poiché sono stati progettati con obiettivi leggermente diversi. Bitcoin è stato creato come riserva di valore, mentre XRP è stato creato per digitalizzare le transazioni tra le banche all'interno del sistema.

Veloce ed economico

L'elaborazione delle transazioni in Ripple richiede solo quattro secondi poiché è significativamente meno attiva rispetto al bitcoin. Questo ha il vantaggio aggiuntivo di commissioni di transazione più economiche, mentre il prezzo per le transazioni in bitcoin è in aumento ultimamente dal momento che sempre più persone si sono interessate alla piattaforma.

Mining free

Come detto prima, esistono già tutti i 100 miliardi di XRP. Anche se non sono tutti sul mercato, non c'è bisogno di

minare in quanto non c'è più valore da aggiungere, a differenza delle criptovalute più tradizionali.

LITECOIN

Cos'è Litecoin?

Sempre più persone stanno abbracciando il mondo della criptovalute, molte di queste sono alla ricerca di opportunità di investimento, Litecoin sembra essere una alternativa a Bitcoin ed Ethereum abbastanza popolare. Il prezzo del Litecoin infatti è aumentato del 7.291% dall'inizio del 2017, in confronto, il Bitcoin è aumentato “solo” del 1731%.

Le origini di Litecoin

Mentre l'identità del creatore di Bitcoin è abbastanza misteriosa, il creatore di Litecoin, Charlie Lee, è molto attivo sui social media e sul suo blog. Charlie Lee è un ex dipendente di

Google che ha avuto l'intuizione di creare una versione più leggera del Bitcoin.

Mentre Bitcoin è considerato una riserva di valore per scopi a lungo termine, Litecoin è visto un mezzo di transazione per scopi più economici e quotidiani, al momento è la seconda valuta minabile a più alta capitalizzazione. Il 7 ottobre 2011, Litecoin è stato rilasciato tramite un client open source su GitHub. La Rete Litecoin è stata attivata dal 13 ottobre 2011. È fondamentalmente un fork del client Bitcoin Core.

Quali sono le differenze tra

Litecoin e Bitcoin?

Se vogliamo veramente capire Litecoin non c'è niente di meglio che raffrontarlo con il Bitcoin. Litecoin, è un clone di Bitcoin eppure le due criptovalute differiscono anche per importanti aspetti. Di seguito, confronterò le loro differenze più importanti, passando dalle più semplici alle più complesse.

Quantità totale di monete

Una delle principali differenze tra Bitcoin e Litecoin riguarda il numero limite totale di monete. La rete Bitcoin non potrà mai superare i 21 milioni di monete, mentre Litecoin potrà

raggiungere fino a 84 milioni di monete. Potrebbe sembrare un significativo vantaggio nei confronti del Litecoin, ma i suoi reali effetti possono essere trascurabili. Ciò è dovuto al fatto che sia Bitcoin che Litecoin sono divisibili in quantità quasi infinitesimali. In effetti, la quantità minima di bitcoin trasferibile è cento milionesimi di BTC (0,00000001 btc) conosciuti colloquialmente come un "satoshi". Gli utenti di entrambe le valute non dovrebbero quindi avere difficoltà ad acquistare beni o servizi a basso prezzo, indipendentemente dall'alto valore che può assumere un singolo Bitcoin o Litecoin. Nonostante ciò, il maggior numero di monete di Litecoin potrebbe offrire un vantaggio

psicologico rispetto a Bitcoin, a causa del suo prezzo (finora) inferiore per una singola unità. In una video intervista pubblicata dalla divisione bancaria di IBM nel novembre 2013, l'executive di IBM Richard Brown ha sollevato la prospettiva che alcuni utenti preferiscano effettuare transazioni in unità intere piuttosto che in frazioni di unità: un potenziale vantaggio per Litecoin. Tuttavia, supponendo che sia vero , questo problema può essere risolto attraverso semplici modifiche apportate al software dei portafogli digitali attraverso cui vengono effettuate le transazioni Bitcoin. Come sottolinea Tristan Winters in un articolo di Bitcoin Magazine del novembre 2013, "The

Psychology of Decimals", i wallet Bitcoin come Multibit ed Electrum offrono già agli utenti la possibilità di mostrare il valore dei loro btc in termini di valute ufficiali (o fiat) tali come il dollaro USA. Questo può aiutare a eludere l'avversione psicologica nel trattare le frazioni quando si usa il bitcoin.

Differenze di transazione

La differenza principale è che la rete Litecoin può confermare le transazioni molto più velocemente della rete Bitcoin. Sebbene tecnicamente le transazioni avvengano istantaneamente su entrambe le reti Bitcoin e Litecoin, è

necessario del tempo affinché tali transazioni possano essere confermate da altri partecipanti alla rete. Secondo i dati di Blockchain.info, il tempo medio di conferma delle transazioni a lungo termine della rete Bitcoin è di poco più di 9 minuti per transazione. La cifra equivalente per Litecoin è di circa 2,5 minuti, secondo i dati di BitInfoCharts.com.

- Litecoin è in grado di gestire un volume maggiore di transazioni grazie alla generazione di blocchi più rapida. Bitcoin richiederebbe aggiornamenti significativi del codice attualmente in esecuzione per poter competere.

- Lo svantaggio di questo volume maggiore di blocchi è che la blockchain di Litecoin sarà proporzionalmente più grande di quella di bitcoin, con più blocchi orfani (Blocchi validi che non fanno parte della main chain. Possono verificarsi in modo naturale quando due minatori producono blocchi in momenti simili).

- Il block-time più veloce di Litecoin riduce il rischio di attacchi a doppia spesa (nel caso in cui entrambe le reti abbiano la stessa potenza di hashing).

- Ipotizzando di attendere per un minimo di due conferme con Litecoin avremmo impiegato solo cinque minuti, mentre avremmo dovuto aspettare 10 minuti per una sola conferma con bitcoin. Questa differenza potrebbe rendere più attraente Litecoin ai commercianti

che comunque possono sempre optare per accettare le transazioni senza attendere alcuna conferma. La sicurezza di tali transazioni a conferma zero è oggetto di alcuni dibattiti. Tuttavia, recenti innovazioni come il sistema di pagamenti proposto da Bitpay (soprannominato "Impulse") possono rendere questo tipo di transazioni istantanee significativamente più sicure, mitigando il vantaggio di tempo di conferma più veloce di Litecoin.

Algoritmi differenti: SHA-256 vs Litecoin Scrypt

Anche Litecoin è una criptovaluta minabile, la motivazione alla base della sua creazione era di migliorare il Bitcoin.

Di gran lunga la differenza tecnica più fondamentale tra Bitcoin e Litecoin sono i diversi algoritmi crittografici che impiegano. Bitcoin utilizza il vecchio algoritmo SHA-256, mentre Litecoin utilizza un algoritmo relativamente nuovo noto come Scrypt.

L'uso di questi diversi algoritmi influisce principalmente sul processo di "estrazione" di nuove monete. Sia per Bitcoin che Litecoin, il processo di conferma delle transazioni richiede una notevole potenza di calcolo.

Bitcoin infatti utilizza l'algoritmo hash SHA-256, che implica calcoli che possono essere notevolmente accelerati nell'elaborazione parallela. Di conseguenza, i minatori Bitcoin negli ultimi anni hanno utilizzato metodi sempre più sofisticati per estrarre bitcoin nel modo più efficiente possibile. È questa caratteristica che ha dato origine all'intensa corsa nella tecnologia ASIC e ha causato un aumento esponenziale del livello di difficoltà nel minare bitcoin, con la conseguenza di rendere il processo di estrazione improduttivo per gli utenti di tutti i giorni.

Litecoin, invece, utilizza l'algoritmo

scrypt, originariamente chiamato s-crypt, ma pronunciato come 'script'. Scrypt, al contrario, è stato deliberatamente progettato per essere meno suscettibile ai tipi di soluzioni hardware personalizzate utilizzate nell'estrazione basata su ASIC.

Questo algoritmo incorpora l'algoritmo SHA-256, ma i suoi calcoli sono molto più serializzati rispetto a quelli utilizzati per bitcoin. Le conseguenze dell'uso di scrypt hanno reso più accessibile il processo di estrazione per gli utenti che desiderano partecipare alla rete come minatori. Negli ultimi anni, tuttavia, aziende come Zeus e Flower Technology hanno

introdotto Scrypt AISC sul mercato, suggerendo che l'estrazione di monete accessibile per tutti gli utenti potrebbe diventare presto un ricordo del passato.

Litecoin ha attivato SegWit

Il concetto di SegWit è stato formulato per la prima volta dal Dr. Pieter Wuille. SegWit è il processo mediante il quale il limite della dimensione del blocco su una blockchain viene aumentato, rimuovendo i dati delle firme dalle transazioni. Quando alcune parti di una transazione vengono rimosse si libera spazio per aggiungere più transazioni alla catena.

Da quando Litecoin ha implementato

Segwit, il carico sulla sua blockchain è notevolmente diminuito.

INVESTIRE IN CRIPTOVALUTE

Perché dovresti investire in criptovalute?

In questo capitolo cercherò di dare risposte esaustive ed immediate alle domande più comuni sull'investimento in criptovalute.

Se hai acquistato questo libro, potresti essere già interessato a investire in criptovalute. Attualmente le valute virtuali quali Bitcoin, Ethereum &co sono di gran lunga l'investimento più alla moda disponibile. I sostenitori più accaniti delle "crypto" immaginano un futuro in cui Bitcoin o altre criptomonete sostituiranno Euro, Dollaro e tutte le altre divise, creando per la prima volta una valuta mondiale e libera.

Comprare e conservare valute virtuali è il modo più semplice per

prendere parte a questa impresa ed è una scommessa sul successo di questa silenziosa rivoluzione monetaria.

Gli investitori che fin dall'inizio hanno visto un'opportunità in questa innovazione hanno avuto finora un incredibile successo. Infatti il mercato delle criptovalute nel suo complesso è salito del 10.000% dalla metà del 2013.

Puoi fidarti ancora ad investire dopo questo incredibile rialzo? Non è una bolla?

Certo sarebbe stato meglio investire un anno fa, due anni fa o magari sei anni fa. Se riesci a comprendere il potenziale

delle criptovalute e se credi in questa nuova concezione del denaro, allora non è ancora troppo tardi per iniziare a investire.

Dobbiamo comunque ricordarci che le criptovalute non sono un investimento normale. La volatilità supera ampiamente quella di qualsiasi altra classe di investimento e non ci sono ancora regolamentatazioni. Esisitono inoltre parecchi rischii, come ad esempio che le criptovalute possano essere messe fuori legge, che gli scambi vengano violati o che tu possa perdere la tua chiave privata. Bisogna quindi procedere con molta prudenza, perchè le criptovalute sono un investimento ad

alto rischio.

Se stai pensando di investire in criptovalute, potrebbe essere meglio considerare l'investimento nello stesso modo in cui trattateresti qualsiasi altra operazione altamente speculativa. In altre parole, devi riconoscere il rischio di poter perdere la maggior parte del tuo investimento, se non del tutto. Una criptovaluta non ha alcun valore intrinseco oltre a quello che un acquirente è disposto a pagare per questo in un determinato momento; ciò rende molto suscettibili i prezzi esponendoli ad enormi oscillazioni.

Perché investire in criptovalute e

perché no?

Se sostieni la visione sociale retrostante alle criptovalute e ne capisci e apprezzi la tecnologia allora hai delle buone motivazioni per investirci.

Tuttavia, ci sono anche dei pessimi motivi per investire in criptovalute.

Molte persone sono vittime del classico clamore che circonda ogni grande rialzo. C'è sempre qualcuno catturato dalla paura di perdere l'opportunità di non partecipare al prossimo "banchetto", che compra in maniera massiccia nella speranza di fare soldi veloci, mentre in realtà non capisce affatto le motivazioni

dell'investimento. Questa è una cattiva abitudine. Non farlo. Impara prima di investire.

Quali criptovalute dovrei comprare? Costruire il tuo portafoglio.

Pochi anni fà Bitcoin era pressochè l'unica alternativa, non c'era molto altro. Investire nel successo delle criptovalute, singificava comprare Bitcoin. Le poche altre criptovalute, avevano un valore trascurabile ed erano presenti solo in qualche exchange online poco raccomandabile, per lo più utilizzate per mettere in pratica il

cosidetto “pump and dump” (pompare il prezzo per poi scaricare le monete).

Tuttavia la situazione durante il 2017 si è evoluta molto rapidamente. Il Bitcoin è ancora la criptovaluta dominante, ma la crescente popolarità di Ethereum, Ripple e delle altre valute digitali, evidenzia che presto potrebbero spodestarlo dal trono. Ancora una volta è importante tenere gli occhi ben aperti ed essere pronti a cogliere le opportunità che si potrebbero presentare. Se si desidera investire, Bitcoin è comunque ancora un elemento standard di ogni portafoglio, ma attualmente non è interessante quanto altre criptovalute. In ogni portafoglio

ben bilanciato oggi trovi altre monete, come quelle menzionate in questo libro.

Prima di investire in una criptovaluta, come ogni altro investimento, devi prenderti un po' di tempo per raccogliere informazioni, leggere e studiare il progetto. Ti consiglio di procedere all'acquisto soltanto se ne capisci veramente la visone e ne apprezzi l'idea.

Dove Comprare Criptovalute? Cosa sono gli Exchange?

Gli exchange sono siti web che permettono di acquistare, vendere o scambiare criptovalute con altre valute digitali o valute tradizionali come

dollari USA o euro. Se vuoi solo fare scambi occasionali e semplici, ci sono anche piattaforme di cui puoi usufruire senza dover aprire un account.

E' possibile acquistare Bitcoin anche nei punti ATM, in Italia sono già stati installati, nei quali è possibile prelevare o versare contanti nel proprio conto bitcoin, i quali verranno convertiti secondo il tasso di cambio vigente in quel momento. Prima di utilizzare un ATM bitcoin è necessario installare il portafoglio elettronico nel proprio smartphone e generare il proprio indirizzo Bitcoin e il relativo QR Code da far riconoscere alla macchina per il successivo

accreditamento o prelievo di valuta bitcoin. Non è comunque consigliabile utilizzare questo metodo per un investimento poichè le commissioni sono elevate.

Come scegliere un exchange?

È importante sapere cosa dovresti controllare e quali requisiti deve avere un buon exchange, prima di aprire un account ed acquistare criptovalute.

Reputazione

Il modo migliore per reperire informazioni circa un exchange è la ricerca di recensioni in rete da parte degli utenti e di noti siti web del settore

come ad esempio BitcoinTalk o Reddit.

Tariffe

Un buon exchange deve sempre informare i propri utenti riguardo alle tariffe applicate. Prima di aprire un account assicurati di aver ben compreso le spese di deposito, transazione e prelievo. Le tariffe possono differire in modo sostanziale a seconda della piattaforma che utilizzi.

Metodi di pagamento

Quali metodi di pagamento sono disponibili? Se un exchange ha opzioni di pagamento limitate, potrebbe non essere conveniente utilizzarlo. Ricordati

che l'acquisto di criptovalute con una carta di credito richiede sempre la verifica dell'identità, inoltre dovrai pagare un sovvraprezzo in quanto vi è un alto rischio di frode e maggiori costi di transazione ed elaborazione. L'acquisto di criptovaluta tramite bonifico bancario richiede invece l'elaborazione da parte delle banche e quindi impiegherà molto più tempo.

Requisiti di verifica

La stragrande maggioranza delle piattaforme di scambio richiedono una sorta di verifica dell' identità per effettuare depositi e prelievi. La verifica può richiedere alcuni giorni, e sebbene possa sembrare un problema protegge

l’exchange da tutti i tipi di truffe e dal riciclaggio di denaro.

Restrizioni geografiche

Alcune funzioni specifiche offerte dalle piattaforme di scambio sono accessibili solo da alcuni paesi. Assicurati quindi che l’exchange che intendi scegliere consenta l'accesso completo a tutti gli strumenti e le funzioni della piattaforma, nel paese in cui vivi attualmente.

Tasso di cambio

Gli exchange hanno diversi tassi di cambio. Resterai sorpreso di quanto puoi risparmiare se ti guardi intorno.

Non è infrequente che le tariffe oscillino addirittura del 10% e persino di più in alcuni casi.

ICO - Initial Coin Offerings

Le ICO possono essere considerate come una forma alternativa di crowdfunding nata al di fuori del sistema finanziario tradizionale. Questo modello ha aiutato molti progetti di successo, aiutando le aziende ha ottenere i finanziamenti necessari per avviare la propria attività.

È uno dei metodi più semplici ed efficienti per le aziende e gli individui che desiderano finanziare i loro progetti.

Per gli utenti comuni invece costituisce un'opportunita per investire in progetti a cui attribuiscono valore. Un ICO è quindi un evento che si estende di solito per una settimana o più e a tutti è consentito acquistare i nuovi token in cambio di criptovalute come Bitcoin (BTC) o Ether (ETH).

In un ICO, può esserci un obiettivo o un limite specifico per il finanziamento del progetto, nel senso che ogni token avrà un prezzo prestabilito che non cambierà durante il periodo dell'ICO, il che significa anche che il numero di token emessi è immutabile.

È anche possibile che vengano emessi un numero predeterminato di

token ma con un obiettivo di finanziamento dinamico, in cui la distribuzione di token sarà effettuata in base ai fondi ricevuti. Il che significa che più fondi riceverà il progetto più alto sarà il prezzo di ogni token.

È inoltre possibile anche che i token vengano emessi in maniera dinamica, in funzione dei fondi ricevuti. Il che significa che il prezzo per ogni token è statico, e quindi ogni volta che l'ammontare dei fondi aumenta vengono creati nuovi token. Un limite può essere comunque impostato in termini di obiettivi o tempi.

Leggere il Whitepaper

Un whitepaper viene preparato prima di lanciare una nuova criptovaluta, e generalmente è scaricabile dal sito web del progetto. Descrive in dettaglio tutto ciò che è necessario sapere prima di prendere una decisione nel caso si desideri investire. Ciò include i dettagli commerciali, tecnologici e finanziari di una nuova moneta descritti in un linguaggio comprensibile anche ai non esperti. Il white paper è un componente fondamentale delle Initial Coin Offerings (ICO).

Per quale motivo viene realizzato il Whitepaper?

- Per informare il pubblico del progetto,
- Per presentare il progetto che si vuole realizzare,
- Per quali motivi si crede che il prodotto sia necessario,
- Per far conoscere la tabella di marcia, presentando cronologicamente le fasi che si vogliono raggiungere,
- Per sapere con quali metodi si raggiungeranno gli obiettivi prefissati,
- (Se si terrà un ICO), è inoltre possibile scoprire in che modo verranno distribuiti i token creati.

Leggere il whitepaper ti aiuterà a

comprendere meglio tutto ciò che serve alla creazione di nuove criptovalute. Per i principianti i white paper sono ottimi strumenti per essere esposti ad un livello di conoscenze superiore. Non aver paura di cercare il significato di parole che non conosci e non aver paura di imparare qualcosa di nuovo. Se sei interessato ad approfondire la tua conoscenza in questo ambito, i white paper sono una buona soluzione e costituiscono una preziosa fonte di informazioni da esplorare.

Dopo averne letti un pò, inizierai a capire ciò che rende un whitepaper migliore di altri e sicuramente sarà utile anche ad indentificare i progetti più

interessanti.

Dove conservare le proprie criptovalute?

Cosa è un wallett?

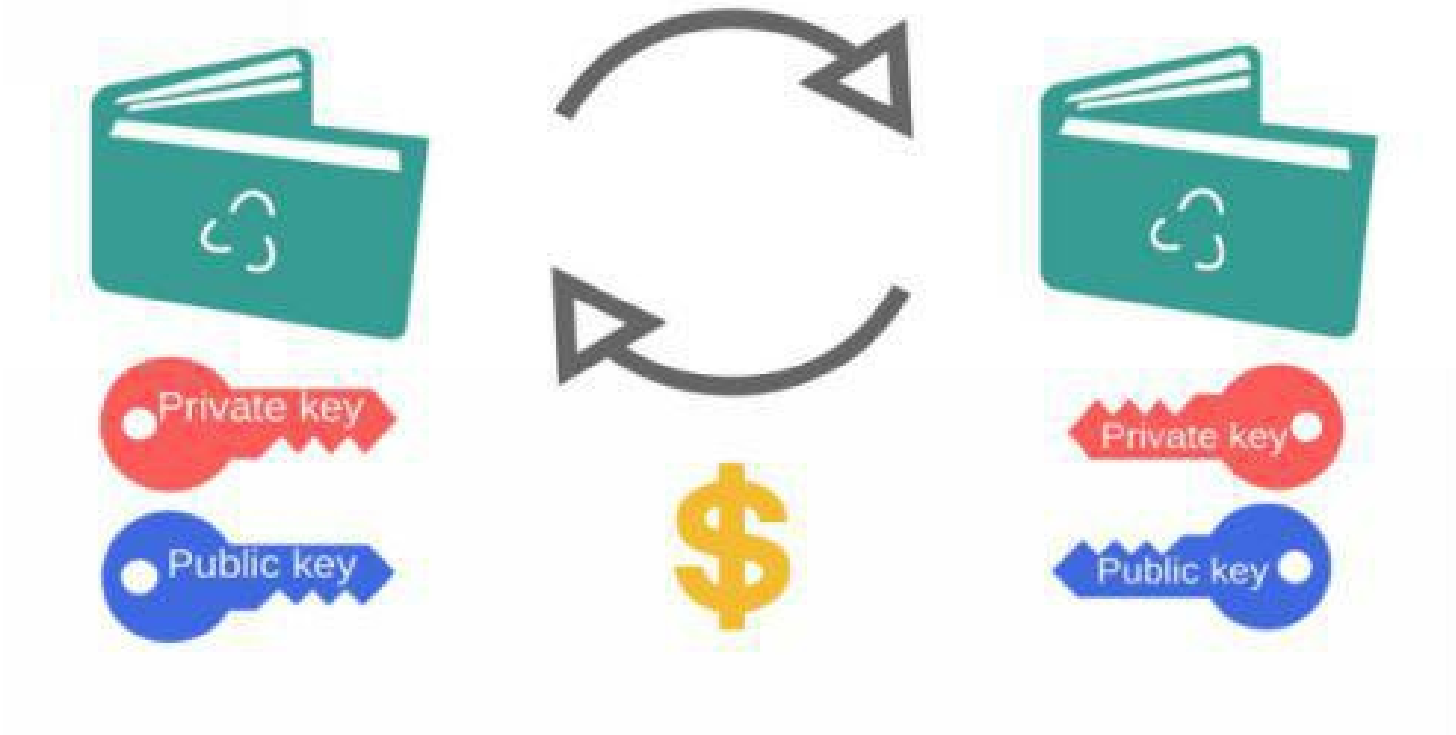
Un wallett o portafoglio in italiano, è un software che memorizza le tue chiavi pubbliche e private e si interfaccia con vari blockchain in modo che gli utenti possano monitorare il loro saldo, inviare denaro e condurre altre operazioni. Se vuoi utilizzare/conservare Bitcoin o qualsiasi altra criptovaluta, è necessario disporre di un portafoglio digitale.

Come funzionano?

Milioni di persone utilizzano un portafoglio digitale per depositare le proprie criptovalute, ma non sono in molti a sapere come funzionano realmente.

A differenza dei tradizionali portafogli tascabili, i portafogli digitali "non contengono nulla". Le criptovalute non vengono memorizzate in una singola posizione e ovviamente non esistono in nessuna forma fisica. Tutto ciò che esiste sono soltanto registrazioni di transazioni memorizzate sulla blockchain.
Quando una persona ti manda Bitcoin o qualsiasi altro tipo di valuta digitale, in sostanza sta firmando il cambio di

proprietà delle monete registrandole all’indirizzo del tuo portafoglio. Per ricevere e poi di conseguenza spendere queste monete, la chiave privata memorizzata nel tuo portafoglio deve corrispondere all'indirizzo pubblico a cui ti è stata inviata la valuta. Se le chiavi pubbliche e private corrispondono, il saldo nel tuo portafoglio digitale aumenterà e di conseguenza quello dei mittenti diminuirà.



Diversi tipi di wallets

Esistono diversi tipi di portafogli che offrono molteplici opzioni per depositare e accedere alle tue criptovalute. I portafogli possono essere suddivisi in tre categorie distinte:

software (suddivisi in: desktop, mobile, online), hardware e paper.

Desktop

Il software del tuo wallet viene scaricato ed installato sul tuo Pc e risulterà accessibile solo da quel singolo computer. I desktop wallets offrono uno dei più alti livelli di sicurezza, tuttavia se il tuo computer viene hackerato o viene colpito da un virus, esiste la possibilità che tu possa perdere tutti i tuoi fondi.

Online

I portafogli funzionano sul cloud e sono accessibili da qualsiasi dispositivo

in qualsiasi luogo. Accedere risulta quindi semplice e comodo anche se non hai a disposizione il tuo Pc, ma i portafogli online memorizzano le chiavi private in rete e sono controllati da terze parti il che li rende più vulnerabili agli attacchi e ai furti degli hacker.

Mobile

I wallet vengono eseguiti tramite un'app installata sul tuo telefono e risultano utili perché possono essere utilizzati ovunque, inclusi i negozi al dettaglio. I wallet mobile di solito sono molto più semplici e basilari a differenza di quelli versione desktop.

Hardware

I wallet hardware differiscono dai portafogli software in quanto memorizzano le chiavi private di un utente su un dispositivo hardware simile ad una chiavetta USB. Sebbene i portafogli hardware permettano le transazioni online, sono archiviati offline e offrono maggiore sicurezza. I portafogli hardware possono supportare diverse valute, dipende solo da quale modello si decide di acquistare. Inoltre, fare una transazione è facile. Gli utenti devono semplicemente collegare il proprio wallet a qualsiasi computer o dispositivo abilitato a Internet, inserire un pin, inviare valuta e confermare. I portafogli hardware consentono di effettuare facilmente transazioni

mantenendo allo stesso tempo il denaro offline e lontano dai pericoli.

Paper

I paper wallets fanno riferimento a una copia fisica o alla stampa delle chiavi pubbliche e private, oppure a un software che viene utilizzato per generare in modo sicuro un paio di chiavi che vengono poi stampate.

Questi walletts sono facili da usare e forniscono un livello molto alto di sicurezza.

Il trasferimento di Bitcoin o di qualsiasi altra valuta nel tuo paper wallet si effettua tramite l'utilizzo

dell'indirizzo pubblico a cui fà riferimento.

Se invece desideri prelevare o spendere valuta, tutto ciò che devi fare è trasferire fondi dal tuo paper wallet al tuo portafoglio software. Questo processo, può essere eseguito manualmente inserendo le chiavi private o eseguendo la scansione del codice QR sul paper wallet.

I wallet sono sicuri?

Il livello di sicurezza dipende dal tipo di portafoglio utilizzato (desktop, mobile, online, cartaceo, hardware) e dal fornitore di servizi. Un server web è un ambiente molto più rischioso per

mantenere le tue criptovalute rispetto ad un wallet offline. I portafogli online possono esporre gli utenti a possibili vulnerabilità nella piattaforma, che possono essere sfruttate dagli hacker per rubare i fondi. I portafogli offline, d'altra parte, non possono essere violati perché semplicemente non sono connessi a una rete online e non si affidano a terzi per motivi di sicurezza.

Sebbene i wallet online si siano dimostrati più vulnerabili e inclini agli attacchi di hacker, è necessario implementare e seguire diligenti precauzioni di sicurezza quando si utilizza qualsiasi tipo di portafoglio. Ricorda che, indipendentemente dal

portafoglio che usi, smarrire le tue chiavi private ti farà perdere tutto il tuo denaro. Allo stesso modo, se il tuo wallet viene violato o se invii denaro a un truffatore, non c'è modo di recuperare le monete perdute o di invertire la transazione. Devi prendere precauzioni e stare molto attento!

Sul tuo computer o sullo smartphone archivia solo piccole quantità di valuta per l'uso quotidiano online, mantenendo la stragrande maggioranza dei tuoi fondi in un ambiente ad alta sicurezza (un hardware wallet è la miglior soluzione). Se si sceglie di utilizzare un portafoglio online, esistono rischi intrinseci che non possono essere sempre protetti. Utilizza

in ogni caso wallet che hanno una buona reputazione e forniscono livelli di sicurezza aggiuntivi, come l'autenticazione a due fattori e l'uso di codici pin aggiuntivi ogni volta che viene eseguito.

Prima di scegliere un portafoglio, dovresti comunque considerare come intendi utilizzare le tue criptovalute (investimento, acquisti online, trading ecc..).

I portafogli di criptovaluta sono anonimi?

I wallet non sono legati all'identità reale di un utente, ma ad uno pseudonimo che corrisponde al suo

indirizzo, tutte le transazioni sono comunque memorizzate pubblicamente e permanentemente sulla blockchain.

Multivaluta o no?

Sebbene il Bitcoin sia di gran lunga la valuta digitale più conosciuta e popolare, sono emerse centinaia di nuove criptovalute (denominate altcoin), ciascuna con ecosistemi e infrastrutture distintive. Se sei interessato all'utilizzo di una varietà di criptovalute, la buona notizia è che non è necessario creare un portafoglio separato per ogni valuta. Invece di utilizzare un wallet che supporta una singola valuta, se necessario è meglio adoperare un portafoglio multi-valuta che ti permetta

di utilizzare diverse valute.

Esistono delle commissioni di transazione?

In genere, le commissioni di transazione sono cifre di poco conto. Le tasse devono essere pagate per determinati tipi di transazioni ai minatori della rete come “tassa di elaborazione”, mentre alcune transazioni non hanno alcun costo.

È possibile impostare la commissione manualmente.

Tuttavia se si scegli di impostare una tariffa molto bassa, la transazione potrebbe avere bassa priorità e potrebbe

essere necessario attendere ore o addirittura giorni affinché la transazione venga confermata. Se hai bisogno che la transazione sia completata e confermata tempestivamente, potresti dover aumentare l'importo che sei disposto a pagare.

In ogni caso qualunque sia il portafoglio che usi, le commissioni di transazione non sono qualcosa di cui dovresti preoccuparti.

CONCLUSIONI

Qual è il futuro delle Criptovalute?

Alcune delle limitazioni che le criptovalute devono affrontare possono essere superate nel tempo attraverso i progressi tecnologici. Quello che sarà più difficile da superare è il paradosso fondamentale che tormenta le criptovalute cioè che più diventeranno popolari, più attireranno la regolamentazione e il controllo del governo, il che erode la premessa fondamentale per la loro esistenza.

Il numero di commercianti che accettano criptovalute è aumentato costantemente, ma nonostante tutto sono ancora in netta minoranza. Per far sì che le criptovalute vengano utilizzate più ampiamente, devono prima ottenere un consenso diffuso sopratutto tra i consumatori. Tuttavia, la loro relativa complessità rispetto alle valute convenzionali probabilmente scoraggerà la maggior parte delle persone.

Una criptovaluta che aspira a diventare parte del sistema finanziario tradizionale potrebbe dover soddisfare criteri ampiamente divergenti. Dovrebbe essere matematicamente complesso (per evitare frodi e attacchi di hacker) ma

facile da comprendere per i consumatori; decentralizzato ma con adeguate garanzie e protezione del consumatore; preservare l'anonimato degli utenti senza essere un canale per l'evasione fiscale, il riciclaggio di denaro sporco e altre attività illegali. Non c'è dubbio che il successo o il fallimento di Bitcoin nell'affrontare le prossime sfide possa determinare le sorti anche delle altre criptovalute negli anni a venire.

-Un mercato selvaggio

La situazione attualmente è in continuo mutamento. Il mercato delle criptovalute è veloce e selvaggio, quasi ogni giorno emergono nuove

criptovalute e ne muoiono altre; qualcuno si arrichisce velocemente e qualcun altro perde molto denaro.

Ogni criptomoneta racchiude in sè grandi propositi, ma sono poche poi quelle che sopravvivono ai primi mesi, infatti molte delle nuove criptovalute vengono usate dagli speculatori per trarne il maggior profitto possibile praticando il cosidetto “pump&dump”.

I mercati non sono ancora sicuri, risultano poco comprensibili e chiaramente manipolati, ma questo non cambia il fatto che le criptovalute siano qui per restare e qui per cambiare l’avvenire.

La rivoluzione è già iniziata

Ci sono molte motivazioni per cui non bisognerebbe porre troppa fiducia nell'attuale sistema monetario, secondo dati ufficiali il dollaro americano, come si vede in figura, ha perso circa il 95% del suo valore dall'inizio del XX secolo. Le persone hanno quindi intravisto nel Bitcoin e nelle altre valute digitali la possibilità di proteggersi dalla svalutazione della loro valuta nazionale.

Soprattutto in Asia è emerso un vivido interesse per le criptovalute che stanno prosperando; anche gli investitori istituzionali si sono accorti di questa tendenza ed hanno iniziato a collocare

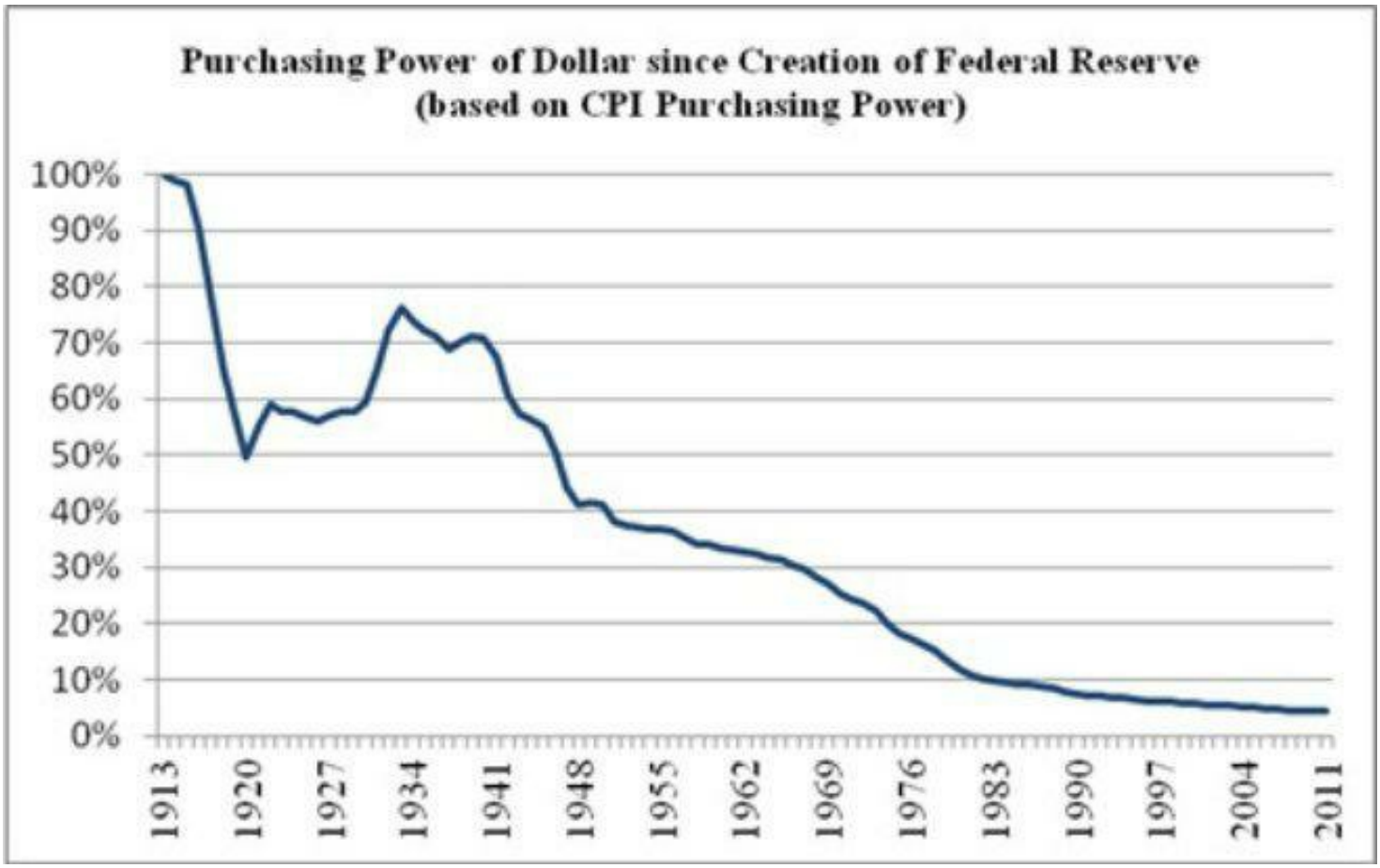
cospicue somme di denaro sul mercato. Molte aziende invece stanno scoprendo il potere degli Smart Contracts di Ethereum, dando vita alle prime applicazioni nel mondo reale della tecnologia blockchain.

Ritengo che la tecnologia blockchain sia lo strumento più adatto per risolvere il problema per cui è stata ideata e cioè il trasferimento di denaro.

Credo che tra qualche anno le criptovalute saranno più mature e cresceranno in uso e accettazione, guadagneranno legittimità come protocollo per le transazioni commerciali e per i micro-pagamenti , sorpassando finalmente i sistemi

tradizionali odierni.

Ci saranno grandi istituzioni finanziarie e aziende che useranno le criptovalute per la capacità di spostare quasi istantaneamente qualsiasi somma di denaro grazie all'efficienza della tecnologia blockchain.



Nessuno può esercitare un vero controllo

I governi e i regolatori di tutto il mondo, abituati da più di un secolo nel

controllo delle finanze delle persone, ancora non si rendono conto di non poter intervenire e cercano di trattare le valute digitali come qualsiasi altra risorsa.

La caratteristica principale del Bitcoin e delle altre criptovalute è che nessun governo, azienda o singolo può esercitare un vero controllo. Qualsiasi governo nel mondo può esercitare il suo controllo soltanto entro i confini del suo ecosistema. Attualmente soltanto le piattaforme di scambio sono vulnerabili e costituiscono il principale punto di entrata / uscita per le criptovalute.

La maggior parte dei governi del mondo ha quindi il potere di chiudere unilateralmente qualsiasi compagnia che

i suoi burocrati ritengano fare qualcosa di illegale. Ciò non deve destare preoccupazioni perchè presto gli exchange centralizzati cadranno in disuso e verranno sicuramente sostituiti da piattaforme di scambio decentralizzate.

Le criptovalute ci accompagneranno verso una strada alternativa, che può condurci verso una società con meno centralizzazione del potere.