UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in

LE CRIPTOVALUTE: FUNZIONAMENTO E REGOLAMENTAZIONE DELLE MONETE VIRTUALI

THE CRYPTOCURRENCIES : OPERATION AND REGULATION OF VIRTUAL CURRENCIES

Relatore:
Prof. Roberto Esposti

Rapporto Finale di:
Alessia Moschettoni

Anno Accademico 2020/2021

INDICE

INTRODUZIONE

1. LA MONETA E LE CRIPTOVALUTE

    1.1. Bitcoin

    1.2. La nascita del Bitcoin: Satoshi Nakamoto

2. IL FUNZIONAMENTO

    2.1. Blockchain

    2.2. Mining

    2.3. ICO (Initial Coin Offering)

3. LA REGOLAMENTAZIONE GIURIDICA

    3.1. Il caso Ucraina

    3.2. Il regime fiscale in Italia

RINGRAZIAMENTI

BIBLIOGRAFIA/SITOGRAFIA

INTRODUZIONE

Nel corso degli ultimi anni, il mercato delle criptovalute si è fatto teatro di forti innovazioni che hanno portato alla nascita di nuove forme di pagamento, andando così ad integrarsi e a sostituirsi ai metodi più tradizionali. Infatti le monete virtuali stanno diventando sempre di più il fulcro dei sistemi economici e saranno sempre di più al centro dell'attenzione anche nei prossimi anni. Grazie allo sviluppo sempre maggiore della tecnologia, assistiamo all'affermazione del bitcoin, prima, e ritenuta la più significativa, moneta virtuale. La Banca Centrale Europea si è mostrata diffidente in merito a questa questione ed è prorompente il tentativo di proteggere lo status quo messo in dubbio da novità lecite e legali che si vuole far passare per poco sicure. Infatti la BCE riconosce che i progressi tecnologici relativi alla tecnologia di registro distribuito su cui si fondano i metodi di pagamento alternativi come le valute virtuali sono potenzialmente in grado di aumentare l'efficienza, la portata e la scelta dei metodi di pagamento e di trasferimento. La BCE ritiene che gli organi legislativi dell'Unione dovrebbero, tuttavia, porre particolare attenzione a non apparire come propensi a incoraggiare l'utilizzo di valute digitali privatamente istituite, poiché tali mezzi di pagamento alternativi non sono legalmente istituiti come moneta né costituiscono moneta a corso legale emessa da banche centrali e altre pubbliche autorità. Non vi è, infatti, una giurisdizione che autorizzi tutti gli usi correlati alla gestione dei cripto asset.

Nel seguente elaborato affronterò i temi che riguardano le criptovalute e le sue caratteristiche principali.

Il primo capitolo introduce la moneta e le criptovalute, dando ad entrambe una definizione, per poi chiarire i fattori che legano queste due fattispecie. Parlerò, inoltre, della criptovaluta per antonomasia quale il Bitcoin, indagandone la storia del fondatore.

Il secondo capitolo tratta il funzionamento delle monete virtuali, facendo riferimento alla blockchain, al mining e all'ICO.

Il terzo capitolo si focalizza sulla disciplina giuridica e su come questa consideri le criptovalute. In particolare, presenterò l'esempio dell'Ucraina e spiegherò in che termini questo Stato abbia mostrato un atteggiamento favorevole nei confronti delle criptomonete. Proporrò, infine, un focus su come la fiscalità italiana si sia mossa per far fronte all'avvento di queste valute digitali.

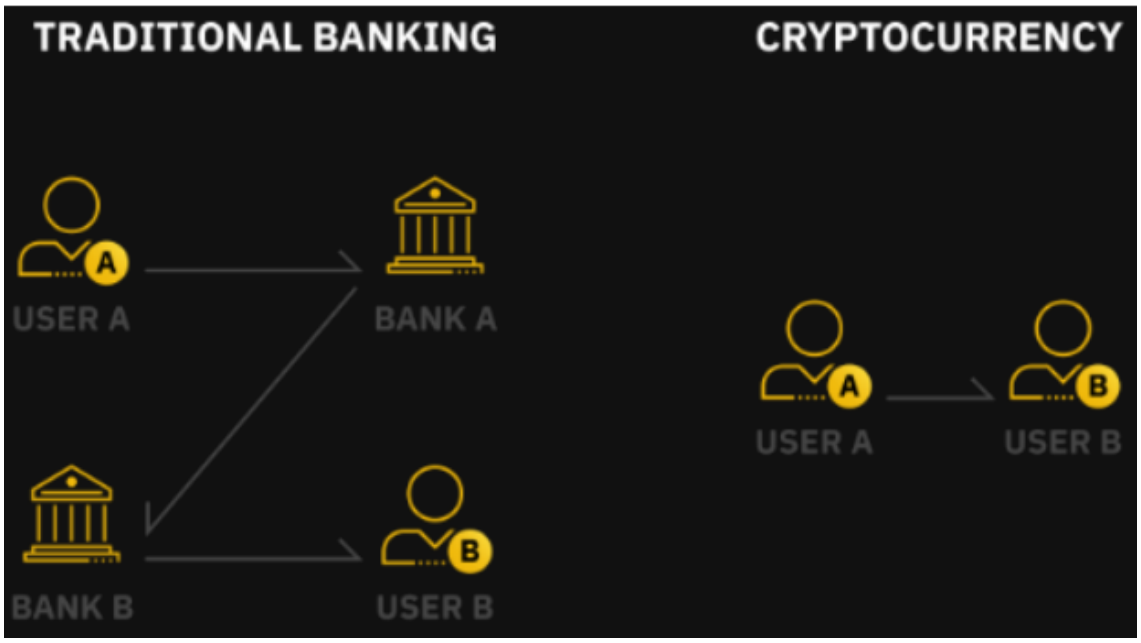
1. LA MONETA E LE CRIPTOVALUTE

Come anticipato nella sezione ‘’Introduzione’’, in questo capitolo andrò a precisare che cosa si intende per criptovalute, analizzando il concetto passo per passo. Partendo dal generale possiamo affermare che le criptovalute sono monete virtuali. Da qui, una prima distinzione, da tenere bene a mente, va fatta tra moneta virtuale e moneta legale. La moneta legale, anche chiamata moneta a corso legale o moneta fiduciaria, è uno strumento di pagamento capace di estinguere le obbligazioni in denaro e viene riconosciuta come tale dall'ordinamento giuridico. L'unica forma di moneta legale è la moneta contante emessa da una banca centrale - per l'euro la Banca Centrale Europea (BCE) - in quanto la sua creazione si basa su rigorose procedure che garantiscono la fiducia generale nella moneta e la stabilità del suo valore nel tempo. In sostanza, acquisisce valore in quanto mezzo di pagamento stabile riconosciuto nell'economia di un certo paese. La relativa stabilità è garantita dal controllo sull'emissione da parte delle banche centrali ed il riconoscimento come mezzo di pagamento è garantito dalla legge. Un ulteriore elemento distintivo è dato dal fatto che il paese che emette la moneta la accetta - anzi, la richiede - come mezzo valido per il pagamento delle imposte ed il potere d'acquisto stabile e giuridicamente riconosciuto della moneta legale è rilevante solo in quanto può essere rivolto a beni e a prodotti finanziari desiderati, che sono prodotti e offerti dal paese in cui circola quella moneta. Infatti, in Italia, il rifiuto di monete aventi corso legale è un illecito amministrativo: chiunque rifiuta di ricevere, per il loro valore, monete aventi corso legale nello Stato, è punito con la sanzione amministrativa fino a euro 30 (art. 693 c.p.). La moneta virtuale viene considerata una “moneta” alternativa a quella tradizionale avente corso legale. Infatti, la valuta virtuale

ha una caratteristica unica: nessuno può controllarne il valore a causa della natura decentralizzata del metodo di creazione della valuta.

La maggior parte delle criptovalute utilizzano sistemi peer to peer su reti i cui nodi sono computer di utenti disseminati ovunque nel mondo. Sui computer vengono eseguiti programmi appositi che svolgono una sorta di funzione di portamonete, per questo non c'è necessità di nessuna autorità che le controlli il sistema è del tutto indipendente, nessuno può intervenire e modificare arbitrariamente il valore della moneta, in più il sistema è indipendente dai circuiti economici internazionali facendo si che molte delle valute virtuali funzionino come veri e propri beni rifugio. Le transazioni delle criptovalute ed il loro rilascio avvengono interamente in rete per questo non c'è alcun tipo di sistema centralizzato nella forma di un edificio fisico altro. Tali monete vengono registrate e conservate nei cosiddetti ''wallet'' o ''portafogli digitali'', che permettono di inviare pagamenti online direttamente da una parte all'altra senza passare attraverso un istituto finanziario e garantiscono la controllabilità delle transazioni e l'anonimato degli utenti, essendo fondati sulla crittografia ed accessibili dai soli titolari mediante apposite credenziali e codificazioni. L'acquisto o la vendita di criptovalute avviene generalmente mediate l'iscrizione a piattaforme online, le quali mettono a disposizione dell'utente un portafoglio elettronico che, una volta collegato ad un conto corrente bancario oppure ad una carta di credito consente lo scambio di valute virtuali tradizionali sulla base di un relativo tasso di cambio. Dopo l'acquisto le monete virtuali vengono detenute su tali portafogli elettronici e possono essere riconvertite nella moneta nazionale o utilizzate per effettuare pagamenti a favore di altri soggetti.

Sintesi del sistema peer to peer:



Fonte: Binance.vision

La moneta a corso legale ha normalmente tre funzioni, ovvero di unità di conto, di mezzo di pagamento e di deposito di valore. Sicuramente non vale per le criptovalute la funzione di unità di conto a causa della loro elevata volatilità: i prezzi delle principali criptovalute sono soggetti a fluttuazioni molto ampie, anche all'interno delle stesse giornate. Relativamente alla funzione di riserva di valore è necessario considerare che, per come sono state progettate, quanto più saranno utilizzate per il pagamento di beni e servizi, tanto più aumenteranno di valore. Questo perché il numero di utilità di criptovalute che possono essere prodotte è limitato, è una creazione contenuta e che si riduce con il tempo. Infine, non sono ancora considerate come deposito di valore, come l'oro, quindi non sono una moneta merce, ma potrebbero assolvere ad una funzione di scambio.

Dunque, possiamo definire le criptovalute delle monete virtuali che costituiscono delle rappresentazioni digitali di valore, finalizzate a stabilire una circolazione monetaria indipendente da Governi e banche centrali, consentendo e agevolando la movimentazione, a livello internazionale e in modo rapido, di consistenti somme di denaro.

Criptovaluta è un termine che si compone di due parole “cripto” e valuta, quindi una valuta nascosta, nel senso che è visibile solo conoscendo un determinato codice informatico. Non esiste in forma fisica ma si genera e si scambia in via telematica e viene custodita in portafogli digitali.

Le criptovalute sono una mera rappresentazione digitale di valore, non sono emesse né garantite da banche centrali né da altra autorità pubblica e non hanno lo status legale di valuta o di moneta. Infatti in quanto moneta decentralizzata, la cripto-valuta è stata sviluppata per essere slegata da qualsiasi supervisione o influenza governativa.

1.1. BITCOIN

Bitcoin è la prima criptovaluta creata e la più famosa. È stata la prima a raggiungere l'adozione di massa, infatti rappresenta la maggioranza della capitalizzazione del mercato cripto. Bitcoin è un software open source emesso sul mercato nel 2009 da Satoshi Nakamoto. La storia relativa al fondatore cela ancora numerosi dubbi e misteri, argomento che approfondirò nel paragrafo successivo.

La circolazione dei bitcoin, quale mezzo di pagamento si fonda sull'accettazione volontaria da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone, quindi, il valore di scambio indipendentemente da un obbligo di legge.

Il processo di generazione dei bitcoin sfrutta la tecnologia peer to peer, nella quale gli utenti fruiscono in modo paritetico delle stesse risorse informative e condividono gli stessi dati a velocità di molto superiori a quelle di un sistema di tipo client-server, nel quale invece il computer che offre i propri servizi (il server), dovendo lavorare per soddisfare le richieste di più client, rischia di rallentare notevolmente le operazioni. Nella logica peer to peer, invece, ogni computer è legato a tutti gli altri e comunica direttamente con ognuno di essi.

Dunque, Bitcoin opera su una rete interconnessa peer-to-peer che non si avvale di alcuna autorità centrale.

I bitcoin vengono generati grazie alla creazione di algoritmi matematici, tramite un processo di mining (letteralmente "estrazione") e i soggetti che creano e sviluppano tali algoritmi sono detti miner. Lo scambio dei predetti codici criptati tra gli utenti (user), operatori sia economici che privati, avviene per mezzo di una applicazione software. Per utilizzare i bitcoin, gli utenti devono entrarne in possesso attraverso due metodi:

possono acquistarli da altri soggetti in cambio di valuta legale o accettarli come corrispettivo per la vendita di beni o servizi. Gli user utilizzano le monete virtuali, in alterativa alle valute tradizionali principalmente come mezzo di pagamento per regolare gli scambi di beni e servizi ma anche per fini speculativi attraverso piattaforme on line che consentono lo scambio di bitcoin con altre valute tradizionali sulla base del relativo tasso cambio

La gestione delle transazioni e l'emissione di bitcoin viene effettuata collettivamente dalla rete attraverso tecnologie crittografiche, le transazioni vengono quindi depositate su un registro distribuito a tutti i nodi della rete.

Le transazioni in Bitcoin sono eseguite in continuazione. Gli unici limiti sono quelli insiti nel protocollo: infatti, la rete Bitcoin è in grado di approvare solo sette pagamenti al minuto, numero molto limitato.

È importante precisare che il Bitcoin è il primo esempio di scarsità digitale, per ora è l'unico esempio digitale non riproducibile all'infinito. Bitcoin è trasferibile ma non duplicabile. La moneta non può essere spesa due volte, ecco perché viene considerato l'oro digitale.

Esistono molte altre criptovalute, ciascuna con particolari caratteristiche e meccanismi.

Analizziamo brevemente le principali:

• **Ethereum:** è una piattaforma decentralizzata finalizzata alla creazione e pubblicazione peer-to-peer di contratti intelligenti, cosiddetti smart contract, considerati a tutti gli effetti denaro digitale. Tecnicamente Ethereum è un sistema strettamente collegato alla valuta Ether, che consente di creare gli smart contracts. Diversamente dal Bitcoin, l'Ethereum non è solo un network per lo scambio di valore monetario, ma una

rete per far girare contratti basati su Ether. La validità di ciascun Ether è garantita dal meccanismo di blockchain.

• **Monero:** è una criptovaluta creata nell'aprile 2014, che, a differenza di molte altre criptovalute che sono derivate dal Bitcoin, si basa sul protocollo CryptoNight, un derivato dell'algoritmo CryptoNote e possiede differenze algoritmiche significative sull'offuscamento della Blockchain.

• **Ripple:** rappresenta sia una valuta digitale che una rete di pagamenti. In sostanza è un protocollo internet open source basato su una valuta chiamata Ripple.

1.2. La nascita del Bitcoin: Satoshi Nakamoto

Innanzi tutto, è importante andare ad inquadrare ed approfondire la nascita di questo fenomeno e la storia del suo fondatore, che risultava, prima della scoperta, avvolta nel mistero. Il documento dal titolo “Bitcoin: A Peer-to-Peer Electronic Cash System”, presentato su Bitcoin.org la notte di Halloween del 2008, conteneva il fondamento teorico della moneta virtuale, il codice e la prima versione del software e portava la firma di un certo Satoshi Nakamoto

In questo white paper si introduce una soluzione che consente la negoziazione tra le parti senza l’intervento di un intermediario fidato, sotto un meccanismo di fiducia basato totalmente sul consenso dei partecipanti della rete rafforzato dalla crittografia alla base della blockchain.

Ecco un estratto del documento presentato in originale:

Bitcoin: A Peer-to-Peer Electronic Cash System

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

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

Fonte: https:/bitcoin.org

Satoshi Nakamoto, ancora oggi, non viene ricondotto ad alcun soggetto determinato; anzi, non sono pochi coloro che ritenevano che, sotto questo pseudonimo, si celava in realtà un vero e proprio team di esperti di informatica ed economia.

Le uniche tracce tangibili dell'esistenza di Satoshi Nakamoto risalgono alle sue conversazioni sui vari forum dedicati ai bitcoin, che però, dall'11 aprile 2011, nel pieno dell'esplosione del fenomeno da lui ideato, non diede più notizie di sé. Naturalmente,

sul tema si sono sviluppate diversi ipotesi, ma nessuna dotata di prove concrete. Ad esempio, secondo alcuni esperti, il codice usato per i bitcoin è piuttosto semplice, ciò dovrebbe far presumere che il suo programmatore non fosse tale di professione, ma più probabilmente un appassionato con grandi conoscenze di crittografia e di reti peer to peer.

Altri ancora hanno analizzato le sue stesse conversazioni sui forum per cercare, tramite il linguaggio dallo stesso utilizzato, quantomeno di circoscrivere il perimetro geografico di ricerca, riscontrando però una grande varietà di inflessioni dialettali, dall'utilizzo di espressioni tipiche dello slang americano a modi di dire assolutamente britannici. Per questo motivo si ritiene, che non si possa trattare di una persona singola, ma di una pluralità di programmatori.

A discapito del nome dell'inventore tipicamente giapponese, il dominio del sito bitcoin.org risulta registrato in Finlandia.

Il primo a cercare di districarsi tra le scarne prove di questa curiosa indagine è stato il giornalista Joshua Philips, del New Worker, che aveva inizialmente dirottato le sue indagini nei confronti di uno studente del Trinity College di Dublino, di nome Michael Clear, che, nel 2008 doveva avere circa 20 anni, ma che nel 2011 aveva pubblicato alcuni articoli per riviste scientifiche, uno in particolare riguardante la crittografia peer to peer. Lo studente smentì categoricamente di esserne l'inventore.

I sospetti si spostarono così, su indicazione dello stesso Michael Clear, sul finlandese Vili Lehndonvirta, ricercatore dell'Helsinki Institute for Information Technology e attivista dell'Electronic Frontier Foundation, ma il risultato fu il medesimo. Il giornalista cominciò allora a prendere in considerazione l'idea che non si trattasse di uno, ma di più Satoshi Nakamoto; per questo, elaborò la sua teoria della Crypto Mano

Group, ossia un team composto da un professore dell'Università del Trinity College di Dublino, un ricercatore e uno studente, rispetto ai quali molti hanno nutrito sospetti in merito, quantomeno, a un loro ruolo nell'implementazione e sviluppo del software.

Altri indirizzarono l'attenzione nei confronti di Jed McCaleb, per il fatto di essere stato il fondatore del primo e più grande mercato valutario per la compravendita di bitcoins, chiamato Mt.Gox e, per essere stato, tra l'altro, lo sviluppatore di eDonkey, ossia uno dei primi sistemi peer to peer mai creati. Si tratta però, anche in questo caso, di mere illazioni di alcuni forum, costruite su congetture e ipotesi e, come tali, deficitarie di sostanziale rilievo.

E ancora, troviamo l'imprenditore australiano Craig StevenWright che, come si evince da alcuni documenti portati alla luce recentemente, insieme ad un informatico americano, deceduto nel 2013, stava lavorando da tempo alla creazione di una moneta virtuale da poter scambiare online. Tuttavia, nella primavera del 2016, in un'intervista, l'imprenditore australiano ha confermato di essere lui l'inventore; a lui si deve la creazione del BTC, hanno rivelato la BBC, The Economist e GQ, portando le prove tecniche della sua invenzione, ovvero le chiavi di crittografia che fanno funzionare il sistema di pagamento e possono essere solo nelle mani del suo creatore. La conferma è arrivata anche da importanti membri della comunità informatica, tra manager e sviluppatori, del BTC. L'intervista della BBC sgombra il campo da qualsiasi dubbio, mostrando al mondo le chiavi di crittografia che l'esperto australiano di sicurezza informatica ha portato per sostenere la sua vera identità. Si tratta di messaggi contrassegnati numericamente e legati ai primi lotti di BTC.

Tra i diversi candidati alla creazione del Bitcoin, ricordiamo, inoltre, Hal Finney, il quale è stato uno dei primi utenti di Bitcoin e il destinatario della prima transazione

Bitcoin e Nick Szabo, un famoso informatico che cercò di lanciare, anni prima della creazione del Bitcoin, il BitGold, senza però riscontrare successo.

2. FUNZIONAMENTO

I mercati delle criptomonete sono decentralizzati, ciò significa che le valute non vengono emesse e non sono protette da un ente centrale come un governo o una banca centrale

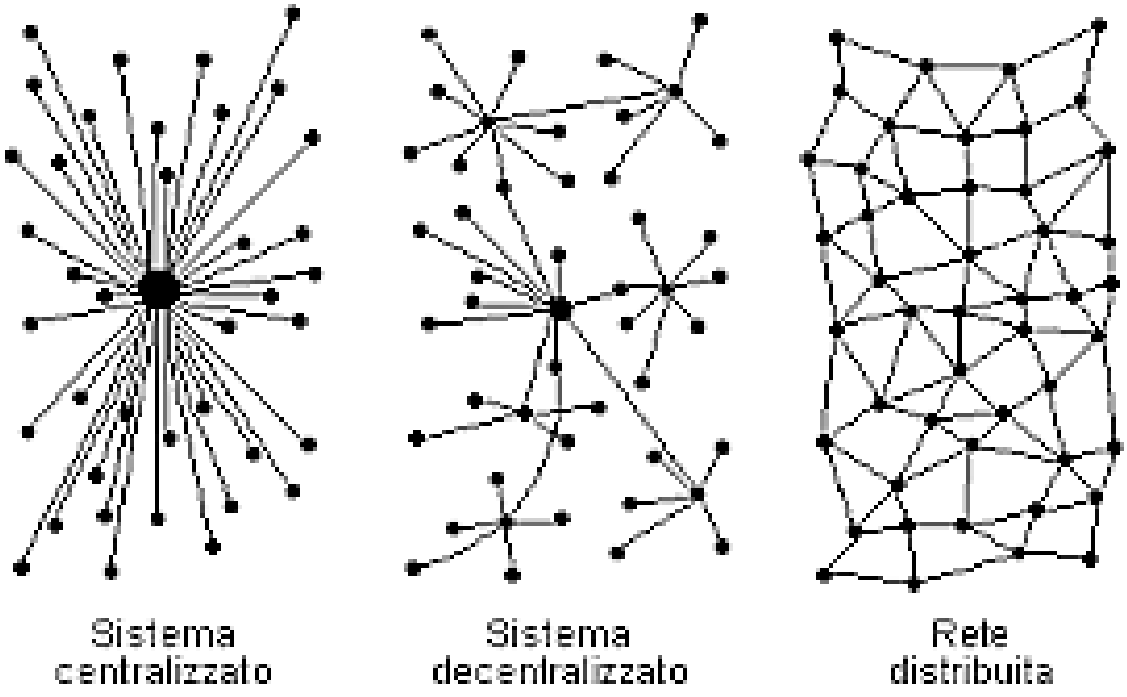
Questo concetto di decentralizzazione appare come decisamente rivoluzionario e in netto contrasto quello di centralizzazione.

Infatti, un sistema centralizzato è caratterizzato dalla centralità di un'Autorità che gestisce e controlla l'organizzazione. In materia di criptovalute, questo implica che un'informazione non può essere inviata o ricevuta senza che questa non passi dal punto centrale.

Una rete decentralizzata non richiede che un'informazione passi da un singolo punto. Ci sono invece tanti punti in connessione tra loro che danno vita ad un network peer-to-peer.

Un'altra tipologia di rete che possiamo trovare è quella distributiva, che spesso viene confusa con quella decentralizzata. La differenza è da ricercare in termini "fisici" relativi al luogo. Infatti un sistema distribuito implica che non tutti i processi delle transazioni siano fatti nello stesso posto.

Nella figura seguente si mostrano i vari tipi di rete:



Fonte: https://www.wizkey.io/it/blog/sistemi-decentralizzati-vs-sistemi-centralizzati-vantaggi-e-applicazioni-2/

Le criptovalute sono gestite da una rete di computer privati e server. E vengono detenute nei 'wallet', o portafogli digitali. Il wallet funge come un servizio di home banking personale e consente di conservare le criptovalute, trasferirle ad altri utenti, ricevere pagamenti, effettuare pagamenti, monitorare lo storico di tutte le transazioni e fare naturalmente acquisti online, sui siti che accettano pagamenti in valute virtuali

Più precisamente, i wallet contengono indirizzi, i quali, a loro volta, sono degli identificatori usati per trasferire gli asset digitali. Ogni portafoglio elettronico ha un proprio indirizzo che sostanzialmente si configura come l'equivalente di un numero di conto corrente bancario. Normalmente quando si installa sul computer un wallet, questo address viene generato automaticamente, ed è rappresentato da una stringa alfanumerica

che nel caso dei Bitcoin è lunga mediamente 33 caratteri. L'indirizzo ha una lettera iniziale differente in base alla criptovaluta di riferimento (B per Bitcoin).

Possiamo distinguere i wallet in 3 tipologie:

• **Wallet software**: è un programma per computer o smartphone con accessibilità solamente sul dispositivo sul quale sono stati installati ed offrono un buon livello di sicurezza anche se si rischia l'irreperibilità delle monete in caso di hackeraggio, virus o distruzione del dispositivo.

• **Wallet online**: è un portafoglio salvato in cloud, accessibile dal web tramite chiave privata. Dato che questo wallet è online è meno sicuro rispetto agli altri.

• **Wallet hardware**: è costituito da un device fisico che si collega al computer tramite una porta USB, la sicurezza di questo wallet è data dal fatto che la chiave privata è custodita in un chip dedicato all'interno dell'hardware e non può essere letta da nessuno.

Per poter utilizzare qualsiasi criptomoneta è necessario utilizzare un portafoglio protetto da crittografia. Il sistema di crittografia rappresenta uno dei requisiti fondamentali per il corretto svolgimento delle transazioni sulla rete di Bitcoin. Infatti, il bitcoin utilizza la crittografia per finalità diverse da quelle tradizionali: non solo permette all'utente di cifrare e decifrare indirizzi e messaggi ma, in più, l'utente potrà acquisire la titolarità delle somme e la legittimazione all'uso delle stesse. In particolare, ogni utente dovrà disporre di due chiavi:

• Una **chiave pubblica** dalla quale si ricava l'indirizzo (bitcoin address): un codice che consente la ricezione di bitcoin. Così come con la chiave pubblica, l'indirizzo bitcoin, che dalla chiave pubblica discende, può essere condivisa liberamente.

• Una **chiave privata**, da tenere segreta, che consente di spendere le somme incassate per mezzo della corrispondente chiave pubblica e dunque indirizzo bitcoin.

La coppia di chiavi consente l'incasso e il trasferimento di bitcoin.

Da un punto di vista tecnico, un indirizzo è il risultato di un'operazione matematica che coinvolge la crittografia a chiave pubblica e l'hashing.

I concetti di hashing e di hash li approfondirò nel capitolo successivo. In questo contesto basta sapere che l'hashing consiste propriamente nel prendere i dati del blocco, passarli attraverso una funzione matematica e trasformarli in un hash, ovvero in algoritmi

Osserviamo le varie fasi di creazione di un indirizzo:

1. Per prima cosa viene generata una chiave privata. È necessario che la chiave privata sia generata da un numero casuale, così da non incombere ad una vulnerabilità critica.

2. Dalla chiave privata deriva la corrispondente chiave pubblica, tramite un processo matematico.

3. La chiave pubblica viene passata attraverso una serie di algoritmi crittografici per ottenere un indirizzo.

In sostanza, da una chiave privata viene generata una chiave pubblica e dalla chiave pubblica viene generato un indirizzo.

Lo scopo di un indirizzo, dunque, è quello di abilitare le transazioni verso e da un'entità unica.

La sicurezza della crittografia a chiave pubblica dipende dalla relazione tra le due chiavi e dunque dall'algoritmo che crea la chiave pubblica dalla privata: dalla chiave pubblica non deve essere possibile risalire alla chiave privata.

Nella figura seguente vediamo, in maniera semplificata, la formazione di un indirizzo a partire dalla chiave privata:

Fonte: Blockchain: Tecnologia e applicazioni per il business, Hoepli, 2019

2.1. BLOCKCHAIN

Veniamo ora alla spiegazione della tecnologia Blockchain.

Il termine Blockchain è apparso per la prima volta per descrivere il sistema di registrazione introdotto dal protocollo Bitcoin, ma ormai è generalmente utilizzato per descrivere qualsiasi forma di tecnologia Distributed Ledger Technology. Le DLT comprendono soluzioni basate su registri distribuiti che consentono la lettura e la modifica da parte di più soggetti partecipanti alla rete.

La legge di conversione 11 febbraio 2019, n. 12, in riferimento al Decreto Legge 14 dicembre 2018, n. 135," dichiara che queste siano:

'' tecnologie e protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. ''

La blockchain è un database decentralizzato che archivia asset e transazioni su una rete di tipo peer-to-peer. È un registro pubblico per la gestione di dati correlati alle transazioni presenti nei blocchi e gestite tramite crittografia dai partecipanti alla rete che verificano, approvano e successivamente registrano tutti i blocchi con tutti i dati di ciascuna transazione su tutti i nodi. La stessa "informazione" è dunque presente su tutti i nodi e pertanto diventa immodificabile se non attraverso una operazione che richiede l'approvazione della maggioranza dei nodi della rete e che in ogni caso non modificherà lo storia di quella stessa informazione.

Le caratteristiche principali della tecnologia blockchain possono essere riassunte in 7 punti chiave:

• **Decentralizzazione:** le informazioni contenute nel registro digitale vengono distribuite tra più nodi, così da garantire sicurezza e resilienza dei sistemi anche in caso di attacco ad uno dei nodi o in caso di perdita di un nodo.

• **Tracciabilità:** ogni elemento salvato nel registro è tracciabile in ogni sua parte e se ne può risalire all'esatta provenienza e alle eventuali modifiche apportate nel corso del tempo, con una precisione assoluta.

• **Disintermediazione:** i singoli nodi della blockchain certificano le informazioni distribuite, rendendo quindi del tutto inutile la presenza di enti centrali o di aziende per la certificazione dei dati.

• **Trasparenza:** il contenuto del registro è visibile a tutti ed è facilmente consultabile e verificabile da ogni nodo della rete ma anche tramite servizi che interrogano la blockchain senza apportare modifiche. Nessuno può nascondere o modificare dati senza che l'intera rete venga a saperlo.

• **Solidità del registro:** dopo aver aggiunto un'informazione al registro, essa non può essere modificata senza il consenso di tutta la rete.

• **Programmabilità:** le operazioni di transazione possono anche essere programmate nel tempo, così da poter attendere il verificarsi di determinate condizioni prima di procedere con l'inserimento o la modifica.

• **Sicurezza e Privacy**: le autorizzazioni e la crittografia permettono ai partecipanti di specificare le informazioni da rendere note, con alcune eccezioni per particolari tipi di partecipanti come i revisori, che potrebbero avere bisogno di più informazioni. Viene assicurata l'identità dei partecipanti e questi non possono manomettere le transazioni, gli errori possono essere invertiti solo con nuove transizioni.

La tecnologia del registro distribuito si presenta come un metodo sicuro per conservare informazioni importanti, inviolabile dal punto di vista informatico, difficile da modificare.

La blockchain è costituita da una catena di blocchi che contengono più transazioni ciascuno. La soluzione per tutte le transazioni è affidata ai nodi che sono chiamati a vedere, controllare e approvare tutte le transazioni creando una rete che condivide su ciascun nodo l'archivio di tutta la blockchain e dunque di tutti i blocchi con tutte le transazioni. Tutte le transazioni presenti nella blockchain, vengono registrate in un Ledger, cioè un registro che consente di verificare la proprietà e l'eventuale trasferimento della proprietà.

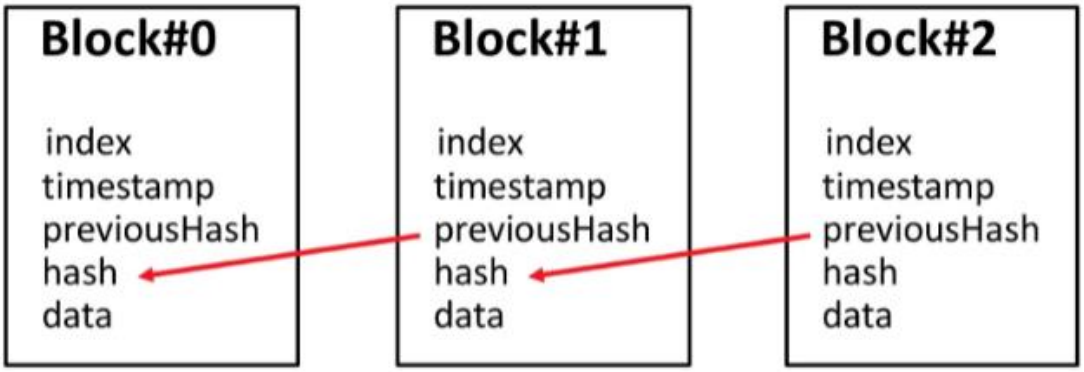
Ogni blocco punta al blocco precedente tramite un riferimento che è essenzialmente il valore di hash del blocco precedente. Il numero massimo di transazioni che può contenere un blocco, dipende dalla dimensione del blocco stesso.

Ogni blocco contiene un valore di hash, ovvero ha una registrazione compatta delle transazioni convalidate da parte dei partecipanti stessi alla rete, il quale è come fosse l'impronta digitale del blocco stesso. Lo scopo dell'algoritmo di hash è quello di trasformare qualsiasi informazione in una combinazione casuale ma calcolabile di numeri e lettere.

I blocchi sono composti da:

• **Block Header**: rappresenta l'intestazione del blocco ed è formato dal numero del blocco, il valore dell'hash del blocco precedente, una rappresentazione dei dati storici del blocco, un timestamp, la dimensione del blocco e il valore nonce.

• **Block Data**: rappresenta un elenco delle transazioni e degli eventi correlati al blocco e inclusi nel ledger, ed eventualmente possono essere presenti altri dati.



Fonte: https://academy.bit2me.com/it/tipi-di-blocchi-in-blockchain/

Come rappresentato in figura, un blocco si compone di:

• **Index:** è il numero del blocco

• **Timestamp:** corrisponde all'orario esatto in cui il blocco viene estratto

• **Previous Hash:** indica il codice del blocco precedente

• **Hash:** indica il valore del blocco in oggetto

I blocchi per essere considerati validi devono, per prima cosa, essere estratti e poi devono raggiungere il consenso da parte della rete. Una volta che il blocco ha ottenuto l'approvazione dalla rete, questo viene incluso nella blockchain e propagato da tutti i suoi nodi. In questo modo, ogni nodo della rete ha il nuovo blocco e funge da punto di verifica per esso.

Questi blocchi sono ciò che consente il funzionamento della blockchain e delle sue transazioni. Ogni blocco valido porta al suo interno una serie di transazioni che vengono convalidate insieme a quel blocco.

Un nodo potrebbe validare anche blocchi diversi contemporaneamente, creando una biforcazione nella blockchain detta ''Fork''. La Fork si genera nel momento in cui c'è stato un aggiornamento nelle regole del protocollo e non tutti ne sono a conoscenza. Esistono due tipi di Fork:

• **Hard Fork:** sono aggiornamenti software non retrocompatibili. Si tratta della creazione di una nuova blockchain che è incompatibile con quella attuale, anche se entrambe utilizzano lo stesso software. I nuovi nodi possono comunicare solo con altri che usano la nuova versione.

Gli Hard Fork possono essere di tipo ‘’Planned’’, ovvero pianificati e programmati, o di tipo ‘’Contentious’’, ovvero che non riescono a trovare il consenso da parte della comunità. Gli Hard Fork Planned trovano approvazione dalla community e questa tipologia non conduce allo sdoppiamento della blockchain e le regole vengono aggiornate in forma di continuità. Gli Hard Fork Contentious prevedono, invece, che il cambiamento proposto al protocollo non trovi un accordo all’interno della community, arrivando così alla creazione di una nuova moneta.

• **Soft Fork:** attua un cambiamento reversibile che consente la partecipazione alla Blockchain anche a tutti quei nodi che decidono di non effettuare l’aggiornamento.

Il motivo per il quale si giunge ad una Fork è dovuto al fatto che, non esistendo un unico decisore centralizzato, quando si vogliono cambiare le regole è necessario mettere d’accordo tutta la rete.

2.2. MINING

Il termine mining, proviene dal gold mining, ossia l'attività di estrazione dell'oro.

L'attività mineraria, tradizionalmente, riguardava l'attività di estrazione dell'oro e di altri metalli dal terreno; tuttavia, oggi abbiamo un nuovo tipo di attività mineraria, che prevede la ricerca di un "tesoro" decisamente diverso.

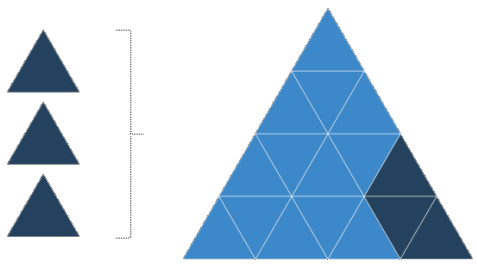
Il ''bitcoin mining'' è il processo che assicura il funzionamento corretto dei bitcoin ed è l'unico metodo per immettere nuova valuta sul mercato. I minatori di Bitcoin sono di vitale importanza per il funzionamento della piattaforma di criptovalute, in quanto effettuano tutte le operazioni di calcolo legate alla blockchain verificano le migliaia di transazioni effettuate ogni giorno dagli utenti, si prendono cura della tutela della rete contro eventuali attacchi degli hacker, tracciano le attività di trading e si occupano anche della creazione di nuove valute da immettere sul mercato.

I miner sono persone fisiche o società che garantiscono la precisione, la potenza dei calcoli e l'operatività della blockchain, tecnologia sulla quale le criptovalute si sviluppano. I server decentralizzati gestiscono tutte le operazioni della piattaforma di criptovalute e hanno la possibilità di "estrarre" i bitcoin appena creati.

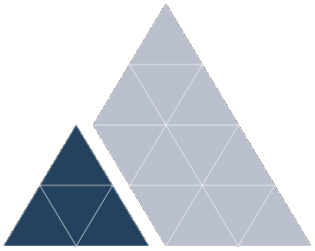
I miner svolgono, inoltre, l'attività di mining, ovvero di convalida dei blocchi tramite il calcolo dell'hash. Infatti, i miner iniziano automaticamente a raccogliere informazioni e, come prima cosa, registrano tutti i dati della transazione in un hash. Questo consente di creare file compressi, di dimensioni contenute, al cui interno abbiamo un grande quantitativo di informazioni, e di crittografare i dati all'interno dell'hash. Terminato il processo di creazione, le informazioni contenute non possono essere modificate. Un altro importante aspetto da considerare è che la blockchain raccoglie i dati in maniera cronologica e il software di mining registra le informazioni partendo dalle transazioni

più recenti. Ogni volta che una transazione viene codificata in un hash, quest'ultimo viene combinato con le informazioni di un'altra transazione, che saranno incluse all'interno di un nuovo hash. I dati delle transazioni vengono mano a mano aggiunte all'interno di un unico hash, fino a formare un blocco di dati. I blocchi, successivamente, si "incastrano" l'uno con l'altro, realizzando la blockchain. Il ruolo del minatore è quello di portare a termine questo processo risolvendo complessi algoritmi. Infatti, modificando la complessità degli algoritmi, i minatori possono fare in modo che il tempo di elaborazione dei blocchi sia più o meno uniforme. La Proof-of-work è l'algoritmo di consenso alla base della rete blockchain. All'interno della catena di blocchi, questo algoritmo viene utilizzato per confermare le transazioni e produrre i nuovi blocchi della catena. Il miner che completa la proof-of-work e aggiunge il blocco dati alla blockchain viene doppiamente ricompensato: riceve i nuovi bitcoin rilasciati dal protocollo e le commissioni sulle transazioni correlate.

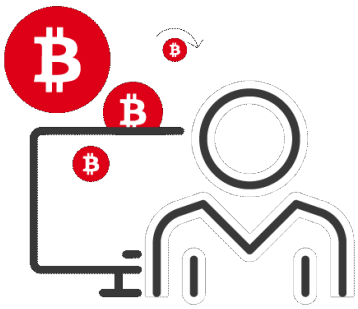
Di seguito riportata una semplificazione del processo:



Il minatore registra le transazioni
in criptovalute in un 'blocco'.



Il blocco dati viene protetto da crittografia
e aggiunto alla blockchain esistente.



Il minatore ottiene un profitto in criptovaluta
per il blocco registrato, che potrà vendere direttamente sul mercato

Fonte: https://www.ig.com/it/criptovalute

Il mining può essere definito, più generalmente, come il processo attraverso il quale i blocchi vengono aggiunti alla blockchain, permettendo così la creazione (o "estrazione") di nuove unità della criptovaluta. Queste unità sono definite "premio del blocco", una sorta di premio per aver contribuito alla validazione delle transazioni.

Vi sono diversi strumento con i quali è possibile minare criptomonete. Principalmente individuiamo due modelli: il primo è noto come **mining pool**. Questa tipologia unisce la potenza di calcolo di molti sistemi informatici singoli per moltiplicare le possibilità di

profitto, anche se spesso questo significa suddividere le stesse percentuali di profitto tra più persone. I mining pool richiedono anche una quota di iscrizione che riduce ulteriormente la redditività.

Il **cloud mining** è il secondo modello. Le persone o le aziende, anziché acquistare hardware costosi e ad elevato consumo energetico, possono noleggiare il sistema informatico di qualcun altro per raccogliere i profitti che la piattaforma accumula in quel periodo. Le aziende che noleggiano questi sistemi informatici hanno molti modi per guadagnare. Alcune addebitano delle tariffe mensili, altre fanno pagare in base al tasso di hash (la quantità di potenza di calcolo utilizzata) e altre ancora aggiungono altri oneri come le tariffe di manutenzione. Il cloud mining può rivelarsi complesso e costoso ma elimina la seccatura e i costi della configurazione e dell'esecuzione di un sistema informatico sviluppato individualmente.

2.3. Initial Coin Offering (ICO)

L'ICO, letteralmente '' Offerta di moneta iniziale'', rappresenta una forma di finanziamento collettiva. Il termine Initial Coin Offering deriva dal più tradizionale "Initial Public Offering" (IPO), ossia di un'offerta pubblica di strumenti finanziari da parte di un soggetto emittente.

Entrambe le procedure hanno l'obiettivo di raccogliere capitali per la realizzazione di un progetto, ma l'ICO si distingue per due motivi principali: nell'oggetto principale dell'offerta, che è in questo caso un coin o token, e nel luogo in cui questa offerta si svolge, che non è un mercato regolamentato, ma una piattaforma Blockchain.

Il processo di realizzazione di una ICO può essere descritto in 4 fasi principali:

1. La stesura di un whitepaper che descriva il progetto e il suo stato di avanzamento, il fabbisogno di finanziamento, quanti token resteranno in mano ai fondatori, con quali criptovalute si potranno acquistare i token e quanto durerà la campagna
2. L'attività di comunicazione che spesso si svolge creando pagine di discussione ad hoc per promuovere l'ICO e attrarre potenziali investitori
3. L'acquisto dei token da parte degli investitori. Se non vengono raggiunti gli obiettivi di raccolta, i fondi vengono restituiti agli investitori. Se invece vengono raggiunti i requisiti, i fondi raccolti vengono utilizzati per iniziare o completare il progetto
4. Al termine della vendita iniziale, i token vengono inseriti nei listini degli exchange e possono essere scambiati tra gli utenti

In particolare le ICO vengono utilizzate da startup o da soggetti che intendono realizzare un determinato progetto.

3. LA REGOLAMENTAZIONE GIURIDICA

Le “cripto-attività”, sono: “una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente”. Così, nel 2018, il Parlamento Europeo si esprime nei confronti delle criptovalute. Di conseguenza, tutti gli stati hanno iniziato a lavorare su una regolamentazione che potesse soddisfare le necessità del mercato e dei consumatori, trovando non poche difficoltà nella determinazione di quelli che sono alcuni parametri fondamentali che una moneta deve seguire. Tre sono le alternative più discusse riguardo la regolamentazione: “isolare”; “regolare”, “integrare”. La prima alternativa consisterebbe nell’impedire che le “cripto-attività” facciano parte dell’intermediazione bancaria e finanziaria; la seconda comporterebbe l’emanazione di una regolamentazione specifica; la terza si baserebbe su un adattamento del quadro regolamentare esistente in modo da accogliere questi nuovi strumenti.

Nel complesso, non emerge ancora un consenso su queste opzioni. Vi è, al contrario, uniformità di vedute sul fatto che si debba separare il tema delle cripto-attività da quello sulla tecnologia sottostante (la Blockchain). Quest’ultima, se tecnologicamente robusta, potrebbe avere grandi potenzialità soprattutto nell’ambito dell’archiviazione crittografica e di alcuni tipi di gettoni digitali. Vi è altresì accordo sul fatto che questi sviluppi tecnologici aprono scenari di vasta e incerta portata per i processi di intermediazione e di organizzazione dei mercati. La peculiare natura economica delle valute virtuali e della sottostante tecnologia basata su un protocollo diffuso e liberamente accessibile tramite internet, rendono difficile la diretta regolamentazione di

questi oggetti. Le autorità competenti si sono pertanto concentrate prevalentemente sui soggetti che operano in tali mercati.

In Italia ad esempio il legislatore si è soffermato principalmente sulla disciplina dell'antiriciclaggio, apportandone modifiche in materia di "valute digitali" tramite il d.lgs 90/2017. In particolare, il legislatore ha riconosciuto tra gli "altri operatori non finanziari" la categoria degli operatori in "valute virtuali" definita come "persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di "valuta virtuale" e alla loro conversione da ovvero in valute aventi corso legale" (art. 1, comma 2, lett. ff.). Questi operatori, una volta approvati i decreti attuativi, saranno obbligati a darne comunicazione al MEF e a iscriversi nel registro tenuto dall'Organismo degli Agenti e dei Mediatori (OAM)48. Essi saranno vigilati dalla Guardia di Finanza. Il decreto ha inoltre previsto che i prestatori di servizi relativi all'utilizzo di "valuta virtuale", "limitatamente allo svolgimento dell'attività di conversione di "valute virtuali" da ovvero in valute aventi corso forzoso" (art. 3, comma 5, lett. i), debbano assolvere agli obblighi antiriciclaggio (obblighi di adeguata verifica, conservazione dei documenti, segnalazione alla Unità di informazione finanziaria (UIF) delle operazioni sospette di riciclaggio e di finanziamento del terrorismo).

In Europa, la prima volta che si è avuta una causa sulle valute virtuali, riguardava una domanda proposta dallo Skatteverket nella causa C-264/14 della Corte di giustizia dell'Unione, sul pagamento dell'imposta del valore aggiunto sui proventi derivanti dall'attività di un exchange con sede in Svezia, cui risultato fu l'inquadramento del bitcoin come «mezzo di pagamento contrattuale»

3.1 IL CASO UCRAINA

Ho deciso di riportare il caso dell'Ucraina perché trovo che sia particolarmente curioso e significativo l'atteggiamento che questo Stato riservi nei confronti delle criptovalute.

Contrariamente a come si può pensare, l'Ucraina risulta essere in testa nella classifica dell'adozione globale delle criptomonete. Questo traguardo si evince dal Global Crypto Adoption Index di Chainalysis, una particolare analisi che utilizza parametri oggettivi, come i tassi di adozione ed i modelli di utilizzo delle criptovalute, per esaminare come questi differiscono nel mondo.

Breve spiegazione della formula:

Il Global Crypto Adoption Index è composto da quattro metriche con le quali vengono classificati 154 paesi. La classifica generale viene calcolata prendendo la media geometrica della classifica di ciascun paese e normalizzando questo numero su una scala da 0 a 1. Più il punteggio è vicino a 1 più alto è il grado di adozione.

Le quattro metriche prese in considerazione sono:

• il valore delle criptovalute transate on-chain a parità di potere d'acquisto (PPP) pro capite

• il valore transato on-chain dagli utenti retail ponderato per PPP pro capite

• il numero di depositi di criptovalute on-chain ponderato in base al numero di utenti Internet

• il volume degli exchange peer-to-peer (P2P) ponderato per PPP pro capite e numero di utenti Internet.

Di seguito riportata la classifica datata al 2020:

Country	Score	Rank	Rank of individual weighted metrics feeding into index			
			On-chain value received	On-chain retail value received	Number of on-chain deposits	P2P exchange trade volume
Ukraine	1	1	4	4	7	11
Russia	0.931	2	7	8	5	9
Venezuela	0.799	3	19	14	15	2
China	0.672	4	1	1	95	53
Kenya	0.645	5	37	11	57	1
United States of America	0.627	6	5	6	39	16
South Africa	0.526	7	12	9	41	10
Nigeria	0.459	8	14	7	112	3
Colombia	0.444	9	25	18	61	4
Vietnam	0.443	10	2	2	44	81

Fonte: https://cryptonomist.ch/2020/09/09/ucraina-global-crypto-adoption-index/

L'8 settembre 2021 il Parlamento dell'Ucraina ha approvato una legge che di fatto legalizza l'uso di Bitcoin e delle criptovalute.

La Verkhovna Rada, ovvero il Parlamento ucraino, infatti ha approvato il disegno di legge numero 3637 "Sugli Asset Virtuali" con 276 voti favorevoli su 376.

La legge, in linea di principio, introduce il concetto giuridico di "patrimonio virtuale", definendolo come un insieme di dati, in forma elettronica, che ha un valore ed esiste nel sistema di circolazione degli asset virtuali.

Ora che la nuova legge è stata approvata, in Ucraina le criptovalute possono essere legalmente possedute, utilizzate e scambiate, sebbene non siano riconosciute come valuta a corso legale.

Inoltre il nuovo status giuridico degli asset virtuali fornisce anche protezione legale a chi li utilizza e li scambia sul mercato.

Nonostante ora vi sia una norma che regolamenti le criptovalute, ciò non toglie che per svolgere un'attività legata ad esse è comunque necessario ottenere uno specifico permesso**,** e questo finirà per regolarizzare anche l'intera industria crypto del Paese.

I requisiti necessari per ottenere questa autorizzazione sono:

• avere una reputazione aziendale impeccabile

• divulgare informazioni sulla struttura proprietaria

• il capitale deve provenire da fonti "pulite".

Inoltre per emettere queste licenze è in fase di creazione un apposito nuovo ente regolatore, ovvero il servizio nazionale per la regolamentazione della circolazione degli asset virtuali (NSVA).

3.2. IL REGIME FISCALE IN ITALIA

Per concludere il rapporto tesi, ritengo interessante riportare brevemente la situazione fiscale che coinvolge il nostro Paese, tema assai delicato e complesso.

Per quanto riguarda il trattamento fiscale applicabile alle operazioni relative alle monete virtuali, non si può prescindere da quanto affermato dalla Corte di Giustizia Europea nella sentenza 22 ottobre 2015, causa C-264/14. In tale occasione, agli effetti dell'IVA, la Corte europea ha riconosciuto che le operazioni che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale e viceversa costituiscono prestazioni di servizi a titolo oneroso. Più precisamente, secondo i giudici europei, tali operazioni rientrano tra le operazioni "relative a divise, banconote e monete con valore liberatorio" di cui all'articolo 135, paragrafo 1, lettera e), della Direttiva 2006/112/Ce. Difatti, la Corte di giustizia dell'Ue, ha stabilito che l'attività di intermediazione di valute tradizionali con bitcoin, fatta in modo professionale ed abituale, costituisce un'attività rilevante oltre agli effetti dell'Iva anche dell'Ires e dell'Irap, soggetta agli obblighi di adeguata verifica della clientela, di registrazione e di segnalazione.

In assenza di una specifica normativa applicabile al sistema delle monete virtuali, la predetta sentenza della Corte di giustizia costituisce necessariamente un punto di riferimento sul piano della disciplina fiscale applicabile alle monete virtuali.

Nella sentenza viene chiarito che le prestazioni in esame, pur riguardando operazioni relative a valute non tradizionali: "costituiscono operazioni finanziarie in quanto tali valute siano state accettate dalle parti di una transazione quale mezzo di pagamento alternativo ai mezzi di pagamento legali e non abbiano altre finalità, oltre a quella di un mezzo di pagamento''. Con l'interpello 9 settembre 2016, n.72/E, l'Agenzia delle Entrate, per la prima volta, ha preso posizione sul regime fiscale impositivo delle

criptovalute. In assenza di uno specifico appiglio normativo e giurisprudenziale, basandosi solamente sulla storica sentenza della CGUE, C-264/14 (Skatteverket v. David Hedqvist), il fisco italiano era giunto alla conclusione che, ai fini della tassazione diretta, le persone giuridiche dovessero essere soggette ad IRES per i componenti positivi di reddito e ad IRAP per il valore della produzione netta. Con riguardo alle persone fisiche, estranee all'esercizio di arti o professioni ovvero ad attività d'impresa, la risoluzione aveva precisato che la compravendita di tali valute non comportasse l'emissione di reddito imponibile in quanto «le operazioni a pronti (acquisti e vendite) di valuta non generano redditi imponibili mancando la finalità speculativa».

La posizione in materia è cambiata radicalmente con il recente interpello 956-39/2018, nel quale vi è stata l'assimilazione delle valute virtuali ai redditi diversi di natura finanziaria e, dunque, soggetti alla tassazione prevista exart. 67, comma 1, lett. C-tere ss. Del T.U.I.R. la normativa, attribuisce rilevanza a particolari fattispecie per le quali è presunta ex lege la finalità d'investimento finanziario, infatti: qualora l'investito abbia maturato una situazione possessoria qualificata in € 51.645,69 per almeno sette giorni lavorativi consecutivi, il prelievo di valuta virtuale dai wallet, sarà oggetto di tassazione quale reddito diverso di natura finanziaria, indifferentemente se vi sia o meno la finalità speculativa dietro tali operazioni.

In tal caso, le plusvalenze derivanti da cessione di criptovalute realizzate da persone fisiche al di fuori dell'attività d'impresa sono assoggettate all'imposta sostitutiva del 26%, senza alcuna franchigia. Tali plusvalenze devono essere dichiarate nel Quadro RT della dichiarazione Modello Redditi PF e ivi liquidate.

In sostanza, la normativa in ambito Bitcoin è ancora lacunosa e discordante per certi aspetti ma la certezza è che le criptovalute sono un fenomeno fiscalmente rilevante. La

regolarizzazione delle criptovalute è un passaggio necessario affinché queste possano essere adottate dal mondo intero e non solo da una nicchia della popolazione.

CONCLUSIONE

Alla luce di quanto detto finora possiamo affermare che l'utilità delle valute virtuali non è solo quella di rappresentare un investimento finanziario, ma l'ambizione è quella di diventare una vera e propria moneta di scambio di beni e servizi.

Certamente l'idea di valuta virtuale è un'idea vincente perché è una tecnologia innovativa che sta per risolvere molti problemi pratici e potrebbe cambiare la vita delle persone, molti trade off potrebbero essere presto superati attraverso questa innovazione. Insomma non c'è nessun indizio che possa far pensare che l'idea delle monete virtuali possa andare a morire, in realtà è chiaro che nel futuro non potrà che andare migliorando ed evolvendosi sempre di più

Concludendo, è possibile dire che la tecnologia blockchain avrà sicuramente risvolti positivi e rivoluzionari per molteplici settori, ma come ogni innovazione ha bisogno di tempo per esprimere a pieno il proprio potenziale.

RINGRAZIAMENTI

In ultima istanza, ringrazio il professore e relatore Dott. Roberto Esposti per la disponibilità e la pazienza che mi ha dimostrato nel percorso che mi ha portato a concludere questo lavoro.

BIBLIOGRAFIA

- Chiap G., Ranalli J., Bianchi R., *Blockchain. Tecnologia e applicazioni per il business*, Hoepli, 2019

SITOGRAFIA

- http://www.dirittoeconomiaimpresa.it/bitcoin-e-criptomonete

- https://www.punto-informatico.it/blockchain-spiegazione

- https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/

- https://academy.binance.com/it/articles/hard-forks-and-soft-forks

- https://cryptonomist.ch/2020/09/09/ucraina-global-crypto-adoption-index/

- https://www.agenziaentrate.gov.it/portale/documents/20143/302984/Risoluzione+n.+72+del+02+settembre+2016_RISOLUZIONE+N.+72+DEL+02+SETTEMBRE+2016E.pdf/8e057611-819f-6c8d-e168-a1fb487468d6

- https://cryptonomist.ch/2021/09/09/ucraina-legalizza-bitcoin-criptovalute/

- https://fiscomania.com/criptovalute-dichiarazione-dei-redditi/

- https://www.consob.it/web/investor-education/criptovalute