UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia e Commercio

CRIPTOVALUTE E BLOCKCHAIN: IL FENOMENO CHE STA RIVOLUZIONANDO IL MONDO

CRYPTOCURRENCIES AND BLOCKCHAIN: THE PHENOMENON THAT IS REVOLUTIONIZING THE WORLD

Relatrice:
Prof.ssa Giulia Bettin

Rapporto Finale di:
Vincenzo Bisconti

Anno Accademico 2020/2021

Ringrazio tutti coloro che mi sono stati vicini e tutti coloro che mi hanno aiutato in questi ultimi tre anni nel mio percorso universitario. Ringrazio la mia famiglia per non avermi messo pressioni addosso e per aver creduto sempre in me. Ma voglio ringraziare anche me stesso per non essermi mai tirato indietro e per aver cercato di fare tutto nel miglior modo possibile nonostante le difficoltà che ci sono state in questi anni. Un ringraziamento va anche alla professoressa Bettin per essermi stata d'aiuto durante la scrittura di questa tesi.

Introduzione

Nell'ultimo decennio siamo stati protagonisti di una esponenziale evoluzione tecnologica che ha portato con se innumerevoli cambiamenti nella maggior parte della quotidianità. Tale sviluppo tecnologico ha coinvolto anche il mondo finanziario dove sono stati introdotti strumenti complessi come le criptovalute. La loro nascita è da collocarsi nel 2009 quando un individuo conosciuto con lo pseudonimo di Satoshi Nakamoto ha presentato per la prima volta quella che poi negli anni è divenuta la criptovaluta più importante in termini di capitalizzazione del mercato e non solo, il Bitcoin. La nascita di tale criptovaluta è da ricondursi alla volontà di creare uno strumento di pagamento che si discostasse dal classico sistema che c'era stato fino a quel momento, siamo inoltre nel periodo in cui una delle più importanti banche di investimenti americana, la Lehman Brothers, crollò in borsa.
Da quel momento in poi le criptovalute hanno preso lentamente sempre più importanza fra i vari strumenti finanziari esistenti, catturando l'interesse di investitori e di istituzioni per via delle loro funzioni ma anche per l'importante ventata di novità che hanno portato sui mercati finanziari.
Le criptovalute sono oggetto di studio della seguente tesi che viene articolata in tre capitoli cercando di dare una spiegazione e di far comprendere sia la tecnologia che vi è dietro sia le possibilità che possono offrire. Nel primo capitolo viene trattato il tema delle criptovalute in generale, se ne illustrano l'origine e le caratteristiche, oltre agli impatti che hanno avuto sull'economia. Nel secondo capitolo viene illustrato in maniera più specifica il funzionamento di tali criptovalute attraverso la tecnologia blockchain. Viene spiegata la struttura della composizione di tale tecnologia oltre al ragionamento che c'è stato dietro alla sua creazione. Nell'ultimo capitolo, il capitolo tre, vengono presentati Bitcoin e Ethereum, ovvero le due criptovalute principali sia in termini di importanza sia in termini di capitalizzazione sul mercato. In conclusione, inoltre, è stato fatto un piccolo confronto in termini numerici anche con alcune delle altre altcoins per permettere di comprendere in maniera più precisa la dimensione effettiva del fenomeno di Bitcoin ed Ethereum.

1. Le criptovalute

1.1. Cosa si intende per criptovalute

Le criptovalute sono una delle più significative applicazioni della tecnologia digitale al settore finanziario. Il termine criptovaluta si compone di due parole: cripto e valuta. Si tratta quindi di una valuta che può esser considerata nascosta, nel senso che l'unico modo per poterla vedere e utilizzare è conoscere e/o condividere un determinato codice informatico.
La criptovaluta non esiste in forma fisica, anche per questo viene definita valuta virtuale, ma si genera e si scambia solo ed esclusivamente per via telematica. Pertanto non sarà possibile trovare alcuna criptovaluta in circolazione sotto forma cartacea o metallica. Per utilizzare le criptovalute bisogna innanzitutto dotarsi di un portafoglio digitale dove immagazzinare le criptomonete, rappresentato da un software o hardware, a seconda delle necessità dell'utente.
Il concetto di portafoglio che tradizionalmente è utilizzato per le monete legali, è stato adattato anche al contesto delle monete virtuali come le criptovalute. Negli ultimi anni, i portafogli digitali sono diventati sempre più popolari, e il panorama del settore continua ad evolversi rapidamente. I portafogli digitali sono di solito disponibili su pagine web oppure su applicazioni per smartphone che permettono ai clienti di aprire conti. I clienti finanziano i loro portafogli usando carta di credito, carta di debito, un pagamento bancario, o pagando in contanti un agente. Una volta che il denaro è stato trasferito dal cliente all'operatore del portafoglio, il cliente vede un saldo nel suo portafoglio, che può essere utilizzato.
I pagamenti consistono nello spostamento di criptovaluta da un portafoglio digitale all'altro di qualsiasi utente che sia interessato a scambiarle. Le transazioni in moneta virtuale sono possibili in qualsiasi momento e luogo, per l'acquisto di beni reali o virtuali, senza l'intermediazione di una terza parte (modalità peer-to-peer, che significa scambio tra due dispositivi direttamente senza necessità di intermediari), che assicuri che il denaro utilizzato per i pagamenti non sia già stato speso o che le transazioni vengano alterate ex-post.
La sicurezza è garantita dalla tecnologia che funge da pilastro centrale di questo sistema, la blockchain, ed è per mezzo di essa che si effettuano le transazioni (vedi capitolo 3).
Le criptovalute sono al momento deregolamentate in molti stati ed escluse dalla sfera di influenza di politiche fiscali e monetarie. La loro stessa emissione non è regolata dallo Stato, Banca Centrale, società o altra autorità centralizzata, bensì

dagli utenti del network attraverso metodi alternativi, a seconda della blockchain su cui operano. Il procedimento più utilizzato, nello specifico caso dei bitcoin, è il mining: il miner ottiene una certa quantità di criptovaluta nuova risolvendo un puzzle di codici prodotto dal sistema stesso, aumentando dunque il numero di bitcoin in circolazione.

1.2. Le origini delle criptovalute

Le criptovalute sono una creazione recente, si inizia a parlarne effettivamente a partire dal 2009.
Il creatore risulta essere un certo Satoshi Nakamoto, il quale ha ideato la prima e più famosa criptovaluta: il bitcoin. Il 31 ottobre 2008, Nakamoto rende noto il suo programma (ovvero il suo white paper intitolato "*Bitcoin: A Peer-to-Peer Electronic Cash System*"): creare un sistema monetario elettronico sfruttando la rete peer-to-peer, ossia una rete paritaria in cui ogni terminale (ogni computer) è client e server (elaboratore e controllore, significa scambiare tra due dispositivi direttamente senza necessità di intermediari) al tempo stesso, sfruttando la tecnologia dei registri condivisi, ossia la blockchain, per evitare che la valuta possa essere copiata.
In seguito nel 2009, per la precisione il 3 gennaio, si realizza il primo blocco, denominato Genesis block, dal quale si svilupperà la blockchain dei bitcoin: il blocco viene, come si dice in gergo tecnico, minato. Il blocco successivo registra la prima transazione di bitcoin tra Nakamoto e Finney, un'attivista crittografo. In seguito il padre delle criptovalute Nakamoto ha minato un milione di bitcoin.
La sua opera poi è stata portata avanti dai cosiddetti minatori, i quali, attraverso complicatissime operazioni, che sono gestite da terminali estremamente performanti, e che necessitano di una quantità di energia notevole, possono minare nuovi bitcoin. Possono cioè decrittare la stringa (l'algoritmo) di un blocco, il quale contiene una certa quantità di criptovalute che vengono assegnate al minatore a mo' di premio. Detta quantità si dimezza ogni 4 anni.
La decrittazione è necessaria per l'aggiornamento delle transazioni, i miner in questa maniera si occupano oltre che dell'emissione di nuovi bitcoin, di garantire l'autenticità e la regolarità di ogni operazione senza necessità di un'autorità centrale.
L'emissione di nuova moneta è però limitata e non può superare i 21 milioni di unità; attualmente si dovrebbe stare attorno ai 19 milioni di unità cioè attorno al

90% del totale. Quando si raggiungerà la soglia prestabilita di unità, sarà il sistema stesso a fornire le valute necessarie per remunerare i minatori.

1.3. Caratteristiche delle criptovalute

Le criptovalute come possiamo vedere qui di seguito hanno delle proprie caratteristiche fondamentali che le rendono riconoscibili rispetto ad altre valute, ed esse sono:

- Sistema decentralizzato: rispetto alle normali valute tradizionali non esiste una banca centrale che si occupa di stampare il denaro e controllarne il flusso
- Anonimato: molte criptovalute riescono a garantire un alto livello di anonimato negli scambi che avvengono tra gli utenti
- Numero limitato: la maggior parte delle criptovalute ha un numero limitato di moneta che può essere prodotta
- Sicurezza: le transazioni che avvengono sono sicure al 100%, grazie al particolare network che utilizzano
- Natura virtuale: le criptovalute sono monete digitali, non prevedono quindi banconote o monete, infatti sono contenute in portafogli elettronici, definiti wallet. Tutte le transazioni avvengono online, anche se stanno diventando mezzo di pagamento nei negozi fisici, o uno strumento per cambiare e prelevare denaro contante;
- Protocollo: cioè un codice informatico che specifica il modo in cui i partecipanti possono effettuare le transazioni
- Libro mastro (blockchain): che memorizza la storia della transazioni dell'utente
- Rete decentralizzata di partecipanti che aggiornano, conservano e consultano le transazioni

Per comprendere meglio le varie caratteristiche è possibile, anche, analizzare i tre gruppi distinti di clienti a cui la criptovaluta si rivolge:
Il primo gruppo è composto da appassionati di tecnologia che adottano i bitcoin per il commercio sulla rete. Poiché sempre più transazioni commerciali vengono effettuate online, questi utenti ritengono che il valore delle criptovalute dovrebbe aumentare a causa della domanda di transazioni e citano anche i loro vantaggi in

termini di costi rispetto ad altri sistemi di pagamento per la normale vendita al dettaglio.
Un secondo gruppo trova allettante l'idea di una valuta sconnessa da qualsiasi governo. Alcuni di questi aderenti diffidano apertamente del sistema finanziario mondiale, e la tempistica dell'introduzione di bitcoin, che coincide con la fase più critica della crisi finanziaria globale, ha probabilmente contribuito ad aumentare le loro fila.
Il terzo gruppo è composto da individui che vedono nelle criptovalute un espediente per commerciare illegalmente, a causa della protezione della privacy e dunque dell'anonimato che esse, in maniera più o meno efficace, garantiscono, come nel caso del sito di transazioni illegali Silk Road, e più in generale del cosiddetto dark web.

1.4. Vantaggi e rischi delle criptovalute

Le criptovalute, proprio come il denaro fisico (il contante), hanno sia dei punti di forza che spingono i loro sostenitori ad incrementarne la domanda, ma allo stesso tempo possiedono dei punti di debolezza che rendono un po' scettica la platea di potenziali utilizzatori, andando a favorire altri strumenti di pagamento/investimento come il contante stesso.

Tra i vantaggi delle criptovalute troviamo:

1. Trasferimento di denaro. Trattandosi, infatti, di una forma di valuta che esiste in modo digitale, è possibile inviare e ricevere denaro in qualsiasi parte del mondo. Non devi neppure preoccuparti delle limitazioni per il trasferimento di denaro come i confini o i giorni festivi. Dal momento poi che le valute digitali non sono controllate da un'autorità centrale, si ha sempre il pieno il controllo del denaro durante i trasferimenti.
2. Trasferimento delle informazioni. Ogni volta che si tratta di trasferire denaro, la trasparenza delle informazioni è sempre una delle principali priorità. Con la tecnologia blockchain, infatti, tutte le transazioni finali diventano disponibili agli occhi del pubblico solo dopo essere state approvate dalla rete. Tuttavia, se tutte le transazioni sono disponibili per tutti, le tue informazioni personali sono nascoste. Ciò significa che, anche se l'indirizzo del tuo portafoglio è visibile, i tuoi dati non lo sono. Questo

determina l'impossibilità che la criptovaluta sia in qualche modo manipolata da qualsiasi persona, organizzazione o governo.

3. Controllo e sicurezza. Le criptovalute consentono agli utenti di avere il pieno controllo delle proprie transazioni, rimanendo al sicuro e nascoste nel loro portafoglio digitale. Le informazioni personali non sono infatti richieste quando si tratta di transazioni. Questo aiuta a proteggere gli utenti dal furto di identità.
4. Meno rischi per i venditori. Con le criptovalute anche i commercianti hanno meno rischi poiché le transazioni non possono essere annullate, non trasportano informazioni personali e sono sicure. I venditori sono quindi più protetti dalle perdite che potrebbero derivare da eventuali frodi permettendo ai venditori di svolgere la propria attività in luoghi pericolosi, dove i tassi di criminalità e i tassi di frode sono elevati.
5. Commissioni basse, un altro vantaggio del denaro digitale sono le commissioni basse sulle varie transazioni. Possono tuttavia esserci commissioni più elevate per garantire una priorità alla transazione.

Passiamo ad analizzare anche alcuni degli svantaggi, in quanto anche quando si tratta di criptovaluta non è tutto positivo quello che le riguarda, quindi occorre sempre valutarne con attenzione i pro e i contro prima di prendere in considerazione il loro utilizzo.

1. Rischio e volatilità. Il rischio e la volatilità di tutte le criptovalute sono sempre stati uno dei maggiori problemi. Nel caso dei bitcoin, ad esempio, la volatilità deriva dal fatto che c'è una disponibilità limitata di monete (21 milioni di bitcoin e almeno il 90% di quei 21 milioni è già stato assegnato) e la loro domanda è sempre crescente. Per questo il prezzo del bitcoin così come delle altre valute digitali non è mai stabile ma fluttua ogni giorno.
2. Poca informazione e scarso sviluppo. Un altro motivo per cui le persone spesso pensano due volte all'investimento in criptovalute è che si tratta di un trading ancora nella sua fase iniziale. Ci sono caratteristiche che devono ancora essere ulteriormente sviluppate, come ad esempio funzionalità che rendano le valute più sicure e accessibili. La poca informazione e l'incertezza su quello che saranno le criptovalute in futuro non sono di certo un incentivo a far sì che le persone investano in esse.

3. Pericolo di truffe. La natura relativamente anonima delle valute digitali le ha rese molto attraenti per i criminali, che potrebbero utilizzarle per riciclaggio di denaro sporco e altre attività illegali. Secondo gli esperti del settore, le criptovalute possono comportare rischi notevoli anche con riguardo alle truffe. Ci sono quindi ancora numerosi interrogativi in termini di protezione dei consumatori/investitori.
4. Scarsa tutela legale. L'assenza di un quadro giuridico preciso determina l'impossibilità di attuare un'efficace tutela legale e/o contrattuale degli interessi degli utenti, che possono trovarsi esposti a dover subire grandi perdite economiche.

1.5. L'impatto delle criptovalute sull'economia

Le criptovalute vogliono proporsi come forma innovativa di moneta scambiabile. Di conseguenza ci si chiede se possono davvero essere considerate una forma di denaro. Rimandiamo questo discorso al paragrafo 4.1.3. dove viene affrontato il tema in maniera più specifica andando a confrontare le caratteristiche del bitcoin, la criptovaluta più utilizzata, con le caratteristiche della moneta fiat (ovvero le monete legali).

1.5.1. Criptovaluta e criminalità

Le criptovalute come abbiamo detto precedentemente non sono emesse da banche e non sono governate da un'autorità centrale, quindi qualsiasi organizzazione di sicurezza (polizia o quant'altro) non può monitorare tali transazioni. E se tali criptovalute vengono identificate come utilizzate in operazioni criminali, non si ha modo di congelare le risorse come nel normale sistema bancario.
La tecnologia della blockchain (libro mastro decentralizzato), su cui si appoggiano le varie criptovalute, opera con transazioni verificabili in modo indipendente e ciò ha un enorme fascino, specialmente in un'epoca in cui la gestione centralizzata suscita preoccupazioni sia per hacking dall'esterno che per la manipolazione interna. Eppure, la maggioranza delle transazioni avvengono su piattaforme centralizzate, come Coinbase (piattaforma per acquistare e vendere), dove le criptovalute vengono scambiate con denaro tradizionale. Questi scambi operano in

gran parte al di fuori della portata delle autorità di regolamentazione finanziaria con una trasparenza spesso limitata.
Limitata trasparenza sembra essere un problema ricorrente, un utente del sistema bitcoin gode di un certo anonimato, in quanto il pubblico può vedere che in un determinato momento una certa somma viene scambiata, ma non ha a disposizione informazioni che riconducano alla persona coinvolta: "È simile al livello di informazioni diffuse dalle borse, dove il tempo e le dimensioni dei singoli scambi, il nastro, sono resi pubblici, ma senza dire chi erano le parti" (affermò Nakamoto nel 2008).
È bene specificare che il grado di anonimato di cui gli utenti godono non è sempre lo stesso ma bensì è variabile, spaziando dall'anonimato completo allo pseudo-anonimato. Bitcoin è pseudo-anonimo, in quanto, con grande utilizzo di risorse e capacità tecniche, è possibile risalire all'identità di un utilizzatore da una transazione. La protezione dell'anonimato, sia essa assoluta o meno, trasforma le criptovalute nei paradisi fiscali di domani, nonché in strumenti per il riciclo di denaro e addirittura finanziamento del terrorismo.
Il metodo per rintracciare utilizzatori di criptomonete pseudo-anonime è utile, ma è troppo impegnativo per diventare la risposta generale al problema. Il fatto che la blockchain non sia limitata dai confini nazionali aggrava il pericolo, in quanto il riciclaggio potrebbe avvenire in paesi dotati di un insufficiente apparato per individuare e combattere riciclaggio di denaro e finanziamento del terrorismo. Il caso più emblematico e famoso di attività illecite condotte attraverso l'uso di criptovalute è quello di Silk Road (figura 1).
Quest'ultimo era il più grande mercato nero che si poteva trovare su internet, situato nel Deep Web (una parte della rete inaccessibile per il comune utente, luogo di commercio illegale e materiale censurato dal governo), dove si vendevano narcotici, armi e contratti di assassinio.
Silk Road fungeva da intermediario tra le parti, che rimanevano anonime ed effettuavano pagamenti solo ed esclusivamente in bitcoin. Il sito fu chiuso nell'Ottobre 2013 in seguito all'arresto del fondatore, Ross Ulbricht, colto in fragrante mentre si offriva di pagare per l'assassinio di un suo collaboratore. Casi come quello di Silk Road hanno evidenziato la necessità di implementare un sistema di leggi che possa scongiurare l'abuso di questa tecnologia, inoltre la mancanza di un organismo centrale ha spinto a chiedersi chi debba essere regolamentato e come rimuovere il velo di anonimato delle transazioni sulla blockchain. La possibilità che misure troppo stringenti soffocassero l'innovazione

prima ancora che realizzasse il suo pieno potenziale hanno reso ancora più difficile intervenire.

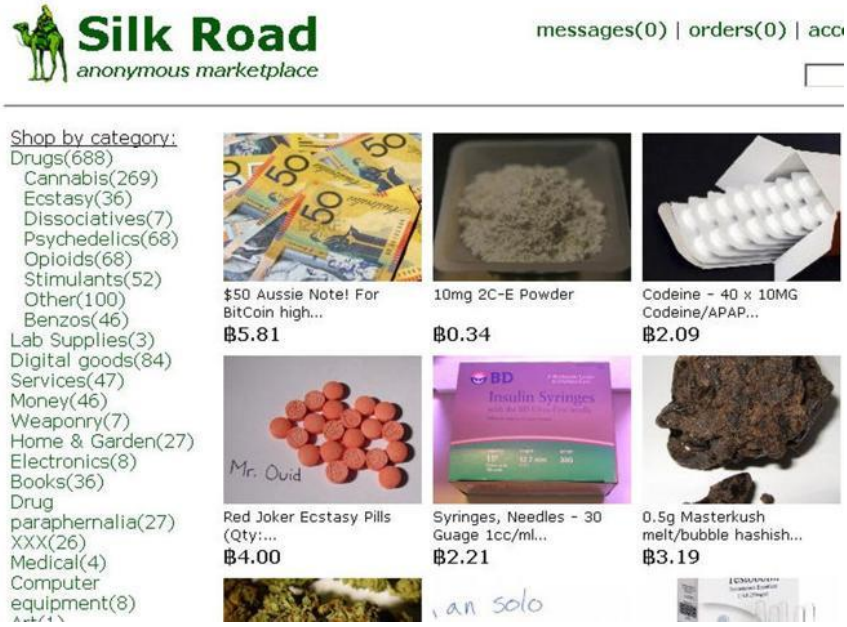

Figura 1 HomePage del sito Silk Road

Fonte: www.corriere.it

2. Le blockchain

2.1. Che cosa è una blockchain?

La blockchain è l'equivalente informatico di un libro mastro pubblico di tutte le transazioni eseguite fino ad un dato momento. Essa può essere pensata come una catena formata da un insieme di blocchi, i quali a loro volta sono formati da un insieme di transazioni. La catena ha la caratteristica di registrare e archiviare tutte le transazioni effettuate all'interno del network, senza la necessità di una terza parte che si occupi della gestione del sistema. Il libro mastro è in continua crescita con la registrazione al suo interno dei dati relativi a tutte le operazioni. I dati sono dotati di un meccanismo di difesa, basato sulla crittografia. Le transazioni avvengono con frequenza continua nel network. In questo modo ogni blocco viene disposto sulla catena in sequenza cronologica a partire dal blocco originale, il cosiddetto Genesis block. Un blocco è la parte corrente della blockchain, esso può essere visto come un contenitore all'interno del quale sono ferme tutte le transazioni in attesa di autenticazione. Il numero di dati iscrivibili in ogni singolo blocco è definito e limitato, ad un massimo di 4200 transazioni (una ogni sette secondi circa). Ogni blocco viene riempito di scritture contabili, corrispondenti alle singole transazioni (per esempio A trasferisce a B un numero X di bitcoin), le quali operano in maniera simile ad un IBAN bancario. Una volta completato ed autenticato, il blocco viene legato alla blockchain e registrato in maniera definitiva nel database (la transazione non può essere in alcun modo annullata). La rete globale effettua il concatenamento ogni 10 minuti circa, ovvero prima dell'autenticazione del nuovo blocco, verifica l'effettivo collegamento di tutti i blocchi della catena (tutti i blocchi dal genesis block fino all'ultimo blocco autenticato). Tramite il meccanismo appena descritto è possibile verificare in ogni momento che le transazioni siano avvenute correttamente, in modo che ogni bitcoin sia trasferito una sola volta, evitando la cosiddetta doppia spesa. In questo modo il funzionamento della blockchain evita che un soggetto invii uno stesso bitcoin a due individui diversi. Ogni nodo, ossia tutti i computer connessi alla rete, detiene una copia della blockchain, che viene scaricata automaticamente da ogni miner che si unisce alla rete bitcoin. La struttura della catena si può quindi schematizzare come nella figura 2 sottostante.

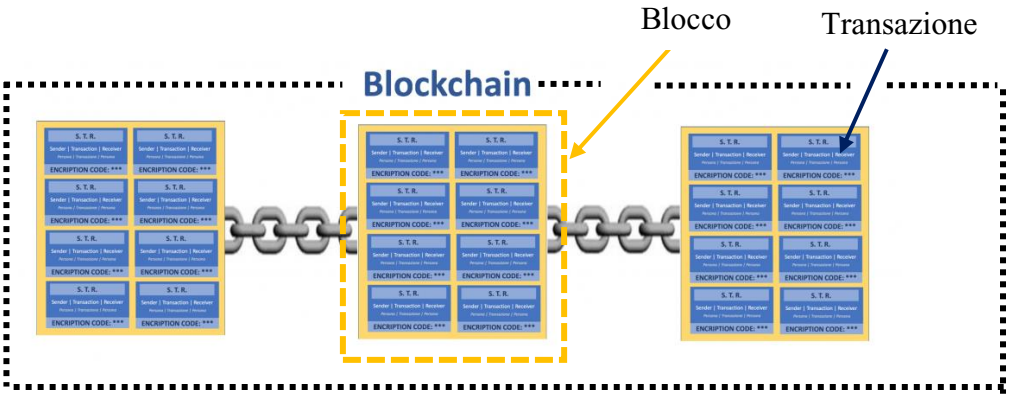

Figura 2 *Fonte: www.blockchain4innovation.it*

Le transazioni contenute all'interno dei blocchi hanno un funzionamento simile a quello della catena blockchain, la differenza sta nel fatto che le transazioni non sono collegate una all'altra secondo un ordine cronologico, ma sono legate alla precedente transazione che ha fornito al mittente i bitcoin con i quali effettua l'attuale trasferimento (l'utente che nella transazione precedente era il ricevente, nella transazione in atto diventa il mittente).
La blockchain è un sistema la cui particella più piccola è la singola transazione, cioè la scrittura contabile base, l'insieme di più transazioni forma un blocco, l'insieme di tutti i blocchi la catena, come raffigurato in figura 2.
Fino a pochi anni fa la blockchain era utilizzata solo per il funzionamento della rete bitcoin, nel senso che non si erano ancora individuati tutti i possibili ambiti in cui una simile tecnologia avrebbe potuto essere applicata. Negli ultimi anni invece, l'interesse per questa tecnologia è aumentato. In quest'ottica è da leggere la nascita di moltissime criptovalute, interessanti non tanto per le valute in sé, ma piuttosto per le tecnologie e le possibilità di utilizzo che offrono. Molto spesso infatti a creare la propria valuta sono società che si occupano di sviluppare una blockchain.

2.2. Storia della blockchain

La prima blockchain fu introdotta, nel 2008, ad opera di Satoshi Nakamoto, e implementata l'anno seguente, con l'obiettivo di fungere da libro mastro della nascente valuta digitale bitcoin. Nakamoto usava le parole block e chain in modo separato nell'articolo originale del 2008. Nel 2009 la creazione di Nakamoto, il bitcoin, fu utilizzata per la prima volta per l'acquisto di un bene fisico, una pizza.

Nell'agosto del 2014, col bitcoin che già aveva raggiunto una certa fama a livello globale, la dimensione della sua blockchain raggiunse i 20 gigabyte mentre nel marzo del 2018 superò i 162 gigabyte.
Nel 2014 si iniziò ad usare il termine blockchain 2.0 per riferirsi a un nuovo modo d'impiego della blockchain. L'idea era quella di permettere alle persone escluse dall'attuale monetizzazione di poter entrare in possesso di un deposito monetario affidabile e sicuro con la possibilità di proteggere la privacy e monetizzare le proprie risorse.

2.3. Come funziona la blockchain

La blockchain presenta uno schema funzionale basato su un registro distribuito, un database che viene reso disponibile a tutti i nodi (computer) presenti nella rete, consentendo così di decentralizzare il controllo rispetto ai classici modelli server/client, in cui la validazione avviene ad esclusiva discrezione di un nodo centrale, gerarchicamente più autorevole di tutti gli altri. Come funziona esattamente questo modello peer-to-peer? Per comprenderne logiche e principi, analizziamo i componenti base di una blockchain e come funziona un protocollo di validazione, prendendo spunto dall'esempio di bitcoin.

2.3.1. Le componenti di una blockchain

Una blockchain è composta almeno da cinque elementi fondamentali:

- Nodi: sono i computer su cui è installato il programma che consente di verificare lo stato dei registri, dei blocchi e delle transazioni in essi contenuti. La rete dei nodi è di natura peer-to-peer, pertanto chiunque può contribuire alla sua implementazione, godendo degli stessi diritti di tutti gli altri, mentre la gestione è demandata ad un programma open source (disponibile a tutti) che gestisce ogni aspetto del funzionamento della blockchain.
- Transazione: è costituita dai dati relativi ad uno scambio di valuta, alla stipulazione / deposito di un contratto. Gli estremi della transazione vengono validati con strumenti crittografici ed archiviati nei blocchi.
- Blocco: contengono le transazioni validate e sono concatenati tramite un valore crittografico che lega un singolo blocco a quello successivo, formando appunto una catena di blocchi (quindi la blockchain).
- Ledger: registro pubblico che contiene i blocchi validati, il cui database è distribuito a tutti i nodi della blockchain. Una volta inseriti ed approvati dalla

maggioranza dei nodi, i blocchi diventano immutabili a livello cronologico. Questo particolare consente di evitare il double spending, ossia la possibilità di scambiare lo stesso bitcoin a più soggetti.

- Hash: è un'operazione basata sulla crittografia asimmetrica, che consente di codificare una stringa di testo/numeri in maniera irreversibile, in modo che qualsiasi nodo possa verificare la sua validità, senza poter leggere espressamente il contenuto della transazione.

A livello di funzionamento, dall'esordio di una transazione all'archiviazione di un blocco intervengono vari momenti, soggetti ad una validazione basata su elementi crittografici. Questo consente di avere una condizione di imparzialità che dà maggiore libertà ai vari nodi, non ci si deve preoccupare dell'operato altrui. Se vi sono anomalie, la natura stessa degli elementi ne rivelerà immediatamente l'evidenza, invalidando i blocchi sospetti.
La forma di transazione più ricorrente su una blockchain è caratterizzata da un trasferimento di bitcoin tra due soggetti. La transazione è sostenuta da una crittografia a doppia chiave. Una chiave privata, che consente ai due soggetti di accedere e rendere disponibile il quantitativo di bitcoin accordato per lo scambio, ed una chiave pubblica, che cifra il contenuto della transazione per consentire la validazione e il successivo inserimento dei blocchi attraverso uno dei protocolli di validazione previsti. L'esigenza di una chiave privata rileva subito una differenza fondamentale rispetto ai sistemi centralizzati. Per capire il concetto possiamo citare i wallet digitali, ossia i portafogli che contengono le criptovalute. Queste applicazioni consentono di conservare ad esempio i nostri bitcoin, ma comportano una grande responsabilità. Nel caso in cui dovessimo perdere la password di accesso, non avremo alcun modo di recuperare i bitcoin presenti nel wallet. È successo a molti che hanno acquistato o minato i bitcoin molti anni fa, dimenticandosi nel frattempo di averli. Ciò avviene perché non c'è nessun soggetto terzo fidato in grado di poterci garantire un recupero dei dati smarriti.
La grande libertà offerta dalla blockchain ha dunque un prezzo da pagare, i servizi che effettua si occupano di gestire il flusso delle transazioni, ma non possono nulla nel controllare il possesso delle risorse, la cui garanzia è data unicamente dal possesso della chiave privata per potervi accedere. La chiave privata può esser vista come un'informazione esclusiva del proprietario di un determinato bene, responsabile della sua conservazione. Tornando a parlare delle transazioni, una

volta chiusa, per essere archiviata, la transazione va inserita in un blocco. Il mittente sottopone la propria transazione alla blockchain di riferimento, pagando una commissione per il lavoro computazionale che i validatori devono effettuare durante la prova di lavoro. Nei periodi di picco, può capitare che vi siano molte transazioni da archiviare ed in tal caso il sistema procederà dando la precedenza a quelle con la commissione più alta, lasciando in attesa le altre. Il blocco contiene l'elenco delle transazioni validate e un Hash identificativo, risultante dalla prova di lavoro necessaria per validarla, che viene riportato nell'intestazione del blocco immediatamente successivo. Questo sistema, come accennato, contribuisce a generare una catena di blocchi molto difficile da corrompere. Dal momento che l'Hash dipende strettamente, in maniera univoca ed irreversibile dal contenuto cifrato, se io provassi a cambiare il contenuto di un blocco, l'Hash non sarebbe più verificato e questo farebbe saltare non soltanto il blocco in questione, ma tutti i blocchi concatenati in seguito. La sicurezza della blockchain viene garantita praticamente a tutti i livelli dal sistema democratico che la regola, dal codice open source del programma di gestione che mette in chiaro le regole del gioco, fino alla massiccia presenza di crittografia in ogni fase prevista che rende assolutamente improbabile il successo delle manipolazioni. Per contro, i privati devono prestare molta attenzione nei confronti della conservazione dei loro dati di accesso, in primis su tutti la chiave privata.

2.3.2. I protocolli di validazione

Le varie blockchain utilizzano differenti protocolli di validazione dei loro blocchi. Il più popolare, nonché quello utilizzato da bitcoin è il cosiddetto proof-of-work (prova di lavoro) e consiste nella risoluzione di un problema matematico, ossia la generazione di un Hash caratterizzato da un determinato quantitativo di zeri iniziali, il cui numero può variare per consentire l'adattamento della difficoltà del problema. Ma perché è necessaria una prova di lavoro?

In un sistema decentralizzato non c'è un soggetto centrale, che gode dei privilegi esclusivi per poter dichiarare valida o meno un insieme di transazioni. Pertanto cosa impedirebbe ad un nodo di validare delle informazioni non coerenti, invalidando la catena? Nulla, se non ci fosse un processo riservato a rendere autorevole e verificabile la validazione dei blocchi, nel pieno interesse di tutti gli individui che partecipano alla blockchain stessa. La prova di lavoro è calcolata dai cosiddetti miner, che in competizione tra loro, devono risolvere nel più breve tempo possibile il problema e comunicare l'Hash ai nodi della rete, che a loro volta

procederanno con una ulteriore verifica prima di dare il consenso di maggioranza necessario per inserire definitivamente il blocco alla sequenza della catena.
La ricompensa dei miner è stabilita in bitcoin, che vengono creati esclusivamente in questo modo, autofinanziando il lavoro necessario al funzionamento della blockchain. Dato che il modello di emissione prevede una rarità che aumenta sempre di più, il quantitativo di bitcoin rilasciato ai miner si dimezza ogni 210.000 blocchi inseriti nella catena, equivalente di circa quattro anni. Attualmente nel 2021 per ogni blocco è prevista una ricompensa di 6.25 bitcoin, cifra che verrà dimezzata nel 2024, nel 2028, nel 2032 ecc. Negli primi periodi era molto semplice minare bitcoin, non occorrevano grandi risorse e i quantitativi ottenuti erano consistenti. Questo spiega perché molti che sono nel giro delle criptovalute fin dalle origini abbiano nel giro di pochi anni accumulato una considerevole quanto inattesa fortuna economica. Attualmente minare bitcoin è molto più impegnativo perché si necessità di maggiori risorse computazionali e le ricompense ottenute sono calate con il passare degli anni, ma anche perché il sistema è in grado di autoregolamentare la difficoltà della generazione del Hash in modo da garantire sempre la validazione di un blocco di transazioni ogni dieci minuti.
Dei 21 milioni di bitcoin previsti da Satoshi Nakamoto, oggi ne sono stati minati quasi 19 milioni, circa il 90% del totale. Il ritmo di emissione calerà drasticamente ad avvicinarsi alla soglia dei 21 milioni di bitcoin in circolazione, ma il fatto che sia estremamente frazionabile (fino a 8 cifre decimali) e il fatto che la sua domanda sia in costante aumento dovrebbe appunto compensare la rarità con l'aumento di valore.

2.4. Tipi di reti blockchain

Le reti blockchain possono essere di tre tipologie: pubbliche, private, con autorizzazione o di consorzio.
Una blockchain pubblica è una rete a cui chiunque può accedere e partecipare, come ad esempio bitcoin. Gli inconvenienti potrebbero includere: la necessità di una notevole potenza di calcolo, poca o nessuna privacy a tutela delle transazioni e scarsa sicurezza.
Una rete blockchain privata, simile a una rete blockchain pubblica, è una rete peer-to-peer decentralizzata. Tuttavia, una singola organizzazione governa la rete, controllando chi è autorizzato a partecipare, eseguire un protocollo di consenso e mantenere il registro condiviso. A seconda del caso d'utilizzo, questo tipo di rete

può incentivare in modo significativo la fiducia e la sicurezza tra i partecipanti. Una blockchain privata può essere gestita dietro un firewall aziendale[1] e addirittura essere ospitata in una blockchain pubblica, usando lo stesso codice, ma rendendola valida solo per il contesto specifico.
Le attività di business che impostano una blockchain privata imposteranno generalmente una rete blockchain basata sulle autorizzazioni. È importante tenere presente che anche le reti blockchain pubbliche possono essere basate su autorizzazioni. Questo pone limitazioni a chi è autorizzato a partecipare alla rete e in specifiche transazioni. I partecipanti devono ottenere un invito o un permesso per partecipare.
Più organizzazioni possono infine condividere le responsabilità della gestione di una blockchain. Queste organizzazioni pre-selezionate stabiliranno chi può inoltrare transazioni o accedere ai dati. Una blockchain di consorzio è la scelta ideale per le attività di business, quando tutti i partecipanti devono essere autorizzati e avere una responsabilità condivisa per la blockchain.

2.5. Vantaggi blockchain

Le varie operazioni al di fuori della tecnologia blockchain spesso sprecano troppe energie nella conservazione di dati duplicati e per le convalide di terze parti. I sistemi di conservazione dei dati, inoltre, possono essere vulnerabili a frodi e attacchi informatici e la trasparenza limitata può rallentare la verifica dei dati. Tutto questo rallenta l'attività di business e incide negativamente sul risultato finanziario e significa che ci serve un modo migliore che incrementi l'efficienza andando a garantire piu sicurezza e minori costi. La blockchain in se offre alcune soluzioni:

- Maggiore fiducia Con la blockchain, in qualità di membro di una rete di soli membri, puoi confidare nel fatto che stai ricevendo dati accurati e tempestivi e che i tuoi stessi dati registrati nella blockchain saranno condivisi solo con i membri della rete a cui hai specificamente concesso l'accesso.
- Maggiore sicurezza: Il consenso sull'accuratezza dei dati è richiesto da tutti i membri della rete e tutte le transazioni convalidate sono immutabili perché vengono registrate in modo permanente. Nessuno, nemmeno un amministratore di sistema, può eliminare una transazione.

[1] Il firewall è un dispositivo per la sicurezza della rete che permette di monitorare il traffico in entrata e in uscita utilizzando una serie predefinita di regole di sicurezza per consentire o bloccare gli eventi.

- Più efficienza: Con un registro distribuito che viene condiviso tra i membri di una rete, vengono eliminate le inutili ripetizioni di dati. E per accelerare le transazioni, un set di regole, detto contratto intelligente (smart contract), può essere memorizzato sulla blockchain ed eseguito automaticamente.

2.6. Svantaggi/rischi blockchain

Nonostante le blockchain offrano nuove opportunità per rendere le dinamiche del settore finanziario (e non solo) più veloci, sicure ed economicamente sostenibili, è possibile fare riferimento ad alcuni svantaggi non ancora superati che sono propri della natura di tali tecnologie.

Mancanza di privacy: Una blockchain per definizione è un database pubblico. Sono nate varie forme di blockchain, come abbiamo visto nel paragrafo 3.4, che hanno declinato in maniera differente questo concetto. Se da una parte rafforza il concetto di trasparenza, dall'altra elimina il concetto di privacy. I nostri dati, le nostre transazioni diventano di dominio pubblico. Chiunque può conoscere il saldo di un wallet, perchè chiunque deve essere in grado di certificare la veridicità del dato. Questo concetto, se da una parte è rivoluzionario, dall'altra disincentiva molte persone ad utilizzare questa tecnologia e, soprattutto, rende questa tecnologia inapplicabile a determinati business.

Password dimenticata/persa: Possiamo paragonare ciò che è conservato in una blockchain, nel nostro caso criptovalute, a delle banconote. Se vengono perse o distrutte non hanno più valore. In questo caso, se la password viene dimenticata o non si riesce più ad accedere al proprio wallet (es: il computer viene formattato), non è più possibile recuperare la propria criptovaluta.

Ci sono moltissimi casi di portafogli dispersi o password dimenticate, basta pensare a quante persone per gioco hanno creato un wallet bitcoin nel primo periodo di nascita di tale fenomeno e poi hanno dimenticato la password in qualche vecchio cellulare o hanno cambiato il computer. È impossibile recuperare una password o un wallet dimenticato. Questa problematica naturalmente non è da sottovalutare e per molte persone è un rischio troppo elevato.

Inalterabilità delle transazioni: Se da una parte è una funzionalità indispensabile per evitare contraffazioni, dall'altra è un limite nel momento in cui non si è l'esecutore di tale transazione. Supponiamo che la nostra password venga rubata e un utente

con cattive intenzioni riesca ad effettuare una transazione, i nostri soldi non torneranno mai più indietro.
Rischio di contraffare la rete: è possibile che la maggior parte dei nodi della rete sia controllata da un'unica entità. In questo caso si disporrebbe della maggior parte della rete e si potrebbe teoricamente creare nuovi blocchi contraffatti.
Nuova tecnologia ancora in fase embrionale: Siamo ancora agli inizi di questa tecnologia che ha enormi potenzialità, ma è ancora immatura in quanto ci sono ancora punti aperti da dover risolvere. Inoltre c'è ancora scetticismo su questa tecnologia. Non tutti comprendono ancora a pieno le sue potenzialità e i problemi che teoricamente potrebbe risolvere. Effettivamente è una tecnologia molto complessa che non ha un riscontro nella vita di tutti i giorni. È qualcosa che è nato nell'ombra e si muove nell'ombra.
Costi: Effettuare una transazione sulla blockchain di bitcoin ha un costo molto elevato, che ad oggi si aggira intorno agli 11 €. Nelle transazioni che hanno ad oggetto lo scambio di somme elevate tale commissione non è un problema ma lo è nelle transazioni che potrebbero essere effettuate quotidianamente. Proprio per questo stanno nascendo alcune blockchain specializzate nelle micro transazioni.
Sostenibilità: Con l'attuale algoritmo di consenso, basato su proof of work il costo elettrico per mantenere la blockchain è molto elevato. Ad oggi si stima che il costo di mantenimento della blockchain di bitcoin sia pari all'elettricità impiegata per alimentare l'Irlanda.
Regolamentazione: Al momento le criptovalute non sono regolamentate a livello finanziario e legale. Ciò comporta dei rischi in termini di frodi e riciclo di denaro. All'inizio, infatti, i bitcoin venivano (e probabilmente ancora vengono) utilizzati all'interno del Deep Web nel sito Silk Road, come abbiamo citato nel paragrafo 2.6. Droga, armi e attività illegali venivano acquistate tramite questa criptovaluta.
L'introduzione di regolamentazione potrebbe però aumentare il rischio di abbandono di questa tecnologia in ambito finanziario, con conseguente impatto sul valore di mercato.

2.7. Possibili applicazioni della blockchain

La tecnologia blockchain funziona dal 2009 ed è stata ampiamente testata dai bitcoin. La blockchain è tuttavia un protocollo trasversale che non tocca solo un esclusivo settore ma anche altri ambiti potenzialmente molto diversi tra loro. Le

possibili applicazioni di questa tecnologia come vedremo di seguito sono molteplici:

- Settore finanziario: L'ambito finanziario è in generale quello più attivo sul tema blockchain. Le banche e la finanza si basano sullo scambio di valori o titoli attraverso sistemi complessi di regolamentazione per garantire l'autenticità delle transazioni. La tecnologia blockchain offre quindi grandi benefici in termini di semplificazione, sicurezza, abbattimento dei costi, eliminazione di intermediari.
- Transazioni di valori mobiliari e immobiliari attraverso un registro distribuito.
- Assicurazioni: Attraverso la tecnologia blockchain è possibile sottoscrivere micro assicurazioni personalizzate su prodotti ad alto valore scambiati tra individui eliminando l'intervento di un'autorità garante nel contratto di assicurazione.
- Identità digitale: Una sperimentazione interessante è quella di Bitnation, che mira a riconoscere l'identità e i diritti dei rifugiati a livello transnazionale, fornendo loro atti di proprietà basati sulla tecnologia blockchain.
- Sanità: Le blockchain applicate al settore della sanità permettono a ospedali e ad altre strutture sanitarie di condividere l'accesso ai loro network senza compromettere la sicurezza e l'integrità dei dati.
- Beneficenza e ONG: L'utilizzo della blockchain permette di monitorare con precisione la tracciabilità dei fondi provenienti dalle donazioni di privati o aziende in modo da ottenere una gestione più efficiente e trasparente del denaro.
- Gestione della catena di distribuzione: Uno degli aspetti più interessanti della tecnologia blockchain è che consente un controllo più sicuro e trasparente delle operazioni nella catena produttivo-logistica. Le catene di approvvigionamento e fornitura sono fondamentalmente una serie di nodi transazionali che permettono di trasferire e spostare i prodotti dalla fabbrica al punto vendita. Grazie alla blockchain, infatti, le transazioni che intercorrono tra i diversi operatori di una filiera (dalla produzione alla vendita) possono essere documentate in un registro decentralizzato riducendo così i costi di trascrizione, i ritardi e i possibili errori umani.
- Networking: diverse multinazionali specializzate in telecomunicazioni stanno lavorando su un concetto di rete decentrata che utilizza una tecnologia simile

alle blockchain per gestire la comunicazione tra dispositivi anche senza un sistema di controllo centrale.

- Legittimazione del voto elettorale: La blockchain può garantire il monitoraggio e il conteggio dei voti, eliminando il rischio di qualsiasi tentativo di frode elettorale, perdita di dati e voti.
- Scuola e mondo accademico: L'utilizzo di registri distribuiti permette di assicurare una maggior trasparenza nella gestione dei certificati accademici e nella trascrizione di crediti legittimamente guadagnati dagli studenti.
- Enti governativi e pubblica amministrazione: La Pubblica Amministrazione e in generale la gestione del sistema del welfare sono settori nei quali le blockchain possono contribuire a semplificare le procedure di erogazione degli aiuti e servizi pubblici.
- Archiviazione di dati nel cloud: Le soluzioni abilitano l'archiviazione decentrata e permettono di ridurre l'esposizione del sistema ad attacchi che possono causare danni sistemici, la perdita o la diffusione dei dati depositati.

3. Le principali criptovalute

3.1. Bitcoin

3.1.1. Cosa è il bitcoin?

Bitcoin nasce nel 2009 ed esso fornisce il nome sia al sistema di pagamento elettronico vero e proprio che alla moneta virtuale utilizzata all'interno del sistema. Il sistema bitcoin utilizza una rete di tipo peer-to-peer (P2P), cioè una rete che non ha una gerarchia. Essa fa parte dei sistemi client/server in cui qualsiasi nodo può operare come client o come server a seconda delle circostanze. Questi nodi possono essere rappresentati da un computer o da un qualsiasi altro dispositivo elettronico in grado di far funzionare il software. Bitcoin quindi non ha sostegno fisico: le valute possono essere detenute in appositi portafogli (wallet) installati sui propri dispositivi elettronici attraverso l'istallazione di un software, oppure in portafogli online gestiti da alcuni portali che svolgono questo servizio.

Questo sistema sfrutta principalmente tre fattori: la tecnologia blockchain per tenere traccia delle transazioni, la crittografia per la gestione degli aspetti funzionali e il meccanismo di mining per la generazione di nuova moneta e la verifica delle transazioni.

Uno dei rischi principali a cui sono esposte le monete digitali è rappresentato dal double spending, ovvero dalla possibilità che la stessa moneta venga spesa più volte. Per questo motivo ogni transazione va verificata e convalidata prima di essere conclusa. Sono proprio gli utenti, i miner, che utilizzano la rete che convalidano le transazioni, mettendo a disposizione la potenza dei loro computer. Ogni volta che un miner convalida un blocco, esso viene trasmesso alla rete in modo che si possa aggiungere alla blockchain, e in cambio riceverà un certo numero di bitcoin di nuova emissione. La blockchain quindi svolge funzioni simili ad un libro mastro, annotando tutte le transazioni effettuate e tutti gli utenti che partecipano alla rete. Il quantitativo di bitcoin che ricevono i miner per la convalida dei blocchi è deciso dal protocollo, come detto precedentemente, ed è stato programmato in modo tale da dimezzarsi ogni quattro anni proprio per evitare di superare il limite di 21 milioni di bitcoin in circolazione. Il protocollo crittografico utilizzato per far sì che i miner risolvano il problema computazionale che porta alla verifica delle transazioni, è noto come Proof-of-Work (PoW).

Va detto inoltre che il software su cui si basa il sistema bitcoin è un software open source, ossia non protetto da copyright, e nel quale tutti i partecipanti possono modificare il sistema, contribuendo alla sua evoluzione e al suo perfezionamento.

Bitcoin oggi è la prima moneta virtuale al mondo. Nei suoi dodici anni di vita esso ha subito alti e bassi, crescendo sicuramente di popolarità ma generando comunque molti interrogativi. Per comprendere meglio i motivi di tali fenomeni, bisogna partire dallo studio delle sue origini storiche, fino ad arrivare allo studio in tempi più recenti.

3.1.2. Storia e sviluppo del bitcoin

La nascita di bitcoin è un fenomeno piuttosto recente ma per capirne fino in fondo le origini è necessario fare qualche passo indietro cominciando dalla storia della crittografia. Inizialmente la crittografia era uno strumento utilizzato esclusivamente dalle istituzioni per mantenere la segretezza di piani o operazioni, ma negli anni '70 ci fu un cambiamento sostanziale in questo ambito a causa del quale la crittografia diviene pubblica e alla portata di tutti. Tale cambiamento è stato stimolato e sostenuto dalla rapida espansione dell'era digitale avvenuta in questi anni.
Una conseguenza della disponibilità pubblica della crittografia e della diffusione di dispositivi tecnologici fu inizialmente il miglioramento della privacy nei servizi di pagamento offerti dalle banche, e in un secondo momento, la nascita di sistemi di pagamento elettronici che usavano denaro virtuale.
Verso la fine degli anni '80 nacquero i Cypherpunks ovvero un gruppo di attivisti che diedero vita ad un movimento che prevedeva l'uso cospicuo della crittografia informatica come base per scatenare un percorso di rivolte sociali e politiche (ad esempio rendendo pubbliche verità scoperte e non dichiarate). Questi esperti di crittografia discutevano e si organizzavano tramite una mailing list, cioè una piattaforma online con lo scopo di condividere idee e progetti. Tale movimento ebbe quindi il merito di riunire molti esperti in materia e di fungere da incubatore di idee dal quale nacquero progetti innovativi, per questo motivo può definirsi il precursore e la fonte di molti cambiamenti in ambito informatico ed economico, come appunto l'avvento di bitcoin.
In realtà l'idea di una criptomoneta in sé stessa non risulta essere innovativa. Sin dai primi periodi di internet, infatti, ci sono stati tentativi di creazione di una moneta virtuale, tuttavia non si è mai riusciti a risolvere problematiche connesse alla natura intrinseca del dato informatico in quanto digitale e afflitto da fenomeni non autorizzati di copia.
Nel 1983 venne creato il primo sistema di pagamenti virtuali denominato e-cash ad opera della Digicash Inc. fondata dal crittografo americano David Chaum. L'innovazione introdotta da tale sistema era che il denaro virtuale veniva tenuto nel

proprio computer e poteva essere speso per acquisti su Internet o nei negozi che lo accettavano, il tutto quindi senza passare attraverso le banche che si limitavano a controllare crittograficamente il denaro in questione. Tuttavia le banche si dimostrarono ostili a questo sistema di pagamenti e in molte non lo accettarono, impedendo così ad e-cash di crescere e facendo fallire la Digicash nel 1998.
Un altro esempio di un predecessore di bitcoin è quello di e-gold, una moneta digitale creata dalla società Gold & Silver Reserve Inc. (GSR) nel 1996 e scambiata in cambio di depositi in oro o argento. Detenere questa valuta quindi significava detenere una certa quantità di metalli preziosi presso la GSR come riserva. E-gold poteva essere usata sia per trasferire denaro tra privati sia per gli acquisti on-line e questo comportò l'adozione di questa valuta da sempre più persone fino a che nel 1999 il mercato crebbe talmente tanto da provocare la nascita di piattaforme di exchange indipendenti. Nel 2007 e-gold venne accusato di permettere il riciclaggio del denaro provocando il definitivo blocco degli account e delle transazioni nel 2009. La gran parte dei sistemi di pagamento virtuali esistenti fino a prima degli anni 2000, tra cui quelli appena descritti, erano sistemi centralizzati ovvero avevano come pilastro portante una banca o un'istituzione che ne regolava il funzionamento e ne garantiva le transazioni.
La svolta dal punto di vista concettuale avvenne nel 1998 anno in cui il programmatore Wei Dai e il crittografo Nick Szabo propongono entrambi separatamente due diversi sistemi di pagamento decentralizzati.
Wei Dai creò una moneta chiamata b-money basata su alcune proprietà che si riscontrano tutt'ora in bitcoin: la creazione di moneta si effettua tramite risoluzione di problemi grazie ad una certa potenza di calcolo (cardine di bitcoin), le transazioni avvengono mediante uso della firma digitale e infine gli utenti si registrano in un network anonimo tramite pseudonimi o nomi che non ne rivelino l'identità.
Nick Szabo ideò nello stesso periodo bit-gold, che a sua volta possedeva alcuni caratteri che contribuirono alla nascita di bitcoin. Anche nel caso di bit-gold la creazione di moneta avveniva grazie a calcoli effettuati da diversi computer, proprio come previsto dall'idea di Wei Dai, ma in questo specifico caso i computer devono trovare la cosiddetta challenge string dove l'utente che riesce a rintracciare per primo la stringa e riesce a risolverla la fa propria come se fosse un premio, in questo modo nel sistema bit-gold viene generata moneta.
Tutti i fenomeni e gli eventi appena descritti contribuirono in modi diversi alla nascita di bitcoin. Nel Novembre del 2008 un certo Satoshi Nakamoto pubblicò su internet un documento intitolato "Bitcoin: A Peer-to-Peer Electronic Cash System"

(Nakamoto, 2008) il cui obiettivo era spiegare come fosse possibile il trasferimento di denaro digitale senza il tramite di istituzioni finanziarie o qualsiasi altro ente del genere. Sull'identità di Satoshi Nakamoto, il creatore di bitcoin, si sa ben poco e si ritiene che tale nome sia in realtà uno pseudonimo che nasconde una persona (o un gruppo di persone) estremamente esperta di crittografia.
La data ufficiale in cui è stato emesso il primo blocco di bitcoin (Genesis block) è il 3 Gennaio 2009 e il 12 Gennaio dello stesso anno venne registrata la prima transazione con cui Satoshi Nakamoto invia 10 bitcoin ad un esperto crittografo facente parte dei Cypherpunks. Nei primi mesi di vita dei bitcoin il loro valore era irrilevante e gli unici a possederne erano gli sviluppatori che li avevano generati. Inizialmente non esistevano nemmeno piattaforme online che permettevano il cambio con la valuta tradizionale (i cosiddetti exchange) e quindi le compravendite avvenivano esclusivamente nel forum del progetto bitcoin (bitcointalk.org).
L'obiettivo principale degli sviluppatori e di questo forum era diffondere sia la conoscenza della criptovaluta che la criptovaluta stessa in modo da coinvolgere sempre più utenti e in modo da ingrandire il sistema bitcoin. Per raggiungere tale scopo vennero create transazioni di qualsiasi tipo tramite le quali i possessori di bitcoin acquistavano praticamente qualsiasi cosa al solo fine di diffondere informazioni.
Nel 2010 vennero creati i primi exchange e ciò provocò una perdita di controllo sulle transazioni per gli sviluppatori, con gravi conseguenze. Venne scovato un punto debole nel sistema di sicurezza, ovvero le transazioni non venivano controllate in modo preciso ed esaustivo prima di venire registrate, ciò permise ad un gruppo di hacker anonimi di generare dal nulla un blocco del valore di 184 milioni di bitcoin. In poco tempo gli sviluppatori intervennero correggendo il bug del sistema e annullando le transazioni fasulle. Negli anni successivi il valore di bitcoin ha avuto un andamento generalmente positivo, con varie fluttuazioni di segno negativo ma il trend del valore a livello globale era di crescita sostenuta.
Il 2011 è l'anno in cui ci si è iniziati a rendere conto dell'esistenza di bitcoin, infatti il suo utilizzo crebbe rapidamente (nel giro di pochi giorni il suo valore è passato da 1$ a circa 32$), molte associazioni iniziarono ad accettare tale criptovaluta per le donazioni e vennero aperti siti web per scambiare bitcoin con prodotti di qualsiasi tipo.
Tra il 2012 e il 2013 aumentò il numero dei commercianti in grado di accettare pagamenti in bitcoin grazie soprattutto ad alcuni servizi di pagamento (ad esempio

Bitpay, CoinBase e GoCoin) che permettono ai negozianti e alle imprese di convertire i bitcoin in valuta locale.
In quel periodo inoltre venne creata la Fondazione bitcoin con l'obiettivo di promuovere e proteggere tale valuta garantendo sicurezza agli utilizzatori e aumentando la loro fiducia verso questo sistema di pagamento. Nell'Aprile del 2013 il prezzo di un bitcoin supera per la prima volta i 100$ e a Novembre dello stesso anno raggiunge la prima quota record di 1000$.
Il 2014 è stato un anno che ha visto il prezzo di bitcoin decrescere progressivamente, nel mese di Gennaio un bitcoin era scambiato con circa 800$ fino a sfiorare i 900$, mentre da Febbraio è iniziato un forte calo che ha visto il prezzo di Bitcoin chiudere a fine anno attorno ai 400$ con una perdita di circa il 50%. Le cause che spiegano questo declino sono molteplici: la più importante e incisiva è stata sicuramente il fallimento di Mtgox che era una tra le principali e più utilizzate piattaforme di exchange a livello globale che si dimostrò insolvente a causa di numerosi attacchi hacker che provocarono ingenti danni ai portafogli degli utenti. Questo fatto non solo fece perdere molti risparmi agli utenti, ma soprattutto contribuì a diminuire ulteriormente la già instabile fiducia nei confronti di bitcoin.
Un'altra causa è stata la chiusura di Silk Road 2.0 (poi definito l'Amazon delle droghe), un sito online nato nel 2011 per la compravendita di droghe, materiali pericolosi e altri prodotti illegali in cambio di bitcoin. Tale sito ebbe parecchio successo e tutti i suoi utilizzatori, costretti ad acquistare bitcoin per comprare quella merce, contribuirono in modo rilevante alla crescita e alla diffusione della criptovaluta. La prima versione di Silk Road venne chiusa nel 2013 ma successivamente venne aperto Silk Road 2.0, una piattaforma ancora più grande e che attirò ancora più utenti con un circolo di bitcoin ancora maggiore, la sua chiusura provocò un calo negli acquisti della criptovaluta comportando un relativo calo anche nel suo prezzo.
A fare da contrappeso a questa tendenza al ribasso del prezzo di bitcoin, alcune multinazionali tra cui Microsoft e Dell iniziarono ad accettare la criptovaluta come mezzo di pagamento contribuendo ad aumentarne la diffusione e soprattutto rivestendo di importanza e di sicurezze questa valuta ancora per molti sconosciuta.
Il 2015 è stato un anno complessivamente positivo per il bitcoin anche se ha subito alcuni shock (ad Agosto il prezzo di bitcoin scese del 19% in appena 30 minuti a causa di un attacco hacker ai danni di un importante exchange) ma nonostante tutto in poco tempo è riuscito a risollevarsi e a fine Dicembre arriva a sfiorare la soglia dei 500$.

Nel 2016 bitcoin ha registrato crescite lente ma sostenute e continuative, confermando così il ruolo di criptovaluta leader del mercato e di investimento alternativo estremamente interessante per qualsiasi tipo di investitore. A fine anno il prezzo di un bitcoin stava per raggiungere quota 1.000$.
Le crescite record che dimostrarono il potenziale di bitcoin si sono registrate nel 2017, precisamente tra Marzo, quando 1 bitcoin aveva raggiunto un valore appena superiore ai 1.000$, e Giugno, quando 1 bitcoin veniva scambiato per 3.000$ circa.
La principale causa di questa crescita esponenziale risiede in una delle caratteristiche principali di bitcoin, la non tracciabilità. A Marzo 2017 infatti possiamo vedere che c'è stato un attacco da parte di un gruppo di hacker russi che ha colpito moltissime tra le imprese più grandi del mondo (imprese del calibro di Renault), questi hacker hanno chiesto un riscatto pari all'equivalente di 600$ in bitcoin (per non essere rintracciati) per ogni computer infettato dal loro virus, chiamato virus wannacry.

Figura 3

Fonte: www.it.wikipedia.org

Ovviamente le imprese furono costrette ad acquistare bitcoin per pagare il riscatto, e in tempi rapidi per non fermare la produzione e non perdere dati importanti. Tale acquisto di massa fece esplodere il prezzo della criptovaluta. L'ascesa del prezzo del bitcoin lo porta ad avere un valore di circa 16.000$ alla fine del 2017.
All'inizio del 2018 il prezzo del bitcoin si riassesta al valore medio dell'anno precedente, tornando a circa $ 6.000.
Lo sviluppo del bitcoin riprende però la sua evoluzione, con Lightning Network, protocollo in grado di velocizzare le operazioni sulla rete e nei pagamenti. Il potenziale della moneta di conseguenza attira l'interesse di molte banche e operatori

istituzionali, ponendo le basi per la crescita del valore del bitcoin. L'ingresso di questi attori nel settore ha elevata un'importanza che consente di aumentare la possibilità di accedere al mercato di bitcoin, aumentandone la domanda, da parte di una platea di investitori privati. L'aumento della domanda che ne deriva si ripercuote sul valore di scambio, tra il 2019-2020 il valore è rimasto all'incirca attorno ai 10.000$ in media (ha avuto picchi massimi di 13000$ circa e picchi minimi di 7000$).
Nel 2021 si raggiunge un record per il valore di questa criptovaluta, che nel mese di Aprile valeva 63 mila dollari. Tutto ciò è avvenuto proprio alla vigilia dell'ingresso in borsa di Coinbase, il primo exchange pubblico di criptovalute della storia. La quotazione di Coinbase risulta quasi essere un evento rassicurante per la solidità delle criptovalute, che non sono protette da alcuna banca centrale, stimolando il loro uso e possesso.

3.1.3. Caratteristiche del bitcoin e differenze con la moneta fiat

Per moneta fiat si intende ogni valuta legale istituita e rilasciata da un'autorità centrale, accettata dalle persone in cambio di beni e servizi grazie alla fiducia che questi ripongono in quell'autorità. È possibile quindi affermare che il fattore su cui si basano le monete fiat è proprio la fiducia. Invece bitcoin è una moneta virtuale che non è gestita da un'autorità centrale bensì da tutti gli utenti facenti parte al sistema.
Per evidenziare le differenze tra criptovalute e monete fiat è utile considerare le principali funzioni della moneta e vedere come le une e le altre vi si approcciano.

Mezzo di scambio: La moneta fiat può essere scambiata istantaneamente con beni e servizi, l'acquirente consegna moneta al venditore e in questo modo si libera da ogni obbligo nei confronti di quest'ultimo che, accettandola, ne riconosce il valore. Il bitcoin come mezzo di scambio ha alcune caratteristiche interessanti. Possiamo dire che è il primo bene digitale di valore che può essere trasferito su internet senza che nessuna terza parte specifica debba approvare la transazione o possa negarla. È anche un bene che viene trasferito da un proprietario ad un altro piuttosto che muoversi attraverso una serie di debiti e crediti di terze parti, ad esempio attraverso più banche. Rispetto al bitcoin come mezzo di scambio ci sono ancora molti dubbi, visto il fatto che difficilmente viene accettato come mezzo effettivo di pagamento da parte dei commercianti. Nella maggior parte dei casi coloro che li accettano si

appoggiano a degli intermediari che citano un prezzo al cliente in bitcoin e poi trasferiscono una quantità equivalente di valuta convenzionale in uno specifico conto corrente.

Riserva di valore: La moneta fiat permette di spostare nel tempo la quota di reddito che non viene utilizzata immediatamente per consumare beni e servizi. In altri termini, consente di conservare (risparmiare) una quota del reddito corrente per spenderlo in futuro. Il bitcoin come riserva di valore assume un ruolo particolare. Bisogna farsi delle domande, cosa si vuole dalla riserva di valore? Qual è il suo compito? Il suo compito è quello di arricchirci, oppure quello di mantenere il suo valore per pianificare al meglio la nostra vita? Qual è il rischio che si è disposti a sopportare? Stiamo parlando di una riserva a breve termine, forse un investimento speculativo, o una riserva di valore a lungo termine (spesso un bene a basso rischio)?
Queste sono delle domande che sorge spontaneo porsi quando si vuole comporre la propria riserva di valore in bitcoin. Come investimento speculativo il bitcoin si è comportato molto bene, ha iniziato nel 2009 ad un valore pari a zero e ora dopo dieci anni vale migliaia di dollari. Possiamo dire quindi con certezza che il bitcoin per via della sua volatilità di prezzo, molto elevata rispetto alla maggior parte delle valute fiat, fallisce nell'essere una riserva di valore a lungo termine.

Unità di conto: La moneta fiat si usa per confrontare in maniera omogenea il valore di prodotti e servizi molto diversi tra loro, agevolando così le decisioni economiche e gli accordi contrattuali. Il bitcoin come unità di conto fallisce miseramente, a causa della sua volatilità di prezzo rispetto al dollaro e a tutte le altre valute legali. Il fatto che non ci sia quasi nessun commerciante che sia disposto a prezzare oggetti in bitcoin è la prova che non sono una buona unità di conto. C'è solo un caso (di nicchia) in cui il bitcoin può essere usato come unità di conto, ossia quando si valutano carrelli di altre cripovalute. Se sei un trader di criptovalute, probabilmente vuoi ancora capire il valore totale del tuo patrimonio nella valuta nazionale, ma in questo caso molto specifico, potresti anche voler capire il tuo saldo totale in bitcoin poiché leader mondiale delle criptovalute; si potrebbe dire che il bitcoin è il dollaro delle criptovalute.

Facendo un focus sulle valute fiat, esse non hanno un valore intrinseco e convertibile. Sono dichiarate dalla legge come valuta legale, il che significa che in

quella giurisdizione legale devono essere accettate come pagamento valido per un debito. Perciò la gente la usa. In secondo luogo perché i governi accettano solo il proprio fiat per il pagamento delle tasse. Questo dà alle valute fiat un'utilità fondamentale, dato che tutti devono pagare le tasse. Le criptovalute sono quindi estremamente connesse alle fiat, ma ad oggi, ma non sono dichiarate a corso legale in nessuna nazione.
Tornando a parlare di bitcoin vale la pena ripetere che quest'ultimo è il primo bene digitale che può essere trasferito su internet senza che una terza parte specifica debba approvare la transazione o possa negarla. Tra le caratteristiche principali del bitcoin possiamo citare:

- Natura decentralizzata: come già anticipato, bitcoin non è gestito da un'autorità centrale e i partecipanti apprezzano proprio che le transazioni non coinvolgano terze parti nel processo, questo vuol dire che non interviene nessuna istituzione finanziaria. La decentralizzazione inoltre, assicura al sistema che nessun soggetto possa aumentare o diminuire la quantità di moneta in circolazione poiché essa è stabilita a priori dal protocollo.
- Transazioni a bassi costi: proprio il fatto che le transazioni non debbano passare attraverso gli intermediari, fa sì che i costi per approvarle siano molto più bassi rispetto alle comuni transazioni bancarie.
- Transazioni facili e veloci: grazie all'utilizzo di bitcoin è possibile spostare il proprio denaro a livello globale in modo facile e veloce, è come inviare un messaggio, la liquidazione è istantanea. Invece nel caso delle transazioni bancarie, la somma impiega minimo tre giorni lavorativi affinché avvenga il regolamento.
- Transazioni trasparenti: il libro mastro della blockchain è pubblico e ciò permette ad ogni utente di poter visualizzare qualsiasi transazione di bitcoin dalla prima all'ultima.
- Nessuna inflazione: sappiamo che il numero totale di bitcoin che può essere emesso tende asintoticamente al limite di 21 milioni, il quale frena un po' la sua diffusione generale. Il bitcoin nasce quindi come moneta che non può essere soggetta ad inflazione perché ha un limite massimo di emissione, ma è addirittura una moneta deflattiva, perché andando avanti nel tempo, l'offerta tenderà a diminuire e conseguentemente il prezzo tenderà a salire.

- Utilizzo di pseudonimi: per partecipare alla rete basta registrarsi fornendo un indirizzo IP cosicché non venga utilizzato il vero nome dell'utente bensì uno pseudonimo. Quindi nel momento in cui gli utenti entrano in contatto, sarà visibile solo il loro pseudonimo. I partecipanti utilizzano quindi gli pseudonimi per rimanere anonimi e proteggere la propria identità.
- Software open code per l'estrazione della moneta: bitcoin applica gli stessi algoritmi che vengono utilizzati nell'online banking, l'unica differenza è la divulgazione delle informazioni sugli utenti. Tutte le informazioni relative alle transazioni nella rete bitcoin sono condivise, ma non ci sono dati sul destinatario o sul mittente delle criptovalute.

3.1.4. Tecnologia utilizzata dal bitcoin

Bitcoin è un sistema che utilizza diverse tecnologie che garantiscono il suo funzionamento, sono la rete Peer-to-Peer e la blockchain. Il Peer-to-Peer è una delle tipologie dei sistemi distribuiti, essi infatti si dividono in:

- Sistemi Client-Server: in questo sistema il server è l'unità centrale di registrazione, nonché l'unico fornitore di contenuti e servizi. Ogni client può solamente richiedere un contenuto o l'esecuzione di un servizio, senza condividere i propri servizi ad altri client.

- Sistemi Peer-to-Peer (p2p): questi sistemi invece sono una particolare rete distribuita, in cui ciascun sistema informatico all'interno della rete è chiamato nodo. Questi nodi sono tra loro equivalenti, autonomi e collegati in modo altamente dinamico, essi condividono una parte delle proprie risorse come potenza di elaborazione, archiviazione, software e contenuti dei file. Ogni nodo può svolgere sia la funzione di client che quella di server verso tutti gli altri nodi della rete.

Bitcoin utilizza proprio la rete Peer-to-Peer nel suo sistema, tale rete è costruita in modo tale che ogni utente che partecipa condivide le informazioni delle transazioni con gli altri utenti, dunque non è presente nessun intermediario che fa da tramite. Ciò riconferma la natura decentralizzata del sistema in cui non interviene nessuna autorità centrale come banche o altri intermediari.

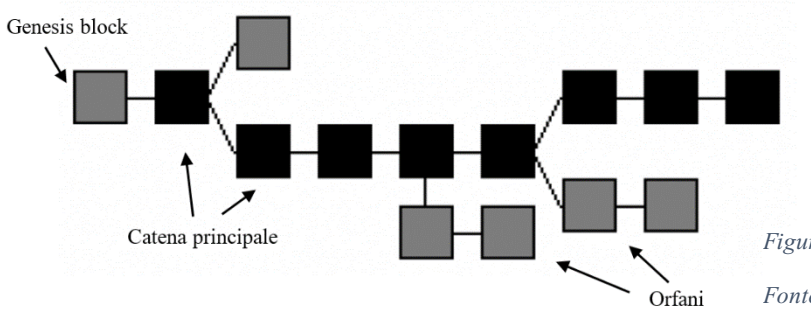

Figura 4

Fonte: www.en.wikipedia.org

Nella figura 4 è rappresentata la catena iniziale della blockchain di bitcoin, essa comincia dal cosiddetto Genesis block, dopo di che continua con una catena principale e da altri vari blocchi, detti orfani. I blocchi seguono un ordine cronologico e sono legati tra loro attraverso la crittografia, è proprio grazie all'utilizzo della crittografia che i dati sono protetti, inoltre essa è utilizzata anche per verificare le transazioni, elaborare i pagamenti e controllare la fornitura di bitcoin. Bitcoin in particolare sfrutta una crittografia di tipo asimmetrica in cui vengono utilizzate sempre due chiavi: una pubblica e una privata. Ogni utente può interagire con la rete attraverso la creazione di un indirizzo chiamato bitcoin address ed è proprio questo che garantisce la riservatezza della propria identità. La capacità di inviare pagamenti attraverso i bitcoin address è controllata tramite firme digitali, che coinvolgono la chiave pubblica e la chiave privata. In particolare ogni indirizzo bitcoin è identificato da un ID pubblico e univoco, ovvero un identificatore alfanumerico che corrisponde alla chiave pubblica. La chiave privata è la controparte della chiave pubblica e dà il controllo sui bitcoin contenuti in questo indirizzo.

3.1.5. Come ottenere bitcoin

Esistono quattro modi per ottenere bitcoin:

- Cambiare una valuta in bitcoin: ovvero acquistare bitcoin presso gli exchange online in cambio di valuta legale o di altre criptovalute. Il tasso di cambio a cui comprare o vendere bitcoin è fissato dalla stessa piattaforma online che quindi svolge il ruolo di market maker. I migliori e più famosi bitcoin exchange al momento, ovvero quelli più usati e più votati dagli utenti, sono Coinbase, LocalBitcoins e Poloniex.

- Bitcoin ATMs (o Bancomat Bitcoin): si tratta di dispositivi fisici in cui è possibile acquistare bitcoin con un enorme abbattimento dei tempi per l'autenticazione richiesti dagli exchange online, infatti se si è già in possesso di un wallet la transazione avviene in meno di 30 secondi. Il primo bitcoin ATM è stato prodotto dall'azienda americana Robocoin ed installato nel 2013 a Vancouver, Canada. Visto l'aumento dell'offerta di bitcoin nel mondo, il numero di Bitcoin ATMs sta aumentando proporzionalmente.
- Vendere beni o servizi in cambio di bitcoin: nel mondo sono sempre più numerosi i negozi fisici e i siti di compravendita online che accettano pagamenti in bitcoin.
- Fare mining: I primi tre metodi sono tradizionali e possono essere applicati a qualsiasi valuta mentre il mining è una tecnica che viene utilizzata da bitcoin (e da gran parte delle altre criptovalute esistenti) per ovviare alla mancanza di un intermediario finanziario che garantisca la sicurezza nelle transazioni.

Come già accennato, uno dei punti cardine su cui è stato creato il bitcoin è la totale decentralizzazione quindi l'indipendenza dalle banche o da qualsiasi altra istituzione. E' stato anche detto che la blockchain ha come scopo garantire la sicurezza delle transazioni, ma com'è possibile che le transazioni siano sicure in un sistema autonomo e lontano da tutte quelle che fino ad oggi erano considerate le certezze fisiche per quanto riguarda gli scambi di denaro? Come sopperire alla mancanza di un'autorità centrale? Come garantire la fiducia in un sistema così diverso da ciò a cui siamo abituati?
La risposta a questi quesiti viene fornita da un processo chiamato mining. Il mining è un processo basato sulla risoluzione di un proof-of-work (prova di lavoro) che consente ad ogni individuo (detto anche miner) di mettere a disposizione del sistema bitcoin la potenza di calcolo di un proprio computer (tramite un software open source e gratuito), facendo in modo che quest'ultimo lavori per decriptare e verificare le informazioni scambiate in ogni transazione, per poi creare un blocco che raggruppi tutte le transazioni effettuate e validate in un certo intervallo di tempo, tutto questo allo scopo di mantenere l'integrità della blockchain.
Ma come fa bitcoin a verificare la correttezza di ogni transazione?
Il sistema impone la risoluzione di una funzione hash per ottenere un hash identificativo (come anticipato nel paragrafo 3.3.1), ovvero una stringa composta da numeri e lettere di lunghezza prefissata. Ai dati della transazione iniziale è associato un unico hash identificativo ed è quindi l'unico elemento che, una volta

trovato dai miners, può accertare la transazione e creare il blocco. Questo processo ha un elevato grado di sicurezza in quanto anche un minimo cambiamento nei dati iniziali modifica completamente l'hash. Un ulteriore elemento che aumenta la sicurezza del bitcoin è che ogni nuovo hash contiene informazioni su tutti i blocchi precedenti, ciò significa che nemmeno a posteriori è possibile modificare o falsificare i dati di uno scambio avvenuto in precedenza altrimenti tutto il sistema se ne accorgerebbe.

Tutti i nodi della rete competono per essere i primi a trovare una soluzione ad un problema di crittografia che riguarda il blocco candidato, il problema non può essere risolto in altri modi se non tramite un enorme numero di tentativi con cui si cerca di trovare la stringa che riesca a chiudere il blocco. Quando un nodo trova l'hash identificativo corretto lo annuncia al resto della rete attribuendosi così i bitcoin in premio previsti dal protocollo, i nodi che ricevono il nuovo blocco lo verificano e lo aggiungono alla catena, ricominciando il lavoro di mining al di sopra del blocco appena ricevuto. Per ogni blocco completato si ottiene come ricompensa una frazione in bitcoin, frazione che dipende da molte variabili tra cui la complessità di ogni transazione e la capacità computazionale messa a disposizione del sistema bitcoin, e delle commissioni di transazione.

Nel sistema bitcoin le regole per il mining sono stabilite con estrema precisione. Infatti ogni due settimane si devono produrre mediamente 2.016 nuovi blocchi, indipendentemente dal numero di transazioni presenti nel sistema. Alla fine del periodo di due settimane se i nuovi blocchi prodotti si discostano dal numero obiettivo di 2.016, la difficoltà di produzione di un nuovo blocco viene diminuita o aumentata, a seconda che la creazione di nuovi blocchi sia stata inferiore o superiore alla soglia.

Anche la quantità di nuovi bitcoin emessi ad ogni produzione di un nuovo blocco è fissata (ovvero la ricompensa per i minatori). Tale importo si attestava originariamente in 50 bitcoin per blocco, e viene dimezzata progressivamente ogni 210.000 nuovi blocchi, attualmente (nel 2021) dovrebbero essere circa 6.25 bitcoin a blocco se le previsioni sono state rispettate. Questa ricompensa attribuita ai miners che risolvono un blocco è l'unico modo che il sistema bitcoin ha per emettere moneta.

Alla luce di quanto detto è confermato che non solo la quantità delle transazioni ma anche il numero di miners aumenta sempre di più nel tempo, e quindi anche la difficoltà di creare ogni singolo blocco cresce ad un tasso elevato. Infatti più miners sono presenti nel sistema e più potenza di calcolo viene erogata per risolvere il

blocco, ma quando quest'ultima aumenta il sistema fa in modo di rendere più complessi gli algoritmi da decriptare, aumentando di conseguenza il numero di calcoli mediamente necessari a creare un nuovo blocco e aumentando quindi il costo di creazione dello stesso.
A tale proposito si noti la Figura sottostante che ci mostra il grado di difficolta del processo di mining dalla nascita del bitcoin. Il grado di difficoltà viene misurato in funzione del numero di transazioni che vengono effettuate, visibili nell'asse dello ordinate nel grafico sottostante, necessarie per creare il blocco.

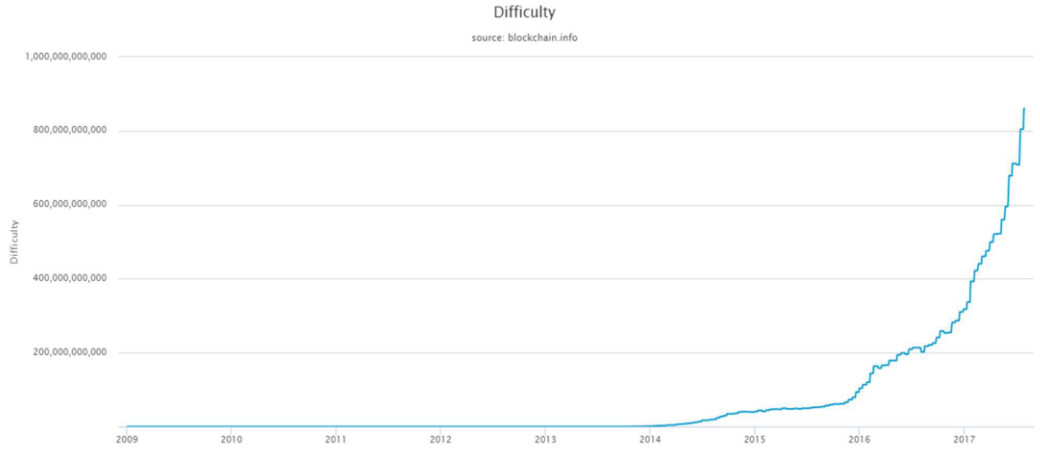

Figura 5

Fonte: www.blockchain.info

In parole povere il mining è stato ideato da Satoshi Nakamoto per rendere sicura la blockchain e tale sicurezza è garantita dallo stesso protocollo attraverso un particolare sistema di attribuzione di ricompense.
C'è da dire però che il mining è un processo molto costoso per i miners in quanto i calcolatori appositi hanno prezzi elevati, vengono sfruttati al massimo della loro CPU (e quindi si usurano in poco tempo) e il processo in sé consuma molta energia elettrica.
Ad oggi per fare mining è necessario iscriversi ad una pool, cioè un gruppo di miners che riunisce la capacità computazionale di ogni individuo in modo da impiegare meno tempo a risolvere un blocco e quindi avere più probabilità di essere

ricompensati, e per l'adesione a queste pool è necessario pagare una tassa pari ad una percentuale variabile per ogni ricompensa ricevuta.

3.1.6. Come detenere bitcoin

Per poter utilizzare i bitcoin, gli individui devono creare una sorta di portafoglio virtuale chiamato wallet.
I wallet si trovano su un server remoto e accessibile attraverso un sito web così da non occupare spazio sul disco rigido del proprio computer ed essere accessibile ovunque. Questo portafoglio contiene un file regolarmente aggiornato che elenca tutte le transazioni bitcoin effettuate, così che analizzandole si può risalire al saldo. Per trasferire bitcoin ad altri portafogli, gli utenti utilizzano una combinazione di crittografia a chiave pubblica e privata. La transazione contiene la quantità di bitcoin e una firma digitale univoca della transazione, protetta appunto da una chiave privata, mentre la chiave pubblica è fornita dal destinatario e funge da indirizzo di invio. La combinazione di chiavi pubbliche e private garantisce un certo livello di privacy tra coloro che si scambiano i bitcoin sulla rete. Però nel caso in cui la chiave privata venisse smarrita, i bitcoin interessati andrebbero persi per sempre. Esistono diversi tipi di wallet ed è possibile suddividerli in base a diverse caratteristiche. La prima suddivisione è riferita alla possibilità di funzionare offline oppure solo online, distinguiamo quindi gli Hot wallet dai Cold wallet. Gli Hot wallet funzionano per lo più online e le transazioni possono essere eseguite in qualsiasi momento. Tra questi troviamo gli online wallet, i desktop wallet ed i mobile wallet. I Cold wallet invece funzionano offline e cercano di evitare possibili attacchi internet. Tra questi troviamo i paper wallet e gli hardware wallet. Ovviamente essi sono esposti ad altri tipi rischi e quindi non è possibile stabilire di preciso quale tipologia di portafoglio sia più sicura. È possibile distinguere anche i portafogli in deterministici e non deterministici, in base ai metodi di generazione delle chiavi. I portafogli deterministici generano tutte le chiavi a partire da un seed che viene chiamato singol key o root key e sono generalmente suddivisi in base ai livelli di sicurezza. Il portafoglio non deterministico invece, genera chiavi casuali e indipendenti che richiedono il backup di tutte le chiavi e la memorizzazione delle stesse.
La classificazione più comune però viene fatta in base alle esigenze degli utenti e al luogo in cui vengono custodite le chiavi, e possiamo quindi distinguere:

Paper wallet: essi non vengono utilizzati da soli e rientrano, come già detto, nella categoria dei Cold wallet. Sui paper wallet ci sono due codici QR, uno serve a codificare l'indirizzo dell'utente per ricevere le monete e l'altro serve a codificare la chiave privata dell'utente per spendere le monete. La particolarità di questi wallet risiede nel custodire in formato cartaceo la coppia di chiavi utilizzate per le transazioni. In questo modo è possibile proteggersi dagli attacchi internet. Nella Figura 6 è possibile vedere un esempio di Paper wallet.

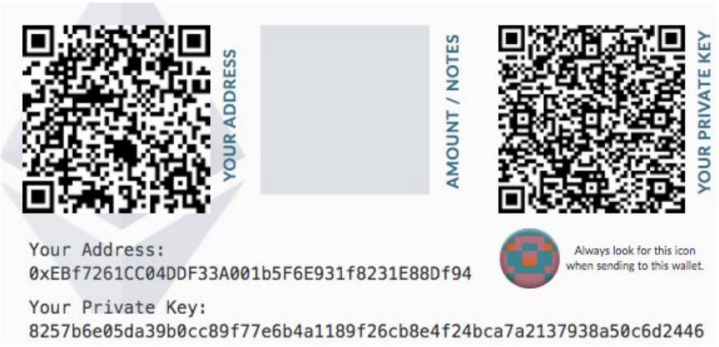

Figura 6

Fonte: www.ilbitcoin.news

Hardware wallet: rientrano nella categoria dei Cold wallet, quindi la conservazione delle chiavi sensibili avviene offline rendendo questi portafogli più sicuri di altri tipi. Gli attacchi online ai quali sono soggetti sono previsti solo durante lo svolgimento di una transazione, cioè quando un utente collega il portafoglio hardware ad un computer per effettuare una transazione. Ci sono però almeno altri due rischi che caratterizzano questi wallet, ossia la possibile perdita dell'hardware o il suo guasto. Questi inconvenienti possono causare la perdita dell'intero portafoglio, laddove non fosse stato eseguito un backup in un altro dispositivo

Mobile wallet: rientrano nella categoria degli Hot wallet. A differenza dei precedenti, forniscono una maggiore comodità di conservazione delle chiavi private. Essi infatti sono delle particolari applicazioni per dispositivi mobili che consentono ai proprietari di utilizzarli quasi ovunque e in qualsiasi momento. Usano inoltre un altro vantaggio dell'essere Hot wallet, la verifica della validità della transazione è svolta senza scaricare l'intera blockchain.

Desktop wallet: questo tipo di portafogli sono rappresentati da un software che viene installato sul proprio PC, limitando quindi la possibilità di accesso a quel solo dispositivo. In questo caso però viene scaricata l'intera blockchain, che quindi andrà ad occupare parte della memoria del computer dell'utente. I Desktop wallet hanno capacità più elevate rispetto ad altri tipi di wallet, bisogna però fare attenzione a proteggere adeguatamente il dispositivo sia dagli attacchi della rete che dai virus.

Online wallet: vengono chiamati anche Cloud wallet, e sono portafogli basati sul web, ossia è possibile accedervi da un qualsiasi dispositivo in grado di collegarsi alla rete internet. Essi funzionano su sistemi cloud gestiti da intermediari nei quali gli utenti devono nutrire sufficiente fiducia, dato che la conservazione delle chiavi private all'interno dei cloud li rende il bersaglio principale degli hacker.

3.2. Ethereum

3.2.1. Cosa è ethereum

Ethereum è una piattaforma decentralizzata per la gestione di contratti intelligenti. Mentre bitcoin ha lo scopo di fungere da moneta virtuale, il fondatore di ethereum (Vitalik Burerim) non ha voluto limitare solo a questa funzione il suo progetto. La sua caratteristica principale è quella di essere una piattaforma all'interno della quale è possibile sviluppare applicazioni, software e Smart Contract, come andremo ad analizzare nel paragrafo 4.2.3. Il funzionamento di questi contratti si sostanzia nella programmazione di applicazioni che eseguono in maniera autonoma esattamente quanto è stato programmato al momento dell'accordo tra le parti. In questo modo non vi è alcuna possibilità di tempi di fermo, censura, frode o interferenza da parte di terzi.

L'idea alla base del progetto è sfruttare al massimo le potenzialità della blockchain, il fondatore riteneva che un utilizzo della tecnologia come semplice libro mastro degli scambi di una criptovaluta fosse limitante.

Lo sviluppo di ethereum è iniziato nel 2013 e la prima versione del software è divenuta disponibile a partire dall'anno successivo. Da allora sono state rese pubbliche una serie di versioni del software che hanno introdotto e sviluppato tre diversi linguaggi di programmazione per la scrittura di smart contract.

Per il finanziamento dello sviluppo della piattaforma venne lanciata per la prima volta un'offerta pubblica che andava ad anticipare l'effettiva vendita di ether, la quale ha permesso di raccogliere circa 19 milioni di dollari in bitcoin.

Riassumendo in estrema semplicità, ethereum potrebbe essere presentato come il più grande computer condiviso che è in grado di erogare una enorme potenza disponibile ovunque e per sempre. Ethereum è in altre parole una piattaforma di tipo computazionale che viene remunerata attraverso scambi che vengono effettuati per consentire il transito di Ether. È una piattaforma che può essere adottata da tutti quanti coloro che desiderano entrare a far parte del progetto e che in questo modo avranno a disposizione una soluzione che consente ai partecipanti di disporre di un archivio condiviso ed immutabile. Il progetto ethereum inoltre è molto flessibile e adatto all'utilizzo in diversi ambiti applicativi, si può definire come una blockchain programmabile che non si limita a permettere di svolgere operazioni predefinite e standardizzate, ma permette agli utenti di creare le proprie personali operazioni in base all'effettivo bisogno.

3.2.2. Tecnologia utilizzata dall'ethereum

Alla base del funzionamento di tutta la rete ethereum vi è la criptovaluta della piattaforma, l'ether. Esso è utilizzato per garantire l'effettuazione di tutte le transazioni e le operazioni all'interno della piattaforma, ad esempio un utente che voglia far girare un proprio contratto all'interno di ethereum deve pagare tale servizio al sistema in ether. In modo analogo, uno sviluppatore di un'applicazione o di un software per il tramite della piattaforma deve pagare il servizio offerto da ethereum.

Il pagamento può avvenire attraverso esborsi di ether, ovvero attraverso il lavoro del soggetto, cioè attraverso la concessione della potenza computazionale dei propri dispositivi per garantire il funzionamento e la continuità del sistema Ethereum.

Per quanto riguarda il funzionamento della blockchain di ethereum essa ha le stesse caratteristiche di quella bitcoin, una medesima funzione fondamentale è quella svolta dai minatori che creano i blocchi e convalidano le transazioni. Un blocco viene generato in media ogni 15 secondi e come ricompensa per il lavoro svolto i minatori ricevono 15 ether a blocco. Inoltre a differenza dello stesso bitcoin non è stato previsto dal sistema un numero massimo di ether che possano essere emessi. Il numero di ether, secondo quando previsto attualmente dal sistema, continuerà ad aumentare costantemente. Non è però da escludere che possa essere proposta daglii sviluppatori e dagli utilizzatori una modifica alla crescita illimitata del numero di ether che, se accettata dalla rete potrebbe portare ad una riduzione graduale della loro emissione, come avviene per esempio con bitcoin

3.2.3. Smart contracts

La caratteristica principale che fa emergere l'ethereum in maniera differente, che viene vista come la sua innovazione più importante, è l'introduzione degli smart contracts.

Gli smart contracts, o contratti intelligenti, sono considerati come dei protocolli informatici che consentono di facilitare, verificare, o far rispettare la negoziazione o l'esecuzione parziale o totale di un contratto. Sostanzialmente sono dei contratti che vengono eseguiti in maniera automatica da un sistema, in questo caso il sistema ethereum. Con dei contratti di questo tipo molti tipi di clausole contrattuali possono essere automatizzate, parzialmente o integralmente, e/o autottemperanti, in grado di essere adempiute in maniera autonoma.

Gli smart contracts puntano ad assicurare una sicurezza superiore alla contrattualistica esistente e a ridurre i costi delle transazioni associate. A garanzia di tali smart contracts è posta la piattaforma ethereum stessa, la quale si occupa di autorizzare, convalidare e autenticare i contratti.

3.3. Confronto tra bitcoin ed ethereum

Di seguito viene proposta una tabella che mette a confronto la tecnologia ethereum con quelle bitcoin. La tabella mette in evidenza le caratteristiche più importanti delle due criptovalute e le loro principali differenze.

Tabella 1: bitcoin e ethereum a confronto

	ethereum	bitcoin
n° massimo unità (della valuta) in circolazione	illimitato	21 milioni
teconologia usata per convalidare le transazioni	blockchain	blockchain
velocità convalida operazioni	15 sec	10 min
intervallo creazione blocchi	40/sec	7/sec
specificità	smart contract	- - -

Fonte dati: www.ig.com

Sebbene entrambe le reti (bitcoin e ether) siano alimentate dal principio della blockchain e della crittografia, le due differiscono tecnicamente in molti modi. Ad esempio, le transazioni sulla rete ethereum possono contenere un programma eseguibile (smart contract), mentre i dati apposti sulle transazioni sulla rete bitcoin sono generalmente solo per nota. Un'ulteriore differenza è il tempo di creazione di un blocco da aggiungere alla catena, una transazione ether viene confermata in secondi rispetto ai minuti per bitcoin.
La differenza più importante tra bitcoin e ethereum sta nel loro obiettivo generale, mentre bitcoin è stato creato come alternativa alle valute legali e quindi aspira ad essere un mezzo di scambio e una riserva di valore, ethereum è stato concepito come una piattaforma per facilitare contratti e applicazioni tramite la propria valuta. Tuttavia, la popolarità di ether lo ha spinto a mettersi in concorrenza con tutte le criptovalute in circolazione, e infatti dal lancio in poi è stato sempre abbastanza vicino al bitcoin nelle classifiche delle migliori criptovalute per capitalizzazione di mercato. Detto questo, è importante tenere presente che l'ecosistema di ether è molto più piccolo di quello di bitcoin, a gennaio 2020 la capitalizzazione di mercato di ether era di poco inferiore a 16 miliardi di dollari, mentre quella di bitcoin era quasi 10 volte superiore e pari a 147 miliardi di dollari. Per capire meglio quanto appena detto, nella figura 7 e 8 è possibile vedere il valore di cambio di tali criptovalute con l'euro e ciò ci permette di vedere effettivamente la differenza dei due ecosistemi

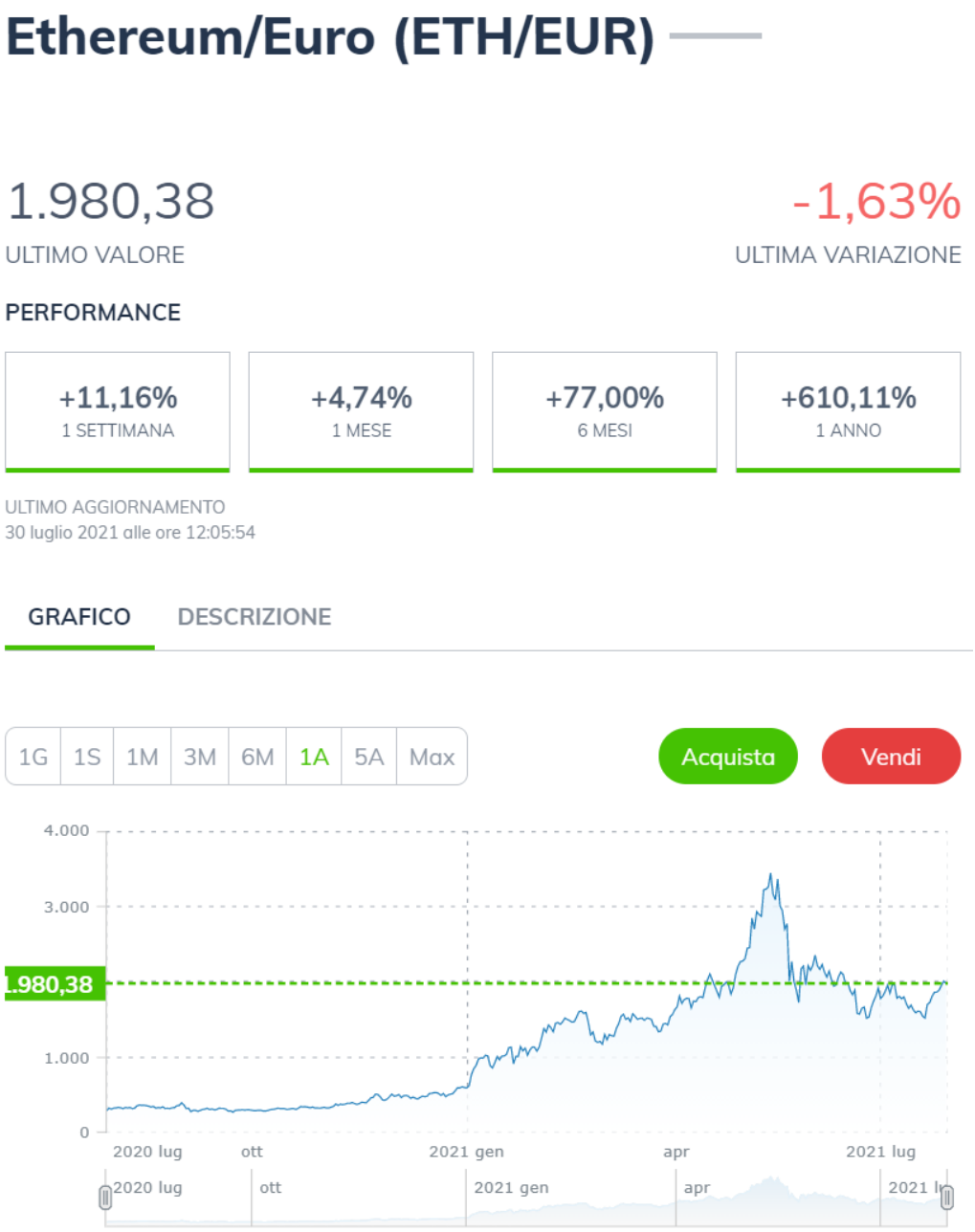

Figura 7

Grafico e valore ethereum risalente al 30.7.2021

Fonte: www.money.it

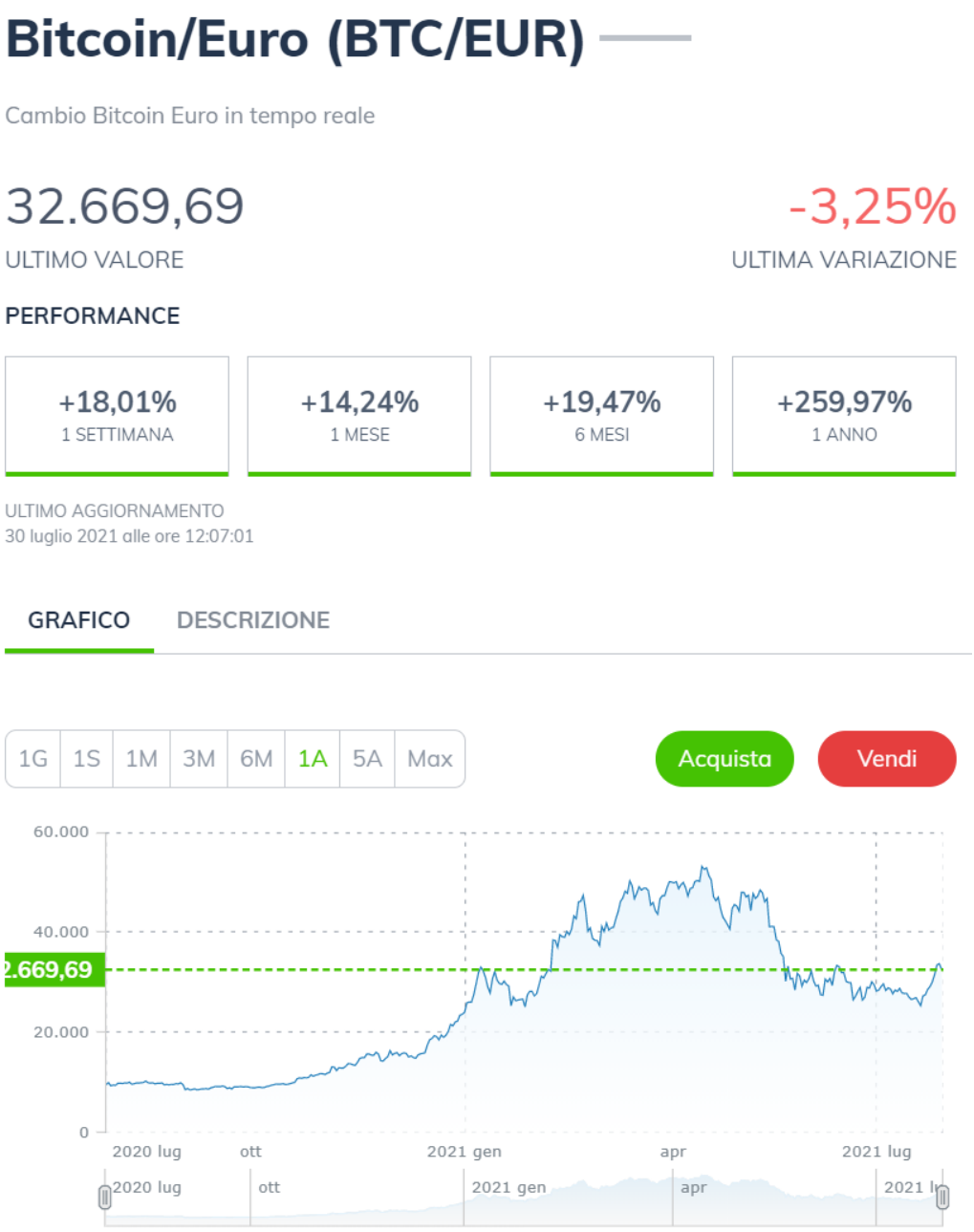

Figura 8

Grafico e valore bitcoin risalente al 30.7.2021

Fonte: www.money.it

3.4 Panoramica generale sulle altre criptovalute esistenti (Altcoins)

Fino al 2011, bitcoin ha rappresentato l'unica criptovaluta esistente al mondo. Il suo successo però ha portato alla nascita di innumerevoli criptovalute alternative che prendono il nome di altcoins, ossia alternative coins.
Una delle ragioni principali per cui sono state create queste valute alternative è da ricondurre sicuramente alla volontà di migliorare alcuni difetti del sistema bitcoin. Questa nuova disponibilità di valute alternative crea dinamiche di sostituzione, cioè gli utenti potrebbero trovare vantaggioso sostituire una criptovaluta con un'altra.
Possiamo distingue due tipi differenti di altcoins:

- Quelle costruite utilizzando il protocollo originale open-source del bitcoin, ma con una serie di modifiche ai suoi codici di base così da creare una nuova moneta con una serie di caratteristiche diverse.
- Quelle che non sono basate sul protocollo open-source di bitcoin, ma che hanno un proprio protocollo e un registro distribuito; un esempio è Ethereum.

Nella Figura 9 è possibile osservare il grafico che mostra la capitalizzazione di mercato delle varie criptovalute dall'aprile 2013 fino a giugno 2021. Il 2017 è stato caratterizzato da una rapida diversificazione delle valute crittografiche, sono state lanciate oltre 800 nuove valute alternative e questo è avvenuto in coincidenza con il declino del predominio di bitcoin sul mercato. All'inizio del 2017 infatti il bitcoin rappresentava oltre l'85% della capitalizzazione totale di mercato, mentre alla fine dello stesso anno è sceso a meno del 40%.

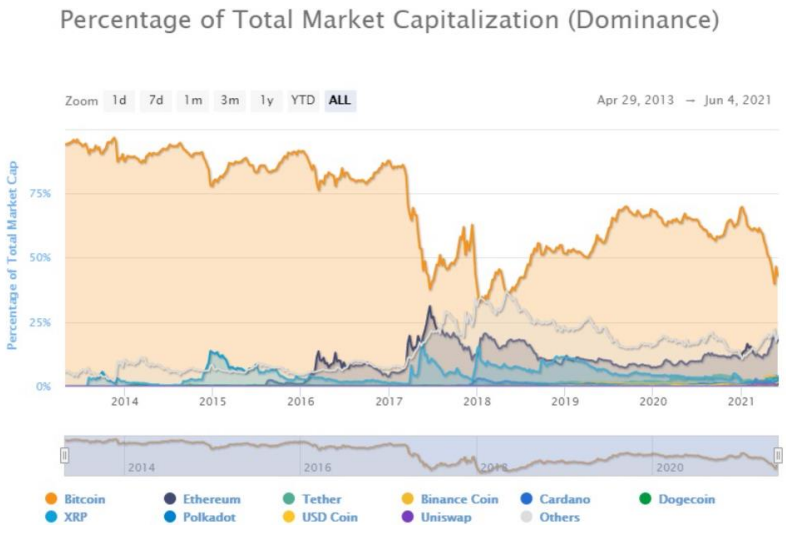

Figura 9

Fonte: www.cointelegraph.com

Attualmente esistono 5140 altcoins create in diversi paesi del mondo con funzioni aggiuntive o migliorate rispetto al bitcoin. Questa impennata dell'ingresso nel mercato delle criptovalute è stata probabilmente dovuta a due fattori: da un lato il basso costo d'ingresso nel mercato, e dall'altro i notevoli profitti che i fondatori delle monete hanno realizzato.
I prezzi di queste altcoins fluttuano molto di più rispetto alle monete fiat. Possiamo dire inoltre che le altcoins hanno un meccanismo di formulazione del prezzo che è interdipendente al bitcoin, ma ancora si sa poco a riguardo. Esistono infatti due ragioni per credere che i prezzi di bitcoin e delle altcoins possano essere interdipendenti, innanzitutto bitcoin è la valuta virtuale dominante e quindi possiamo dire che molti modelli per la determinazione dei prezzi di bitcoin e delle altcoins sono simili, un altro motivo può essere dato dal fatto che una grande maggioranza degli acquisti di altcoins sono eseguiti in bitcoin.

Nella tabella 2 sono stati riportati i principali dati relativi a bitcoin e tre altcoins, le più scambiate sui vari mercati di criptovalute. I dati fanno riferimento a (inserire data e aggiungere qualche breve commento sulla diversità delle cifre.

Tabella 2:

Nome	simbolo		capitalizzazione di mercato	limite massimo	prezzo
bitcoin		BTC	$ 174.586.420.256	21.000.000 BTC	$ 40.552,30
ethereum		ETH	$ 27.796.375.846	nessun limite	$ 2.749,25
litecoin		LTC	$ 4.388.593.761	84.000.000 LTC	$ 144,51
ripple		XRP	$ 11.813.038.205	99.991.083.433 XRP	$ 0.73

Fonte dati: www.ig.com

Conclusioni

Abbiamo potuto osservare che la creazione delle criptovalute ha proposto un cambiamento radicale non solo nei sistemi di pagamento ma anche in una tecnologia – la blockchain – che inizialmente era poco considerata e col tempo ha preso sempre più importanza, fino al punto che le grandi aziende hanno deciso di testare le sue applicazioni anche in contesti separati da quello delle criptovalute.

Le criptovalute, e più nello specifico Bitcoin, avevano inizialmente la finalità principale di presentarsi come una alternativa ad un sistema nel quale si era persa fiducia all'indomani della crisi finanziaria internazionale del 2007-2008. Questa sfiducia nei confronti del sistema economico si è tradotta in una forte spinta alla decentralizzazione. Le criptovalute si proponevano quindi come uno strumento indipendente da altre entità finanziarie, e a differenza delle monete fiat, che sono gestite da una specifica autorità, nessuno può alterarlo o modificarlo. Tuttavia, lo scenario creato dalle criptovalute comporta anche diversi rischi, di cui si è parlato in maniera approfondita nella parte finale del primo capitolo. Tra i rischi più importanti troviamo l'utilizzo per finalità illecite, conseguenza dell'anonimato che molti di questi strumenti garantiscono, ma non vanno trascurati altri problemi, come il rischio informatico, l'assenza di tutele legali e l'eccessiva volatilità. Quest'ultimo problema è la questione principale che frena la diffusione delle criptovalute come moneta di uso comune. Laddove tale uso comune si potesse diffondere a tutta la collettività, lo scenario economico cambierebbe molto rispetto a quello che troviamo oggi, cambierebbe il modo di condurre i vari business ma cambierebbe anche la semplice operazione di acquisto di beni e/o servizi da parte dei clienti. Tuttavia se i problemi che abbiamo discusso nei capitoli precedenti non venissero risolti, si assisterebbe solamente ad una proliferazione di strumenti finanziari alternativi come le cripto-attività che non sono valute, ma un bene speculativo ovvero un investimento potenzialmente molto rischioso.

Attualmente quindi ci sono delle realtà, prevalentemente multinazionali, che utilizzano e/o accettano le criptovalute come effettiva moneta per l'acquisto di beni e/o servizi ma possiamo definirle delle realtà di nicchia. È ancora molto difficile trovare il semplice negozio di quartiere che accetti le criptovalute, perché è un qualcosa che nonostante già esista da più di un decennio non dà sicurezza per la quotidianità. Tutto ciò sarà possibile solo ed esclusivamente quando si riuscirà a trovare una formula che non sia estremamente volatile e che venga adeguatamente regolamentata. Infatti al giorno d'oggi troviamo molte istituzioni che investono in criptovalute ma nessuna che ne ha creata una propria. È quindi ancora difficile dare

una risposta se tale fenomeno cambierà del tutto la struttura e il sistema dei pagamenti oppure se resterà una realtà di nicchia troppo piccola per rappresentare una svolta al livello globale oppure se magari è un qualcosa fine a se stesso che col tempo andrà svanendo accompagnato dal malcontento e dalla sfiducia.

Bibliografia

Amato Massimo, Fantacci Luca (2018) "P*er un pugno di Bitcoin".* Università Boconi Editore

Gates Mark (2018) "*Ethereum"*. Pubblicazione indipendente

Nakamoto Satoshi (2008) "*Bitcoin: A Peer-to-Peer Electronic Cash System"*. Bitcoin.org

Stone Henry D. (2021) "*Criptovalute & Blockchain, dalla crittografia a Bitcoin"*. Pubblicazione indipendente

Sitografia

agendadigitale.eu
area_business.net
bancadItalia.it
bitcoin.org
blockchain.com
blockchain.info
blockchain4innovation.it
borsainside.com
borsaitaliana.it
cmcmarkets.com
cointelegraph.com

coinmarketcap.com
consob.it
corriere.it
criptomag.it
criptovaluta.it
criptovalute24.com
criptovalutenews.com
cryptominando.it
economist.com
en.wikipedia.org
etherevolution.it
ethereum.org
everyeye.it
finanzaonline.it
finaria.it
huffingtonpost.it
ibm.com
ig.com
ilbitcoin.it
ilbitcoin.news
ilpost.it
ilsole24ore.com
iltascabile.com
investing.com
it.wikipedia.org
italiaue.it
iusinitinere.it

kondradsgraf.com
lanazione.it
lecriptovalute.org
mercati24.it
modis.com
money.it
movimentolibertario.com
okforex.it
plus500.it
quaderni.sanprecario.info
quifinanza.it
rivistaeuropae.eu
soldionline.it
startingfinance.it
steemit.com
techdirt.com
tech4future.info
techprincess.it
tradingonline.com
valutevirtuali.it
webnews.it
wired.com