



Dipartimento di Impresa e Management

Cattedra di Analisi Finanziaria

**Criptovalute**  
**Un'analisi contabile e fiscale**

Relatore

Prof. Fabrizio Di Lazzaro

Correlatore

Prof. Francesca Di Donato

Candidato

Gianmarco Russo

Matr.721841

Anno Accademico 2020/2021



# Indice

<b>Introduzione</b> .....	7
 <b>Capitolo 1</b>	
<b>1.1 Storia: Blind Signatures for Untraceable payments</b> .....	10
<i>(Segue) Le Funzioni <math>f(x)</math></i>	
<i>(Segue) Verificabilità delle Firme cieche</i>	
<i>(Segue) Le ipotesi di Chaum e la loro effettiva realizzazione.</i>	
<b>1.2 Chaum e Digicash</b> .....	14
<b>1.3 Wei dai e b-money</b> .....	15
<i>(Segue) I Protocolli di B-Money</i>	
<b>1.4 La nascita di Bitcoin:La prima Blockchain e la prima Criptoaluta</b> .....	17
<b>1.5 La Blockchain</b> .....	19
<i>(Segue) Rete Peer to Peer</i>	
<i>(Segue) Possibili applicazioni della blockchain</i>	
<i>(Segue) Il protocollo Cryptonote</i>	
<b>1.6 Le Criptoalute</b> .....	33
<i>I Bitcoin</i>	
<i>Bitcoin cash</i>	
<i>Ripple</i>	
<i>Ethereum</i>	
<b>1.7 Il fenomeno degli nft</b> .....	37
<i>(Segue) Gli inizi degli NFT</i>	
<i>(Segue) I Bored Ape</i>	
<i>(Segue) I limiti degli NFT</i>	
<b>1.8 I Wallet</b> .....	42
<b>1.9 La Creazione di valore delle criptoalute</b> .....	43
<b>1.9.1 Initial Coin Offering</b> .....	44

<b>1.9.2 Hard Fork</b> .....	47
<i>(Segue) Ethereum e il suo Hard fork per il risarcimento</i>	
<i>(Segue) Hard Fork e Soft Fork</i>	
<b>1.9.3 Yeld Farming</b> .....	49
<i>(Segue) Gli indici della DeFi</i>	
<b>1.9.4 Airdrop</b> .....	53
<b>1.9.5 Il Mining</b> .....	54

## Capitolo 2

<b>2.1 Analisi giuridica e rappresentazione in bilancio delle criptovalute</b> .....	57
<b>2.2 Criptovalute e qualificazione giuridica</b> .....	59
<i>(Segue) Le Funzioni della moneta legale</i>	
<i>(Segue) Le ipotesi di rappresentazione giuridica</i>	
<b>2.3 Primo arbitrato italiano sulle Criptovalute: Il Caso Marcianise 2018</b> .....	66
<b>2.4 Conferimenti di criptovalute in società di capitali</b> .....	67
<b>2.5 Rappresentazione in Bilancio delle Criptovalute</b> .....	70
<i>(Segue) IAS 7</i>	
<i>(Segue) IAS 32</i>	
<i>(Segue) Paragrafo AG 3 di IAS 32</i>	
<i>(Segue) IAS 38</i>	
<i>(Segue) IAS 2</i>	
<b>2.6 Valore di Iscrizione in Bilancio</b> .....	78
<b>2.7 Il Fair Value delle criptovalute</b> .....	80
<b>2.8 L’impatto dei principi contabili internazionali sul piano naziona</b> .....	83
<i>(Segue) OIC 24</i>	
<i>(Segue) OIC 13</i>	
<b>2.9 CASO AZIENDALE: ORACLIZE</b> .....	85

## **CAPITOLO 3**

<b>3.1 ANALISI FISCALE</b> .....	92
<b>3.2 risoluzione 72/e -agenzia delle entrate</b> .....	94
<b>3.3 Il trattamento ai fini delle imposte indirette</b> .....	96
<b>3.4 Il trattamento ai fini delle imposte dirette</b> .....	97
<i>(Segue) Criptovalute e IRAP</i>	
<b>3.5 I vafe e monitoraggio fiscale</b> .....	100
<b>3.6 Le criptovalute e l'ordinamento USA</b> .....	104

## **CAPITOLO 4**

<b>4.1 LE CONTROVERSIE DELLE CRIPTOVALUTE</b> .....	106
<b>4.2 L'impatto ambientale</b> .....	106
<b>4.3 Il riciclaggio di denaro</b> .....	109
<b>4.4 Il finanziamento del terrorismo</b> .....	110

<b>CONCLUSIONI</b> .....	114
--------------------------	-----

## **BIBLIOGRAFIA E SITOGRAFIA**



## Introduzione

*“Ogni persona informata ha bisogno di conoscere il Bitcoin perché potrebbe essere uno degli sviluppi più importanti del mondo.”*

Leon Luow, intellettuale e nominato Premio Nobel per la Pace

Marzo 2020, il mondo è nel pieno della pandemia, la parola lockdown riecheggia per le strade vuote di ogni singola città.

Il mondo è fermo, le attività al di fuori di quelle “necessarie” sono chiuse. Conseguenza di questa situazione pandemica è il crollo della borsa, Il Ftse Mib chiuse le contrattazioni con un ribasso dell’11,17% a 18.475 punti base, facendo entrare il 9 marzo 2020 nella storia del listino come il secondo peggior crollo di sempre.

Contemporaneamente a questi accadimenti un mercato invece è più attivo che mai ed è quello delle criptomonete. Bitcoin nel marzo 2020 presentava un valore di circa 5.000 euro e precisamente un anno dopo nel 2021, registrò un valore al di sopra di 50.000 euro, un andamento di mercato poco prevedibile.

Il mercato delle criptovalute ha inesorabilmente attratto molti investitori, basti pensare che l’impresa Tesla a fine 2021 nel suo report finanziario ha dichiarato di aver ottenuto 272 milioni di dollari di profitti proprio dalla vendita di questi asset digitali. Musk CEO dell’impresa americana, inoltre, ha affermato di “credere nel potenziale a lungo termine degli asset digitali, sia come investimento, sia come alternativa liquida al contante”.

Sostanzialmente il mercato delle criptovalute è altamente attrattivo o per fini meramente speculativi o per fini invece (similmente a quelli di Musk) di disruption del sistema monetario mondiale vertendo per un mondo ancor più digitale.

Molti degli investitori, o dei semplici spettatori di questo mondo, però hanno poca conoscenza delle criptovalute e della loro tecnologia.

Scopo di questo elaborato è di limare questa poca conoscenza.

Il testo è suddiviso in quattro capitoli, i quali descrivono le criptovalute su più versanti, tra questi vi è un versante storico, un versante economico in cui si analizzerà l’aspetto contabile e fiscale ed infine un versante inerente alla presenza o no di sostenibilità nella tecnologia che sorregge le criptovalute.

Il primo capitolo descrive la storia del mondo cripto; a partire dall'idea di Chaum delle "firme cieche", un sistema di firma digitale che si rivelerà fondamentale nel prodotto finale della blockchain, passando da Wei Dai e il suo protocollo B-money fonte d'ispirazione del più noto protocollo Bitcoin, sino alla registrazione del dominio della più famosa Blockchain.

Nel primo capitolo inoltre verrà descritto il sistema blockchain e le criptovalute originate da questa struttura, e per citarne qualcuna: Bitcoin, Ethereum, Ripple, ecc...

Verranno esposti ulteriori argomenti come il recente fenomeno degli NFT, token non fungibili che presentano un mercato a sé stante altamente profittevole, in cui partecipano non solo i grandi speculatori ma anche personaggi famosi.

Saranno anche descritti i processi di elaborazione e lancio delle criptovalute, mostrando come ormai questo mondo è quasi paragonabile a quello della borsa, inevitabile il confronto tra IPO (offerta pubblica iniziale di azioni di una società che vuole entrare nel mercato azionario) e ICO (l'offerta iniziale di criptovalute).

Il secondo capitolo invece analizzerà le criptovalute da un punto di vista contabile, mostrando come a distanza di anni dal loro lancio vi è ancora forte incertezza da parte delle istituzioni internazionali e nazionali nella loro rappresentazione contabile. Fondamentali saranno i principi IAS e il loro confronto al fine di poter comprendere quale sia la voce più corretta in cui inserire le criptovalute.

All'interno del secondo capitolo inoltre verrà esposto un caso aziendale la "ORACLE srl", società italiana che vanta il primato di aver effettuato i conferimenti del capitale sociale tramite bitcoin, nel cui bilancio appaiono le criptovalute.



Argomento del terzo capitolo sarà invece il trattamento fiscale delle criptovalute. Ad oggi svariate società e persone fisiche partecipano attivamente nel mercato delle criptovalute ed una delucidazione sul loro trattamento fiscale è estremamente necessaria, con lo scopo di informare non solo gli investitori ma anche i professionisti che debbono adempiere come sostituti nella dichiarazione dei redditi.

Per l'elaborazione di questo capitolo fondamentale è stato lo studio ed analisi della risoluzione 72/E dell'agenzia delle Entrate, la quale ha chiarito i forti dubbi riguardo la sfera fiscale del nostro ordinamento nei confronti delle criptovalute.

Il quarto capitolo invece espone i lati negativi dei bitcoin e anche delle altre criptomonete. Si illustrerà il forte impatto ambientale ed il finanziamento al terrorismo, informando così il lettore anche degli effetti negativi che questo mercato comporta.

Per concludere, vi saranno spunti riflessivi, nati dallo studio e dalle consultazioni di svariati testi, utili per la preparazione dell'elaborato in analisi.

## 1.1 Storia

### Blind Signatures for Untraceable payments

BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science  
University of California  
Santa Barbara, CA

#### INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of the new electronic payments system may have a substantial impact on personal privacy as well as on the nature and extent of criminal use of payments. Ideally a new payments system should address both of these seemingly conflicting sets of concerns.

Parte dell'articolo di David Chaum

Nel 1982 David Chaum pubblicò l'articolo intitolato "Blind Signatures for Untraceable payments", in cui asseriva che l'automazione nelle modalità di pagamento di beni e servizi fosse un fenomeno oramai avviato, di notevole impatto sostanziale sulla privacy personale, nonché sulla natura e la portata dell'uso criminale dei pagamenti. Da questa affermazione introdusse il concetto di crittografia e "blind Signatures", una forma di firma digitale in cui il contenuto di un messaggio viene mascherato (accecato) prima di essere firmato. Egli spiegava che la firma cieca risultante può essere verificata pubblicamente rispetto al messaggio originale non nascosto come una normale firma digitale. Le firme cieche sono in genere utilizzate nei protocolli relativi alla privacy in cui il firmatario e l'autore del messaggio sono parti diverse. Chaum utilizzò l'esempio semplificato delle buste elettorali, ovvero buste rivestite con carta carbone, per spiegare il sistema di tracciabilità delle firme digitali, tale sistema funziona così:

- 1-Un elettore racchiude una scheda anonima completata in una speciale busta foderata di carbone che ha le credenziali dell'elettore prestampate all'esterno.

2-Un funzionario verifica le credenziali e firma la busta, trasferendo così la sua firma alla scheda interna attraverso carta carbone.

3-Una volta firmato, il pacchetto viene restituito all'elettore, che trasferisce la scheda firmata in una nuova busta normale non segnata.

4-Allora, il firmatario non vede il contenuto del messaggio, ma un terzo può successivamente verificare la firma e sapere che la firma è valida entro le limitazioni dello schema di firma sottostante.

Il voto elettronico è stato uno dei principali casi di utilizzo delle blind signatures

*(Segue) Le Funzioni  $f(x)$*

Chaum descrisse le seguenti tre funzioni che costituivano il sistema crittografico della firma cieca:

1- Una funzione di firma  $s'$  nota solo al firmatario, e le corrispondenti inverse pubblicamente note, tali che  $s'(s'(x))=x$  e  $s$  non danno alcun indizio su  $s$ .

2- Una funzione di commutazione  $c$  e la sua inversa  $c'$ , entrambe note solo al provider, tali che  $c'(s'(c(x)))=s'(x)$ , e  $c(x)$  e  $c'$  non danno indizio su  $x$ .

3- Un predicatore di controllo della ridondanza  $r$ , che verifica la ridondanza sufficiente per rendere impraticabile la ricerca di firme valide.

Protocollo:

Il modo in cui queste funzioni vengono utilizzate ricorda il modo in cui sono state utilizzate le buste foderate di carta carbone nell'esempio sopra descritto:

1-Il provider sceglie  $x$  a caso in modo tale che  $r(x)$ , formi  $c(x)$  e fornisca  $c(x)$  al firmatario.

2-Il firmatario firma  $c(x)$  applicando  $s'$  e restituisce l'argomento firmato  $s'(c(x))$  al provider.

3-Il fornitore spoglia la materia firmata mediante l'applicazione di  $c'$ , cedendo  $C'(s'(c(X)))=s'(X)$ .

Chiunque può verificare che la materia spogliata  $s'(x)$  sia stata formata dal firmatario, applicando le chiavi pubbliche del firmatario e verificando che  $r(s(s'(x)))$ .

*(Chaum, Blind Signatures for Untraceable Payments 1982)*

Queste caratteristiche dei sistemi di firma cieca, introdotti sopra, possono essere utilizzate per effettuare un sistema di pagamenti non rintracciabile. Il concetto fondamentale è che la banca firmerà qualsiasi cosa con la sua chiave privata, ma qualsiasi cosa così firmata varrà un importo fisso. (Chaum,1982)

Gli attori nel sistema di pagamento sono una banca, un pagatore e un beneficiario. Un'unica "banconota" sarà formata dal pagatore, firmata dalla banca, sottratta quindi al pagatore, fornita al beneficiario e sdoganata dalla banca.

*(Segue) Verificabilità delle Firme cieche*

La pratica di tale sistema di pagamento suggerisce che i pagatori ricevano ricevute digitali dai beneficiari. Queste ricevute includerebbero la consueta descrizione dei beni o servizi acquistati e la data. Inoltre, la ricevuta potrebbe includere anche una copia della nota. In circostanze eccezionali, come una verifica, la nota consentirebbe al pagatore, con la collaborazione della banca (e della stanza di compensazione<sup>1</sup>), di verificare su quale conto è stata effettivamente depositata la nota.

---

<sup>1</sup> Sono istituti cui si possono associare tutte le banche operanti in una determinata zona, allo scopo di facilitare la regolamentazione dei rapporti di debito e credito originati, fra le stesse, dagli assegni bancari messi in circolazione dai titolari dei depositi in conto corrente. Quando una banca riceve da parte dei propri correntisti la richiesta di accredito di assegni tratti su una delle altre banche associate, anziché entrare in contatto direttamente con ognuna di esse per l'incasso di ciascun assegno e per tutte le altre conseguenti operazioni che comportino l'effettivo trasferimento della moneta, si rivolge alla stanza di compensazione. Giornalmente ogni banca invia alla stanza di compensazione l'elenco degli assegni a credito tratti sulle altre anche; dalla differenza tra questi e gli assegni a debito verso le altre associate si calcola l'ammontare del dare e dell'avere in quel determinato giorno e solo le differenze eventualmente in essere vengono liquidate dalla stanza di compensazione.

Una ricevuta che indica che una nota è stata depositata su un conto diverso dal conto effettivamente depositato sarebbe prova di frode. Un cliente potrebbe rivelare, in caso di contraddizione della transazione, una banconota proveniente o destinata al mercato nero, riconducendola al conto di provenienza o destinazione. Le banconote non liquidate segnalate come rubate potrebbero essere incluse negli elenchi delle stanze di compensazione e quindi essere impediti di essere utilizzate e quelle rubate o cancellate potrebbero essere rintracciate.

Le ricevute emesse dal beneficiario al pagatore forniscono il controllo su tutti i flussi. Un contribuente potrebbe fornire ricevute verificabili per qualsiasi spesa necessaria per la verifica fiscale.

*(Segue) Le ipotesi di Chaum e la loro effettiva realizzazione.*

Chaum nel suo elaborato aveva ipotizzato che il sistema delle transazioni con firma cieca potesse essere esteso in vari modi per fornire un'economia dei meccanismi, disaggregazione dei servizi e decentralizzazione.

Una delle ipotesi era quella della divisione tra le funzioni bancarie e le stanze di compensazione, divisione che effettivamente avvenne infatti dal 1° aprile 2019 la Banca d'Italia ha chiuso le stanze di compensazione, luogo deputato allo scambio materiale di assegni tra le banche.

Come previsto da Chaum, l'efficienza e l'economicità del sistema di pagamenti digitali è stato promosso a sostituire il sistema delle stanze, uno dei motivi fondamentali è la considerevole riduzione dei costi per gli intermediari.

Il regolamento interbancario degli assegni, ora digitalizzati, continua ad avvenire tramite procedure elettroniche che alimentano il sistema di compensazione gestito dalla Banca d'Italia.

([www.bancaditalia.it](http://www.bancaditalia.it), 8 marzo 2019)

## 1.2 Chaum e Digicash

Nel 1989, Chaum decise di fondare Digicash Inc. società elettronica il cui Core business era gestione dei pagamenti online e della moneta elettronica, fondamentale quindi era l'utilizzo (già preannunciata) della crittografia asimmetrica, la quale permetteva il totale anonimato degli users.

Digicash però fallì secondo il capitolo 11 della "Bankruptcy"<sup>2</sup> ovvero presentazione da parte dell'impresa di un piano di riorganizzazione al tribunale fallimentare.

Nonostante il fallimento di Digicash e della sua idea quindi di tracciabilità dei pagamenti online, Chaum influenzò molto i movimenti futuristici che condividevano idee e opinioni sulla privacy.

*"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."*

(Hughes, 1993)

---

<sup>2</sup> Conosciuto anche come procedura di riorganizzazione del Capitolo 11 e talvolta indicato come "protezione dal fallimento".

Il capitolo 11 fa riferimento al capitolo del codice fallimentare statunitense che stabilisce la procedura legale per le procedure di riorganizzazione ai sensi del diritto fallimentare statunitense.

In generale, un debitore che ha proprietà negli Stati Uniti può presentare una petizione per avviare il procedimento del Capitolo 11. Il debitore non deve essere insolvente. Al momento della presentazione dell'istanza, entra in vigore una sospensione automatica che impedisce qualsiasi azione esecutiva o l'avvio o il proseguimento di altri procedimenti legali nei confronti del debitore. Il soggiorno automatico si estende tecnicamente in tutto il mondo. Ciò può essere paragonato alla giurisdizione discrezionale del tribunale inglese di estendere la moratoria nei procedimenti amministrativi al di fuori del Regno Unito. Una volta che il debitore ha avviato il procedimento di cui al capitolo 11, è concesso un termine esclusivo di 120 giorni per presentare al tribunale un piano di riorganizzazione, che esponga una proposta di compromesso dei suoi debiti e/o di riorganizzazione della sua attività.

I creditori possono proporre il proprio piano trascorsi 180 giorni senza che il piano del debitore sia approvato. Un piano è approvato se è accettato da almeno due terzi del valore di ciascuna classe di creditori "deteriorati", agendo in buona fede ( § 1126, Capitolo 11, Titolo 11, Codice USA ). Da [https://uk.practicallaw.thomsonreuters.com/4-107-5889?transitionType=Default&contextData=\(sc.Default\)](https://uk.practicallaw.thomsonreuters.com/4-107-5889?transitionType=Default&contextData=(sc.Default))

Queste erano le parole scritte nel manifesto del 1993 da Eric Hughes, uno dei maggiori esponenti del Cyberpunk <sup>3</sup>, un genere letterario che ha considerevolmente basato parte dei suoi scritti su Chaum ed i suoi elaborati.

### 1.3 Wei dai e B-money

Tra i tanti maggiori esponenti del gruppo cyberpunk, che basò il suo lavoro sul pensiero di Chaum, è **Wei Dai**.

Wei Dai è noto per la pubblicazione nel 1998 del testo “b-money, un sistema di contante elettronico distribuito e anonimo”. Dai descrisse b-money come "uno schema per un gruppo di pseudonimi digitali non rintracciabili per pagarsi l'un l'altro con denaro e far rispettare i contratti tra di loro senza un aiuto esterno".

B-money presentava una serie di caratteristiche specifiche tra cui: il requisito del lavoro computazionale per facilitare la valuta digitale, la stipula che questo lavoro deve essere verificato dalla comunità in un registro collettivo, e premiare i lavoratori per il loro contributo. Per garantire che le transazioni rimanessero organizzate, Dai propose una contabilità collettiva, con protocolli crittografici che aiutassero ad autenticare le transazioni. Inoltre, l'autore del testo B-Money suggerì l'uso di firme digitali (*Blind Signatures* di Chaum), o chiavi pubbliche, per l'autenticazione delle transazioni e l'applicazione dei contratti.

---

<sup>3</sup> TRECCANI cyberpunk Genere narrativo in cui temi legati alla realtà delle società postindustriali (cibernetica, robotica, telematica, realtà virtuale, biotecnologie, clonazione) vengono elaborati fantasticamente nel segno di un'ideologia contestataria, di ribellione e critica sociale, analoga a quella del movimento punk o della musica punk rock. Originale sintesi di suggestioni tecnologiche e cultura underground, il c. si è affermato negli Stati Uniti nel corso degli anni 1980 grazie soprattutto al romanzo *Neuromancer* (1984) di William Gibson e a un'antologia di racconti di autori vari pubblicata da B. Sterling nel 1986, *Mirrorshades*. Adottando modalità narrative proprie della fantascienza, il c. si è poi aperto alla contaminazione con altri generi, particolarmente il noir, avendo tra i propri antecedenti il romanzo *hard-boiled* e tra i modelli più vicini autori come l'inglese J.G. Ballard o lo statunitense Philip K. Dick, autore di *Do androids dream of electric sheep?* (1968), da cui R. Scott trasse ispirazione per il film *Blade runner* (1982), uno dei sicuri punti di riferimento dell'immaginario

*(Segue) I Protocolli di B-Money*

Nel B-Money di Wei Dai erano inclusi due protocolli:

Il primo protocollo prevedeva l'utilizzo di un *proof of work*, inteso come strumento per creare moneta online.

Il secondo protocollo, invece, aveva la funzione di notificare agli users del network se il proprio importo non fosse stato soggetto a inflazione.

le linee di partecipazione alla rete affermando che una somma di denaro era un requisito fondamentale per diventare server della rete, ma poteva essere perso se il server stesso si rivelava "disonesto".

Tuttavia, anche se furono notevoli i progressi dell'Information Technology, il meccanismo teorizzato faceva attrito con l'impossibilità di una sua implementazione pratica funzionale.

Il problema riguardava infatti il fenomeno della double spending, ovvero il processo che consentiva di duplicare lo stesso gettone e spenderlo più volte.

Il B-Money di Wei Dai però rimase solo un documento e un'idea di uno dei componenti del cyberpunk senza alcuna realizzazione di tale moneta digitale, ma che, comunque, influì profondamente i futuri progetti delle cripto-monete.



## 1.4 La nascita di Bitcoin

### La prima Blockchain e la prima Criptovaluta

A un decennio dalla proposta di B-money di Dai, e più precisamente, il 18 Agosto 2008 su "anonymousspeech.com" fu registrato un *dominio*<sup>4</sup>.

Il dominio era a nome di bitcoin.org, ma per parlare del protocollo e delle criptovalute che avrebbero influenzato il mondo finanziario si dovrà aspettare il 31 Ottobre 2008, giorno in cui il programmatore Satoshi Nakamoto pubblicò "Bitcoin: a peer to peer electronic cash system".

Nell'elaborato spiegava il funzionamento del "protocollo Bitcoin" o meglio, le caratteristiche tecniche della criptovaluta e la fondamentale tracciabilità delle transazioni e non delle monete digitali.

Il problema quindi del *double spending* del B-money, con la tracciabilità delle transazioni, fu debellato.

Successivamente alla registrazione del dominio bitcoin.org e della pubblicazione del protocollo del sistema Satoshi Nakamoto, il 3 Gennaio del 2009 effettuò il lancio del primo blocco *proof to work*, il **Genesis Block** conosciuto in Italia anche come *blocco Zero*.

---

<sup>4</sup> "un insieme di computer che condividono un database di risorse di rete e che vengono amministrati come un'unità con regole e procedure comuni"

(Microsoft).

In informatica, il dominio è l'espressione alfanumerica che identifica in maniera univoca un server Internet. A essa è abbinato un indirizzo numerico (indirizzo ip) utilizzato per il trasferimento dei dati. Il nome del dominio è diviso in tre livelli separati da un punto. Il primo livello indica la nazione (it per l'Italia, fr per la Francia, uk per il Regno Unito ecc.) oppure il tipo (com per siti commerciali, edu per i siti di carattere educativo, gov per i siti governativi ecc.). L'organizzazione internazionale che gestisce il sistema dei nomi a domini di primo livello è l'icann (Internet Corporation for Assigned Names and Numbers). Il dominio di secondo livello generalmente corrisponde al nome dell'ente o persona proprietari del dominio stesso oppure è attinente al contenuto del sito. Il dominio di terzo livello può essere scelto arbitrariamente per indicare il nome della macchina, del sistema operativo o del servizio a disposizione. In genere, il dominio di terzo livello è www (World Wide Web), ma è possibile trovare domini con qualsiasi nome, come per esempio www2, ftp, lnx ecc.

Da Enciclopedia Treccani

Il Genesis Block sfrutta una blockchain, che è composta da una serie di così chiamati “blocchi” la cui funzione è di memorizzazione di informazioni relative alle transazioni che si verificano nel network blockchain.

### Bitcoin's Genesis Block

```

00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;f!yz{.2zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ā`ŠQ2:Ÿ_#
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)=_Iÿÿ...~+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ÿÿÿÿM.ÿÿ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksÿÿÿÿ..ò.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠÿ"pUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gn|q0-.\"Ö" (à9.¡
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybâé.ab†IÖ¿LI8Ā
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 óU.Ā.Ā.P\8M+9...W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 ŠLp+kñ._~....

```

(Source: bitcoin.com)

Ciascuno dei blocchi contiene un'intestazione univoca e ciascuno di questi blocchi è identificato individualmente dall'hash dell'intestazione del blocco. Questi blocchi vengono stratificati, uno sopra l'altro, con il blocco Genesis come base, e crescono in altezza fino a raggiungere la fine della blockchain e la sequenza è completa. Gli strati e la storia profonda di ogni sequenza sono una delle cose che rende una criptovaluta basata su blockchain così sicura.

Il Genesis Block è il modello per tutti gli altri blocchi nella sua blockchain.

## 1.6 La Blockchain

La blockchain (letteralmente "catena di blocchi") è una struttura dati condivisa e "immutabile". È definita come un registro digitale le cui voci sono raggruppate in "blocchi", concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia. Sebbene la sua dimensione sia destinata a crescere nel tempo, è immutabile in quanto, di norma, il suo contenuto una volta scritto non è più né modificabile né eliminabile, a meno di non invalidare l'intera struttura. Tale invalidità è dovuta anche alla presenza di una "marca temporale" per ogni blocco. (<https://it.wikipedia.org/wiki/Blockchain>), s.d.)

Nella Blockchain i blocchi sono scanditi e quindi intervallati da una frazione di tempo  $t$ , ogni blocco quindi ottiene e conserva i dati relativi ad ogni singola transazione che viene effettuata in tale asse temporale.

Terminata la frazione di tempo, sul blocco interessato viene applicato quindi il *Timestamp* o marca temporale.

Il sistema del timestamp implica quindi che la produzione dei blocchi è inarrestabile. Ogni 10 minuti si costituirà un nuovo blocco che conterrà quindi le ultime transazioni in bitcoin effettuate dagli users del network e confermate dai miners<sup>5</sup>. Quindi la Blockchain è un file incrementale che si innalza sempre col passare del tempo per contenere gli ultimi aggiornamenti del sistema (le nuove transazioni). Processo quindi che non presenta limiti né nella struttura della blockchain, né nel numero di blocchi che verranno formati, sostanzialmente un processo di formazioni dei blocchi infinito nel tempo.

---

<sup>5</sup> Coloro che svolgono il data mining:insieme di tecniche e metodi per estrarre dati significativi ancorché impliciti, rispetto a un particolare scopo, da un database o comunque da una qualunque fonte informativa. Per esempio, tecniche del genere possono tradursi in algoritmi che, indagando statisticamente i tipi di siti Internet visitati dagli indirizzi ip degli utenti, inviano a tali utenti messaggi pubblicitari mirati.

I blocchi oltre al timestamp presentano un “*Puntatore Hash*”<sup>6</sup>. la cui funzione è di identificare in maniera univoca e inequivocabile un blocco della Blockchain.

Il sistema Blockchain, grazie alla sua complessa ma affascinante tecnologia, permette di avere quindi un’ articolata rete, le cui componenti archiviali sono condivisibili ma custodite, presentando le transazioni con i loro importi e gli “pseudonimi” di chi le effettua.

Tale caratteristica di network fortemente articolata rende la Blockchain inviolabile.

Questo vuol dire che la Blockchain sia un registro digitale, consultabile da tutti presentando quindi trasparenza, tracciabilità e contemporaneamente una forte sicurezza. Il suo sistema decentrato è più resistente ad attacchi informatici o a incidenti operativi rispetto a un sistema accentrato, in quanto i suoi algoritmi continuano ad operare anche quando uno o più nodi smettono di funzionare. Grazie a tali caratteristiche, la blockchain è considerata pertanto un'alternativa alle banche dati e ai registri gestiti in maniera centralizzata da autorità riconosciute e regolamentate.

Le tecnologie sono incluse nella famiglia dei Distributed Ledger, possono essere definite come un insieme di sistemi concettualmente caratterizzati dal fatto di fare riferimento a un registro distribuito, ossia sistemi che possono essere letti e modificati da più nodi di una rete.

---

<sup>6</sup> In informatica, nella programmazione, tipo di dato il cui valore è l’indirizzo di un altro elemento, sia esso costante, variabile o più in generale un oggetto software. Generalmente i p. vengono utilizzati per gestire le strutture dati, quali array/”>array e liste concatenate, o per gestire il passaggio dei dati tra programmi. Il puntatore Hash, da Enciclopedia Treccani



Rappresentazione grafica dei “nodi” della Blockchain.

Immagine ottenuta da focus.it

Non è richiesto che i nodi coinvolti conoscano l'identità reciproca o si fidino l'uno dell'altro. Difatti, per garantire la coerenza tra le varie copie, l'aggiunta di un nuovo blocco è globalmente regolata da un protocollo condiviso. Una volta autorizzata l'aggiunta del nuovo blocco, ogni nodo aggiorna la propria copia privata: la natura stessa della struttura dati garantisce l'assenza di una sua manipolazione futura.

Le caratteristiche che accomunano i sistemi sviluppati con le tecnologie Blockchain e Distributed Ledger sono digitalizzazione dei dati, decentralizzazione, disintermediazione, tracciabilità dei trasferimenti, trasparenza/verificabilità, immutabilità del registro e programmabilità dei trasferimenti.

Nello specifico un registro distribuito è un database condiviso e sincronizzato consensualmente su più siti, istituzioni o aree geografiche, accessibile da più persone.

Consente alle transazioni di avere "testimonianze" pubbliche. Il partecipante a ciascun nodo della rete può accedere alle registrazioni condivise su quella rete e può possederne una copia identica. Eventuali modifiche o aggiunte apportate al libro mastro vengono riflesse e copiate a tutti i partecipanti in pochi secondi o minuti.

Un libro mastro distribuito è in contrasto con un libro mastro centralizzato, che è il tipo di libro mastro utilizzato dalla maggior parte delle aziende. Un registro centralizzato è più soggetto ad attacchi informatici e frodi, poiché ha un unico punto di errore.

Alla base dei registri distribuiti c'è la stessa tecnologia utilizzata dalla blockchain, che è la tecnologia utilizzata dal bitcoin

Fin dall'antichità, i libri mastri sono stati al centro delle transazioni economiche, con lo scopo di registrare contratti, pagamenti, operazioni di compravendita o spostare beni o proprietà. Il viaggio iniziato con la registrazione su tavolette di argilla o papiro ha fatto un grande salto con l'invenzione della carta.

Negli ultimi due decenni, i computer hanno fornito il processo di registrazione e manutenzione dei registri con grande comodità e velocità. Oggi, con l'innovazione, le informazioni archiviate sui computer si stanno spostando verso forme molto più elevate, che sono protette crittograficamente, veloci e decentralizzate. Le aziende possono trarre vantaggio da questa tecnologia in molte forme, un modo è attraverso registri distribuiti.

Un libro mastro distribuito può essere descritto come un registro di qualsiasi transazione o contratto mantenuto in forma decentralizzata tra luoghi e persone diverse, eliminando la necessità di un'autorità centrale per controllare la manipolazione. In questo modo, non è necessaria un'autorità centrale per autorizzare o convalidare alcuna transazione.

Tutte le informazioni sul libro mastro sono archiviate in modo sicuro e accurato utilizzando la crittografia e sono accessibili tramite chiavi e firme crittografiche. Una volta archiviate, le informazioni diventano un database immutabile, governato dalle regole della rete.

Mentre i registri centralizzati sono soggetti ad attacchi informatici, i registri distribuiti sono intrinsecamente più difficili da attaccare perché tutte le copie distribuite devono essere attaccate contemporaneamente affinché un attacco abbia successo. Inoltre, questi record sono resistenti alle modifiche dannose da parte di una singola parte. Essendo difficili da manipolare e attaccare, i registri distribuiti consentono un'ampia trasparenza.

I registri distribuiti riducono anche le inefficienze operative, accelerano il tempo necessario per completare una transazione, sono automatizzati e quindi funzionano 24 ore su 24, 7 giorni su 7, il che riduce i costi complessivi per le entità che li utilizzano.

I registri distribuiti forniscono anche un facile flusso di informazioni, il che rende facile seguire una traccia di controllo per i contabili quando conducono revisioni dei rendiconti finanziari. Questo aiuta a rimuovere la possibilità che si verifichino frodi sui libri finanziari di un'azienda. La riduzione dell'uso della carta è anche un vantaggio per l'ambiente.

Le DLT prevedono l'utilizzo di algoritmi crittografici che abilitano l'utente all'utilizzo del sistema, mettendogli a disposizione una chiave pubblica ed una privata che viene usata per sottoscrivere le transazioni o per attivare gli smart contract o altri servizi collegati alla blockchain.

Gli smart contract hanno il compito di verificare l'avverarsi di determinate condizioni e di autoeseguire in automatico azioni (o dare disposizione affinché si possano eseguire determinate azioni) nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate. In altre parole, lo Smart Contract è basato su un codice che "legge" sia le clausole che sono state concordate, sia le condizioni operative nelle quali devono verificarsi le condizioni concordate e si autoesegue automaticamente nel momento in cui i dati riferiti alle situazioni reali corrispondono ai dati riferiti alle condizioni e alle clausole concordate.

Le DLT prevedono pertanto un meccanismo di validazione, a sua volta distribuito, basato sul concetto di consenso, vale a dire su meccanismi che governano anche questo tipo di partecipazione dei nodi. Il consenso all'interno della blockchain è regolamentato da due protocolli: il Proof of Work e il Proof of Stake.

Da sottolineare che le modalità di gestione del consenso, unitamente alle logiche di impostazione del registro, rappresentano due fra i principali punti qualificanti della carta d'identità delle tecnologie Distributed ledger.

Il concetto di Proof of work (Pow), esisteva già prima del Bitcoin ed è forse tra le più grandi idee alla base del white paper di Nakamoto, perché realizza un consenso senza fiducia e distribuito.

Proof-of-Work, o PoW, è semplicemente l'algoritmo di consenso originale in una rete Blockchain. Un sistema di consenso affidabile e distribuito significa che se si desidera inviare e / o ricevere denaro da qualcuno non è necessario affidarsi a servizi di terzi, a differenza di quando si utilizzano i metodi di pagamento tradizionali, dove è necessario servirsi di una terza parte per impostare la transazione( [www.lecriptovalute.org](http://www.lecriptovalute.org))

Effettuata quindi l'operazione, le parti coinvolte manterranno il proprio registro privato che memorizza la cronologia delle transazioni e i saldi di ciascun account.

Il Proof of stake è un modo diverso per convalidare le transazioni e ottenere il consenso distribuito. È ancora un algoritmo e lo scopo è lo stesso del proof of work, ma il processo per raggiungere l'obiettivo è diverso.

A differenza del proof of work, dove l'algoritmo premia i minatori che risolvono problemi matematici con l'obiettivo di convalidare le transazioni e creare nuovi blocchi, con il proof of stake, il creatore di un nuovo blocco viene scelto in modo deterministico, a seconda della sua ricchezza, definita anche come "stake".

Inoltre, tutte le valute digitali sono state create in precedenza all'inizio e il loro numero non cambia mai.

Ciò significa che nel sistema PoS non vi è alcun premio di blocco; quindi, i minatori accettano le commissioni di transazione.

Altro fattore determinante è quello che garantisce la non duplicabilità delle informazioni, mediante una tecnica complessa che permette la creazione di blocchi crittografati concatenati tra di loro tramite chiavi crittografate immutabili.

A dimostrazione della sicurezza e della inviolabilità di tale organizzazione tecnologica, va detto che dal 2009 ad oggi, infatti, sono stati compiuti innumerevoli tentativi di violazione della blockchain, ma nessuno ci è mai riuscito; la blockchain è pubblica e quindi chiunque può avervi accesso, ma è inviolabile proprio per il fatto che è distribuita in una quantità enorme di computer e quindi non ci sarebbe un unico server da modificare, ma una cifra elevatissima.



Si basa dunque su una rete chiamata peer-to-peer, con acronimo P2P, cioè una rete informatica nella quale i computer degli utenti connessi fungono nello stesso tempo da client e da server.

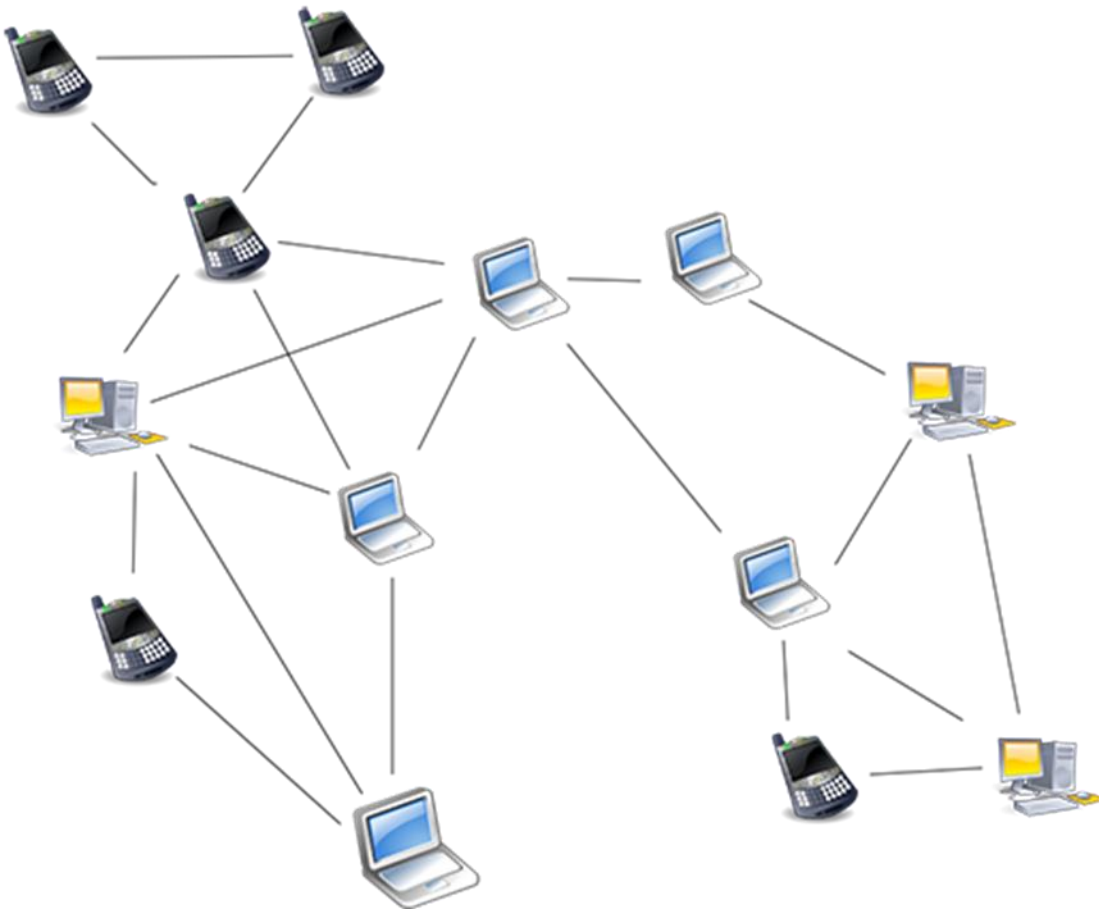
*(Segue) Rete Peer to Peer*

Un network peer-to-peer è costituito minimamente da due computer che scambiano file tra di loro sfruttando un cavo USB come mezzo di comunicazione. La prima piattaforma ad applicare una rete P2P fu Napster<sup>7</sup> nel 1999.

Nella rete P2P rientrano anche le LAN aziendali, composte da una decina di computer collegati tra loro con doppini di rame o cavi Ethernet, o reti più estese che utilizzano protocolli ad hoc per mettere in comunicazione i vari nodi che la compongono e consentire così lo scambio di dati. Un network dunque, si forma quando due o più device sono in grado di comunicare tra di loro e inviarsi reciprocamente delle informazioni senza che ci sia la necessità di passare attraverso un calcolatore centrale (o server).

---

<sup>7</sup> Napster era un programma di file sharing creato da Shawn Fanning e Sean Parker e attivo dal giugno 1999 fino al luglio 2001. Dopo l'acquisizione da parte di Roxio, è divenuto un servizio legalizzato a pagamento con una prova gratuita di 30 giorni.  
fonte Wikipedia



Rappresentazione grafica di una rete P2P

Immagine proveniente da Fastweb.it

Volendone dare una definizione, si può dire che una rete peer-to-peer è un'architettura di calcolo distribuito nella quale i vari nodi condividono tra di loro parte delle loro risorse informatiche (come la potenza di calcolo della CPU, lo spazio sull'hard disk e la memoria RAM, la larghezza di banda e così via) senza che ci sia bisogno di un nodo centrale – il già citato server – che coordini il tutto.

I nodi, dunque, non sono gerarchizzati tramite il binomio client e server, ma si tratta di nodi paritari (peer in inglese, per l'appunto), in grado di svolgere sia il "ruolo" di cliente, sia quello di fornitore.

In tal modo, gli utenti sono in grado di accedere direttamente l'uno al computer dell'altro, visionando e prelevando i file presenti nelle memorie di massa e mettendo a loro volta a disposizione i file che desiderano condividere. Le reti peer-to-peer sono usate in particolare per scambiare file audio o video.

### *(Segue) Possibili applicazioni della blockchain*

La tecnologia blockchain funziona dal 2009 ed è stata ampiamente testata dai bitcoin. Blockchain è tuttavia un protocollo trasversale: non tocca solo un settore, ma molti ambiti anche molto diversi tra loro.

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 terze parti.

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.

Transazioni di valori mobiliari e immobiliari attraverso un registro distribuito;

Leasing e compravendita di automobili;

Networking e IoT. IBM e Samsung stanno lavorando su un concetto di rete decentrata, noto come ADEPT, che utilizza una tecnologia simile alle blockchain per gestire la comunicazione tra dispositivi anche senza un sistema di controllo central;

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;

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;

Supply Chain Management. 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;

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 student;

Analisi finanziarie, scommesse sportive e attività di previsione;

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 garantire una miglior governance pubblica delle iniziative;

Archiviazione di dati nel cloud. Le soluzioni di cloud storage basate sui distributed ledger 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 immagazzinati.

Nel 2017 varie aziende si sono avvicinate al mondo della Blockchain, aumentando in maniera esponenziale il loro *trust* nei confronti di questa tecnologia, applicandola in uno dei settori sopra elencati. I risultati che si stanno ottenendo danno prospettive estremamente positive, tra i vari si possono evidenziare:

-Maggior efficienza dei flussi di lavoro;

-Significativa riduzione dei tempi e dei costi gestionali;

-Sicurezza dei dati aumentata in maniera esponenziale con una forte trasparenza tra le parti.

*La crittografia, inoltre, è un fattore fondamentale per rendere i dati immutabili e incorruttibili.*

La blockchain ha il suo ampio utilizzo nel sistema finanziario e commerciale, ciò ovviamente non esclude l'utilizzo della stessa nell'ambito sociale.

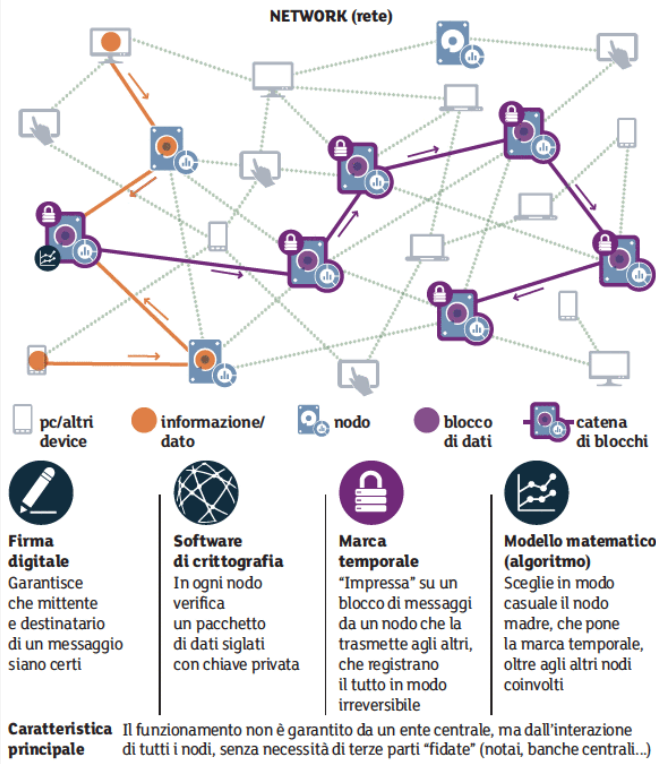
Un esempio pratico è lo sfruttamento di questa tecnologia nel 2017 da parte dell'ONU per il progetto di distribuzione di aiuti in Giordania, in cui era previsto la distribuzione di un tagliando univoco e assegnato ad un preciso numero di persone. L'identità del cittadino che aveva il diritto ad usufruire di tale tagliando era gestita da un sistema che basava il riconoscimento del soggetto tramite l'iride.

La tecnologia di contabilità distribuita ha un grande potenziale per rivoluzionare il modo di lavorare di governi, istituzioni e aziende. Può aiutare i governi nella riscossione delle tasse, nell'emissione di passaporti, nella registrazione dei registri catastali, nelle licenze e nell'esborso delle prestazioni di sicurezza sociale, nonché nelle procedure di voto.

# Blockchain: il nuovo paradigma

## La tecnologia della "catena di blocchi"

Sfrutta la rete per realizzare un registro pubblico e condiviso di ogni transazione possibile, un libro contabile che si aggiorna automaticamente ed identicamente su ciascuno dei nodi



<b>Settore finanziario</b> es: Bitcoin crea moneta virtuale	<b>Identità digitale</b> es: Bitnation riconosce diritti dei rifugiati	<b>Principali utilizzi della tecnologia "blockchain"</b>	<b>Transazioni commerciali</b> Beni mobili e immobili	<b>Comunicazione tra device</b> Senza controllo centrale
<b>Settore auto</b> es: gestione leasing	<b>Assicurazioni</b> Contratti senza garante	<b>Sanità</b> Condividere dati in sicurezza	<b>Enti benefici e Ong</b> Tracciabilità dei fondi	<b>Distribuzione di merci</b> Riduce costi ed errori umani
<b>Voti elettorali</b> No brogli o sbagli	<b>Scuola Università</b> Trasparenza di voti e titoli	<b>Attività di previsione</b> es: scommesse sportive	<b>Pubblica Amministrazione</b> es: gestione del Welfare	<b>Cloud storage</b> Anti hacker

Sebbene la tecnologia di contabilità distribuita abbia molteplici vantaggi, è in una fase nascente, in continuo studio su come adottarla nel miglior modo possibile. Sebbene una cosa sia chiara, il formato futuro dei libri mastri secolari deve essere decentralizzato.

Ci sono oggi oltre 1.000 piattaforme e ne nascono di nuove ogni giorno. Ciascuna è connotata da configurazioni differenti, tuttavia è possibile identificare 7 caratteristiche comuni proprie della tecnologia Blockchain. La prima fa ovviamente riferimento alla *Digitalizzazione e alla trasformazione dei dati in formato digitale*.

Di seguito le altre sei:

### *Decentralizzazione*

Le informazioni vengono registrate distribuendole tra più nodi per garantire sicurezza informatica e resilienza dei sistemi.

- *tracciabilità dei trasferimenti*

Ciascun elemento sul registro è tracciabile in ogni sua parte e se ne può risalire all'esatta provenienza

- *Disintermediazione*

Le piattaforme consentono di gestire le transazioni senza intermediari, ossia senza la presenza di enti centrali fidati

- *Trasparenza e verificabilità*

Il contenuto del registro è trasparente e visibile a tutti ed è facilmente consultabile e verificabile

- *Immutabilità del registro*

Una volta scritti sul registro, i dati non possono essere modificati senza il consenso della rete

- *Programmabilità dei trasferimenti*

Possibilità di programmare determinate azioni che vengono effettuate al verificarsi di certe condizioni

## *(Segue)Il Protocollo Cryptonote*

Nel 2013 un gruppo di matematici e informatici svilupparono un protocollo al fine di offrire uno strumento decentralizzato, anonimo e sicuro. Simile su alcuni aspetti alla blockchain, presenta una gestione decentralizzata delle transazioni, ma su altri si differenzia totalmente: i blocchi all'interno del protocollo sono composti da meno informazioni accessibili solo alle parti della transazione, presentando così un notevole livello di riservatezza della transazione. Al momento 15 criptovalute fanno utilizzo di tale tecnologia.

Tale protocollo fu lanciato anche per via delle critiche mosse alla blockchain bitcoin, l'anonimato e la privacy non venivano totalmente rispettate dalla tecnologia. Ulteriore critica mossa verso blockchain era la POW (identifica la potenza di lavoro per il calcolo di attività di mining) utilizzata.

La blockchain presenta dei nodi minatori, i quali tramite CPU/GPU danno vita ad ulteriori nodi che immessi nel sistema permettono al minatore di ottenere nuovi *token*.

Per via però dell'incredibile intensità e complessità di calcoli da effettuare, il mining non sarà più accessibile a coloro che intendano lanciarsi in questa attività, bensì a causa dell'enorme diffusione delle *mining farm*\*(vedi sottoparagrafo). sarà concesso solo a un cerchio ristretto di persone.

CryptoNote nasce per questo motivo, permettere l'accessibilità al mining a coloro che vogliono usare il loro GPU. La prima ad applicare CryptoNote fu *MONERO*, criptovaluta nata nel 2014, prima chiamata BITMONERO, successivamente modificata nell'attuale nome, presenta caratteristiche di alta privacy, decentralizzazione, fungibilità e scalabilità. Il protocollo di base è CryptoNight, derivato di CryptoNote e per via della sua fungibilità un'unità di Monero su CryptoNote è uguale ad un Monero nella blockchain.

Il progetto CryptoNote pone le sue basi nella decentralizzazione dei miners, evitando quindi il possesso del mercato in mano a poche persone(oligopolio).



## 1.6 Criptovalute



Il vocabolo criptovaluta o criptomoneta [è l'italianizzazione del termine inglese cryptocurrency e si riferisce ad una rappresentazione digitale di valore basata sulla crittografia. L'etimologia del vocabolo deriva dalla fusione di "cryptography" (crittografia) e "currency" (valuta): si tratta di una risorsa digitale paritaria e decentralizzata. (Treccani)

Le criptovalute (o criptomonete) utilizzano tecnologie di tipo peer-to-peer (p2p) su reti i cui nodi risultano costituiti da computer di utenti, situati potenzialmente in tutto il globo. Su questi computer vengono eseguiti appositi programmi che svolgono funzioni di portamonete. Non c'è attualmente alcuna autorità centrale che le controlla. Le transazioni ed il rilascio avvengono collettivamente in rete, pertanto non c'è una gestione di tipo "centralizzato". Queste proprietà, uniche nel loro genere, non possono essere esplicate dai sistemi di pagamento tradizionale. (Wikipedia)

Le criptovalute o valute virtuali, presentano varie caratteristiche che comportano la formazione di 3 principali sottocategorie:

-1 **Criptovalute Tradizionali:** il valore di tali criptovalute è determinato dall'incontro tra domanda e offerta nei propri mercati, esempi di cripto tradizionali sono: Bitcoin, Ethereum, ecc.

-2 **Stablecoin:** criptovalute progettate per avere una valorizzazione legata ad un asset o a un paniere di assets, questa tipologia di cripto presentano a loro volta un'ulteriore suddivisione di categoria.

i) *asset-backed stablecoin:* criptovalute legate da una garanzia di un asset o di un paniere di assets, i quali possono essere convenzionali (assets

finanziari e non) o criptovalute stesse, tenuti in custodia dall'emittente della stablecoin.

ii) *algorithmic smart contract*: programmati per regolarizzare l'emissione e il riscatto tra domanda e offerta, riducendo la volatilità del mercato.

**-3 Central Bank Digital Currencies:** valute digitali, ovvero dematerializzate, emesse dalle banche centrali, le quali acquistate accendono un debito diretto della banca emittente nei confronti di chi le possiede. Su tali valute digitali le discussioni sono molto accentuate, rilevante è "L'overview" di Pwc la quale asserisce che "*L'impatto che le CBDC potrebbero avere sul sistema economico e finanziario è uno dei temi più rilevanti [...] esse potrebbero costituire un game-changer, con la potenzialità di mutare le radici del sistema bancario tradizionale.*"

### *1 BITCOIN*

La cripto più famosa, nata nel 2009 dallo anonimo informatico, con pseudonimo: Satoshi Nakamoto.

Moneta non controllata da alcun organo, e quindi, non regolamentata nel mercato. Caratteristica peculiare di tale criptovaluta è la capacità di poter effettuare pagamenti elettronici a livello mondiale, istantaneamente senza alcun controllo. Motivo per cui paesi come Giappone e Cina cercano di ostacolare la diffusione del bitcoin, temendo le conseguenze del metodo pagamento, prima descritto.

Per il Bitcoin il metodo di produzione è il già citato *mininig*, accessibile inizialmente a chiunque, successivamente per via delle difficoltà di calcolo, degli elevati costi che richiede l'estrazione, il mining è concesso solo a chi possiede hardware e tecnologie altamente specializzate.

Il Bitcoin ritrova la ragione della sua enorme diffusione anche per via del senso di sfiducia nei confronti delle istituzioni finanziarie a causa della crisi del 2008, la criptovaluta presentava un *do ut des* di garanzie nelle transazioni ineguagliabili.

## *BITCOIN CASH*

Il Bitcoin Cash è l'*Hard Fork* di Bitcoin, quindi può essere reputato come lo "scisma" della famosa criptovaluta, presentando caratteristiche del progetto differenti dal suo protocollo di origine.

Nato nel 2017 da un team di sviluppatori, presenta quindi una storia molto breve ma contemporaneamente molto fiduciose sono le prospettive future legato ad esso.

L'hard fork si è verificato a causa di un disaccordo sull'aumentare o no il limite di dimensioni del singolo blocco. Coloro che erano d'accordo con l'aumento del limite si impegnarono nella creazione del **bitcoin cash**. I sostenitori del bitcoin cash credevano che esso assomigliasse di più alla visione originale di Satoshi Nakamoto, lo pseudonimo della persona sconosciuta (o il gruppo di persone) che ha creato il bitcoin, e che aveva progettato e implementato un limite di 1 MB, Nakamoto però asserì che eventualmente "migliorie" sarebbero state apportate alla criptovaluta in caso di necessità, questo rafforzò la teoria degli "scissionisti".

Queste dimensioni aumentate (che raggiungono gli 8MB contro il solo 1MB di Bitcoin) rendono Bitcoin Cash incompatibile con la blockchain di Bitcoin.

## *RIPPLE*

Si basa su un protocollo Internet open source<sup>8</sup>, sono monete digitali, Xrp è il simbolo, protette da misure di sicurezza che bloccano l'eventuale violazione (comportando eventuali duplicazioni o falsificazioni), presentano un sistema di hash crittografico e convalida per impedire le possibili frodi.

Caratteristica di Ripple è lo scambio di euro, yen e dollari, oltre alle criptovalute come bitcoin, nel suo sistema.

La Banca Santander ha annunciato di utilizzare Ripple per le transazioni internazionali.

## *ETHEREUM*

Ethereum nasce come piattaforma decentralizzata nel 2015, ma già menzionata nel 2013 da Vitalik Buterin nel Bitcoin Magazine, appartiene alla famiglia delle piattaforme 3.0 dette di "nuova generazione". Utilizzata per la creazione e pubblicazione peer to peer di smart contracts<sup>9</sup>, caratterizzati da un determinato linguaggio di programmazione.

---

<sup>8</sup> Con open source (in italiano sorgente aperto), in informatica, si indica un tipo di software o il suo modello di sviluppo o distribuzione.

Un software open source è reso tale per mezzo di una licenza attraverso cui i detentori dei diritti favoriscono la modifica, lo studio, l'utilizzo e la redistribuzione del codice sorgente. Caratteristica principale dunque delle licenze open source è la pubblicazione del codice sorgente (da cui il nome). Il fenomeno ha tratto grande beneficio da Internet, perché esso permette a programmatori distanti di coordinarsi e lavorare allo stesso progetto.

Alla filosofia del movimento open source si ispira il movimento di contenuto aperto: in questo caso, ad essere liberamente disponibile non è il codice sorgente di un software, ma contenuti editoriali quali testi, immagini, video e musica. Wikipedia è un chiaro esempio dei frutti di questo movimento. Attualmente, l'open source tende ad assumere rilievo filosofico, consistendo in una nuova concezione della vita, aperta ed ostile a qualsiasi appannaggio esclusivo, che l'open source si propone di superare mediante la condivisione della conoscenza.

Open source e software libero, seppure siano sovente utilizzati come sinonimi, hanno definizioni differenti: l'Open Source Initiative ha definito il termine "open source" per descrivere soprattutto libertà sul codice sorgente di un'opera. Il concetto di software libero descrive più generalmente le libertà applicate ad un'opera ed è prerequisito che il suo codice sia consultabile e modificabile, rientrando generalmente nella definizione di open source. Fonte Wikipedia

Per svolgere la sua funzione peer to peer, Ethereum nei suoi smart contracts “paga” l'utilizzo della sua potenza computazionale, la cui unità di misura è ETHER, avendo la duplice funzionalità quindi di criptovaluta e motore di azioni.

La caratteristica di ethereum è quindi non solo essere un network per lo scambio di valore monetario ma un network per far girare i contratti basati su di esso.

Particolare storico di Ethereum è il suo lancio di offerta pubblica per ottenere finanziamenti per il suo sviluppo, l'offerta pubblica ebbe una durata di 42 giorni, con risultato finale di 31.591 bitcoin raccolti, presentando un controvalore in dollari di circa 18,4 milioni.

Ethereum necessita, come di protocollo per le altre criptovalute, di un wallet (che si differenziano tra loro) ovvero un software che genera i codici per svolgere le transazioni.

Il wallet tramite il riconoscimento della chiave privata rende il sistema estremamente sicuro, ovviamente la perdita di una chiave privata comprometterà la possibilità di poter accedere al portafoglio e quindi l'impossibilità a ritirare o trasferire il proprio conto crypto. Fondamentale è la conservazione delle chiavi.

## 1.7 IL FENOMENO DEGLI NFT

NFT è l'acronimo di Non Fungible Token – token non fungibile – un tipo di token crittografico che rappresenta l'atto di proprietà e il certificato di autenticità di un bene unico, sia digitale che fisico, che non può essere sostituito con qualcos'altro. (<https://laboratorioapertoravenna.it/cosa-sono-gli-nft-i-token-non-fungibili-star-del-metaverso-e-non-solo/>).

---

<sup>9</sup> Gli smart contract (in italiano: contratto intelligente) sono protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale. Gli smart contract, di solito, hanno anche un'interfaccia utente e spesso simulano la logica delle clausole contrattuali.

Fonte Wikipedia

I beni soggetti agli NFT sono tutti beni digitali, caratterizzati da non fungibilità, o meglio, unici e non sostituibili. Gli NFT essendo digitali, sono tutti quei beni caratterizzanti l'era dell'informazione e quindi: Immagini, Video, disegni, GIF ( acronimo di Graphics Interchange Format)<sup>10</sup>... ecc.

Per via della sua non fungibilità e quindi incapacità ad essere scambiato, un NFT presenta un valore estremamente elevato, vari acquisti avvenuti a partire dal momento del loro lancio (come l'immagine di LeBron James, qui sotto) hanno superato il centinaio di migliaia di euro.



La clip di LeBron James dal valore di 100.000\$

*(Segue) Gli inizi degli NFT*

Gli NFT furono menzionati per la prima volta nel 2014 a New York, durante una conferenza al New Museum per la quinta edizione del “Seven o Seven”, tra gli speakers di tale conferenza figurano **Anil Dash e Kevin McCoy**.

Il primo è un imprenditore che si affacciato in quel periodo al mondo dei social media, il secondo, invece, è un artista affermato.

I due sono caratterizzati da una forte *sinergia* (ed effettivamente è il termine che descrive gli NFT), la loro presentazione preme sul concetto di collaborazione tra un artista digitale ed un programmatore di criptovalute, espandere quindi i confini del mondo crypto.

---

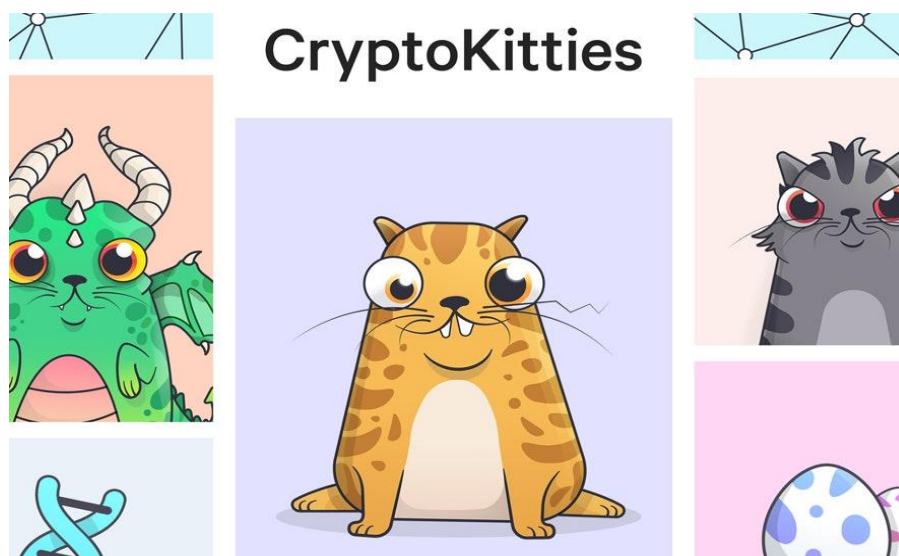
<sup>10</sup> Graphics Interchange Format è un formato di file per immagini digitali di tipo bitmap utilizzato nella grafica digitale, inventato il 15 giugno 1987 da una squadra guidata da Steve Wilhite. L'estensione **.gif** viene usata per i file di grafica memorizzati secondo uno standard definito da CompuServe e divenuto molto diffuso grazie a Internet.

Bitmap: tecnica usata per descrivere un'immagine in formato digitale

Motivo di questa collaborazione è che nel campo dell'arte digitale la maggior parte delle opere è trattata come fosse senza valore causa la sua non fisicità. Con lo scopo di aumentare la visibilità e, a maggior ragione, la circolazione della propria arte un artista è spesso portato a regalare una delle sue creazioni, creando così una tensione tra la promozione e la costruzione di un mercato (Artribune 2021). Il potenziale della blockchain (asserirono) che non andava semplicemente alle criptovalute ma doveva essere espanso i nuovi ed inesplorati campi. I campi che potevano e dovevano essere interessati dalla Blockchain erano campi che ricoprivano il tessuto culturale e sociale. Sfruttando le forti caratteristiche della Blockchain di unicità e di una provenienza associata a una catena di proprietà, gli artisti avrebbero incrementato il valore delle loro opere, dando alla tecnologia Bitcoin una funzione sociale e culturale estremamente interessante. Grazie alla fusione delle due problematiche iniziali, un soggetto avrebbe potuto verificare la proprietà di un'immagine tramite hash depositato su blockchain e un'immagine avrebbe ottenuto, così, l'autentica creazione di un artista.

Con questo nuovo modo di intendere l'arte e la tecnologia Blockchain, si è aperto il confine per una nuova tipologia di mercato, basato non più sul prodotto (a prescindere dalla bellezza estetica o culturale) ma dalla proprietà dello stesso.

I primi NFT furono venduti nel 2017 trattavano il gioco denominato CRYPTOKITTIES (sotto l'immagine rappresentante tali NFT).



*I CryptoKitties, fonte Wired Italia*

CryptoKitties è un blockchain gioco su Ethereum sviluppato nello studio Dapper Labs che permette ai giocatori di acquistare, raccogliere, allevare e vendere i gatti virtuali. Fu uno dei primi tentativi di implementare la tecnologia blockchain per il tempo libero. Il gioco nel dicembre 2017 raggiunse una tale popolarità che congestionò la rete di Ethereum, facendola raggiungere il massimo storico nel numero di transazioni e rallentandolo in modo significativo.

Il boom di CryptoKitties, risiede proprio nell'unicità di questi avatar<sup>11</sup> felini, in quanto neanche i programmatori del gioco stesso possono sostituirsi o privare gli utenti della gestione dei loro cryptokitties.

### *(Segue) I Bored Ape*

L'esclusività degli Avatar ha permesso il nascere di un movimento di collezionisti di determinati avatar, I Bored Ape.

Di questi avatar ne esistono al mondo **diecimila** esemplari, è nel numero così esiguo che si è avviata una moda tra i grandi investitori digitali e i ricchi della società. Il possesso di un bored ape concede al detentore della proprietà uno status elevato.

Tra i personaggi più famosi detentori degli avatar vi sono: Snoop Dogg, Jimmy Fallon, Eminem, Paris Hilton e tanti altri.

Il prezzo di un Bored Ape può raggiungere le centinaia di migliaia di euro.

---

<sup>11</sup> INFORM In Internet, l'immagine o la rappresentazione grafica scelta da un utente per rappresentare se stesso all'interno di una comunità virtuale. Hoepli 2018





*I Bored Ape, fonte news.artnet.com*

### *(Segue) I limiti degli NFT*

Andando ad esaminare nel dettaglio che cosa è un NFT e cosa viene effettivamente registrato su blockchain ci rendiamo conto che ben poco del “contratto” di acquisto è contenuto su questo registro distribuito e che tutti gli altri dati (l’opera stessa, le condizioni del suo acquisto e i diritti del “proprietario”) sono in realtà al di fuori del registro, con severi problemi di conservazione e di accessibilità nel tempo del dato.

Da sottolineare che questi NFT non dipendono solo dalla tecnologia blockchain, ma anche da altre soluzioni (come il processo di hashing) che potrebbero essere superate nel tempo (il continuo aumento della potenza di calcolo potrebbe infatti permettere di “rompere” alcuni di questi algoritmi, rendendo così ben poco affidabile il riferimento univoco all’NFT).

Dal punto di vista giuridico ci accorgiamo che il valore (l'unicità) dell'NFT non poggia davvero sulla tecnologia blockchain, ma sulla fiducia intercorrente fra il venditore e l'acquirente, con il primo che confida sul fatto che il secondo non venderà o non abbia già venduto la stessa identica opera più e più volte, riducendo quell'NFT (pagato magari milioni di dollari) a un valore irrisorio (perché se non può esistere un NFT uguale all'altro, ne possono esistere un'infinità di estremamente simili e tutti rivolti a trasferimenti della medesima opera.

(<https://www.agendadigitale.eu/documenti/nft-che-cosa-sono-come-funzionano-come-investire-sui-non-fungible-token/>)

## 1.8 I WALLET

I wallet<sup>12</sup> sono applicazioni utilizzate per generare, gestire ed archiviare le chiavi pubbliche e private delle crypto-transazioni. I wallet non sono tutti uguali, esistono quattro macrocategorie di essi, distinguibili se presentano o no un formato software o hardware, totale o parziale e se sono gestiti da terzi oppure no:

1. **Hot custodial wallet** : Sono wallet custoditi da terzi, non presentano una componente fisica, sono online e l'utente (proprietario) del wallet per accedere utilizzerà una forma crittografica.

2. **Hot non custodial wallet**: Si differenzia dalla prima categoria per via dell'assenza di un terzo, gestore del portafoglio, l'utente scaricherà un software sul proprio device per accedere al proprio wallet e le chiavi che contiene.

3. **Cold Hardware wallet**: è un dispositivo fisico come chiavette USB, collegabile con qualsiasi device in caso di necessità.

---

<sup>12</sup> La traduzione italiana del termine "wallet" è precisamente *portafoglio*, fondamentale per l'utilizzo delle criptovalute.

4. **Cold paper wallet:** La traduzione del nome rende l'idea, sono fogli di carta che presentano indirizzo e chiavi del proprio portafoglio, generabili tramite software, ma il procedimento di generazione e stampa richiederà ovviamente un device offline.

I wallet presentano una crittografia asimmetrica, ovvero, la loro lettura e funzione sono dovute ad una coppia di chiavi, una pubblica ed una privata. La chiave privata rimane in possesso dell'utente, che verrà utilizzata nel momento della transazione per "firmarla", post firma la controparte potrà validare la transazione e la sua sotto scrittura grazie alla chiave pubblica. Approvata la transazione, esse vengono compilate in un blocco in ordine cronologico, i blocchi andranno a formare perciò la *blockchain*.

## 1.9 La Creazione di valore delle criptovalute

Una criptovaluta presenta procedimenti di creazione di valore complessi e in continua evoluzione. Tale creazione però, se in possesso di capacità o risorse, è un procedimento accessibile a chiunque; quindi, in qualsiasi momento ci possono essere centinaia o persino migliaia di criptovalute in circolazione. Le modalità per la creazione di criptovalute sono varie, ma quelle di più comune utilizzo sono le seguenti:

*i) Initial Coin Offering*

*ii) Hard Fork*

*iii) Yeld Farming*

*iv) AirDrop*

*v) Mining*

Le quali saranno descritte nei paragrafi successivi.

## 1.9.1 Initial Coin Offering

Una Initial Coin Offerings, o ICO, è il termine con cui si identifica un meccanismo finalizzato alla raccolta di fondi necessari a finanziare un progetto imprenditoriale, in maniera simile alle "Initial Public Offering"<sup>13</sup> (IPO) e all'equity crowdfunding. A differenza di questi ultimi, l'ICO implica l'emissione di c.d. coin o token digitali in luogo di strumenti finanziari tradizionali (es. azioni). I token vengono offerti agli investitori che li acquistano contro cash (USD, EUR...) oppure, più spesso, criptovalute. Il possesso dei tokens, però, non è regolamentato e potrebbe non garantire alcun diritto agli investitori (ulteriore differenza sostanziale tra ICO e IPO dove quest'ultima ha come garante per i nuovi shareholders la CONSOB). La nascita delle ICO si deve per le caratteristiche e novità di Ethereum e in particolare al suo sistema blockchain. Ethereum, come è risaputo, sfrutta la tecnologia Blockchain per la trasmissione di denaro virtuale e, non solo, introduce la possibilità di creare smart contracts (contratti intelligenti), ovvero sia protocolli informatici che automatizzano e verificano la negoziazione o l'esecuzione di un contratto senza l'intromissione di terze parti. L'introduzione di questi contratti digitali permette di garantire una sicurezza superiore rispetto ai normali accordi di natura patrimoniale, riducendo i costi di transazione associati alla contrattazione.

L'implicazione principale di questi smart contracts trova la massima utilità nelle Initial Coin Offerings.

I tokens sono, quindi, prima di tutto, degli smart contracts che il possessore -nel nostro caso l'azienda che vuole lanciare l'ICO distribuisce ad altri indirizzi annotando i saldi di ogni investitore.

---

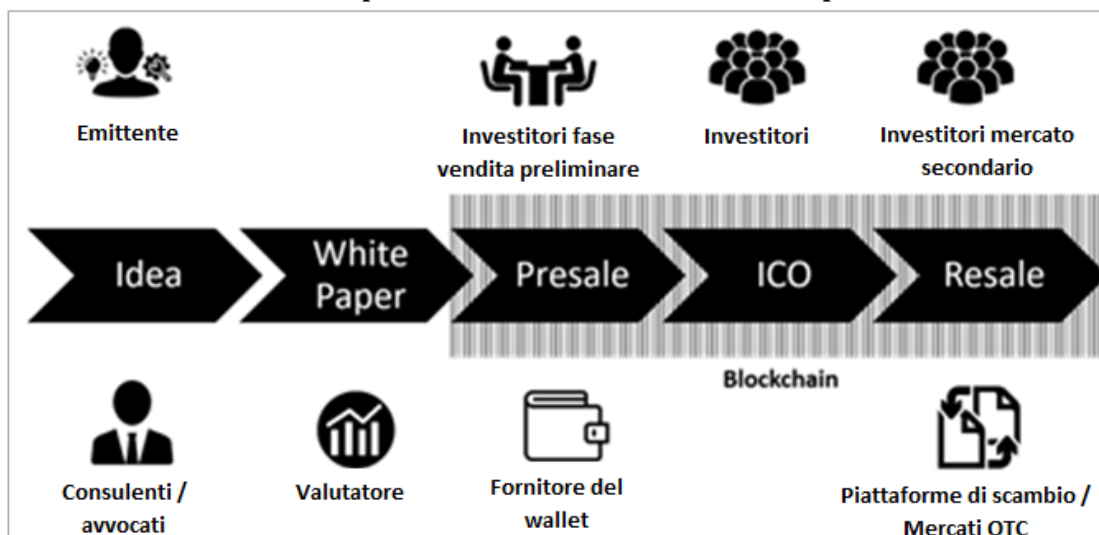
<sup>13</sup> L'offerta pubblica iniziale (o IPO) costituisce lo strumento attraverso il quale una società ottiene la diffusione dei titoli tra il pubblico (la c.d. creazione del flottante), che è requisito necessario per ottenere la quotazione dei propri titoli su un mercato regolamentato.

L'IPO, essendo rivolta al pubblico indistinto degli investitori, costituisce una fattispecie di sollecitazione all'investimento, pertanto la società emittente dovrà organizzare l'operazione avendo cura di osservare la disciplina del Testo Unico della Finanza (D.Lgs. 58/1998) finalizzata a garantire un'informazione trasparente ai destinatari dell'offerta.

<https://www.borsaitaliana.it/borsa/glossario/ipo-offerta-pubblica-iniziale.html>

Tuttavia, poiché questi contratti vengono scritti al computer attraverso specifici linguaggi di programmazione, e poiché è molto facile scrivere un codice non sicuro, sono stati proposti degli standard di sicurezza per realizzare un token che fosse il meno vulnerabile possibile.

L'interfaccia ERC20<sup>14</sup> (Ethereum Request for Comment 20) fornisce un elenco di regole che un token costruito sulla Blockchain di Ethereum deve possedere. A partire da gennaio 2018, sono stati creati oltre 21.000 tokens basati su ERC20, corrispondenti a oltre l'80% della quota di mercato<sup>7</sup>.



Rappresentazione grafica delle fasi dell'ICO. Fonte CONSOB.IT

Il ciclo di vita di una initial coin offerings, si articola principalmente in quattro fasi (Momtaz, 2018): innanzitutto il progetto viene sviluppato (e successivamente diffuso tra gli investitori), in seguito si passa alla fase di prevendita e vendita dei token e, infine, il token viene quotato sul mercato. Uno dei momenti fondamentali delle Initial Public Offerings riguarda l'evento Roadshow (Ritter & Welch, 2002), la strategia di marketing mediante cui un'azienda che intende quotarsi sui mercati, diffonde la propria vision attraverso convegni e manifestazioni.

Nelle Initial Coin Offerings il concetto di Roadshow subisce notevoli cambiamenti in quanto l'interazione faccia a faccia con i potenziali clienti viene meno per lasciare spazio a forme di comunicazione più moderne, tra cui il ricorso a siti web dinamici, un intenso utilizzo dei social media e dirette video sui principali social network con lo scopo di aumentare l'interesse degli investitori. Si ricorda che il valore di una nuova criptomoneta è strettamente legato alla grandezza del network. In accordo con quanto sostenuto da Momtaz (2018), dopo che è stata definita la

<sup>14</sup> ERC20 è lo standard tecnico dietro i contratti intelligenti che servono per l'implementazione dei token sulla blockchain di Ethereum ([www.bitpanda.com](http://www.bitpanda.com))

strategia aziendale, questa viene trasmessa agli investitori attraverso un documento, chiamato whitepaper, che viene pubblicato sul sito internet dell'azienda, contenente informazioni dettagliate sul progetto e sulla modalità mediante cui verranno emessi i tokens.

Viene anche presentata una linea temporale, roadmap, che riporta le date entro cui verranno raggiunti gli obiettivi prefissati. Dopo che sono state definite le condizioni di vendita dei tokens, si procede alla fase di emissione. La maggior parte delle imprese decide di condurre una pre-ICO, ossia una prevendita in cui i tokens vengono venduti ad un prezzo più vantaggioso per incentivare i possibili investitori. I motivi che inducono un'azienda a compiere una pre-ICO si ritrovano nel beneficio di poter coprire i costi di pubblicità per la successiva ICO e di ridurre il fenomeno dell'underpricing, potendo prevedere in maniera più precisa la domanda di tokens durante la fase di vendita (Benedetti & Kostovetsky, 2018). Una caratteristica interessante di questa prevendita è che essa può essere vista come un metodo per ottenere informazioni dai potenziali investitori sul prezzo equo del token e sull'ammontare totale del finanziamento che è possibile richiedere.

Dopo la prevendita si passa alla vera e propria Initial Coin Offerings. Non esistono regole generali sulle modalità attraverso cui una ICO deve avvenire, alcune si concludono entro le 24 ore, altre durano anche per un anno.

Il funzionamento delle attuali ICO non è complesso: l'impresa emittente crea un indirizzo digitale, paragonabile a un conto corrente, contenente il totale dei tokens, che verrà poi distribuito tra gli investitori.

Successivamente gli investitori verseranno i fondi in moneta fiat all'indirizzo dell'azienda e infine riceveranno un ammontare di tokens equivalente alla somma precedentemente versata. Una volta che i nuovi token sono stati emessi, l'ICO si conclude con la fase della quotazione.

La quotazione garantisce la possibilità che i token possano essere scambiati nei mercati secondari, fornendo così una fonte di liquidità per gli investitori.

Binance<sup>15</sup>, il più grande exchange esistente al mondo, consente agli utenti di comprare e vendere circa 400 criptomonete con un volume di scambi mensile che sfiora i 30 miliardi di dollari. Al secondo posto si trova OKEX<sup>16</sup>, con un volume di scambi di 27 milioni di dollari e un mercato di 522 criptomonete

Gli exchange, per la quotazione della moneta, richiedono il nome del token, la descrizione del progetto, la data di lancio dell'ICO, il link contenente il codice sorgente della moneta e una serie di informazioni innocue, come la quantità di denaro raccolto, la lista degli altri exchange su cui verrà quotato il token e com'è stato raccolto il denaro.

## 1.9.2 Hard Fork

Un hard fork (o hardfork), in relazione alla tecnologia blockchain, è un cambiamento radicale del protocollo di una rete che rende validi i blocchi e le transazioni precedentemente non validi, o viceversa. Un hard fork richiede che tutti i nodi o gli utenti si aggiornino all'ultima versione del software del protocollo.

I fork possono essere avviati da sviluppatori o membri di una comunità crittografica che non sono soddisfatti delle funzionalità offerte dalle implementazioni blockchain esistenti. Possono anche emergere come un modo per raccogliere fondi per nuovi progetti tecnologici o offerte di criptovalute.

---

<sup>15</sup> Binance è una piattaforma di scambio di criptovalute fondata nel 2017. A maggio 2021, Binance è l'exchange di assets digitali più grande del mondo in termini di volume di scambi.

Il fondatore della compagnia è Changpeng Zhao, comunemente noto come "CZ", uno sviluppatore cinese che precedentemente sviluppò un software di high-frequency trading. Inizialmente, la sede di Binance si trovava in Cina: in seguito venne spostata dal Paese a causa dell'incremento delle restrizioni sulle criptovalute.

Nel luglio 2021, in un provvedimento inerente alle sezioni denominate "derivatives" e "stock token", la Consob ha diramato una nota in cui spiega che le società del «Gruppo Binance» non sono autorizzate a prestare servizi e attività di investimento in Italia.

<sup>16</sup> Piattaforma per la negoziazione di diverse cryptocurrencies. Alcune delle caratteristiche principali dello scambio includono il trading spot e derivati.

Un hard fork si ha quando i nodi della versione più recente di una blockchain non accettano più le regole precedentemente emanate. Per avviare un Hard Fork però tutti i minatori devono essere d'accordo sulle nuove regole e su cosa comprende un blocco valido nella catena. La modifica delle regole della blockchain richiede quindi, una "diramazione" come un bivio in una strada - per indicare che c'è stato un cambiamento o una deviazione al protocollo. Gli sviluppatori possono quindi aggiornare tutto il software per riflettere le nuove regole.

È grazie a questo processo di diramazione che sono nate varie valute digitali con nomi simili a bitcoin: bitcoin cash, bitcoin gold e altri.

Ci sono una serie di ragioni per cui gli sviluppatori possono implementare un hard fork, come correggere importanti rischi per la sicurezza presenti nelle versioni precedenti del software, aggiungere nuove funzionalità o invertire le transazioni, come quando la blockchain di Ethereum ha creato un hard fork per invertire l'hacking dell'Organizzazione Autonoma Decentralizzata (DAO).

*(Segue) Ethereum e il suo Hard fork per il risarcimento*

Dopo l'hack<sup>17</sup>, la comunità di Ethereum ha votato quasi all'unanimità a favore di un hard fork per ripristinare le transazioni che hanno sottratto decine di milioni di dollari di valuta digitale da un hacker anonimo. L'hard fork ha anche aiutato i possessori di token DAO a ottenere la restituzione dei loro fondi ether (ETH).

La proposta di un hard fork non ha esattamente mutato la cronologia delle transazioni della rete, piuttosto, ha trasferito i fondi legati alla DAO in uno smart contract di nuova creazione con l'unico scopo di consentire ai proprietari originali di ritirare i propri fondi.

*(Segue) Hard Fork e Soft Fork*

Hard fork e soft fork sono essenzialmente la stessa cosa, nel senso che entrambi consistono in una modifica del codice esistente di una piattaforma di criptovaluta, una vecchia versione rimane sulla rete mentre viene creata la nuova versione, coesistendo.

---

<sup>17</sup> Un hack è un codice sorgente scritto con particolare ingegno e originalità che modifica il funzionamento di un software già esistente. ([www.andreaminini.com](http://www.andreaminini.com))



Questo è il caso dell'hard fork. Con un soft fork, invece, solo una blockchain rimarrà valida, e man mano che gli utenti adotteranno l'aggiornamento, la versione precedente verrà totalmente sostituita.

Vi sono notevoli differenze a livelli di sicurezza tra hard fork e soft fork, tendenzialmente quasi tutti gli utenti e gli sviluppatori richiedono un hard fork, nonostante l'efficienza del lavoro computazionale del soft fork. Questa richiesta risiede nel fatto che la revisione dei blocchi in una blockchain richiede un'enorme quantità di potenza di calcolo, una potenza di calcolo però inferiore nel caso dell'hard fork, per via della "semplice" deviazione strutturale della blockchain rispetto ad una totale ristrutturazione della stessa, tipica dei soft fork.

### 1.9.3 YELD FARMING

Lo yield farming, conosciuto anche come liquidity mining, è un modo per guadagnare utilizzando fondi in criptovalute, ovvero, significa bloccare criptovalute per ricevere ricompense.

Da un certo punto di vista, lo yield farming può essere paragonato allo staking<sup>18</sup>. Tuttavia, sullo sfondo c'è molta più complessità. In molti casi, coinvolge utenti chiamati liquidity provider (LP), o fornitori di liquidità, che aggiungono fondi a pool di liquidità.

Un pool di liquidità, sostanzialmente, è uno smart contract che contiene fondi. In cambio della liquidità fornita alla pool, i LP ricevono una ricompensa, che può essere composta da commissioni generate dalla piattaforma DeFi<sup>19</sup> sottostante o proveniente da altre fonti.

---

<sup>18</sup> Lo staking è l'alternativa al mining che richiede l'impiego di meno risorse. Si tratta di tenere fondi in uno wallet di criptovalute per sostenere la sicurezza e le operazioni di un network blockchain. In poche parole, lo staking è l'atto di bloccare criptovalute per ricevere ricompense. <https://academy.binance.com/it/articles/what-is-staking>

<sup>19</sup> Acronimo per Finanza Decentralizzata, ecosistema emergente di applicazioni e protocolli finanziari costruiti mediante l'organizzazione di servizi, simili a quelli bancari, basati su infrastrutture che presuppongono l'assenza di gerarchie, come la blockchain, o comunque meno centralizzati rispetto al sistema bancario. Una delle caratteristiche rilevanti di questo tipo di progetto è rappresentato dagli automatismi che permettono di eseguire le transazioni senza interventi esterni, spesso basandosi

Alcune pool di liquidità distribuiscono le ricompense in diversi token, che possono essere depositati in altre liquidity pool per guadagnare anche da lì, e così via. Sostanzialmente un liquidity provider deposita fondi in una pool di liquidità, in attesa questi fruttino, una sorta di investimento a “lungo” termine.

Lo yield farming avviene solitamente su Ethereum con token ERC-20, e anche le ricompense sono in genere un tipo di token ERC-20. Tuttavia, questo potrebbe cambiare in futuro. Perché? Al momento, gran parte delle attività di questo tipo si trova nell'ecosistema di Ethereum. Tuttavia, in futuro i ponti cross-chain e altri progressi simili potrebbero consentire alle applicazioni DeFi di diventare indipendenti da una particolare blockchain. Questo significa che potrebbero essere eseguite su altre blockchain che supportano funzionalità di smart contract.

Di solito, gli yield farmer spostano spesso i propri fondi da un protocollo all'altro in cerca di alti rendimenti. Di conseguenza, le piattaforme DeFi potrebbero fornire anche altri incentivi economici per attirare più capitale. Come per gli exchange centralizzati, la liquidità tende ad attirare più liquidità.

Le ragioni per cui lo Yield Farming ha riscontrato molto interesse da parte degli investitori è il lancio di **COMP**, il token di governance dell'ecosistema Compound Finance. I token di questo genere generano diritti di governance ai possessori. La distribuzione dei token avviene tramite algoritmi, sfruttando degli incentivi alla liquidità, un incentivo al provider a “farmare” il token per attribuire liquidità al protocollo stesso.

## **Gli indici della DeFi**

La Finanza decentralizzata è un settore in continua evoluzione e con un bacino di investitori in continuo aumento, saper valutare il suo stato di salute e la sua capacità di produrre profitti è fondamentale. La valutazione della DeFi è affidata agli indicatori che, in maniera efficiente, sono utili ad attribuire dati provenienti dalle misurazioni e confronti dei vari protocolli.

*Valore totale bloccato (TVL)* il valore totale bloccato è l'importo aggregato di fondi bloccati in un protocollo DeFi. Si può considerare il TVL come tutta la liquidità nelle pool di un certo mercato monetario. Attribuisce un'informazione utile sull'interesse complessivo nella DeFi. Confronta la "quota di mercato" di protocolli DeFi differenti. Questo può essere particolarmente utile per gli investitori alla ricerca di progetti DeFi sottovalutati.

*Price-to-sales ratio (rapporto P/S)* Rapporto utilizzato per la valutazione di aziende "tradizionali", mette a confronto il prezzo dell'azione e il fatturato dell'azienda stessa. Per la DeFi, invece, per applicare tale ratio si utilizzano altri parametri, cioè dividendo la capitalizzazione di mercato del protocollo per i suoi ricavi. L'idea di base è che più basso il rapporto risultante, più il protocollo è sottovalutato.

Vi sono inoltre, una categoria di indicatori basati su modelli empirici, ovvero ricerche che basano le conclusioni sull'osservazione diretta o indiretta dei fatti. Tra questi:

*i) Offerta di token su exchange:*

Implica il monitoraggio dell'offerta di token sugli exchange di criptovalute. Quando i venditori vogliono vendere token, solitamente lo fanno su exchange centralizzati (CEX), nonostante ciò, ci sono sempre più opzioni disponibili agli utenti su exchange decentralizzati (DEX) che non richiedono fiducia in un intermediario. Tuttavia, le piattaforme centralizzate tendono a offrire una liquidità molto più elevata. Per questo è importante prestare attenzione all'offerta di token sui CEX.

*ii) Cambiamenti del saldo di token su exchange:*

Lo studio dei saldi dei token è un fattore fondamentale per calcolare la **volatilità** dei token, l'incertezza quindi, circa i futuri movimenti del prezzo di un bene o di una attività finanziaria. Al crescere della volatilità cresce la probabilità che la performance risulti molto elevata oppure molto contenuta, ossia cresce la probabilità che i movimenti di prezzo siano molto ampi, sia in aumento che in diminuzione.

### iii) Numero di indirizzi unici:

È un parametro che presenta forte limiti. I token o monete se presentano un alto numero di indirizzi, indica che si è in presenza di un maggior utilizzo del token in questione.

Il limite è dovuto alla possibilità di ingannare l'investitore, ovvero creando più indirizzi e distribuendo i fondi, distorcendo quindi il vero valore del token. Nonostante ciò, se preso insieme ad altri fattori, si potrebbe rivelare un indice rilevante.

### iv) Utilizzo non speculativo:

Essere a conoscenza dell'utilizzo del token, è un fattore fondamentale per la scelta di un investimento nella cripto-finanza. Non è un indice semplice da acquisire, un buon inizio sarebbe analizzare i trasferimenti che non interessano exchange decentralizzati o centralizzati. L'obiettivo è verificare che gli altri investitori stiano usando il token.

Un fattore utile a comprendere se o no il trader si ritrovi nel classico Schema Ponzi<sup>20</sup>, questo perchè lo schema delle monete virtuali è facilmente descrivibile in: una struttura piramidale con il token concentrato nei portafogli dei primi entranti, un rendimento prefissato e riconosciuto a chi mette a disposizione capacità di calcolo, ed alla fine la necessità di continui nuovi entranti per sostenerne il valore.

Per concludere la forte incertezza e la volatilità sono attributi pervasivi dei mercati dei capitali, le decisioni effettuate durante il mercato sono ricche di poche conoscenze sugli ambienti, i contesti sociali e la situazione economica-finanziaria futura, sicchè il risultato di un determinato investimento presenterà sempre un determinato tasso di rischio. Ebbene nel mercato delle cripto-valute tali incertezze e poche conoscenze si accentuano, il crypto-trading è un fenomeno che ha incredibilmente

---

<sup>20</sup> Lo schema Ponzi è un modello economico di vendita basato sulla truffa ideato da Charles Ponzi (1882-1949), che promette forti guadagni ai primi investitori, a discapito di nuovi "investitori", a loro volta vittime della truffa.

Fasi dello schema Ponzi:

Fase A. Al potenziale cliente viene promesso un investimento con rendimenti superiori ai tassi di mercato, in tempi ravvicinati.

Fase B. Dopo poco tempo viene restituita parte della somma investita, facendo credere che il sistema funzioni veramente.

Fase C. Si sparge la voce dell'investimento molto redditizio; altri clienti cadono nella rete. Si continuano a pagare gli interessi con i soldi via via incassati (la finanziaria ha capitale sociale zero, ma gli investitori non lo sanno).

Fase D. Lo schema si interrompe quando le richieste di rimborso superano i nuovi versamenti.

Fonte Wikipedia

arricchito vari investitori ma anche depauperato un numero non poco rilevante di altri trader. Sicuramente svolgere una determinata e attenta ricerca sulla “giusta” cripto-valuta su cui porre la propria attenzione è utile per un investimento, soprattutto se effettuata con gli indici elencati sopra, di certo però la piena certezza in un mercato così *volatile* non si avrà mai.

#### **1.9.4 AIRDROP**

L' Airdrop è la campagna pubblicitaria che cerca di lanciare o pubblicizzare una moneta per renderla visibile all'interno delle tipologie di criptovalute da 1.500 dollari, riuscendo ad attirare l'attenzione di tutti gli analisti e gli investitori.

Tale campagna pubblicitaria avviene tramite la distribuzione di token gratuiti, questo fenomeno ha la sua utilità per aumentare la conoscenza e la consapevolezza di un nuovo progetto nascente su una determinata criptovaluta.

In questo processo, ciò che viene fatto è inviare i token o le criptovalute ai gestori, che li inoltrano a un numero specifico di utenti. Spesso gli utenti sono *influencer*, ovvero utenti capaci di attirare fortemente altri utenti, aumentando l'appetibilità del lancio di un nuovo token.

I token o le monete sono distribuiti in maniera gratuita e questo tipo di campagna ha i seguenti vantaggi:

- Attira l'attenzione dei mass media generando che i progetti di nuovi bitcoin o dei bitcoin attuali possono essere promossi aumentandone il valore nel mercato.

- Garantire la distribuzione delle criptovalute: la consegna di token e monete è resa dinamica attraverso la consegna di monete che regolano il mercato e i prezzi di mercato.

Gli airdrop si distinguono in varie categorie e sono:

- 1) **Task Airdrop**: è una tipologia di Airdrop che richiede di svolgere un qualche tipo di task specifico che solitamente è legato ai social network, al fine di ottenere token o monete gratuiti come ricompensa.

2) **Airdrop con Scambi:** è una tipologia di Airdrop realizzata dagli ideatori del progetto; che selezionano direttamente coloro che riceveranno il tipo di valuta o token.

3) **Airdrop con portamonete:** è una tipologia di Airdrop che viene consegnato a chi acquista i servizi delle borsette o portafogli; al fine di promuovere sia i servizi di moneta che di portafoglio.

4) **Airdrop per il possesso:** è un tipo di Airdrop che consegna tramite il possesso o il patrimonio di determinate valute agli utenti come ricompensa per l'utilizzo di bitcoin.

5) **Airdrop da app:** viene utilizzato da alcune pagine come premio per i nuovi utenti o per chi utilizza da tempo alcune applicazioni.

### 1.9.5 Il Mining



Miner di Bitcoin, immagine di businesspeople.it

Il termine inglese mining, proveniente dal verbo *to mine*, significa *estrazione* ed effettivamente come i minatori sfruttano le cave per estrarre metalli ed ori preziosi così un “miner” informatico sfrutta la blockchain per estrarre valute digitali da esso, ottenendo così un prezioso compenso. Strumento per l'estrazione dei miners è la potenza di elaborazione dei computer, fattore fondamentale per un buon mining; infatti, i minatori sono gli individui o le società i cui investimenti e i loro profitti derivano da tale potenza.

Questo potere computazionale è finalizzato alla risoluzione di complessi problemi informatico-matematici, veri e propri puzzle crittografici, e permette al sistema di basarsi su un consenso decentralizzato e distribuito, a differenza del consenso che si formerebbe in un sistema con la presenza di un'istituzione centralizzata garante..

La logica che sta alla base del meccanismo di consenso/approvazione deriva dalla necessità di creare ostacoli e complicazioni durante tutto il processo di validazione, con la finalità di evitare tentativi di frodi da parte dei nodi che compongono la rete P2P.

I problemi di carattere informatico-matematico sono stati ideati per porre in competizione fra loro tutti i nodi, poiché tutti, con la loro potenza di calcolo, tentano di raggiungere la risoluzione del problema.

Il nodo che, fra tutti gli altri, riuscirà per primo a risolvere il puzzle crittografico otterrà il diritto alla validazione del blocco di transazioni presentando alla rete la soluzione del puzzle. L'impegno speso nella risoluzione, e il risultato ottenuto determinano per il miner vincitore un compenso in valuta digitale, che rappresenta emissione e creazione di nuova valuta virtuale.

La ricompensa diminuisce le commissioni di transazione creando un incentivo per contribuire alla potenza di elaborazione della rete. La velocità di generazione degli hash, che convalidano qualsiasi transazione, è stata aumentata dall'uso di macchine specializzate come FPGA e ASIC che eseguono algoritmi di hashing complessi come SHA-256 e Scrypt.

(Wikipedia)

Dalla nascita di Bitcoin, è cominciata una specie di "corsa agli armamenti" per ottenere macchine meno costose ma efficienti. Per via della capacità attrattiva del mining sempre più persone si sono avventurate nel mondo delle monete virtuali, ma conseguenza di ciò ha reso la generazione di hash sempre più complessa nel corso degli anni. I minatori per sopperire a questa complessità, ovviamente, hanno avviato una campagna di investimenti di ingenti somme di denaro impiegando più macchine ad alte prestazioni. Pertanto, il valore della valuta ottenuta per trovare un hash spesso non giustifica la quantità di denaro speso per l'installazione delle macchine, le strutture di raffreddamento per superare l'enorme quantità di calore che producono e l'elettricità necessaria per gestirle.





## Capitolo 2

### 2.1 Analisi Giuridica e rappresentazione in bilancio delle Criptovalute

Funzioni, oramai ben conosciute, delle criptovalute, sono: possibilità di compiere operazioni (transazioni online), sicurezza e anonimato. La crittografia è lo strumento che permette di avere tali caratteristiche nel mondo delle criptovalute. Va ricordato che tali assets digitali:

- sono creati da un emittente privato o, in via diffusa, da utenti che utilizzano **software** altamente sofisticati;
- non sono fisicamente detenute dall'utente, e sono movimentate attraverso un **conto personalizzato** (c.d. *e-wallet*), generalmente sviluppato e fornito da appositi soggetti (c.d. *wallet providers*);
- possono essere acquistate con **moneta tradizionale** su una piattaforma di scambio. (<https://locait.net/criptovalute-e-bitcoin-trattamento-contabile-e-fiscale/>, s.d.)

Il numero di transazioni giornaliere con i soli bitcoin (le criptovalute più soggette a queste transazioni) sono cresciute in modo esponenziale. La diffusione è dovuta alle caratteristiche, tendenzialmente comuni, delle varie le cryptovalute, le quali sono:

-Decentralizzazione: esse non sono istituite né controllate da alcuna autorità centrale. Il controllo sulle transazioni è eseguito da tante entità indipendenti (rete peer-to-peer) in maniera decentralizzata e distribuita, per cui la presenza di banche e altri soggetti regolamentati non è più necessaria.

-Indipendenza da politiche monetarie: l'assenza di un'autorità centrale comporta anche l'impossibilità che un qualsiasi soggetto eserciti azioni coercitive sulla valuta, come ad esempio l'aumento o la diminuzione delle unità di valuta in circolazione.

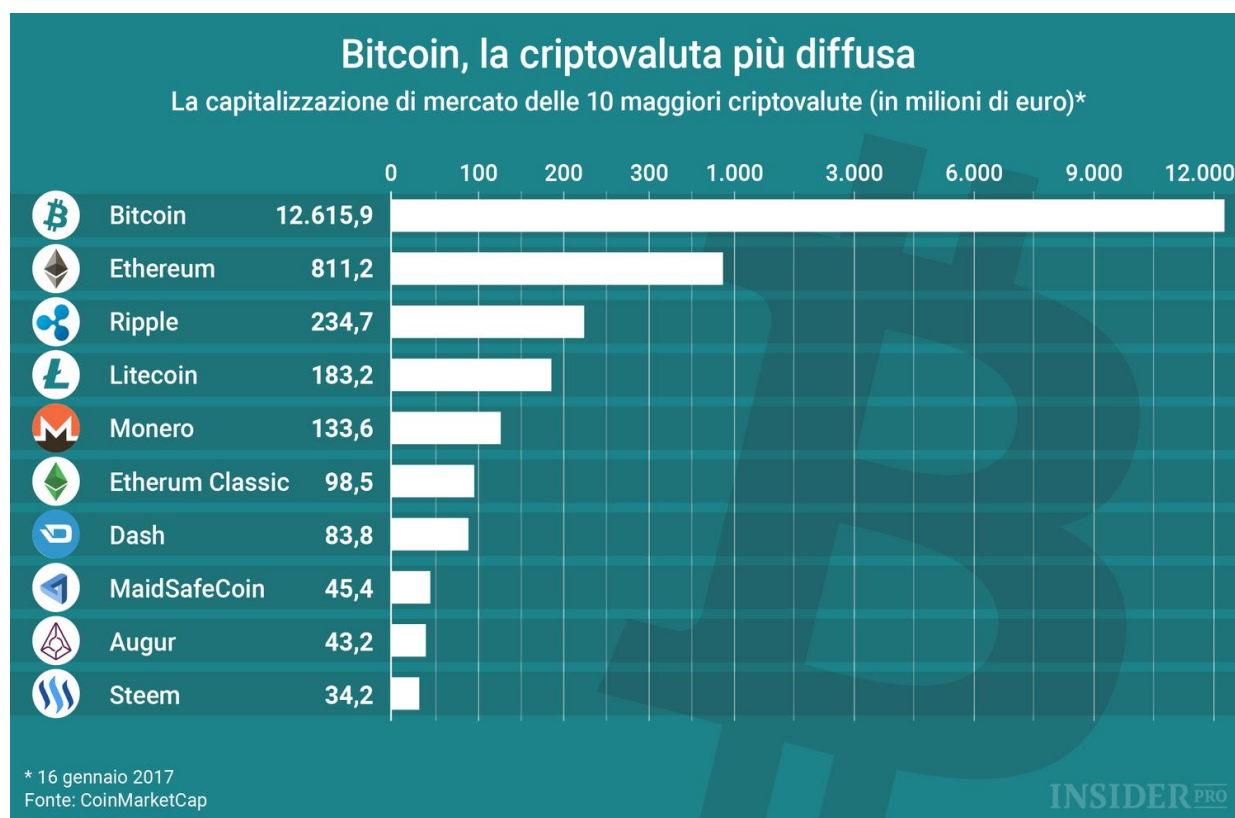
-Non hanno corso legale: esse sono accettate come mezzo di pagamento solo su base volontaria, e dunque non possono essere utilizzati per estinguere delle obbligazioni pecuniarie se il creditore si rifiuta di accettarli.

-Anonimato delle parti nelle transazioni: le transazioni avvengono tra indirizzi pubblici a partire dai quali è praticamente impossibile risalire alla reale identità della persona fisica o giuridica che processa lo scambio di bitcoin. Gli indirizzi sono punti di ricezione e invio, e si presentano sottoforma di codici alfanumerici di 33 o 34 caratteri, in modo da non contenere alcun riferimento dell'utente utilizzatore, facendo sì che sia un sistema di pagamento anonimo.

-Trasparenza: Le transazioni sono registrate nel libro contabile pubblico, la blockchain, che ognuno può visualizzare. Esplorando la blockchain è possibile sapere quante criptovalute dispone un determinato indirizzo in un preciso istante temporale, potendo inoltre risalire agli indirizzi che glieli hanno forniti.

-Bassi costi di transazione: l'assenza di soggetti che intermediano nelle transazioni ha la conseguenza di abbatterne i costi.

-Transazioni veloci e irreversibili: ogni transazione impiega mediamente 10 minuti per essere confermata. Tali transazioni sono irreversibili, ovvero non è possibile annullarle.



Ebbene il numero massivo di transazioni, l'incredibile aumento del valore delle criptovalute ha attirato l'attenzione di molti investitori e speculatori, pronti ad allocare ingenti risorse finanziarie per ottenere gli appetitosi profitti del mercato delle criptovalute.

In presenza di investimenti e profitti, quindi, è importante saper classificare contabilmente e fiscalmente tali assets digitali. Questo capitolo ed il successivo tratteranno queste tematiche, per dare delle delucidazioni a riguardo.

## 2.2 Criptovalute e qualificazione giuridica

L'impiego delle c.d. criptovalute quale mezzo di scambio e/o pagamento nell'ambito di transazioni economiche di diversa natura, ha conosciuto una considerevole diffusione che, a causa dell'assenza – tanto nell'ordinamento nazionale, quanto negli ordinamenti stranieri – di una regolamentazione sistematica, ha dato origine a dubbi ed incertezze che, ancora oggi, non paiono aver trovato soluzioni univoche. (Corasaniti)

L'assenza di una specifica disciplina di riferimento ha posto il problema per i vari organismi di contabilità se assegnare o no alle criptovalute la classificazione di *immobilizzazioni immateriali*.

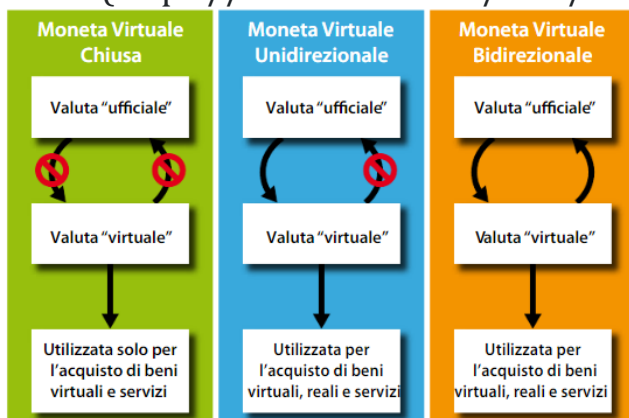
Se da un lato i principi contabili ancora non si sono occupati della rappresentazione delle criptovalute in bilancio, dall'altro lato i principi generali, e in particolare quello che prevede la distinzione tra investimenti posseduti per la negoziazione e quelli detenuti durevolmente, consentirebbero una rappresentazione contabile calcolata in funzione della finalità sottesa al loro **impiego**.

(<https://www.revilaw.it/2020/03/20/criptovalute-il-problema-della-corretta-contabilizzazione-in-bilancio/>, s.d.)

## *(Segue) Le Funzioni della moneta legale*

Per la sua qualificazione giuridica<sup>21</sup> e successivamente per la rappresentazione in bilancio, è importante delineare la funzione della moneta virtuale.

Fondamentale per comprendere che funzione possa o no svolgere una moneta virtuale è comprendere la sua natura, ovvero se è previsto che sia una moneta virtuale 'chiusa', 'unidirezionale' e 'bidirezionale'. La differenza tra le tre fattispecie risiede nella possibilità o meno di poter scambiare la criptovaluta con moneta a corso legale (o valuta 'ufficiale' o 'moneta fiat', secondo altre comuni denominazioni) e nella tipologia di beni/servizi acquistabili. Il bitcoin, ad esempio, è una moneta virtuale bidirezionale in quanto può essere facilmente convertita con le principali valute ufficiali e viceversa. (<https://www.consob.it/web/investor-education/cryptovalute>,



s.d.)

Fonte: <http://www.telecomitalia.com/tit/it/notiziariotecnico/2014-01/capitolo-06.html>

<sup>21</sup> ISTITUTO GIURIDICO. - Il termine, nel suo significato più comune, designa il complesso delle norme giuridiche relative a rapporti tra loro connessi (B. Windscheid, N. Coviello); o, con definizione più complessa, l'"unione organica delle norme e dei principî che regolano un fenomeno sociale, unione non artificiale e aprioristica, ma determinata dalla natura e dai fini di quello" (P. De Francisci): così parliamo dell'istituto giuridico della proprietà, del possesso, del testamento, per designare il complesso delle norme che regolano quella molteplicità di rapporti in cui un soggetto di diritto può venirsi a trovare per il fatto di essere proprietario o possessore o a cui può dar luogo la formazione di un testamento. Di solito, mentre designiamo col nome d'"istituto" un complesso di norme relative a un gruppo di rapporti, astruendo da quella ch'è la vita sociale dei rapporti medesimi, parliamo invece d'"istituzione" quando guardiamo alla realtà sociale del rapporto, al modo con cui esso vive e si comporta: in questo senso, ad es., diciamo "l'istituzione della famiglia è salda tra noi" e "l'istituto della famiglia è saviamente regolato nelle nostre leggi". La distinzione terminologica non è però universalmente accettata: vi è chi (W. Cesarini Sforza) parla d'istituti allorché si abbia un complesso di fenomeni giuridici aventi gli stessi soggetti (matrimonio) e d'istituzioni allorché si abbia un complesso di tali fenomeni con diversi soggetti (famiglia); vi è chi adopera i due termini indifferentemente, e i giuristi francesi in specie preferiscono il termine institution. ([https://www.treccani.it/enciclopedia/istituto-giuridico\\_%28Enciclopedia-Italiana%29/](https://www.treccani.it/enciclopedia/istituto-giuridico_%28Enciclopedia-Italiana%29/), s.d.)

Effettuando un confronto con le funzioni della moneta legale, semplificherà il riconoscere la qualificazione giuridica delle criptovalute, ed eventualmente, se rientrerà o no nella categoria delle monete oppure di altro istituto giuridico.

Sappiamo che alle monete a corso legale vengono solitamente riconosciute le funzioni di unità di conto, di mezzo di pagamento e di deposito di valore. Nello specifico:

-La funzione di **pagamento** consiste nel semplice e storico scambio di beni di fronte a un corrispettivo. La moneta viene quindi accettata convenzionalmente per facilitare l'acquisto di beni. Nel caso delle criptovalute non avendo corso legale in nessun paese, per essere accettate come mezzo di scambio vi deve esserci una volontà dalla controparte. Nonostante ciò vari sono stati i casi di accettazione da parte di aziende di criptovalute come mezzo di scambio (Tesla fino ad Aprile 2021 accettava tali monete) anche se successivamente hanno ripiegato nel rifiutarle in quanto comportava dei costi estremamente elevati.( vedere capitolo sulle Controversie.)

- La seconda funzione è quella di **unità di conto**. Tale funzione adempie a quella di unità di misurazione del valore delle attività reali e finanziarie, degli scambi dei beni e servizi e dei debiti e crediti.L'elevata volatilità delle criptovalute non consente sicuramente il corretto svolgimento di "unità di conto": i prezzi delle principali criptovalute sono soggetti a fluttuazioni molto ampie, anche all'interno delle stesse giornate. Quindi è altamente inefficiente, per non dire impossibile, prezzare beni e servizi in unità di criptovalute. Ulteriore caratteristica delle criptovalute che fa sì che non svolga la funzione di unità di conto è la loro divisibilità infinita, presentano infatti svariati valori decimali.

Per quanto riguarda la funzione di **riserva di valore**, si intende il riutilizzo della moneta per l'acquisto, ovviamente, di beni e servizi.

Per avere funzione di riserva una moneta non deve deteriorarsi, o meglio, il suo valore non deve subire decrementi considerevoli. Il valore di una moneta deve perdurare nel tempo, perciò la detenzione senza utilizzo deve far mantenere il potere di acquisto della valuta. Le criptovalute invece, per la loro struttura progettuale, basano il loro valore sull'accumulo di utilizzo, ovvero, maggiori sono il numero di transazioni effettuate con la moneta più il loro valore incrementerà. Questo è uno dei presupposti per cui le

criptovalute non possono svolgere tale funzione, il secondo è per il loro rischio di forti decrementi di valore che possono raggiungere.

Le valute standard sono sottoposte alla garanzia antiinflazionistica della politica monetaria delle banche centrali, le criptovalute, non essendo regolamentate e gestite, non hanno la stessa stabilità del potere di acquisto delle monete tradizionali.

## Quotazione e grafico BTC/EUR



Fonte <https://www.money.it/Quanto-vale-un-bitcoin-in-euro>. Il grafico mostra l'andamento del valore del bitcoin in euro, dal 2018 a inizio aprile 2019

Le criptovalute quindi non assolvono tutte le tipiche funzioni delle monete tradizionali; quindi, è fondamentale definire la sua qualificazione giuridica<sup>22</sup> in quanto ora è uno strumento di negoziazione subentrato nelle dinamiche sociali e utilizzato come mezzo di regolamentazione delle transazioni tra privati e aziende.

<sup>22</sup> Per approfondire si consiglia RAZZANTE R., *Bitcoin e monete digitali: problematiche giuridiche*, in *Rivista italiana di Intelligence*

*(Segue) Le ipotesi di rappresentazione giuridica*

Le criptovalute sono utilizzate come mezzo di pagamento ma non essendo emesse da un ente finanziario come una banca, da un istituto di credito o da un istituto di moneta elettronica non possono essere definite come moneta in senso tecnico e pertanto non è possibile applicare la regolamentazione valutaria utilizzata per le monete avente corso legale né per le monete elettroniche. (R. Razzante, Bitcoin e criptovalute: profili fiscali, giuridici e finanziari 2018) Inoltre, non possono essere qualificate come strumenti finanziari in quanto il **Testo Unico delle disposizioni in materia di intermediazione finanziaria**, o più semplicemente TUF con l'art. 1 comma 2 definisce tali strumenti come un insieme di tutti i prodotti finanziari e di ogni altra forma di investimento di natura finanziaria.

Tali strumenti per la Legge Draghi (nome alternativo al TUF) sono intesi:

- le azioni e gli altri titoli rappresentativi di capitale di rischio negoziabili sul mercato dei capitali;
- le obbligazioni, i titoli di Stato e gli altri titoli di debito negoziabili sul mercato dei capitali;
- le quote di fondi comuni di investimento;
- i titoli normalmente negoziati sul mercato monetario;
- qualsiasi altro titolo normalmente negoziato che permetta di acquisire gli strumenti precedentemente indicati;
- i contratti futures su strumenti finanziari, su tassi di interesse, su valute, su merci e sui relativi indici;
- i contratti di scambio a pronti e a termine (swaps) su tassi di interesse, su valute, su merci nonché su indici azionari (equity swaps);
- i contratti a termine collegati a strumenti finanziari, a tassi d'interesse, a valute, a merci e ai relativi indici;
- i contratti di opzione per acquistare o vendere gli strumenti indicati nelle precedenti lettere e i relativi indici, nonché i contratti di opzione su valute, su tassi d'interesse, su merci e sui relativi indici;
- le combinazioni di contratti o di titoli indicati precedentemente.

I mezzi di pagamento non sono considerati strumenti finanziari.



La direttiva 2007/64/CE all'art.4 punto 3 descrive i servizi di pagamento, i quali sono: il contante (banconote e monete) e i sistemi alternativi ad esso, ovvero assegni, bonifici, addebito diretto, carte di pagamento, servizi di pagamento via internet e su dispositivi portatili.

Punto chiave della Direttiva Europea è l'autorizzazione dei servizi di pagamento. Un istituto che offre servizi di pagamento deve ottenere l'autorizzazione per svolgere le sue attività di pagamento nell'UE. Ogni paese dell'UE possiede un organismo nazionale responsabile della concessione delle autorizzazioni. L'istituto è autorizzato solo se ha solidi dispositivi di governo in atto per la sua attività ed è in possesso di una certa quantità di capitale. (<https://eur-lex.europa.eu/legal-content/IT/LSU/?uri=celex:32007L0064>, s.d.)

Le criptovalute proprio per questa autorizzazione da parte di un istituto, necessaria per essere annoverati tra i servizi di pagamento, non possono essere incluse in tale categoria, avendo un'autorizzazione delle transazioni solo tra le controparti.

Ulteriore ipotesi di rappresentazione giuridica delle criptovalute è stata quella di annoverarli nella categoria dei **Beni Immateriali**, i quali sono disciplinati dal Codice civile all'art.810 che recita: "Sono beni<sup>23</sup> le cose che possono formare oggetto di diritti". Una criptovaluta è quindi un bene mobile e immateriale, non essendoci data la sua natura digitale tangibilità. Il contrasto avviene però per la natura non monetaria dei beni, per via del requisito di patrimonialità che difetta nelle criptovalute.

---

<sup>23</sup> Bene giuridico è una cosa caratterizzata dall'utilità, cioè idoneità a soddisfare una necessità dell'uomo; dall'accessibilità, intesa come possibilità di subire espropriazione; dalla limitatezza, quale disponibilità limitata in natura. Questa definizione si distingue, perciò, da quella naturalistica di cosa: è possibile, infatti, che vi siano cose non beni giuridici, basti citare a questo proposito l'aria, e beni giuridici che non siano allo stesso tempo cose. Basti pensare, a tale riguardo, alle opere dell'ingegno.

Da <https://www.brocardi.it/codice-civile/libro-terzo/titolo-i/capo-i/art810.html>



Altri regolatori hanno invece evidenziato le similitudini delle valute virtuali rispetto a **Beni Materiali** come i metalli preziosi, i combustibili e i prodotti agricoli, riconducendo le criptovalute alla nozione di *commodities*<sup>24</sup>, ossia, di prodotti che possono essere utilizzati a scopo di investimento o speculativo.

Nel luglio 2014 la European Banking Authority (EBA) ha pubblicato una opinion indirizzata alle istituzioni dell'UE ed alle autorità di vigilanza degli Stati Membri, nella quale ha analizzato le caratteristiche e i rischi connessi alle valute virtuali. In tale opinion, le criptovalute vengono definite come rappresentazioni digitali di valore non emesse da banche centrali o da altre autorità pubbliche, le quali possono essere accettate da persone fisiche o giuridiche come mezzo di pagamento. Nel riconoscere alcuni potenziali benefici delle valute virtuali – come, ad esempio, minori costi delle transazioni, velocità e inclusione finanziaria – l'EBA ha sottolineato l'esistenza di numerosi rischi per i consumatori, per l'integrità dei mercati finanziari (come, ad esempio, in ambito antiriciclaggio e contrasto al finanziamento del terrorismo), per i sistemi di pagamento basati su monete tradizionali e per le autorità di vigilanza.

Sulla stessa linea si è pronunciata anche la BCE nel mese di febbraio 2015, precisando che le valute virtuali possono essere definite come “rappresentazioni digitali di valore non emesse da banche centrali, istituti di credito o istituti di moneta elettronica, le quali, in alcune circostanze, possono essere utilizzate come un'alternativa al denaro.”

La Risoluzione 72/E dell'Agenzia delle Entrate, qualificò l'operazione come: “operazione che consiste nel cambio di valuta tradizionale contro unità della valuta virtuale bitcoin e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra il prezzo di acquisto delle valute e quello di vendita praticato dall'operatore ai propri clienti, costituiscono prestazioni di servizio a titolo oneroso. Più precisamente, secondo i giudici europei, tali operazioni rientrano tra le operazioni “relative a divise, banconote e monete con valore liberatorio”.

---

<sup>24</sup> Commodity è un termine inglese che indica un bene per cui c'è domanda ma che è offerto senza differenze qualitative sul mercato ed è fungibile, cioè il prodotto è lo stesso indipendentemente da chi lo produce, come per esempio il petrolio o i metalli. Da Wikipedia

A partire da queste definizioni del bitcoin e di conseguenza delle altre criptovalute, si delineò anche il profilo fiscale riguardo a queste operazioni (trattato nel successivo capitolo).

## **2.3 Primo arbitrato italiano sulle Criptovalute:**

### ***IL Caso Marcianise 2018***

Nella provincia di Caserta, a Marcianise per precisione, nel 2018 c'è stato il lodo arbitrale riguardo la fattispecie di un contratto di consulenza avvenuto a metà del mese di aprile.

Tale contratto prevedeva che metà del compenso fosse elargito in criptovalute "Eurocrediti", del circuito di pagamento "Visotrade", come mezzo di pagamento e la restante parte in euro. La controparte, nonostante ciò, aveva convenuto nell'ottenere la metà del compenso non più in criptovaluta ma in moneta ordinaria o standard.

L'arbitro unico però, dato il comune accordo iniziale del contratto, ricondusse l'obbligazione nella categoria delle obbligazioni pecuniarie, o meglio, qualificò il pagamento con criptovaluta equiparabile al pagamento in valuta estera o non avente corso legale nello stato in cui avvenuto il fatto, rifacendosi quindi all'art.1278 del Codice civile, cioè: "Se la somma dovuta è determinata in una moneta non avente corso legale nello Stato, il debitore ha facoltà di pagare in moneta legale, al corso del cambio nel giorno della scadenza e nel luogo stabilito per il pagamento"

L'articolo però del Codice civile rende l'obbligazione pecuniaria tramite valuta estera come un'obbligazione facoltativa passiva<sup>25</sup>, il che andava contro il regolamento contrattuale stabilito. L'arbitro di Marcianise stabilì perciò, adeguandosi al contratto, che se la metà del compenso in criptovaluta rientrasse come obbligazione in valuta estera, ma non era facoltà della controparte richiedere il pagamento del compenso in toto per le prestazioni di consulenza in moneta a corso legale.

---

<sup>25</sup> Le obbligazioni facoltative sono le obbligazioni nelle quali la prestazione dovuta è una sola (obbligazione semplice), ma al debitore viene attribuita la facoltà di liberarsi dando un'altra cosa. Vi sono una sola prestazione e due possibilità di adempimento. (digilander.libero.it, s.d.)

L'obbligazione del contratto sicuramente è stata annoverata come obbligazione pecuniaria, in quanto l'estinzione dell'obbligo del debitore fosse dovuto per metà in euro, ma tale aspetto non è da sottovalutare in quanto il Giudice del lodo arbitrale ha stabilito *per analogia iuris*<sup>26</sup> che tale caso va applicato anche per le obbligazioni in moneta estera e criptovaluta.

Dal lodo arbitrale di Marcianise si può evincere, quindi, che la criptovaluta sia un **Bene Polivalente**, ha natura sia pecuniaria sia di merce.

Nel caso in cui sia il corrispettivo per uno scambio di beni e servizi avrà funzione e natura pecuniaria, in altri casi però può assumere la funzione di *merce*. Un esempio è il contratto di cambio valute in quanto è un contratto di compra/vendita.

Da precisare che l'art. poteva essere applicato senza alcuna analogia in quanto: "Se la somma [...] non avente corso legale nello stato" il che presuppone che l'art. si rifa in maniera generale a qualsiasi moneta non legale, includendo quindi in questo insieme anche le criptovalute.

Non poco rilevanti sono ovviamente le condizioni della fattispecie delle obbligazioni pecuniarie e in particolar modo l'applicazione degli interessi ai sensi dell'art.1282 del c.c.: "I crediti liquidi ed esigibili di somme di denaro producono interessi di pieno diritto, salvo che la legge o il titolo stabiliscano diversamente." Nella sentenza di Varese del '89 tale fattispecie fu applicata anche per le obbligazioni in valuta estera, quindi per analogia *iuris*, può trovarsi applicazione anche nel caso degli obblighi in criptovaluta.

In conclusione, l'assimilazione delle criptovalute all'interno del nostro ordinamento giuridico non è di semplice ed immediata realizzazione. La natura polivalente delle stesse però può essere un fattore a favore, applicando più fattispecie a seconda del caso in oggetto, come nel Lodo arbitrale di Marcianise.

---

<sup>26</sup> L'analogia, in diritto, è un procedimento logico di carattere interpretativo, utilizzato nel diritto in relazione all'attività di giurisdizione. Esso ha luogo allorquando, a fronte di una lacuna dell'ordinamento giuridico, il giudice si veda nella necessità di dover offrire un obiettivo criterio di valutazione giuridica, in ordine a categorie di soggetti o di rapporti, il cui status o la cui regolamentazione non appaia espressamente contemplata dalla lettera della norma. (Wikipedia, s.d.)

## 2.4 Conferimenti di criptovalute in società di capitali

Particolare è il fatto giuridico dei conferimenti da parte dei soci<sup>27</sup>, una forte problematica per i legislatori per via della natura stessa delle criptovalute, la domanda che si pongono è: I conferimenti effettuati con tali valute sono da ritenere legittimi o no?

Alla prima domanda la maggioranza preme sul **no** della legittimità dei conferimenti, sia per la costituzione di una società di capitali o per l'aumento di capitale da parte dei soci. Il decreto n. 7556/2018 del 18 luglio 2018 del Tribunale di Brescia, poi confermata dal successivo decreto n. 207/2018 del 24 ottobre della Corte appello di Brescia hanno dato una chiarezza su tale fatto giuridico.

Nel caso di Brescia, l'assemblea dei soci una s.r.l. con amministratore unico aveva deliberato su il conferimento da parte dei soci di beni in natura con criptovalute, tale delibera ha comportato controversie.

L'art. 2465 del c.c. stabilisce che: *“Chi conferisce beni in natura o crediti deve presentare la relazione giurata di un esperto o di una società di revisione iscritti nel registro dei revisori contabili o di una società di revisione iscritta nell'apposito registro albo.*

*La relazione, che deve contenere la descrizione dei beni o crediti conferiti, l'indicazione dei criteri di valutazione adottati e l'attestazione che il loro valore è almeno pari a quello ad essi attribuito ai fini della determinazione del capitale sociale e dell'eventuale soprapprezzo, deve essere allegata all'atto costitutivo.”*

Al momento del conferimento, ai sensi dell'articolo sopra citato, fu consegnata la relazione giurata di stima sul bene (le criptovalute), ma il notaio rogante rifiutò tale conferimento con giusta motivazione ovvero: “le criptovalute, stante la loro volatilità, non consentono una valutazione concreta del quantum destinato alla liberazione dell'aumento di capitale sottoscritto” rispettando il comma 2 dell'art. 2465.

---

<sup>27</sup> Per approfondire si rimanda al libro “Diritto commerciale vol.II : Diritto delle società” di G.F. Campobasso

La S.R.L. rifiutando la decisione notarile effettuò ricorso, il quale poneva le sue basi di difesa sull'ex art. 2464 del c.c. "Possono essere conferiti tutti gli elementi dell'attivo suscettibili di valutazione economica".

Le argomentazioni si fondavano su alcune caratteristiche specifiche dei beni oggetto del conferimento. Più precisamente si evidenziava:

- L'**esistenza**, nonché la messa a disposizione da parte della Società e del socio conferente, delle credenziali di accesso con le quali era reso possibile ed immediato il passaggio della titolarità della criptovaluta in questione;
- L'**esistenza di una valutazione** della criptovaluta attuale, concreta, precisa ed attendibile in termini monetari, risultante da perizia di stima debitamente prodotta;
- La discreta **scambiabilità** della moneta virtuale in oggetto su di una precisa piattaforma raggiungibile da un preciso indirizzo Internet;
- La **liceità** dell'iscrizione del conferimento in natura nel bilancio, potendo la criptovaluta essere considerata, come ad esempio il diritto di proprietà intellettuale, alla stregua di qualsiasi altro bene immateriale. (iusinitinere.it)

Il tribunale di Brescia, inizialmente deciso ad astenersi nella presa di posizione, stabilì di incentrare le indagini giuridiche sull'idoneità dei conferimenti delle criptovalute e sui loro requisiti. Basandosi sempre su l'art.2464 comma 2 del c.c. stilò le caratteristiche dei conferimenti atti ad una valutazione. Le caratteristiche erano:

- Idoneità alla valutazione in un determinato momento storico, ovviamente le fluttuazioni del mercato delle criptovalute non si presta a tale caratteristica.

- Idoneità all'essere bersaglio degli eventuali creditori sociali. Le società di capitali basano la loro esistenza proprio sulla loro capacità di soddisfare i creditori sociali senza intaccare il patrimonio personale dei soci (autonomia patrimoniale perfetta<sup>28</sup> delle società di capitali), le costanti fluttuazioni del valore delle criptovalute possono portare ad una profonda svalutazione patrimoniale, cadendo nel caso dell'annacquamento del capitale<sup>29</sup>.

Il Tribunale di Brescia stabilì che il notaio aveva legittimamente rifiutato la delibera assembleare sull'aumento di capitale tramite il conferimento delle criptovalute.

## 2.5 Rappresentazione in Bilancio delle Criptovalute

Negli Stati Uniti, nei quali il mercato degli scambi in criptovalute è stato particolarmente attivo sin dall'inizio della loro "generazione", diversi sono stati e sono gli operatori imprenditoriali interessati a individuare, nell'incertezza definitoria legale, nella criptovaluta, una digital asset di natura particolare, nuova nello scenario economico ed operativo. È, pertanto, normale che ci si sia anche attivati per definire con quali modalità contabili potessero e possano essere rappresentate le operazioni in criptovaluta e su come procedere per le valutazioni e, ancora, per come esporre nei bilanci e nelle informative finanziarie questo tipo di crypto asset. (Pontani)

---

<sup>28</sup> Con questa espressione si indica il fenomeno per cui tra il patrimonio di un ente e quello dei suoi membri vi sia separazione assoluta. Pertanto, dei debiti contratti dall'ente non rispondono i membri con il loro patrimonio personale, e viceversa.

Tale fenomeno non si verifica in tutti i tipi di persone giuridiche, ma solo nelle società di capitali. (Brocardi.it)

<sup>29</sup> Consiste nella sopravvalutazione arbitraria del capitale nominale d'azienda rispetto all'effettivo valore del patrimonio, ottenuta in seguito a sopravvalutazioni di attività e sottovalutazioni di passività. È l'inverso della riserva occulta. Le pratiche di annacquamento del capitale sono vietate in quanto non rappresentano correttamente l'effettiva situazione aziendale contravvenendo ai principi di redazione del bilancio previsti dall'art. 2423-bis cod. civ. (sapere.it)

Per quel che concerne la contabilizzazione nel bilancio di esercizio delle criptovalute, al momento vi sono pareri discordanti in special modo sulla loro classificazione. I principi contabili non forniscono alcuna indicazione per le imprese ad eccezione di quanto prospettato dallo IAS 8, il quale dispone che “*in assenza di un Principio o un’interpretazione debba essere la direzione aziendale a sviluppare ed applicare un principio contabile*” che sia in grado di fornire un’informativa che possa essere attendibile, rilevante ed in grado di rappresentare fedelmente la situazione patrimoniale e finanziaria della Società.

L’IC, *Interpretation Committee*<sup>30</sup>, si è espresso in merito ai principi contabili da applicare nei confronti delle criptovalute per via delle perplessità presentate dallo IASB, l’organo preposto alla stesura dei principi contabili internazionali.

Fondamentale rammentare che le criptovalute sono monete digitali, utilizzate per lo scambio di beni e servizi oppure detenute in portafoglio come investimento.

È pacifico asserire che le criptovalute possono essere definite come *asset (digitale)*, il problema però è stabilire che categoria di asset appartengono. Gli assets, va ricordato, sono entità materiali o immateriali suscettibili di valutazione economica per un certo soggetto. In assenza di una classificazione soddisfacente, si può ricorrere alla distinzione classica fra attività materiali e immateriali.

Gli assets sono divisibili in quattro grandi categorie che sono:

- I titoli azionari, noti anche come azioni, rappresentano la proprietà delle aziende quotate in borsa. All’interno di questa classe di asset, vi è un’ulteriore suddivisione tra azioni appartenenti alle aziende a grande capitalizzazione, a media capitalizzazione e a piccola capitalizzazione.

---

<sup>30</sup> L’IFRS Interpretations Committee (Interpretations Committee) è l’organo interpretativo dell’International Accounting Standards Board (Board). Il Comitato Interpretazioni collabora con il Consiglio a supporto dell’applicazione degli IFRS. Il Comitato Interpretazioni risponde alle domande sull’applicazione degli Standard e svolge altro lavoro su richiesta del Consiglio. Il Comitato Interpretazioni è composto da 14 membri votanti, nominati dagli Amministratori della Fondazione IFRS. I membri forniscono la migliore competenza tecnica disponibile e la diversità delle esperienze commerciali e di mercato internazionali relative all’applicazione degli standard IFRS. Le riunioni del Comitato Interpretazioni sono aperte al pubblico e sono trasmesse via web. Definizione a cura di IFRS.org



- Gli asset a reddito fisso sono investimenti che fruttano interessi nel corso del tempo per poi venire rimborsati al valore iniziale. Le obbligazioni sono il tipo di asset a reddito fisso più comune.
- Gli asset del mercato valutario sono contanti o equivalenti del contante. Asset liquidi, ma che non lasciano molto spazio alla crescita.
- Gli investimenti alternativi includono alcuni mercati molto popolari, come l'immobiliare e quello delle materie prime, oltre alle criptovalute. (ig.com)

Una delle prime ipotesi è quella di inserire le criptovalute all'interno del gruppo delle financial assets, grazie al loro impiego come mezzo per lo scambio di beni e servizi( <https://it.andersen.com/crypto-currencies-accounting-for-ias-ifs-purposes/>)

*(Segue) IAS 7*

Il principio contabile IAS 7 del 3 novembre 2008 definisce le disponibilità liquide come:

*“Le disponibilità liquide equivalenti sono quelle possedute per soddisfare gli impegni di cassa a breve termine, invece che per investimento o per altri scopi. Perché un investimento possa essere considerato come disponibilità liquida equivalente esso deve essere prontamente convertibile in un ammontare noto di denaro e deve essere soggetto a un irrilevante rischio di variazione del valore. Perciò, un investimento è classificato, solitamente, come disponibilità liquida equivalente solo quando esso è a breve scadenza, cioè, per esempio, a tre mesi o meno dalla data d'acquisto. Gli investimenti finanziari azionari sono esclusi dalla classificazione come disponibilità liquide equivalenti a meno che essi siano, di fatto, equivalenti alle disponibilità liquide, quali, per esempio, le azioni privilegiate acquistate in un momento vicino alla loro scadenza e con una data di rimborso determinata.”*

Stando a tale definizione, le criptovalute non possono essere ritenute come disponibilità liquide equivalenti in quanto:

- incapaci di soddisfare un impegno di cassa a breve termine (si ricorda la *volontarietà* nell'accettare o no la criptovaluta come mezzo di pagamento)
- Sono ovviamente soggette a forti variazioni di valore, il che le rende totalmente incompatibili con i cash and equivalents.



Vi è da aggiungere inoltre che stando allo IAS 7 le disponibilità liquide equivalenti sono emesse e/o garantite da un'istituzione, caratteristica totalmente assente nelle criptovalute.

*(Segue) IAS 32*

Successivo principio contabile internazionale da valutare per assegnare la voce di bilancio delle criptovalute è lo IAS 32.

Il quale asserisce che:

*“Uno strumento finanziario è qualsiasi contratto che dia origine a un'attività finanziaria per un'entità e a una passività finanziaria o a uno strumento rappresentativo di capitale per un'altra entità.*

Una attività finanziaria è qualsiasi attività che sia:

- a) disponibilità liquide;
- b) uno strumento rappresentativo di capitale di un'altra entità;
- c) un diritto contrattuale<sup>31</sup>:

*i) a ricevere disponibilità liquide o un'altra attività finanziaria da un'altra entità; o*

*ii) a scambiare attività o passività finanziarie con un'altra entità a condizioni che sono potenzialmente favorevoli all'entità; o*

d) un contratto che sarà o potrà essere estinto tramite strumenti rappresentativi di capitale dell'entità ed è:

*i) un non derivato per cui l'entità è o può essere obbligata a ricevere un numero variabile di strumenti rappresentativi di capitale dell'entità; o*

*ii) un derivato che sarà o potrà essere estinto con modalità diverse dallo scambio di un importo fisso di disponibilità liquide o di altra attività*

---

<sup>31</sup> Il diritto contrattuale è una branca del diritto civile che disciplina i rapporti contrattuali ossia un accordo tra due o più soggetti tra cui intercorre un rapporto giuridico patrimoniale. Dalla stipula del contratto scaturisce la responsabilità contrattuale in caso di inadempimento, errato o tardivo adempimento degli obblighi previsti dal contratto stesso. (www.studio-comand.com)

*finanziaria contro un numero fisso di strumenti rappresentativi di capitale dell'entità. A tal fine, gli strumenti rappresentativi di capitale dell'entità non includono strumenti finanziari con opzione a vendere classificati come strumenti rappresentativi di capitale conformemente ai paragrafi 16A e 16B, né strumenti che pongano a carico dell'entità un'obbligazione a consegnare a un'altra parte una quota proporzionale dell'attivo netto dell'entità solo in caso di liquidazione e sono classificati come strumenti rappresentativi di capitale conformemente ai paragrafi 16C e 16D, né strumenti che siano contratti per ricevere o consegnare in futuro degli strumenti rappresentativi di capitale dell'entità.”*

L'International Commitee ha stabilito che le criptovalute non possono essere incluse nella definizione di attività finanziaria secondo il principio IAS 32 in quanto:

- Non rappresentano un capitale per un'altra entità, non rientrano nella categoria delle disponibilità liquide
- Non fungono da diritto contrattuale, non vi è alcuna controparte e un'attività in criptovalute non è correlata a una corrispondente passività per un'altra entità.

*(Segue) Paragrafo AG 3 di IAS 32*

*“La moneta (disponibilità liquide) è un'attività finanziaria in quanto rappresenta il mezzo di scambio e per questo è la base sulla quale tutte le operazioni sono misurate e rilevate nel bilancio. Un deposito di disponibilità liquide in una banca o in un analogo istituto finanziario è un'attività finanziaria perché rappresenta il diritto contrattuale del depositante a ottenere disponibilità liquide dall'istituto o a emettere un assegno o uno strumento analogo in favore di un creditore attingendo al deposito per il pagamento di una passività finanziaria”*

Il Comitato ha, inoltre, rilevato che una partecipazione in criptovaluta non è un'attività finanziaria. In merito, l'IC dalla descrizione della liquidità, del paragrafo AG3 dello IAS 32, ha osservato che le disponibilità liquide sono considerate attività finanziarie in quanto utilizzate come mezzo di scambio e come unità monetaria nella determinazione del prezzo di beni e servizi.

Il Comitato ha, però, concluso che una partecipazione in criptovaluta se pur utilizzata come mezzo di scambio e come unità monetaria, non è denaro poiché le stesse non presentano attualmente le caratteristiche richieste.

*(Segue) IAS 38*

*“L’attività è una risorsa:*

*a) controllata dall’entità in conseguenza di eventi passati; e*

*b) dalla quale sono attesi benefici economici futuri per l’entità.”*

Questa è la definizione di un’attività all’interno dello IAS 38, che prosegue con:

*“Un’attività immateriale è un’attività non monetaria identificabile priva di consistenza fisica.”*

Stando alla descrizione di attività immateriale all’interno di questo principio contabile internazionale, le criptovalute possono essere trattate come questa categoria.

Lo IAS 38 stabilisce che un'attività immateriale debba essere identificabile per essere distinta dall'avviamento<sup>32</sup>, il principio contabile stabilisce inoltre che un'attività è identificabile se:

- è separabile, ossia può essere separata o scorporata dall'entità;
- deriva da diritti contrattuali o da altri diritti legali, indipendentemente dal fatto che tali diritti siano trasferibili o separabili dall'entità o da altri diritti obbligazionari.

Stando alle premesse effettuate, secondo lo IAS 38 quindi, le valute crittografiche soddisferebbero la definizione di attività immateriali. Non presentano, quindi, natura monetaria (se per natura monetaria si intende il denaro posseduto o le attività che devono essere incassate in un ammontare di denaro prefissato e determinabile). Sono attività separabili, vendibili e trasferibili o scambiabili individualmente. Infine, sono attività immateriali se il detentore utilizza le criptovalute come assets e non come beni pronti alla vendita come nel normale svolgimento della sua attività.

Tale interpretazione ignora totalmente la funzione di prodotto finanziario speculativo che, nella prassi, sono andate via via ad assumere le criptovalute. (Contributo comparato nella sezione Norme & Tributi su Il Sole 24 Ore).

È da precisare che nell'eventualità di disponibilità in bilancio di tali attività, è necessario il commento in nota integrativa e nella relazione sulla gestione.

---

<sup>32</sup> L'avviamento rappresenta il maggior valore attribuito al complesso aziendale rispetto al suo valore contabile. L'avviamento deriva da qualità oggettive, cioè legate all'azienda, alla sua struttura, alla sua organizzazione e da qualità soggettive, relative alle capacità personali del soggetto economico. ([www.borsaitaliana.it](http://www.borsaitaliana.it))

Per avviamento deve intendersi la capacità dell'azienda di produrre un reddito superiore a quello mediamente atteso per il settore in cui la stessa opera. Se tale capacità esiste si avrà un avviamento positivo (goodwill), mentre se tale capacità è inesistente, vuoi perché il reddito prospettico è inferiore a quello mediamente atteso per il settore in cui l'azienda opera, vuoi perché lo stesso è addirittura negativo, si avrà un avviamento negativo (badwill).

L'avviamento è l'attitudine di un'azienda a produrre utili. Si tratta di un concetto contabile che fa riferimento alla differenza tra capitale economico aziendale e valori di bilancio. Tale valore si esplica nel momento in cui si intende quantificare un complesso di elementi d'azienda capaci di creare valore. ([www.fiscomania.com](http://www.fiscomania.com))

## *(Segue) IAS 2*

Il fenomeno delle criptovalute e del loro mercato ha avuto un exploit rilevante, coinvolgendo la maggior parte dei paesi, imprese e famiglie. Utilizzato al mero fine speculativo si ribadisce che la loro classificazione si baserà sullo IAS 38 come attività immateriale all'interno del bilancio, in quanto non attività legata al core business dell'impresa.

Ma se il bilancio analizzato fosse di un'impresa il cui core business è basato sulle criptovalute?

In questo caso l'IC, ha stabilito che il principio contabile a cui riferirsi in caso di vendita nel corso del business è lo IAS 2, deputando alle criptovalute come merce da acquistare e/o da vendere. È necessario quindi descrivere i che principali attori possono essere:

1. Commercianti di criptovalute, la cui attività principale consiste nell'acquisto e vendita delle stesse.
2. Exchanger di criptovalute, la cui attività principale consiste nel cambiare criptovalute in moneta a corso legale e che detengono criptovalute in garanzia o in conto deposito.
3. Utilizzatori di criptovalute, la cui attività collegata alle criptovalute è la sola accettazione in pagamento.
4. Processori di pagamento, la cui attività è accettare criptovalute per convertirle immediatamente in moneta a corso legale.
5. Miners, la cui attività è la prestazione di servizi per la rete remunerata con emissione di nuova criptovaluta.

(Bilancio di Oraclize)

I quali detengono le criptovalute per due eventuali scopi:

- investimento al fine di guadagnare rendimenti sotto forma di futuri aumenti del valore delle criptovalute;
- l'obiettivo di rivenderli per un profitto nel corso della loro attività.

Le criptovalute verranno inserite nella voce del bilancio di tali attori come “rimanenze”. Definite così dal principio contabile internazionale:

*“Le rimanenze sono beni:*

*a) posseduti per la vendita nel normale svolgimento dell’attività;*

*b) impiegati nei processi produttivi per la vendita; o*

*c) sotto forma di materiali o forniture di beni da impiegarsi nel processo di produzione o nella prestazione di servizi.”*

L’intenzione dell’IC seguendo il punto a) è valutare verosimilmente le criptovalute alle commodities e l’impresa come operatore dedito allo scambio di questi “beni” intangibili e digitali.

## **2.6 Valore di Iscrizione in Bilancio**

La diversa classificazione delle criptovalute a seconda del loro impiego (si ricorda attività immateriale e rimanenze) comporta un diverso criterio di valutazione e rivalutazione in bilancio.

Va ribadito che l’IC ha stabilito che le criptovalute non sono strumenti finanziari, bensì vanno imputate alle voci di attività immateriali (a scopo di investimento) e rimanenze (scopo merce) seguendo rispettivamente i principi IAS 38 e IAS 2.

Nel caso di iscrizione a bilancio come attività immateriale l’IAS 38 paragrafo 24 stabilisce che:

*“Un’attività immateriale deve essere misurata inizialmente al costo.”*

Il costo di una criptovaluta può essere generato in due modalità, il primo ovviamente è il costo di acquisto nel mercato a loro dedito, il secondo-invece. sarà pari al costo di produzione delle stesse. Nel caso di generazione interna, quindi, un miner registrerà le sue scorte di criptovalute al costo della loro estrazione nonché di eventuali costi di energia elettrica e di altri costi di produzione, questi ultimi, vi è da precisare sono costi rilevanti che si vedrà in seguito (capitolo 4 Le Controversie).

Da sottolineare i paragrafi 52 e 53 dello IAS 38 per la valutazione del costo di generazione interna delle criptovalute:

*52. "Per valutare se un'attività immateriale generata internamente soddisfa le condizioni necessarie per essere rilevata in bilancio, l'entità classifica il processo di formazione dell'attività in:*

*a) una fase di ricerca; e*

*b) una fase di sviluppo.*

*Sebbene i termini «ricerca» e «sviluppo» abbiano già una definizione, i termini «fase di ricerca» e «fase di sviluppo» acquisiscono un significato più ampio nel contesto del presente Principio.*

*53. Se un'entità non è in grado di distinguere la fase di ricerca dalla fase di sviluppo di un progetto interno di formazione di un'attività immateriale, l'entità tratta contabilmente il costo derivante da tale progetto come se fosse sostenuto esclusivamente nella fase di ricerca."*

Mentre per la loro valutazione, successiva all'iscrizione in bilancio, i paragrafi 74 e 75, stabiliscono che un'attività vada rilevata in maniera opzionale con due distinti modelli:

#### **Modello del costo**

*Dopo la rilevazione iniziale, un'attività immateriale deve essere iscritta in bilancio al costo al netto degli ammortamenti accumulati e di qualsiasi perdita per riduzione di valore accumulata.*

#### **Modello della rideterminazione del valore**

*Dopo la rilevazione iniziale, un'attività immateriale deve essere iscritta in bilancio all'importo rideterminato, cioè al fair value (valore equo) alla data di rideterminazione del valore al netto di qualsiasi successivo ammortamento accumulato e di qualsiasi successiva perdita per riduzione di valore accumulata. Per l'applicazione delle rideterminazioni del valore in conformità alle disposizioni del presente Principio, il fair value deve essere misurato facendo riferimento a un mercato attivo.*

*Le rideterminazioni devono essere effettuate con una regolarità tale da far sì che alla data di riferimento del bilancio il valore contabile dell'attività non si discosti significativamente dal suo fair value (valore equo).*

le criptovalute rideterminate in bilancio al loro fair value alla data di chiusura dell'esercizio saranno soggette ad una rendicontazione finanziaria, riflettendo nella situazione patrimoniale – economica – finanziaria gli eventuali aumenti o diminuzioni del valore rispetto alla prima iscrizione, i quali saranno riconosciuti come utili o perdite nel Conto Economico.

In caso di rivendita, l'utile (perdita) rilevato sulla cessione sarà costituito dalla differenza rispetto all'ultimo fair value indicato sullo Stato Patrimoniale.

Rimane da stabilire come evincere il fair value delle criptomonete.

## **2.7 Il Fair Value delle criptovalute**

Secondo l'International Financial Reporting Standard, *“il Fair Value è il prezzo che si riceverebbe per vendere un'attività, o che si pagherebbe per trasferire una passività, in una transazione ordinata tra operatori di mercato al momento della misurazione”*.

Va distinto dalla quotazione di mercato, che rappresenta il valore effettivo di un titolo. Il Fair Value ne costituisce il valore teorico, cioè un valore “giusto” (altra traduzione di “fair”) che neutralizzi i fattori non economici (come l'emotività e gli altri che condizionano il valore effettivo) per restituire un prezzo il più possibile oggettivo. Quindi attribuire un fair value ad un asset che presenta un mercato dall'estrema volatilità, ha rilevanti difficoltà.



Perciò, ci sono stati diversi metodi per avvicinarsi alla valutazione. La maggior parte di questi approcci differiscono nel modo in cui si vede la natura di una "moneta" digitale.

I quali sono:

- Expected value
- Costo di produzione
- Incrocio domanda e offerta

*(Segue) Expected value*

Secondo tale approccio la criptovaluta verrà valutata come un titolo azionario o obbligazionario. Il calcolo del valore atteso è definito come il rapporto tra il prezzo iniziale del titolo ed il prezzo finale. Uno dei limiti legati a tale approccio è proprio il prezzo di un'azione, in quanto esso è funzione dei dividendi distribuiti; le criptovalute non distribuiscono dividendi, quindi, per ridurre le problematiche di tale approccio, si è considerato di stabilire il prezzo basandosi sulla "convinzione" percepita della struttura digitale che sostiene la crypto. Un approccio simile di valutazione viene applicato alle start-up che non hanno guadagni o profitti correnti. Una volta previsto un valore atteso, si può iniziare a fare stime sull'attuale fair value.

*(Segue) Costo di produzione*

Un altro approccio per calcolare il valore equo delle criptovalute è quello di assegnarle una natura di commodities. Il valore della merce prodotta è spesso determinato dal costo marginale del prodotto stesso. In un mercato perfettamente concorrenziale il prezzo di vendita di un prodotto, a causa delle strategie di mercato, dovrebbe raggiungere il valore del costo di marginale dello stesso. Da sottolineare il fatto che la produzione di criptovalute (l'estrazione) diventa sempre più difficoltosa, per via dell'aumento dei blocchi all'interno della blockchain, ciò vuol dire che il

costo marginale di produzione di una criptovaluta aumenterà a prescindere dall'offerta.

*(Segue) Incrocio domanda e offerta*

Il valore di una criptovaluta può essere tratto tramite il principio della domanda e dell'offerta.

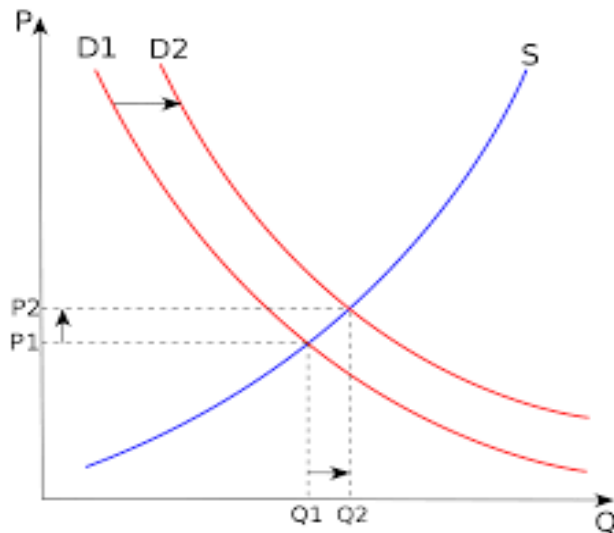


Grafico della domanda e dell'offerta. Fonte Wikipedia.org

Come in qualsiasi mercato, il prezzo di vendita di un prodotto si ottiene tramite l'iterazione tra acquirenti e venditori (incrocio domanda e offerta). Ad un aumento della domanda, il prezzo del prodotto aumenterà. Vi è da aggiungere che le criptovalute sono al momento limitate nel loro numero e disponibilità, possono essere assimilate quindi ad oggetti dall'elevata rarità, il che comporta quindi una domanda delle stesse abbastanza rilevante.

## 2.8 L'IMPATTO DEI PRINCIPI CONTABILI INTERNAZIONALI SUL PIANO NAZIONALE

L'orientamento dell'OIC – I principi contabili nazionali, al momento, non hanno previsto alcun tipo di disciplina in tema delle valute virtuale.

In data 30 Maggio 2019 durante il *Tentative Agenda Decisions*, l'OIC pronunciò osservazioni e perplessità riguardo la classificazione delle criptovalute a beni immateriali, senza tuttavia emettere una proposta alternativa valida.

Pacifico è il fatto che le criptovalute non possano essere catalogate come disponibilità liquide (OIC 14), crediti (OIC 15) o strumenti finanziari (OIC 32), quindi per applicazione analogica agli IFRS il redattore di bilancio inserirà o nella voce “immobilizzazioni immateriali” (OIC 24) e “rimanenze” (OIC 13) le criptovalute.

(Segue) OIC 24

Secondo il principio contabile nazionale 24 par.4 le immobilizzazioni immateriali sono:

*“attività normalmente caratterizzate dalla mancanza di tangibilità. Esse sono costituite da costi che non esauriscono la loro utilità in un solo periodo ma manifestano i benefici economici lungo un arco temporale di più esercizi. Le immobilizzazioni immateriali comprendono:*

- oneri pluriennali (costi di impianto e di ampliamento; costi di sviluppo);*
- beni immateriali (diritti di brevetto industriale e diritti di utilizzazione delle opere dell'ingegno; concessioni, licenze, marchi e diritti simili);*
- avviamento;*
- immobilizzazioni immateriali in corso; e*
- acconti”*

Mentre al par.9 descrivono i beni immateriali come:

*“I beni immateriali sono beni non monetari, individualmente identificabili, privi di consistenza fisica e sono, di norma, rappresentati da diritti giuridicamente tutelati. Un bene immateriale è individualmente identificabile quando:*

*-è separabile [...]*

*- deriva da diritti contrattuali”*

Le descrizioni di immobilizzazioni immateriali prima e beni immateriali dopo, non si discostano dall'IAS 38, rendendo così il principio nazionale conforme all'ordinamento internazionale. Secondo l'OIC 24 la classificazione in immobilizzazione immateriale, però, comporterà la rilevazione iniziale del bene immateriale al costo di acquisto includendo gli oneri accessori ( l' OIC non prevede l'utilizzo del fair value).

In aggiunta, data la loro natura di beni immateriali saranno soggetti obbligatoriamente ad ammortamento <sup>33</sup>, secondo la vita utile del bene stesso. L'OIC 24 par.71 stabilisce che, non essendoci un limite temporale al bene immateriale, la vita utile non deve superare gli anni previsti dal contratto e/o dal limite legale e, sempre e comunque, non può superare 20 anni di periodo di ammortamento.

---

<sup>33</sup> In economia l'ammortamento è il deprezzamento del valore di un bene, in particolare di un bene produttivo o d'investimento, provocato da logorio fisico od obsolescenza tecnica, che determina da parte delle imprese investimenti atti a ricostituire il bene stesso. Gli a. devono essere contabilizzati nei bilanci delle imprese, per valutare correttamente il conto economico e il patrimonio dell'impresa e per ricostituire nel tempo il valore dei beni capitali, anche ai fini della loro sostituzione.

In contabilità, l'a. è il procedimento tecnico per ripartire il costo di talune immobilizzazioni a vita definita (materiali e immateriali) in un dato numero d'esercizi futuri, mediante quote che incidono sul calcolo del reddito dei vari esercizi.

(TRECCANI)

(Segue) OIC 13

*“Le rimanenze di magazzino rappresentano beni destinati alla vendita o che concorrono alla loro produzione nella normale attività della società.”*

Anche nel caso delle rimanenze non si riscontrano differenze tra IAS e OIC, l'art 2424 del c.c. descrive le rimanenze come “prodotti finiti o semilavorati, materie prime e merci”, il che comporta nessun contrasto nell'assegnare a tale voce le criptovalute soggette al core business dell'impresa.

Come nel caso dell'OIC 24, anche le rimanenze devono essere rilevate al costo di acquisto o produzione, inclusi gli oneri accessori e valutate invece secondo i criteri: LIFO e FIFO <sup>34</sup> .

L'OIC 13 stabilisce che vi sarà un obbligo periodico di valutazione delle eventuali perdite di valore delle criptovalute a seconda del “ valore di realizzo di mercato”, ma con impossibilità di rilevare incrementi di valore se non nel limite del costo sostenuto per tali beni (OIC 13 par.54)

Classificare quindi le criptovalute come immobilizzazioni immateriali e rimanenze, prova il fatto che l'applicazione di tali principi sia conforme ai postulati di bilancio del Codice civile ovvero:

-art.2423 bis ; postulato della prudenza *“la valutazione delle voci deve essere fatta secondo prudenza”*

-art 2423 bis-1; postulato della rappresentazione sostanziale *“la rilevazione e la presentazione delle voci è effettuata tenendo conto della sostanza dell'operazione o del contratto”*

In conclusione, le modalità di rilevazione contabile delle criptovalute non sono ancora coperte da standard contabili. È pertanto probabile che in futuro gli Standard Setter e le autorità di controllo emetteranno specifiche linee guida, alla luce dell'evoluzione dello scenario di riferimento, che nel caso delle criptovalute è in continuo fermento. (it.Andersen.com)

---

<sup>34</sup> Acronimi per “Last In First Out e First In First Out”, sono approcci basati sulla media ponderata.

## 2.9 CASO AZIENDALE: ORACLIZE

Nel 2015 ad Arezzo è stata costituita una società a responsabilità limitata la "ORACLIZE".

Il socio e fondatore Thomas Bertani può vantare il primato in Italia di aver costituito la prima impresa il cui capitale sociale è stato conferito totalmente tramite criptovalute (bitcoin), un'operazione eseguita con l'assistenza di Stefano Capaccioli, promotore e co-fondatore di AssoB.it, associazione che ha lo scopo di rappresentare le imprese e di promuovere le attività sulla tecnologia Blockchain. (civile.it)

L'operazione è avvenuta tramite il conferimento di 45 bitcoin dal valore (in quel periodo) di poco più di 10.000 euro, il trasferimento delle criptovalute è partito dal wallet di proprietà di Bertani ed indirizzato ad un secondo wallet "intestato" alla società. Detta modalità rende il conferimento effettivo e realizzato in atto, con assoluta tracciabilità e trasparenza dei vari passaggi, con certezza del passaggio della titolarità dei bitcoin e possibilità di verifica degli ulteriori movimenti, essendo operativa fin dalla costituzione. (civile.it)

Tale evento attirò molta attenzione, il primo motivo risiede nella fondazione per la prima volta nella storia italiana di una società con questa modalità di conferimento e il secondo invece è dovuto alla forte volatilità del prezzo delle criptovalute. Soluzione alla forte volatilità delle criptovalute la espose il commercialista dell'operazione Capaccioli, il quale asseriva che nel caso di svalutazione delle valute virtuali pari o superiore a due terzi del conferimento iniziale, si sarebbe effettuato semplicemente un reintegro del capitale sociale mancante. Assimilando quindi la fattispecie di conferimento di capitale tramite criptovalute ai conferimenti di beni in natura, in quanto "le criptovalute sono rappresentazioni digitali di valore".

### 3 Capitale e strumenti finanziari

<b>Capitale sociale in Euro</b>	Deliberato:	10.000,00
	Sottoscritto:	10.000,00
	Versato:	10.000,00
	Conferimenti in natura	
<b>Conferimenti e benefici</b>	INFORMAZIONE PRESENTE NELLO STATUTO/ATTO COSTITUTIVO	

#### strumenti finanziari previsti dallo statuto

Titoli di debito:  
ARTICOLO 23 DELLO STATUTO  
Altri strumenti finanziari:  
ARTICOLO 10 DELLO STATUTO

### 4 Amministratori

Parte di visura ordinaria della Oraclize srl in cui si può notare i "conferimenti in natura"

Mission di Oraclize è *"fornire parte dell'infrastruttura necessaria per costruire applicazioni decentralizzate intelligenti e utili che nella nostra mente giocheranno un ruolo nuovo e importante negli anni a venire"*.

Realizzare una piattaforma per la creazione di smart contracts, contratti auto-eseguibili basati su protocolli informatici e la cui esecuzione è collegata alla risposta automatica di un "oracolo". L' hightech società ha l'obiettivo di realizzare una piattaforma (<http://oraclize.it>) per la creazione di smart contracts - contratti formalizzati da un software che si concludono automaticamente al verificarsi delle condizioni predisposte. I contratti in questione, grazie ai motori di conoscenza sui quali si basa il servizio, possono dipendere da eventi della vita reale oltre a poter essere definiti in modo intuitivo grazie alla funzionalità di riconoscimento del linguaggio naturale. (<http://oraclize.it>).

La società svolge prevalentemente quindi l'attività di gestione e creazione di algoritmi per la gestione di "Oracoli" nonché la prestazione di servizi e consulenza per attività svolte su blockchain e Smart Contract. L'oracolo deve essere inteso in senso figurativo, vale a dire quale emittente di informazioni, espressione o enunciazione cattedratica e sentenziosa, che non ammette né concede alternativa alcuna, quindi vero per definizione.

Oraclize grazie alla consulenza e ai servizi prestati ha contribuito alla creazione di apps decentralizzate, tra queste una menzione d'onore è: *Flight Delay DApp*

Flight Delay DApp è una app che effettua un risarcimento istantaneo nel caso in cui il volo dello user sia in ritardo, una sorta di assicurazione. Gli smart contracts vengono immediatamente elaborati in caso di ritardo del volo permettendo quindi il recupero del costo del biglietto.

Ulteriore smart contract elaborato da Oraclize è il “*Youtube Contract*”, un sistema di deposito a garanzia automatizzato per YouTuber e i loro sponsor.

Motivo di aver sottoposto a studio tale impresa risiede nel presentare quindi un’attività correlata al mondo delle blockchain e quindi delle criptovalute, il bilancio<sup>35</sup> studiato risale all’anno 2015, scelta di tale anno è per analizzare come il redattore del bilancio si sia comportato in assenza delle linee guida dell’IC e degli OIC, lasciando quindi una totale interpretazione soggettiva del professionista.

Nella Nota Integrativa di Oraclize, la prima parte è dedicata all’enunciazione dei principi di redazione contabile, i quali si basano su quelli nazionali

In particolare:

- la valutazione delle voci è stata effettuata secondo prudenza e nella prospettiva della continuazione dell'attività e tenendo conto della funzione economica di ciascuno degli elementi dell'attivo e del passivo;
- i proventi e gli oneri sono stati considerati secondo il principio della competenza, indipendentemente dalla data dell'incasso o del pagamento;
- i rischi e le perdite di competenza dell'esercizio sono stati considerati anche se conosciuti dopo la chiusura di questo;
- gli utili sono stati inclusi soltanto se realizzati alla data di chiusura dell'esercizio secondo il principio della competenza;
- per ogni voce dello stato patrimoniale e del conto economico è stato indicato l'importo della voce corrispondente dell'esercizio precedente, nel rispetto delle disposizioni dell'art. 2423-ter,  
c.c.;
- gli elementi eterogenei ricompresi nelle singole voci sono stati valutati separatamente.

(bilancio Oraclize)

---

<sup>35</sup> Il Bilancio è visionabile su <http://www.capaccioli.net/files/20151231-bilancio-oraclize.pdf>



Evidenziati i principi contabili rispettati nella redazione del bilancio, si può passare all'analisi della contabilizzazione dei bitcoin.

Si ricorda che al momento della stesura del bilancio, non vi era alcuna linea guida che potesse indirizzare il redattore nell'inserire nella più apposita voce contabile le criptovalute. Pacifico, ed evidenziato in nota integrativa, inserire le criptovalute nell'attivo dello stato patrimoniale in quanto esse presentano "un valore". Seguendo il principio di prevalenza della sostanza sulla forma il professionista redattore non considera le criptovalute come un costo.

Il redattore di bilancio cerca di individuare la categoria di attività in cui inserire le criptovalute seguendo gli schemi di cui ai principi contabili internazionali, non giungendo ad una conclusione da un punto di vista oggettivo.

Seguendo lo stesso schema logico dell'IC analizzò quattro principi IAS, ovvero:

- IAS 2 (rimanenze),
- IAS 7 (disponibilità liquide)
- IAS 32 (attività finanziarie)
- IAS 38 (attività immateriali)

Stando ai requisiti enunciati in ogni singolo principio, il redattore non riscontrò alcuna voce che potesse assimilare le criptovalute in essa.

Per quanto lo IAS 2 (le rimanenze), le criptovalute non potevano essere contabilizzate in tale voce a causa della non detenzione per vendita nella normale attività.

Il redattore non ritenne neanche corretto stabilire che fossero disponibilità liquide (IAS7), in quanto, si ricorda che esse non debbano subire forti svalutazioni di valore e prontamente convertibili in denaro (caratteristiche totalmente assenti nelle criptovalute).

L' applicabilità dello IAS 32 era limitata in quanto le criptovalute non possono essere considerate attività finanziarie dato che non vi è alcuna controparte e un'attività in criptovalute non è correlata a una corrispondente passività per un'altra entità. (Bilancio Oraclize)

Infine, per lo IAS 38, le criptovalute rispettavano i primi due presupposti ovvero identificabilità e controllo dall'entità, ma non presentavano i benefici futuri, in quanto essi si ottengono alla vendita delle criptomonete e non alla detenzione.

Il redattore nella ricerca di un inquadramento oggettivo riscontrò un contrasto con il principio di prevalenza della sostanza sulla forma; perciò, appellandosi al principio IAS 8 il quale asserisce che: *“In assenza di un Principio o di una Interpretazione che si applichi specificamente a una operazione, altro evento o circostanza, la direzione aziendale deve fare uso del proprio giudizio nello sviluppare e applicare un principio contabile al fine di fornire una informativa”*

Decise di rappresentare in bilancio le criptovalute come “attività finanziarie” o meglio IAS 32, la cui rilevazione iniziale sarebbe stata effettuata a fair value.

Successivamente alla redazione del bilancio Oraclize (esercizio 2015), l'IC si espresse per chiarire il dilemma rappresentazione contabile delle criptomonete (nei paragrafi precedenti argomento già trattato), il quale stabilì che la più corretta voce da applicare fosse “attività immateriali” ovvero IAS 38.

Compito del redattore, quindi, rispettare le decisioni dell'IC per i bilanci successivi non classificando più le criptovalute come attività finanziarie ma come attività immateriali.

Le criptomonete, quindi, del bilancio Oraclize dovranno essere sottoposte a un cambiamento del principio contabile, tale modifica è regolamentata dall'OIC 29.

In particolare, il principio contabile nazionale asserisce che:

*“Gli effetti dei cambiamenti di principi contabili sono determinati retroattivamente. Ciò comporta che il cambiamento di un principio contabile è rilevato nell'esercizio in cui viene adottato il nuovo principio contabile e i relativi effetti sono contabilizzati sul saldo d'apertura del patrimonio netto dell'esercizio in corso. Solitamente la rettifica viene rilevata negli utili portati a nuovo. Tuttavia, la rettifica può essere apportata a un'altra componente del patrimonio netto se più appropriato”*

Stando a tale principio quindi, in caso di modifica, le criptovalute di Oraclize contabilizzate in attività Finanziarie tramite il Giroconto contabile<sup>36</sup> verranno trasferite nella voce attività immateriali.

---

<sup>36</sup> Il giroconto è un'operazione che genera un trasferimento di denaro tra due conti.

La modifica dovrà essere esplicitata in Nota integrativa come regolamentata da OIC 29:

*“L’articolo 2423-bis, comma 1, numero 6, codice civile stabilisce che i criteri di valutazione non possono essere modificati da un esercizio all’altro. Il comma 2, inoltre, stabilisce che deroghe a tale principio sono consentite in casi eccezionali e che in questi casi la nota integrativa deve motivare la deroga e indicarne l’influenza sulla rappresentazione della situazione patrimoniale e finanziaria e del risultato economico.”*

## **CAPITOLO 3**

### **3.1 ANALISI FISCALE**

*“Tutti sono tenuti a concorrere alle spese pubbliche in ragione della loro capacità contributiva [...]”*

Articolo 53 della Costituzione Italiana

Il fenomeno delle criptovalute ha avuto la sua nascita nel momento della registrazione del dominio Bitcoin.org risalente al 2009, da quel momento sono sorti dubbi sul corretto trattamento fiscale delle criptovalute.

Nel 2016 l’Agenzia delle Entrate tramite la “Risoluzione 72/E”, ha attenuato i problemi che rotavano nella sfera fiscale delle criptovalute e successivamente ha impostato le linee guida per la corretta interpretazione fiscale.

Essa costituisce il punto di riferimento principale, all’interno dell’ordinamento nazionale, per tutti coloro che intendano porre in essere transazioni in valuta virtuale.

La risoluzione ha tratto origine dalla presentazione di un’istanza di interpello da parte di una Società di capitali intenzionata ad eseguire, per conto della propria clientela, operazioni di acquisto e vendita di bitcoin. (Corasaniti)

### 3.2 RISOLUZIONE 72/E -AGENZIA DELLE ENTRATE

La risoluzione ha tratto origine dalla presentazione di un'istanza di interpello da parte di una Società di capitali intenzionata ad eseguire, per conto della propria clientela, operazioni di acquisto e vendita di bitcoin. (Corasaniti)

La Società, che poneva il quesito all'Agenzia delle entrate, chiedeva in particolare di conoscere:

- il corretto trattamento applicabile alle operazioni di acquisto e di cessione di moneta virtuale, ai fini dell'Iva e delle imposte dirette (Ires e Irap);
- se, in relazione alla attività, sia soggetta agli adempimenti in qualità di sostituto d'imposta.

Insieme al quesito il contribuente presentava una soggettiva interpretazione del trattamento fiscale da porre a riguardo delle operazioni che coinvolgevano le criptovalute, ovvero:

1. ai fini dell'Iva<sup>37</sup>, applicare il regime di esenzione in quanto trattasi di operazioni relative a divise, banconote e monete con valore liberatorio di cui all'articolo 135, paragrafo 1, lettera e), della Direttiva 2006/112/CE;
2. ai fini delle imposte dirette, considerare i capital gain (ovvero capital loss) realizzati, ricavi e costi dell'attività caratteristica e, pertanto, farli concorrere, unitamente agli altri costi e ricavi conseguiti, alla determinazione del risultato d'esercizio civilistico e della base

---

<sup>37</sup> L'IVA (Imposta sul Valore Aggiunto) è un'imposta indiretta che riguarda il valore aggiunto della produzione e lo scambio di beni o servizi. Il sistema di detrazione IVA funziona in modo che l'ammontare sia pari al valore dell'IVA sulle vendite meno l'IVA sugli acquisti. (sumup.it)

imponibile Ires<sup>38</sup> ed Irap<sup>39</sup>. Inoltre, nell'ipotesi in cui la Società detenga in proprio bitcoin a fine esercizio, la stessa sarà obbligata a fornirne adeguata informazione in bilancio, tenendo conto del fair value o valore corrente (come per le valute estere tradizionali). In tale ipotesi, gli utili e le perdite su cambi di natura solo valutativa non assumeranno rilevanza fiscale se non al momento del loro effettivo realizzo;

3. non assumere il ruolo di sostituto d'imposta nei confronti della propria clientela e, dunque, non applicare alcuna ritenuta di imposta sulle somme corrisposte ai clienti (Risoluzione 72/E, 2016).

A tale proposta interpretativa l'Agenzia delle Entrate rispose con una precisazione, ovvero: *“Con riferimento al trattamento fiscale applicabile alle operazioni relative ai bitcoin e, in generale, alle valute virtuali, non si può prescindere da quanto affermato dalla Corte di Giustizia dell'Unione europea nella sentenza 22 ottobre 2015, causa C-264/14”*

La quale dimostra come L'Amministrazione nazionale sia conforme ai principi internazionali, utilizzandoli come punto di riferimento.

Sul primo punto dell'interpretazione del contribuente, l'Agenzia delle Entrate asserisce che le operazioni che coinvolgono bitcoin, e per analogia le altre criptovalute, rientrano come prestazioni a titolo oneroso e ai sensi dell'articolo 10, primo comma, n. 3), del d.P.R. 26 ottobre 1972, n. 633 esenti da imposte IVA. la Corte di Giustizia Europea precisa che tali prestazioni ricadono tra le operazioni, compresa la negoziazione, “relative a divise, banconote e monete con valore liberatorio” le quali, come è noto, sono esenti ai fini IVA a norma dell'art. 135, par. 1, lett.e), della Direttiva 2006/112/CE21. (Conte)

Seguendo sempre le direttive europee, ai fini delle imposte dirette (IRES ed IRAP) l'Agenzia riteneva che le società, le quali effettuavano intermediazione nelle operazioni relative alle criptovalute, dovessero subire imposte sul reddito dell'operazione, al netto dei costi dell'attività su menzionata.

---

<sup>38</sup> L'imposta sul reddito delle società (IRES) è una imposta proporzionale e personale che si ottiene tramite applicazione di un'aliquota unica ai profitti delle società (in inglese, questa tassa presente in tutto il mondo si chiama "corporate tax". (Wikipedia.org)

<sup>39</sup> L'imposta regionale sulle attività produttive - IRAP è dovuta per l'esercizio abituale di una attività autonomamente organizzata diretta alla produzione o allo scambio di beni ovvero alla prestazione di servizi. Costituisce in ogni caso presupposto di imposta l'attività esercitata dalle società e dagli enti, compresi gli organi e le amministrazioni dello Stato. (finanze.gov.it)

Per quanto riguarda le criptovalute che al termine dell'esercizio non sono state soggette all'attività di intermediazione ma presenti come disponibilità (a titolo di proprietà) della Società, l'Agenzia ritiene che debbano essere valutati secondo il cambio in vigore alla data di chiusura dell'esercizio e tale valutazione assume rilievo ai fini fiscali ai sensi dell'articolo 9 del testo unico delle imposte sui redditi approvato con d.P.R. 22 dicembre 1986, n. 917 (Tuir)<sup>40</sup>. Occorre, quindi, far riferimento al valore normale, intendendosi per tale il valore corrispondente alla quotazione degli stessi bitcoin al termine dell'esercizio.

A tal fine potrebbe ben farsi riferimento alla media delle quotazioni ufficiali rinvenibili sulle piattaforme on line in cui avvengono le compravendite di bitcoin.

Per terminare la sintesi della Risoluzione 72/E, l'Agenzia delle entrate precisa che a livello di imposte per le persone fisiche (clientela della Società che ha posto il quesito) le operazioni a pronti (acquisti e vendite) di valuta non generano redditi imponibili mancando la finalità speculativa., perciò per la domanda al punto 3, La società non dovrà effettuare il ruolo di sostituto di imposta.

---

<sup>40</sup>. Articolo 9 TUIR

Comma 1 :I redditi e le perdite che concorrono a formare il reddito complessivo sono determinati distintamente per ciascuna categoria, secondo le disposizioni dei successivi capi, in base al risultato complessivo netto di tutti i cespiti che rientrano nella stessa categoria.

Comma 2: . Per la determinazione dei redditi e delle perdite i corrispettivi, i proventi, le spese e gli oneri in valuta estera sono valutati secondo il cambio del giorno in cui sono stati percepiti o sostenuti o del giorno antecedente piu' prossimo [...]

Comma 3: . Per valore normale, salvo quanto stabilito nel comma 4 per i beni ivi considerati, si intende il prezzo o corrispettivo mediamente praticato per i beni e i servizi della stessa specie o similari, in condizioni di libera concorrenza e al medesimo stadio di commercializzazione, nel tempo e nel luogo in cui i beni o servizi sono stati acquisiti o prestati, e, in mancanza, nel tempo e nel luogo piu' prossimi [...]

Comma 4: Il valore normale e' determinato: a) per le azioni, obbligazioni e altri titoli negoziati in mercati regolamentati italiani o esteri, in base alla media aritmetica dei prezzi rilevati nell'ultimo mese; b) per le altre azioni, per le quote di societa' non azionarie e per i titoli o quote di partecipazione al capitale di enti diversi dalle societa', in proporzione al valore del patrimonio netto della societa' o ente, ovvero, per le societa' o enti di nuova costituzione, all'ammontare complessivo dei conferimenti; c) per le obbligazioni e gli altri titoli diversi da quelli indicati alle lettere a) e b), comparativamente al valore normale dei titoli aventi analoghe caratteristiche negoziati in mercati regolamentati italiani o esteri e, in mancanza, in base ad altri elementi determinabili in modo obiettivo. 5. Ai fini delle imposte sui redditi le disposizioni relative alle cessioni a titolo oneroso valgono anche per gli atti a titolo oneroso che importano costituzione o trasferimento di diritti reali di godimento e per i conferimenti in societa'.

### 3.3 IL TRATTAMENTO AI FINI DELLE IMPOSTE INDIRECTE

Il trattamento ai fini IVA per le criptovalute presenta una disciplina armonizzata a livello nazionale in quanto nel 2006 oggetto della direttiva IVA furono gli strumenti di pagamento, includendo quindi indirettamente le valute virtuali. (Razza)

Il primo ordinamento europeo ai fini delle imposte indirette lo si deve alla sentenza della Corte di Giustizia Europea del 2015, emessa post caso "SKATTEVERT<sup>41</sup>- HEDQVIST".

Il caso riguardava il privato sig. HEDQVIST che richiedeva alla commissione tributaria svedese un parere sul trattamento fiscale che dovevano subire i servizi di cambio valute in valute virtuali che intendeva effettuare.

Il parere emesso dalla commissione (successivamente anche la Corte di Giustizia Europea si esprime nella stessa maniera) si concluse nel far ricadere tale caso di servizi di cambio come prestazioni a titolo oneroso, cadendo nella sfera fiscale dell'esenzione IVA.

Il motivo per cui tali servizi rientravano nel caso di esenzione IVA viene descritto accuratamente dalla Corte di Giustizia europea.

Le criptovalute non sono beni materiali, quindi in caso di scambio con valute legali non possono essere inserite nella fattispecie della cessione di beni.

La prestazione è a titolo oneroso in quanto il costo del servizio risiede nel corrispettivo per il cambio.

Il motivo dell'esenzione è dovuto all'art .135 della direttiva IVA, il quale esclude dall'applicazione dell'imposta operazioni relative a "*divise, banconote e monete con valore liberatorio*", includendo le operazioni quindi cambio valuta tradizionale/virtuale.

In Italia successivamente alla sentenza della Corte di Giustizia Europea, L'Agenzia delle entrate tramite la, su citata, risoluzione 72/E ha richiamato i principi della Corte; assimilando le criptovalute come valute estere, le cui operazioni sono prestazione di servizi a titolo oneroso e quindi esenti IVA. Conseguenza dell'esenzione IVA, quindi, è che gli exchanger che svolgono attività di cambio valute non potranno dedurre IVA sostenuta su acquisti di beni e servizi relativi al loro business.

---

<sup>41</sup> L'amministrazione finanziaria svedese



### 3.4 IL TRATTAMENTO AI FINI DELLE IMPOSTE DIRETTE

Ricapitolando, l’Agenzia si è espressa a favore dell’equiparazione delle criptovalute a quelle estere aventi corso legale, precisando che *“le operazioni a pronti (acquisti e vendite) di valuta non generano redditi imponibili mancando la finalità speculativa”*. Tale posizione è stata declinata in termini forse eccessivamente generici, senza un adeguato coordinamento con la normativa fiscale nazionale: come è noto, infatti, secondo l’articolo 67 del d.P.R. n. 917/1986 (TUIR), sono imponibili non solo le cessioni a termine di valute estere, ma anche quelle a pronti, seppure al ricorrere di talune condizioni. (Commissione Tax&Legal, Approfondimenti, maggio 2018). Per precisare meglio questa posizione l’Agenzia delle entrate ha esplicitato come trattare fiscalmente ai fini delle imposte dirette le operazioni in criptovaluta.

Ai sensi dell’art.67, comma 1 lett.c-ter e comma 1 ter del TUIR, le operazioni di criptovalute detenute al di fuori del regime di impresa (detenute nella sfera del privato) generano redditi ai fini fiscali, imponibili.

Ciò significa che, ai fini IRPEF, ogni conversione di criptovaluta in altra valuta virtuale o a corso legale è rilevabile per

1. cessioni a termine<sup>42</sup>
2. cessioni a pronti<sup>43</sup>

Per il secondo punto viene specificato che la cessione a pronti è rilevabile ai fini IRPEF se la giacenza media del detentore di criptovalute presenta un controvalore di 51.645,69 euro per più di sette giorni lavorativi.

Si parla di giacenza “media”, seppur in assenza di tale termine nella norma, a causa dell’estrema volatilità del mercato delle criptovalute che presenta dei costanti “Sali e scendi” nel valore della moneta virtuale.

---

<sup>42</sup> Il cambio a termine (anche detto tasso di cambio forward o Forward Exchange Rates) è il prezzo di negoziazione di quelle operazioni in cui il ritiro e il pagamento della quantità trattata si effettua a partire dal terzo giorno lavorativo dopo la data della compravendita. Siamo perciò di fronte a un acquisto o a una vendita la cui consegna è “differita”, pur essendo fissato il prezzo all’istante

<sup>43</sup> Il cambio a pronti (anche detto tasso di cambio spot o Spot Exchange Rate) è il prezzo di negoziazione di quelle operazioni di acquisto o vendita di valuta estera in cui il ritiro e pagamento delle quantità trattata avviene il secondo giorno lavorativo dopo la data della compravendita. (solofinanza.it)

La giacenza, inoltre, va calcolata sulla base del rapporto di cambio al 1° gennaio, rilevato sul sito dove il contribuente ha acquistato la valuta virtuale o in mancanza quello dove ha effettuato la maggior parte delle operazioni. (Commissione Tax&Legal, Approfondimenti, maggio 2018).

Viene ipotizzata quindi una natura finanziaria delle operazioni di criptovaluta e ai sensi dell'art. 67, comma 1, lett. da c)-bis a c)-quinqües del TUIR, il contribuente dovrà dichiarare nel quadro RT le plusvalenze ottenute dall'operazione di cambio valuta.

SEZIONE II Plusvalenze assoggettate a imposta sostitutiva del 26%	RT21	Totale dei corrispettivi			,00
	RT22	Totale dei costi o dei valori di acquisto (costo rideterminato <sup>1</sup> ) (costo affrancato <sup>2</sup> )		<sup>3</sup>	,00
	RT23	Plusvalenze (RT21 – RT22 col. 3) (ovvero Minusvalenze <sup>1</sup> ,00 )		<sup>2</sup>	,00
	RT24	Eccedenza minusvalenze (anni prec. <sup>1</sup> ,00 Sez. I <sup>2</sup> ,00 Sez. III <sup>3</sup> ,00 )	<sup>4</sup>	,00	
	RT25	Eccedenza delle minusvalenze certificate dagli intermediari (di cui anni precedenti <sup>1</sup> ,00 )		<sup>2</sup>	,00
	RT26	Differenza (RT23 col. 2 – RT24 col. 3 – RT25 col. 2)			,00
	RT27	Imposta sostitutiva (26% dell'importo di rigo RT26)			,00
	RT28	Eccedenza d'imposta sostitutiva risultante dalla precedente dichiarazione non compensata			,00
	RT29	IMPOSTA SOSTITUTIVA DOVUTA			,00

Quadro RT dell'UNICO. Fonte FISCOETASSE.COM

Il quadro RT componente del modello Unico<sup>44</sup> (o meglio redditi PF), presenta il rigo RT27 corrispondente a “Imposta sostitutiva”, pari al 26%.

Per la determinazione della plusvalenza, utile per la compilazione del quadro RT, derivante dalle operazioni tipiche delle criptovalute, è necessario individuare come valore di riferimento il costo d'acquisto o, nel caso in cui la valuta virtuale venga acquisita per donazione, il costo sostenuto dal donante ai sensi dell'art. 68 co. 6 del T.U.I.R. considerando cedute per prime le criptovalute acquisite più recentemente (cd. criterio del “Last In First Out” o “L.I.F.O.”). (criptovalute-tassazione-e-calcolo-delle-plusvalenze, s.d.).

L'articolo: “*Risposta (non pubblica) all'interpello n. 956-39/2018: profili fiscali della detenzione di criptovalute da parte di persone fisiche residenti in Italia*” a cura di Fabrizio Cancelliere e Armando Tardini, pone un dubbio riguardo l'equiparazione delle criptovalute delle valute estere da parte dell'Agenzia delle entrate.

<sup>44</sup> Il modello Redditi PF (ex Unico) è il modello ordinario di dichiarazione dei redditi; si tratta di un modello unificato tramite il quale è possibile effettuare più dichiarazioni fiscali. A differenza del modello 730, nel modello Redditi (Unico) i versamenti delle imposte sono effettuati direttamente dal contribuente attraverso il modello F24, che deve essere presentato in banca o in posta. Il contribuente può effettuare direttamente la compilazione del modello ed i calcoli dei versamenti o può richiedere assistenza alla compilazione ai CAF, ai professionisti e agli Uffici dell'Agenzia delle Entrate appositamente abilitati a svolgere questa attività.(cafcisl.it)

Nell'articolo si evince che non vi sia una perfetta coerenza con la nuova definizione fornita dalla normativa antiriciclaggio, in base alla quale le criptovalute sono definite come *“rappresentazione digitale di valore non necessariamente collegata a una valuta avente corso legale”*, inoltre paragonare i “wallet” del cripto ai depositi bancari presenta un'incoerenza riguardo l'IVAFE (paragrafo successivo) e il monitoraggio fiscale nel quadro RW. La detenzione del cripto all'interno dei wallet (procedura necessaria data la natura digitale), le plusvalenze originate da detenzione e conversione saranno sempre tassabili e questo è totalmente differente dai depositi bancari delle valute a corso legale.

Intenzione dell'Amministrazione probabilmente è trovare un punto di incontro tra la natura finanziaria speculativa delle criptovalute e quella di mezzo di pagamento, in attesa di norme più specifiche per il nuovo mondo digitale.

Da precisare però che i contribuenti, originati dalle plusvalenze delle operazioni delle criptovalute, godono di vantaggi fiscali rispetto ai contribuenti delle “valute ordinarie”, un esempio: l'esenzione dall'IVAFE, argomento che verrà trattato nel successivo paragrafo.

#### *(Segue) Criptovalute e IRAP*

Particolare è il caso dell'imponibilità per le imprese ai fini IRAP (imposta regionale su attività produttive) sulle criptovalute.

La base imponibile IRAP è regolamentata dall'art.5 del Dlgs 446/1997, il quale asserisce che la base imponibile è data dalla differenza tra valore della produzione e costo della produzione, le lettere rispettivamente A) e B) dell'art.2425 del Codice civile (escludendo voci 9-10c-d-12 e 13), e la differenza tra componenti positivi e negativi straordinari.

Non essendoci alcuna regola specifica a riguardo per le criptovalute, e date le risultanze contabili, si può affermare che esse sono rilevabili ai fini IRAP.

La loro classificazione e qualificazione contabile come immobilizzazione immateriale o rimanenza, comporta quindi effetti positivi/negativi a livello di base imponibile IRAP. (Giacomelli)

### 3.5 IVAFE E MONITORAGGIO FISCALE

La disciplina del monitoraggio fiscale è stata introdotta nel nostro ordinamento dal D.L. n. 167/90, convertito poi dalla Legge n. 227/90.

Il monitoraggio è un adempimento obbligatorio che coinvolge tutti i contribuenti *fiscamente*<sup>45</sup> residenti in Italia.

Mission del monitoraggio fiscale è il controllo e limite alle movimentazioni finanziarie al fine di prevenire atti illegali da parte dei contribuenti.

Soggette al monitoraggio fiscale sono le attività finanziarie estere. Nell'elenco di tali attività, menzioni onorevoli sono:

- Attività i cui redditi sono corrisposti da soggetti non residenti, rientrano in questa categoria: le partecipazioni al capitale o al patrimonio di soggetti non residenti, certificati di massa, obbligazioni estere, depositi in conti correnti esteri e valute estere.
- Contratti di natura finanziaria stipulati da almeno una delle parti non residente
- Metalli preziosi detenuti all'estero

Le attività finanziarie estere vanno sempre indicate nel quadro RW, e secondo l'Agenzia delle entrate, a prescindere dalla loro capacità di produrre redditi imponibili in Italia o che abbiano prodotto redditi imponibili nel periodo d'imposta di competenza.

Codice titolo possesso	Vedere istruzioni	Codice individuaz. bene	Codice Stato estero	Quota di possesso	Criterio determin. valore	Valore iniziale	Valore finale			
1	2	14	VUOTA	100	1	60.000,00	70.000,00			
Valore massimo c/c paesi non collaborativi		Giorni (IVA FE)		IVA FE		Mesi (IVIE)				
9	10	11	12	13			,00			
Credito d'imposta		IVA FE dovuta		Detrazioni		IVIE dovuta		Vedere istruzioni	Quota partecipazione	Solo monitoraggio
14	15	16	17	18	19	20				
Codice fiscale società o altra entità giuridica in caso di titolare effettivo		Codice fiscale altri cointestatori								
21	22	23	24							

QUADRO RW. Fonte MyAccounting.it

<sup>45</sup> È residente in Italia ai fini delle imposte sui redditi chi per la maggior parte dell'anno (almeno 183 giorni l'anno, 184 in quelli bisestili) è iscritto nell'Anagrafe delle persone residenti in Italia, oppure ha il proprio domicilio o la propria dimora abituale in Italia. Sono, inoltre, considerati residenti in Italia i cittadini italiani cancellati dalle anagrafi della popolazione residente ed emigrati in Stati o territori aventi un regime fiscale privilegiato, individuati con il decreto del Ministro delle Finanze 4 maggio 1999 e successive modifiche ed integrazioni. (agenziaentrate.gov.it)

La detenzione di attività finanziarie estere è passibile di imposta patrimoniale, ovvero l'IVAFE.

L'IVAFE presenta un'aliquota del 0,2%, in origine, l'imposta era dovuta dalle sole persone fisiche residenti. A partire dal primo gennaio 2020, invece, essa risulta dovuta anche:

- Dagli enti non commerciali, tra cui anche i trust e le fondazioni;
- Dalle società semplici e gli enti alle stesse equiparati (ex art. 5 del TUIR).

Inoltre, al fine di uniformare la disciplina IVAFE al prelievo previsto dall'imposta di bollo sui conti correnti ed i prodotti finanziari, l'art. 134 del D.L. n. 34/2020 ha modificato l'art. 19 co. 20 del D.L. n. 201/2011 stabilendo:

- La misura fissa di 100,00 euro per l'IVAFE applicabile sui conti correnti e i libretti di risparmio dei soggetti diversi dalle persone fisiche;
- La misura massima dell'imposta dovuta dai soggetti diversi dalle persone fisiche, in misura pari a 14.000 euro come previsto per l'imposta di bollo.

Requisito per essere soggetti all'IVAFE è che le attività siano tenute in custodia e/o depositate presso intermediari non residenti, stesso dicasi per le cassette di sicurezza ubicate all'estero o in luoghi fuori dal territorio nazionale.

Le attività finanziarie estere sono imponibili IVAFE in caso di detenzione per titolo di proprietà o altro diritto reale, nessuna modalità di acquisizione, sia essa acquisto, successione ereditaria o donazione, non presenta alcuna esclusione dall'applicazione di IVAFE.

L'Amministrazione necessita del monitoraggio fiscale, inoltre, per svolgere raccolta di informazioni utili per svolgere attività di accertamento<sup>46</sup> nei confronti dei patrimoni esteri.

Effettuata una breve introduzione alla disciplina del monitoraggio fiscale e dell'IVAFE, si può passare ora all'interpretazione che ha dato a riguardo l'Agenzia.

---

<sup>46</sup> L'accertamento fiscale è volto ad individuare i contribuenti che hanno effettuato trasferimenti fittizi di residenza all'estero è un tema centrale nell'ambito dell'attività accertativa effettuata dall'Agenzia delle Entrate e della Guardia di Finanza. (fiscomania.com)

Assunzione di partenza è che l'Amministrazione ritiene le criptovalute assimilabili a valute estere, o meglio, attività finanziarie estere (per analogia di trattamento fiscale delle monete estere). Conseguenza di tale assunzione è che i detentori di criptovalute, collocate in sistemi non residenti, saranno soggetti alla compilazione del quadro RW.

Ricordando l'immagine, le criptovalute vanno indicate in colonna 3 corrispondente a "Altre attività estere di natura finanziaria e valute virtuali" omettendo la colonna 4 "Codice di stato estero", l'omissione è dovuta all'aterritorialità delle criptovalute (essendo di natura digitali).

La normativa a riguardo della compilazione del quadro RW prevede che se le valute estere gestite da intermediari residenti, non prevede alcun obbligo. Per quanto riguarda la figura di intermediari residenti, tramite la Direttiva 2015/849 dell'UE per l'antiriciclaggio, sono stati introdotti due nuove figure, ovvero, i *custodial wallet* e gli *exchanger*, i quali sono per definizione "ogni 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".

Da sottolineare però che con l'introduzione di questi soggetti economici, la funzione del monitoraggio fiscale perde la sua efficacia in quanto funzione degli intermediari residenti è quella di svolgere la funzione di sostituti d'imposta, ruolo che cade nel campo delle criptovalute.

Altro motivo per cui si necessita un ordinamento ben più specifico nell'ambito di tali assets.

Ulteriore particolarità normativa riguardo la dichiarazione del quadro RW è il caso delle criptovalute detenute in chiavi private, cioè quelle non detenute da un intermediario, il che comporta un'incapacità nel rilevare la localizzazione del detentore del crypto. In un caso del genere la normativa alla dichiarazione in RW in quanto "attività estere detenute in Italia al di fuori del circuito degli intermediari residenti".

Per quanto riguarda il valore da iscrivere nel quadro RW, la normativa prevede che le attività estere sia valorizzate al prezzo di mercato, solo se quest'ultimo è regolamentato, riconosciuto e aperto al pubblico.

L'Agenzia con la Circolare 32/E definisce "mercato regolamentato", un istituto dotato di organizzazione con regole precise per una negoziazione sicura ed efficiente, riconosciuto da autorità competenti e infine capace di incrociare domanda e offerta del pubblico.

Le piattaforme di scambio valute (exchange), però, non coincidono con la definizione dell’Agenzia, non essendo riconosciute da alcuna autorità.

Questo è il motivo per cui le criptovalute all’interno del quadro RW vengono iscritte al loro **costo storico**, non presentando un valore nominale e di rimborso. (Andreoli)

Importante cenno va effettuato riguardo la soglia dei 15000 euro del monitoraggio fiscale.

L’ordinamento prevede che i soggetti che detengono nel proprio deposito bancario una somma superiore a 15000, sono esonerati dall’obbligo di monitoraggio fiscale.

L’applicabilità di tale franchigia sarebbe quindi coerente con il concetto di assimilare i wallet del cripto a depositi bancari ordinari.

Eppure, nonostante questa assimilazione, i wallet delle criptovalute non sono soggetti all’imposta IVAFE, ricordando la circolare 28/E dell’Agenzia delle Entrate, la quale asserisce che l’imposta debba essere applicata ai solo depositi di natura “bancaria”, esonerando perciò i wallet.

### 3.6 LE CRIPTOVALUTE E L'ORDINAMENTO USA

Data la recente nascita del fenomeno delle criptovalute insieme ad una diffusione rapida ed estremamente massiva, vi sono notevoli differenze a livello di regimi fiscali tra i vari paesi.

Questo paragrafo ha la funzione di descrivere sinteticamente il regime fiscale delle criptovalute nell'ordinamento USA e confrontarlo con il regime fiscale, precedentemente descritto, di quello italiano.

Da precisare che l'ordinamento statunitense ha avuto una reazione più decisa nei confronti della regolamentazione delle criptovalute rispetto a quello europeo e, quindi, italiano.

La guida fiscale statunitense è stata emessa nel 2019 da parte dell'International Revenue service (IRS), il corrispettivo della nostra Agenzia delle entrate.

L'IRS definisce i bitcoin e le restanti criptovalute come valute virtuali *convertibili*, definizione che risulta estremamente corretta, in quanto ormai è certo che le criptovalute assolvono funzione di unità di pagamento per beni e servizi ma anche come forma di investimento, essendo possibile la negoziazione digitale fra utenti, tramite il cambio criptovaluta/criptovaluta o criptovaluta/valuta legale.

In alcuni ambienti statunitensi, da sottolineare, le criptovalute (in particolar modo bitcoin) svolgono la funzione di moneta reale come il dollaro statunitense nonostante la loro natura non legale e quindi di non riconoscimento da parte della giurisdizione.

Prima dell'uscita della guida fiscale statunitense i proprietari di criptovalute americani godevano di una situazione non regolamentata e quindi una sorta di paradiso fiscale delle nuove tecnologie.

L'IRS ha stabilito di tassare le criptovalute come un bene immobiliare quindi ai fini fiscali federali, le valute virtuali sono trattate come una proprietà, non come una valuta.

Conseguenza di tale assunzione è che alle transazioni in valuta virtuale si applicano i principi generali di tassazione applicate alle transazioni di proprietà.

Il proprietario delle valute virtuali convertibili, quindi, sarà obbligato a dichiarare il loro possesso, similmente al possesso delle azioni. (cryptonomist.ch, s.d.)



Conseguenza è la dichiarazione del capital gain (le nostre plusvalenze) delle transazioni cripto, il quale è soggetto ad aliquota fiscale pari (al momento) a 23,48%.

Il capital gain si calcola tramite la seguente formula:

Valore equo di mercato - [(Prezzo di acquisto della criptovaluta + Altre spese) / Quantità di proprietà] = Capital gain/perdita di capitale

([www.orcom.fr](http://www.orcom.fr), s.d.)

## Capitolo 4

### 4.1 Le Controversie delle Criptovalute

Dopo aver descritto: storia, caratteristiche, classificazione contabile e trattamento fiscale delle criptovalute; è importante ora elencare e descrivere le controversie che le riguardano.

In aprile del 2021 Elon Musk CEO di Tesla<sup>47</sup>, azienda che da febbraio dello stesso anno aveva cominciato ad accettare i bitcoin come mezzo di pagamento, dichiarò avrebbe effettuato un cambio di rotta non accettando più tali criptovalute in cambio dei suoi prodotti per via del loro alto consumo energetico, e quindi, non andando contro la mission dell'azienda stessa, ovvero essere altamente sostenibile.

L'impatto ambientale è uno dei molti lati negativi delle criptovalute.

È risaputo che tramite le criptovalute, in particolare bitcoin, il terrorismo - stesso dicasi per la criminalità organizzata- è stato finanziato grazie alle operazioni di scambio valute.

Ulteriore elemento negativo delle criptovalute è la possibilità di riciclaggio di denaro.

Sostanzialmente le criptovalute sono una leva all'innovazione tecnologica di vari settori economici ma anche una leva per aumentare le attività illecite e/o nocive.

### 4.2 L'IMPATTO AMBIENTALE

Le criptovalute dal momento della loro nascita hanno raggiunto un prezzo di mercato estremamente elevato (bitcoin ha raggiunto il picco di 63000 euro) nella prima metà del 2021, successivamente al tweet di Musk il prezzo delle criptovalute ha risentito di una forte contrazione. Probabilmente uno dei motivi di tale contrazione del valore di mercato può essere a causa dell'inquinamento effettuato dalle operazioni che coinvolgono le criptovalute.

Dalla pubblicazione del tweet la pubblicità dell'impatto ambientale di queste criptovalute si è accentuata notevolmente, pubblicità che ha fornito molti dati utili.

---

<sup>47</sup> Tesla è un'azienda statunitense specializzata nella produzione di auto elettriche, pannelli fotovoltaici e sistemi di stoccaggio energetico

Elemento incisivo sull'inquinamento ambientale è il mining, per l'estrazione delle criptovalute le macchine consumano enormi quantità di energia, proveniente principalmente da combustibili fossili, tra cui spicca in negativo il carbone, una tra le fonti più inquinanti.

Si è registrato che solo nel 2021 la produzione annuale di anidride carbonica è di circa 37 milioni di tonnellate, pari al volume di un Paese come la Nuova Zelanda, mentre il consumo di energia elettrica è di quasi 78 terawattora, pari a quello di un paese come la Colombia.

Secondo digiconomist, sito citato da diverse testate giornalistiche, una singola transazione in Bitcoin consuma quanto 1 122 196 pagamenti con una carta Visa, equivalenti a 36 giorni di consumo elettrico di una casa di una famiglia media americana e pari a guardare youtube per 84 388 ore. Si stima, secondo diverse testate indipendenti, tra cui cbs che solo il 40% dell'energia consumata dalle criptovalute sia da fonti rinnovabili, e il restante 60% provenga da combustibili fossili. Se il prezzo delle criptovalute salisse, salirebbero anche i consumi elettrici, al momento pari a quelli dell'Argentina per il solo Bitcoin. (wikipedia)

Le contromisure a questo inquinamento ambientale causato dalle criptovalute si sono avviate.

Un esempio è l'Iran, nel paese erano stati registrati un numero rilevante di blackout causati dal mining del cripto, e quindi, come misura a bloccare un così eccessivo consumo di risorse energetiche le autorità hanno avviato il sequestro di mining machine e vietando categoricamente tale attività.

Eventuale contromisura è quella di applicare un'imposta sull'attività stessa del mining. Questa contromisura risulterebbe estremamente proficua per il paese che applica tale tassa in quanto riceverebbe entrate finanziarie da parte di un mercato estremamente ricco e (come messo in evidenza nel precedente capitolo) non ancora pienamente tassato.

Conseguenza di questa imposta però potrebbe essere l'ulteriore contrazione del prezzo delle monete digitali.

Una svolta alla lotta all'inquinamento delle criptovalute però, può provenire dagli *Accordi Climatici Crypto*, ispirati a quelli di Parigi del 2015.

Questa iniziativa parte dal presupposto di rendere le criptovalute "green", o meglio punta alla decarbonizzazione dell'industria crypto entro il 2025, ma soprattutto, nella prospettiva ESG, intende mettere a disposizione standard open source per la misurazione delle emissioni legate alla cryptocurrency industry. (Bellini)

Obiettivo finale di questi accordi è quello di rendere il mondo delle cripto, un mondo che sfrutta il 100% delle risorse rinnovabili nel minor tempo possibile.

Gli accordi puntano ad ottenere una sintesi tra le esigenze di riduzione dell'impatto ambientale collegate al mondo blockchain e le opportunità di sviluppo che stanno accompagnando queste tecnologie con la prospettiva di supportare la diffusione di soluzioni crypto che possano aiutare tante e diverse industry ad essere più sostenibili. (digital-for-esg, s.d.)

Ottenere questa sostenibilità è possibile se vi è una forte innovazione tecnologica a riguardo, sfruttare al massimo le energie rinnovabili e infine che la community degli accordi si espanda sempre di più, dando la possibilità a ogni componente della stessa di apportare un forte contributo a tale causa. La sostenibilità è un requisito oramai fondamentale per le politiche di sviluppo delle imprese, utile a renderle più competitive possibile sul mercato; infatti, i parametri ESG sono parametri che influenzano notevolmente la scelta di un determinato investimento.

Nella community degli Accordi climatici Crypto hanno aderito Ripple CoinShares e ConsenSys, mostrando come il mondo delle nuove tecnologie stia allungando il proprio sguardo verso un mondo totalmente sostenibile.

Un'altra soluzione prettamente italiana sembra arrivare da una startup trentina, *Free Seas Società Benefit*<sup>48</sup>, che vuole unire un sistema digitale di emissione crediti (cioè i token) con il finanziamento di progetti di rigenerazione ambientale.

Il fatto di utilizzare la blockchain diventa un valore aggiunto, dando la garanzia che i progetti ambientali siano vidimati da tutti ciò che vogliono partecipare, perché saranno essi stessi i finanziatori: l'obiettivo a lungo termine è la creazione di un mercato italiano del credito per la rigenerazione ambientale, in cui i token – che attestano la rigenerazione avvenuta – vengano accettati come credito fiscale (o altra forma incentivante) per imprese e privati virtuosi, in quanto concreto investimento a beneficio della collettività.

---

<sup>48</sup> Le società benefit presentano la caratteristica di avere nella ragione sociale il perseguimento sia dello scopo di lucro sia di svolgere attività volte al beneficio sociale e ambientale.

Dal Gennaio 2016 in Italia sono state introdotte, e questo ha reso l'Italia il secondo stato sovrano al mondo - dopo gli USA - a riconoscere questa tipologia di azienda a scopo di lucro. In Italia si contano oltre 900 società benefit, in decine di settori diversi. Queste sono cresciute in modo esponenziale durante la pandemia da Covid-19, durante la quale molte aziende italiane hanno deciso di implementare questa nuova forma giuridica. (wikipedia)

Con questa startup, che sta raccogliendo finanziatori su eppela per il progetto pilota di raccolta di rifiuti in mare, potrebbe nascere allora la prima criptovaluta green italiana: i CfER - acronimo di Coin for Enviromental Regeneration - saranno emessi nel numero finito di 13 miliardi di token, con cui finanziare i progetti di rigenerazione da acquistare sia con valuta corrente che con altre criptovalute.

Con questa raccolta fondi verrà effettivamente validato lo schema di valutazione dell'impatto generato da un problema ambientale, in modo che sia replicabile e scalabile nelle diverse situazioni, realizzando allo stesso tempo la piattaforma blockchain e avviando la produzione di CfER. (bitcoin-inquinamento, s.d.)

### **4.3 IL RICICLAGGIO DI DENARO**

Capitali generati da attività illecite che sono stati sottoposti ad operazioni di "pulizia", attribuendo loro un'origine falsamente lecita, questo è il riciclaggio di denaro.

Svolgere tale attività rientra nella sfera del penale, essendo un reato economico, politico e statale.

Wikipedia definisce il riciclaggio come un "ponte" tra società civile e criminalità, i flussi di denaro riciclato in Italia risulta pari al 10% del PIL nazionale, ciò fa comprendere come questo reato sia rilevante e come la criminalità organizzata sia fortemente infiltrata nel tessuto economico del bel paese.

Le fasi del riciclaggio sono tre:

- Placement
- Layering
- Integration

Il Placement consiste nella raccolta dei capitali ottenuti dalle attività illecite e successivamente depositato da un intermediario finanziario.

Il Layering o stratificazione (in italiano) è la fase più complessa in cui i capitali vengono utilizzati per particolari operazioni finanziarie al fine di cancellare la traccia della natura illecita degli stessi. L'integration è la fase affidata a professionisti i quali trasferiscono in determinate economie statali in cui vige un forte segreto finanziario (isole Cayman è uno degli esempi più noti), permettendo quindi ai capitali di circolare in maniera totalmente "pulita".

Per contrastare quindi il riciclaggio di denaro il dlgs 231 del 2007 , e successiva integrazione da parte del dlgs 90/2017, delinea determinati obblighi a cui devono sottostare gli intermediari finanziari, ovvero conoscere la clientela, tracciare le transazioni ,individuazione ed eventualmente segnalazione dell'attività sospetta.

Base per la lotta al riciclaggio è totale trasparenza di ogni singola fase del ciclo del denaro, ma questa trasparenza nel protocollo di Nakamoto (Bitcoin) non è possibile ottenerla in quanto si ricorda la presenza di anonimato e decentralizzazione.

Sulla blockchain ogni transazione viene registrata e la sua cancellazione o modifica è altamente impossibile, il sistema permette però un alto anonimato in quanto le parti della transazione possono utilizzare un pseudonimo e poter nascondere l'indirizzo IP<sup>49</sup> del proprio device, non concedendo quindi l'individuazione della località degli stessi.

Questo è il motivo per cui le criptovalute sono uno strumento altamente utilizzato per l'attuazione del riciclaggio.

Riciclaggio che grazie al dark web, ha ridotto drasticamente le fasi, in quanto vi è un'estrema accessibilità all'acquisto di armi o droga, mettendo in diretto contatto l'acquirente con il venditore, senza alcun rischio di tracciamento dell'operazione.

Il riciclaggio di denaro tramite criptovalute, inoltre, si è ampiamente diffuso grazie anche al totale abbattimento delle frontiere fisiche grazie alla completa digitalizzazione del mercato.

Al fine di prevenire e contrastare tale fenomeno i Legislatori nazionali sono intervenuti immediatamente e in maniera decisa.

La normativa antiriciclaggio ha subito modifiche tramite il d.lgs. 125/2019, la quale asserisce che i prestatori di servizi di valute virtuali sono soggetti agli obblighi delle norme antiriciclaggio presenti nel d.lgs. 2007.

I prestatori di servizi oltre alle già citate attività di contrasto al riciclaggio come conoscenza del cliente ed individuazione dell'attività illecite, devono adempiere all'obbligo di forzare il controllo delle operazioni effettuate nel sistema tecnologico che gestiscono, per via della possibilità di anonimato.

Segnalata l'operazione sospetta, ovviamente, spetta all'Autorità che ha ricevuto l'input attribuire l'ipotesi di reato.

---

<sup>49</sup> Un indirizzo IP (dall'inglese Internet Protocol address) – in informatica e nelle telecomunicazioni – è un'etichetta numerica che identifica univocamente un dispositivo detto host collegato a una rete informatica che utilizza l'Internet Protocol come protocollo di rete ([www.mio-ip.it](http://www.mio-ip.it))

Ulteriore strumento di repressione sono le sanzioni, il titolo V del D. Lgs. 21.11.2007, n. 231, contiene una nutrita serie di “disposizioni sanzionatorie” di natura sia penale (art. 55) che amministrativa (artt. 56-58), mentre il reato di “indebito utilizzo e falsificazione di carte di credito e di pagamento”, inizialmente previsto dal comma 5 e 6 del già citato art. 55, è oggi disciplinato dall’art. 493 ter cod. pen. ([www.altalex.com](http://www.altalex.com))

In conclusione, il riciclaggio è una fattispecie già conosciuta nell’ordinamento dei paesi, i quali sono provvisti di mezzi per intercettare il reato e coloro che lo compiono potendoli sanzionare. L’integrazione del 125/2019 rende meno problematico il fenomeno del riciclaggio tramite le criptovalute, avendo le norme a supporto per affrontarlo.

#### **4.4 IL FINANZIAMENTO DEL TERRORISMO**

Nel settembre 2021, nella cittadina di Leicester, un certo Hisham Chaudary , un uomo sui 30 anni, fu arrestato dalle forze dell’ordine inglesi con l’accusa di aver collaborato alla raccolta di capitali per finanziare le organizzazioni terroristiche, tra queste l’ISIS<sup>50</sup>.

L’uomo prima dell’arresto era reputato un cittadino ordinario, senza alcun sospetto di collegamento ad una delle cellule terroristiche più temibili degli ultimi anni.

La sua raccolta di capitali e, successivamente, distribuzione alle organizzazioni terroristiche avveniva tramite piattaforme exchange, acquistava quindi criptomonete (bitcoin) che poi inviava all’ISIS, la quale tramite il cambio valuta otteneva moneta legale. Le criptovalute in questo caso non avevano funzione di mezzo di pagamento o investimento bensì una funzione “traghettrice” di capitali.

---

<sup>50</sup> Nome che si è dato a un'organizzazione jihadista salafita attiva in Siria, Yemen e Iraq, dove fino al 2017 controllava militarmente un ampio territorio. Il suo capo Abu Bakr al-Baghdadi ha proclamato la nascita di un califfato nei territori caduti sotto il suo controllo in un'area compresa tra la Siria nord-orientale e l'Iraq occidentale il 29 giugno 2014. Nonostante questo gruppo dichiarò di fondarsi sulla religione Islamica sunnita, molti leader del mondo islamico hanno sostenuto l'illegittimità della proclamazione e il contrasto dell'ideologia del gruppo con la dottrina religiosa. A questa organizzazione si attribuiscono svariati attentati avvenuti a cavallo tra il 2015-2019, purtroppo tra i più famosi si ricordano l’attentato al Bataclan, Charlie Hebdo.

Ovviamente questo non è il solo caso di fundraising del terrorismo tramite criptovalute; infatti, stando ai dati di “COINBASE<sup>51</sup>” il mercato delle criptovalute presenta una percentuale di domanda proveniente proprio dalle organizzazioni terroristiche. Il flusso di capitali dovuto ad operazioni che coinvolgono come una delle parti i terroristi consiste almeno l’1% delle transazioni totali all’interno della blockchain, che espresso in termini monetari, si aggira intorno a 500 milioni di dollari.

Il terrorismo islamico, bisogna precisare, ha saputo sfruttare al meglio le innovazioni tecnologiche offerte dal mondo della blockchain finanziando le sue attività e reclutando anche adepti. (Razzante)

Sono stati lanciati nei vari anni siti web in cui si invitava a vari adepti a donare bitcoin su wallet indicati. Nell’immagine sottostante uno di questi casi.



La propaganda di raccolta fondi lanciata dalle organizzazioni terroristiche. Fonte contecorrenteonline.it

Questo probabilmente è uno degli aspetti più tenebrosi legati al mondo delle criptovalute, ovvero la semplicità con cui tali organizzazioni lancino propagande di raccolta fondi per via dell’assenza di barriere.

---

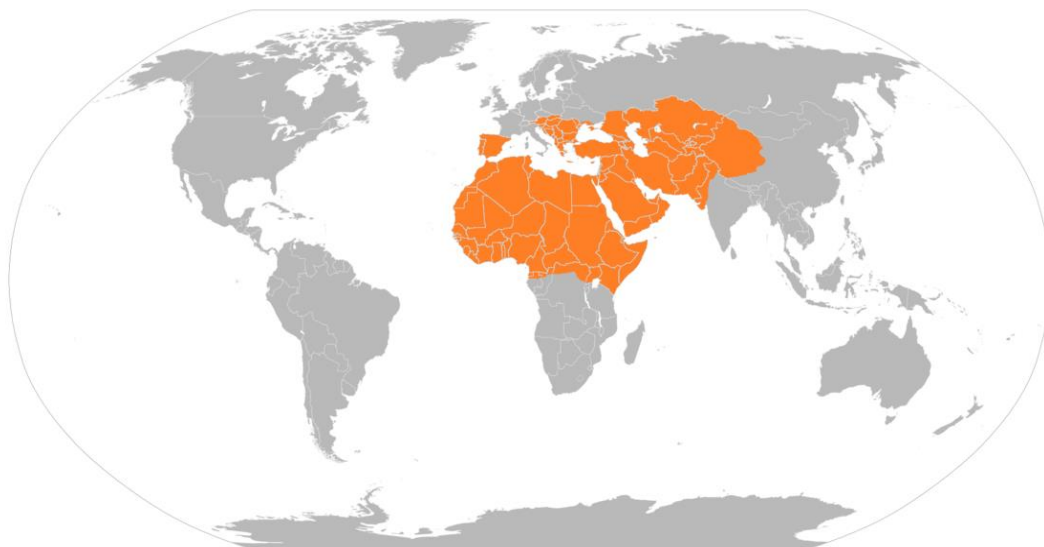
<sup>51</sup> Coinbase è una società di scambio di beni digitali con sede a San Francisco, in California, e fondata a giugno 2012 da Brian Armstrong e Fred Ehrsam.

Opera scambio di Bitcoin (BTC), Ripple (XRP), Ethereum (ETH), Bitcoin Cash (BCH), Ethereum Classic (ETC), Litecoin (LTC) e altri beni digitali con valute di corso legale in 32 nazioni e con transazioni Bitcoin e di deposito in 190 nazioni.

Dal 14 aprile 2021, Coinbase è quotata al Nasdaq, diventando società pubblica. (Wikipedia)



Strumento per arrestare questo finanziamento al terrorismo è il divieto di utilizzo delle criptovalute, strumento che vari paesi stanno adottando tra cui: Marocco, Algeria, Egitto, Nigeria, Iraq, ecc. paesi in cui -si può asserire- abbiano subito forte infiltrazioni nel loro tessuto economico-sociale da parte dei movimenti terroristici.



Isis Power. Fonte: Wikimedia Commons

Purtroppo, le fonti di finanziamento del terrorismo sono svariate e tra queste rientrano quindi le criptovalute che grazie all'anonimato (già citato per il caso del riciclaggio di denaro) delle transazioni è un terreno fertile per l'arricchimento di tali organizzazioni. Un intervento a limitare un mercato da un altissimo potenziale è necessario da parte di tutte le istituzioni mondiali al fine di prevenire una probabile espansione di un fenomeno estremamente pericoloso.

## CONCLUSIONI

Stiamo vivendo nel pieno dell'Industria 4.0, o anche conosciuta come quarta rivoluzione industriale, in cui la produzione industriale è del tutto automatizzata e interconnessa. Indicare la data o il momento di inizio di questa rivoluzione è al momento complicato (a mio personale parere probabilmente l'invenzione degli smartphone o Facebook possono essere date indicative), ma di una cosa si è pur certi la Blockchain e le criptovalute sono elementi alquanto rilevanti di questo fenomeno.

Sicuramente l'impatto rapido e la diffusione su scala mondiale della tecnologia blockchain e delle sue criptovalute hanno comportato non poche conseguenze nel sistema economico mondiale.

La Blockchain può essere ritenuta come una delle più grandi innovazioni del ventunesimo secolo per quanto riguarda il sistema finanziario. Il sistema della catena a blocchi, infatti, permette che effettuata un'operazione finanziaria le parti otterranno un certificato crittografico univoco ed immutabile che garantirà quindi la sicurezza della transazione eliminando totalmente la presenza di una terza parte che faccia da intermediario o garante. Questo è sicuramente un aspetto estremamente rivoluzionario tipico dell'industria 4.0.

Non è invece un caso che la finanza e il settore bancario guardino con diffidenza e riluttanza alle criptovalute, temendo che siffatte evoluzioni, determinando la possibilità di trasmettere valore senza l'intervento degli intermediari, possano finire per spiazzare il business normalmente svolto dall'industria.

Ma, a tal proposito, seguendo il pensiero di Golinelli, ovvero che l'impresa (ipotizzata come un sistema vitale) per sopravvivere debba sapersi adattare all'evoluzione del contesto economico in cui milita; le istituzioni o intermediari che sapranno adattarsi e sfruttare al massimo la potenza delle nuove tecnologie legate ai distributed ledger, otterranno non pochi benefici in futuro.

I benefici saranno tali per cui non si parlerà più di sopravvivenza ma di un vero e proprio predominio sulla concorrenza, in quanto l'appetibilità del servizio offerto sarà elevato e contemporaneamente si registreranno forti risparmi sui costi, rendendo i sistemi organizzativi estremamente efficienti.

È inevitabile quindi che, inserita la blockchain nel nostro sistema economico, bisognerà e si dovrà integrare a pieno anche il fenomeno delle criptovalute, essendo strettamente connesse a tal sistema.

A tal proposito quindi, le istituzioni stanno effettuando interventi al fine di dare alle criptovalute una natura civilistico-contabile e di essere soggette alla sfera fiscale.

L'IC ha stabilito, momentaneamente, che le criptomonete debbano essere contabilizzate come attività immateriali, nonostante non rispettino a pieno i requisiti dello IAS 38. Sarebbe necessario, quindi, che sia istituita una nuova voce contabile che possa assimilare all'interno di essa queste nuove tipologie di assets. Dagli studi e ricerche effettuate si può, comunque, presagire che i vari organi di contabilità stiano valutando la nascita di tale voce, al fine di ottenere una classificazione appropriata dei nuovi assets digitali.

Ciò renderebbe più semplice ed univoca la redazione di bilancio, la quale inevitabilmente sarà secondo l'articolo 2423 del codice civile, chiara veritiera e corretta.

Sicuramente, come il terzo capitolo descrive, l'ambito fiscale delle criptomonete vanta una situazione di maggior chiarezza rispetto a quella contabile. La risoluzione 72/E dell'Agenzia delle entrate assimila le criptovalute come valute estere, sottoponendole quindi ai trattamenti fiscali delle imposte dirette ed indirette delle attività finanziarie.

Sicuramente verrà effettuato un allineamento tra la valutazione contabile e quella fiscale, fornendo quindi un'identità unica per le nuove valute digitali.

Non è da escludere però, che per ottenere un'effettiva integrazione nel nostro sistema economico, la tecnologia Blockchain e le criptovalute debbano raggiungere un livello di sostenibilità.

Come evidenziato nel terzo capitolo, l'impatto ambientale, il finanziamento al terrorismo e il favorire il riciclaggio di denaro sono fonti di timore e incertezza nei confronti di tali tecnologie.

In conclusione, andando a definire uno stato di legalità delle criptovalute, coadiuvato (come stanno effettivamente intervenendo) da un miglior tracciamento delle operazioni ed una precisa identificazione degli accounts, sarà possibile sfruttare al meglio un'innovazione tecnologica che ad oggi ancora non ha espresso il suo vero potenziale.

## Bibliografia e sitografia

- Criptovalute-trattamento-fiscale-e-contabile-le-norme-e-scenari-futuri.pdf
- <https://www.consob.it/web/investor-education/criptovalute>
- <https://forbes.it/2022/02/08/tesla-investimento-bitcoin-seconda-azienda-americana/>
- <https://cryptonomist.ch/2021/11/03/mining-bitcoin-premi-60-milioni-miners/>
- <https://www.lecriptovalute.org/proof-of-work-significato-proof-of-stake/>
- <https://it.wikipedia.org/wiki/Criptovaluta>
- [https://blog.osservatori.net/it\\_it/ico-initial-coin-offering-come-funziona](https://blog.osservatori.net/it_it/ico-initial-coin-offering-come-funziona)
- <https://www.medialaws.eu/initial-coin-offering-natura-giuridica-e-prospettive-regolatorie/>
- <https://www.economyup.it/innovazione/cos-e-l-industria-40-e-perche-e-importante-saperla-affrontare/>
- <https://www.ilsole24ore.com/art/ifrs-criptomonete-non-sono-valuta-ACH1Dwb>
- [https://fiscomania.com/ivafe-attivita-finanziarie-estere/?refresh\\_ce](https://fiscomania.com/ivafe-attivita-finanziarie-estere/?refresh_ce)
- <https://www.abenergie.it/blog/2021/08/bitcoin-inquinamento>
- <https://www.altalex.com/documents/leggi/2008/01/14/iva-servizi-bancari-recupero-crediti-contratti-di-servicing-e-servizi-di-compliance>
- <https://www.blockchain4innovation.it/mercati/blockchain-oracle-scommette-sulla-nuova-degli-smart-contract/>
- <https://www.commercialistatelematico.com/articoli/2021/08/questione-fiscale-criptovalute-imposte-dirette.html>
- [https://www.fiscal-focus.it/dlshop/Dossier\\_Casi\\_n.\\_23\\_del\\_29.06.2021\\_-\\_Bilanci\\_2020](https://www.fiscal-focus.it/dlshop/Dossier_Casi_n._23_del_29.06.2021_-_Bilanci_2020).
- [https://fiscomania.com/capital-gain/#:~:text=Le%20plusvalenze%20derivanti%20dalla%20cessione,partecipazione%20qualificata%20e%20non%20qualificata\).](https://fiscomania.com/capital-gain/#:~:text=Le%20plusvalenze%20derivanti%20dalla%20cessione,partecipazione%20qualificata%20e%20non%20qualificata).)
- <https://finance.kalaway.com/tecnologia-blockchain-fintech>
- <https://fdocumenti.com/document/la-rivoluzione-del-protocollo-bitcoin-protocolli-delle-monete-digitali-ecash-b.html>
- <https://archiviodpc.dirittopenaleuomo.org/d/6006-bitcoin-e-riciclaggio-20>
- <https://www.open.online/2022/01/01/criptovalute-nft-problema-riciclaggio-denaro/>
- <https://www.antiriciclaggiocompliance.it/app/uploads/2020/08/Fontana.pdf>
- <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>

- [https://it.wikipedia.org/wiki/Initial\\_coin\\_offering](https://it.wikipedia.org/wiki/Initial_coin_offering)
- <https://www.diritto.it/cosa-sono-le-initial-coin-offering/>
- <https://corporatefinanceinstitute.com/resources/knowledge/trading-investing/initial-coin-offering-ico/>
- <https://cryptorobin.it/cosa-sono-gli-airdrop/>
- <https://www.criptoinvestire.com/airdrop-cosa-sono-e-perche-regalano-criptovalute-come-funziona.html>
- <https://www.brickken.com/it/blog-airdrop/>
- <https://cointext.com/it/glossario/airdrops/>
- <https://www.icer.it/che-cose-un-airdrop-di-criptovalute/>
- <https://www.avatrade.it/education/trading-for-beginners/mining>
- <https://www.aranzulla.it/locked-chrome.php?p=1293103&fabm=file&rnd=0.7454807313481433>
- <https://n26.com/it-it/blog/cos-e-il-mining>
- <https://www.punto-informatico.it/browser-web-mining-bitcoin/>
- <https://www.linkedin.com/pulse/criptovalute-e-bitcoin-trattamento-contabile-fiscale-cosimo-la-forgia/?originalSubdomain=it>
- <https://www.kreston.com/it/hot-topic-accounting-and-auditing-for-cryptocurrencies/>
- <https://www.bgt-grantthornton.it/notizie-flash/2018/nf-ottobre-2018/criptovalute-criteri-di-contabilizzazione/>
- <https://www.informazionefiscale.it/tassazione-criptovalute-moneta-digitale-regole-fisco>
- <https://fiscomania.com/criptovalute-dichiarazione-dei-redditi/>
- <https://www.rivistadiritto tributario.it/2021/12/22/redditi-derivanti-da-operazioni-in-criptovalute-profilo-di-fiscalita-sostanziale-e-adempimenti-dichiarativi-a-carico-dei-contribuenti/>
- <https://youngplatform.com/faq/taxation/>
- <https://www.fiscoetasse.com/approfondimenti/14140-criptovalute-tassazione-ed-obblighi-di-monitoraggio-fiscale-rw.html>
- Blockchain: <https://www.blockchain.com>
- Ripple: <https://ripple.com/>
- Ethereum: <https://ethereum.org>
- <https://www.ecb.europa.eu/ecb/html/index.it.html>
- Coinmarketcap: <https://coinmarketcap.com>
- Investopedia: <https://www.investopedia.com>
- ORACLIZE: <http://www.oraclize.it/>
- Decreto legislativo 25 maggio 2017, n. 90 (Italia).
- Direttiva (UE) 2015/849, 20 maggio 2015
- Direttiva (UE) 2018/843, 30 maggio 2018.

- Swan M., “Blockchain: Blueprint for a new economy”, 2015
- IAS 2, IAS 7, IAS 8, IAS 9, IAS 32, IAS 38
- OIC 13, OIC 24
- Codice Civile
- RAZZANTE R.,(2018), Codice della normativa antiriciclaggio, Maggioli
- Risoluzione 2 settembre 2016, n. 72, Interpello ai sensi dell'art. 11, legge 27 luglio 2000, n. 212
- (s.d.). Tratto da [https://www.treccani.it/enciclopedia/istituto-giuridico\\_%28Enciclopedia-Italiana%29/](https://www.treccani.it/enciclopedia/istituto-giuridico_%28Enciclopedia-Italiana%29/).
- (s.d.). Tratto da criptovalute-tassazione-e-calcolo-delle-plusvalenze.
- (s.d.). Tratto da criptovalute-tassazione-e-calcolo-delle-plusvalenze.
- (s.d.). Tratto da [www.orcom.fr](http://www.orcom.fr).
- (s.d.). Tratto da [digital-for-esg](http://digital-for-esg).
- (<https://it.wikipedia.org/wiki/Blockchain>). (s.d.).
- Andreoli, B. (s.d.). Sul monitoraggio dei bitcoin cercasi semplificazione.
- bilancio di oraclize. (s.d.).
- bitcoin-inquinamento. (s.d.). Tratto da [www.abenergie.it](http://www.abenergie.it).
- Corasaniti. (s.d.). Il trattamento tributario dei bitcoin tra obblighi di antiriciclaggio e monitoraggio fiscale.
- cryptonomist.ch. (s.d.).
- digilander.libero.it. (s.d.).
- Giacomelli. (s.d.).
- <https://eur-lex.europa.eu/legal-content/IT/LSU/?uri=celex:32007L0064>. (s.d.).
- <https://locait.net/criptovalute-e-bitcoin-trattamento-contabile-e-fiscale/>. (s.d.).
- <https://www.consob.it/web/investor-education/criptovalute>. (s.d.).
- <https://www.revilaw.it/2020/03/20/criptovalute-il-problema-della-corretta-contabilizzazione-in-bilancio/>. (s.d.).
- [ig.com](http://ig.com). (s.d.).
- [it.Andersen.com](http://it.Andersen.com). (s.d.).
- [iusinitinere.it](http://iusinitinere.it). (s.d.).
- Pontani. (s.d.).
- Razzante, R. (s.d.). Bitcoin e criptovalute.
- RAZZANTE, R. (s.d.). BITCOIN E CRIPTOVALUTE.
- Risoluzione 72/E (2016).
- [www.studio-comand.com](http://www.studio-comand.com). (s.d.).

## **SINTESI**

### **STORIA**

Nel 1982 David Chaum pubblicò l'articolo intitolato "Blind Signatures for Untraceable payments". Per la prima volta fu introdotto il concetto di «crittografia», ovvero, una firma digitale in cui il contenuto di un messaggio viene mascherato prima di essere firmato.

Per facilitare la comprensione di questa nuova idea digitale, Chaum utilizzò l'esempio delle buste elettorali.

Il processo di votazione prevede che:

-L'elettore passa la busta sigillata a un funzionario

-Il funzionario post verifica delle credenziali, la firma.

-Il pacco è reso all'elettore, che trasferisce la votazione adesso firmata a una nuova busta normale senza macchie.

Così, il firmatario non vede il contenuto di messaggio, ma terzi possono più tardi verificare la firma e sapere che la firma è valida dentro le restrizioni dello schema di firma sottostante.

Dopo la registrazione del dominio «bitcoin.org», il 31 Ottobre 2008 il programmatore Satoshi Nakamoto pubblicò "Bitcoin: a peer to peer electronic cash system" in cui spiegava il funzionamento del "protocollo Bitcoin" o meglio, le caratteristiche tecniche della criptovaluta e l'importante possibilità di tracciare le transazioni.

Nel 2009 fu effettuato il lancio del primo blocco proof to work, il Genesis Block conosciuto in Italia anche come blocco Zero.

### **La Blockchain**

La blockchain è una struttura dati condivisa e "immutabile". È definita come un registro digitale le cui voci sono raggruppate in "blocchi", concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia.

I blocchi sono raggruppati a intervalli di tempo, a ogni frazione di tempo viene applicato un «Timestamp» o marca temporale.

I blocchi inoltre presentano un «Puntatore Hash» la cui funzione è di identificare in maniera univoca e inequivocabile un blocco della Blockchain.

Tali caratteristiche rendono la Blockchain estremamente sicura e difficilmente inviolabile.

La registrazione delle transazioni o dei contratti avviene in forma decentralizzata tra luoghi e persone diverse.

In questa maniera si elimina la necessità di un'autorità centrale che autorizzi o convalidi alcuna transazione.

È possibile identificare 7 caratteristiche comuni proprie della tecnologia Blockchain:

- Digitalizzazione e alla trasformazione dei dati in formato digitale.
- Tracciabilità dei trasferimenti
- Disintermediazione
- Trasparenza e verificabilità
- Immutabilità del registro
- Programmabilità dei trasferimenti
- Decentralizzazione

### **Le criptovalute**

Una criptovaluta è:

Rappresentazione digitale di valore basata sulla crittografia.

Le criptovalute funzionano in modo autonomo, al di fuori dei tradizionali sistemi bancari e governativi.

Utilizzano tecnologie di tipo peer-to-peer

Utilizzata come mezzo di scambio/servizi

Trasferita, negoziata e archiviata elettronicamente

Non è legata ad una valuta legale

Le criptovalute o valute virtuali, presentano varie caratteristiche che comportano la formazione di 3 principali sottocategorie:

-1 *Criptovalute Tradizionali*: il valore di tali criptovalute è determinato dall'incontro tra domanda e offerta nei propri mercati, esempi di cripto tradizionali sono: Bitcoin, Ethereum, ecc.

-2 *Stablecoin*: criptovalute progettate per avere una valorizzazione legata ad un asset o a un paniere di assets, questa tipologia di cripto presentano a loro volta un'ulteriore suddivisione di categoria.

i) *asset-backed stablecoin*: criptovalute legate da una garanzia di un asset o di un paniere di assets, i quali possono essere convenzionali (assets finanziari e non) o criptovalute stesse, tenuti in custodia dall'emittente della stablecoin.

ii) *algorithmic smart contract*: programmati per regolarizzare l'emissione e il riscatto tra domanda e offerta, riducendo la volatilità del mercato.

-3 *Central Bank Digital Currencies*: valute digitali, ovvero dematerializzate, emesse dalle banche centrali, le quali acquistate accendono un debito diretto della banca emittente nei confronti di chi le possiede. Su tali valute digitali le discussioni sono molto accentuate, rilevante è "L'overview" di PwC la quale asserisce che "L'impatto che le CBDC potrebbero avere sul sistema economico e finanziario è uno dei temi più rilevanti [...] esse potrebbero costituire un game-changer, con la potenzialità di mutare le radici del sistema bancario tradizionale."

## **Il fenomeno degli NFT**

NFT è l'acronimo di Non Fungible Token – token non fungibile – un tipo di token crittografico che rappresenta l'atto di proprietà e il certificato di autenticità di un bene unico, sia digitale che fisico, che non può essere sostituito con qualcos'altro. I beni soggetti agli NFT sono tutti beni digitali, caratterizzati da non fungibilità, o meglio, unici e non sostituibili. Gli NFT essendo digitali, sono tutti quei beni caratterizzanti l'era dell'informazione e quindi: Immagini, Video, disegni, GIF

Per via della sua non fungibilità e quindi incapacità ad essere scambiato, un NFT presenta un valore estremamente elevato, vari acquisti avvenuti a partire dal momento del loro lancio hanno superato il centinaio di migliaia di euro.



## I Wallet

I wallet sono applicazioni utilizzate per generare, gestire ed archiviare le chiavi pubbliche e private delle cripto-transazioni. I wallet non sono tutti uguali, esistono quattro macrocategorie di essi, distinguibili se presentano o no un formato software o hardware, totale o parziale e se sono gestiti da terzi oppure no: Esistono 4 tipologie di wallet:

- *Hot custodial wallet*
- *Hot non custodial wallet*
- *Cold Hardware wallet*
- *Cold paper wallet*

I wallet presentano una crittografia asimmetrica, ovvero, la loro lettura e funzione sono dovute ad una coppia di chiavi, una pubblica ed una privata. La chiave privata rimane in possesso dell'utente, che verrà utilizzata nel momento della transazione per "firmarla", post firma la controparte potrà validare la transazione e la sua sotto scrittura grazie alla chiave pubblica. Approvata la transazione, esse vengono compilate in un blocco in ordine cronologico, i blocchi andranno a formare perciò la blockchain

### La creazione di valore delle criptovalute

Le modalità per la creazione di valore delle criptovalute sono varie, ma quelle di più comune utilizzo sono le seguenti:

*Initial Coin Offering*: Una Initial Coin Offerings, o ICO, è il termine con cui si identifica un meccanismo finalizzato alla raccolta di fondi necessari a finanziare un progetto imprenditoriale, in maniera simile alle "Initial Public Offering

*Hard Fork*: E' un cambiamento radicale del protocollo di una rete, un hard fork si ha quando i nodi della versione più recente di una blockchain non accettano più le regole precedentemente emanate

*Yield Farming*: E' un modo per generare ricompense con le partecipazioni in criptovaluta

*AirDrop*: campagna pubblicitaria che cerca di lanciare o pubblicizzare una moneta per renderla visibile serve ad attirare l'attenzione di tutti gli analisti e gli investitori.

*Mining*: processo informatico che sfrutta la blockchain per estrarre valute digitali, si ottiene così un prezioso compenso

### Rappresentazione giuridica

Le criptovalute sono utilizzate come mezzo di pagamento ma non essendo emesse da un ente finanziario come una banca, da un istituto di credito o da un istituto di moneta elettronica non possono essere definite come moneta in senso tecnico e pertanto non è possibile applicare la regolamentazione valutaria utilizzata per le monete avente corso legale né per le monete elettroniche.

Inoltre, non possono essere qualificate come strumenti finanziari in quanto il Testo Unico delle disposizioni in materia di intermediazione finanziaria, o più semplicemente TUF con l'art. 1 comma 2 definisce tali strumenti come un insieme di tutti i prodotti finanziari e di ogni altra forma di investimento di natura finanziaria.

Unica ipotesi di rappresentazione giuridica delle criptovalute è quella di annoverarle nella categoria dei *Beni Immateriali* perché secondo l'art.810 del c.c. «Sono beni le cose che possono formare oggetto di diritti» Una criptovaluta è quindi un bene mobile e immateriale, non essendoci data la sua natura digitale tangibilità. Il contrasto avviene però per la natura non monetaria dei beni, per via del requisito di patrimonialità che difetta nelle criptovalute.

Altri regolatori hanno invece evidenziato le similitudini delle valute virtuali rispetto a *Beni Materiali* come i metalli preziosi, i combustibili e i prodotti agricoli, riconducendo le criptovalute alla nozione di commodities, ossia, di prodotti che possono essere utilizzati a scopo di investimento o speculativo.

Il lodo arbitrale di Marcianise stabilì che la criptovaluta è un Bene Polivalente. Ha natura sia pecuniaria sia di merce a seconda della funzione che assume in un contratto.

## **Rappresentazione contabile**

### **IAS**

L'Ifrs Interpretations Committee (Ic) si è espressa in merito al trattamento contabile da riservare alle criptovalute:

Secondo lo IAS 2, se detenute per la vendita nell'ambito dell'attività ordinaria le criptovalute dovranno essere contabilizzate come rimanenze e quindi iscritte in bilancio al costo e successivamente valutate al minore tra il costo e il valore netto di realizzo

In caso invece di detenzione non legata all'attività, secondo lo IAS 38 dovranno essere contabilizzate come attività immateriali, la cui valutazione in bilancio potrà essere effettuata o al costo tramite metodo del fair value

### **Fair value delle criptomonete**

il Fair Value è il prezzo che si riceverebbe per vendere un'attività, o che si pagherebbe per trasferire una passività, in una transazione ordinata tra operatori di mercato al momento della misurazione”.

Ci sono diversi metodi per avvicinarsi alla valutazione. La maggior parte di questi approcci differiscono nel modo in cui si vede la natura di una "moneta" digitale.

I quali sono:

- Expected value
- Costo di produzione
- Incrocio domanda e offerta

### **OIC**

L'orientamento dell'OIC – I principi contabili nazionali, al momento, non hanno previsto alcun tipo di disciplina in tema delle valute virtuale, pacifico è il fatto che le criptovalute non possano essere catalogate come disponibilità liquide (OIC 14), crediti (OIC 15) o strumenti finanziari (OIC 32) , quindi per applicazione analogica agli IFRS il redattore di bilancio inserirà o nella voce “immobilizzazioni immateriali” (OIC 24) e “rimanenze” (OIC 13) le criptovalute.

### **Caso Oraclize srl**

La Oraclize srl è la prima società a responsabilità limitata italiana il cui capitale sociale è stato versato interamente in bitcoin.

Conseguenza di ciò:

Assimilazione di conferimenti di capitale tramite criptovalute ai conferimenti di beni in natura, in quanto “le criptovalute sono rappresentazioni digitali di valore”.

Nel Bilancio di Oraclize srl però le criptovalute compaiono nella voce «attività finanziarie» (IAS 32), andando contro le linee guida dell'IC e dimostrando come ancora vi sia una interpretazione soggettiva nella redazione di un bilancio in cui sono presenti le criptovalute.

Successivamente alla redazione del bilancio Oraclize (esercizio 2015), l'IC si espresse per chiarire il dilemma rappresentazione contabile delle criptomonete, il quale stabilì che la più corretta voce da applicare fosse “attività immateriali” ovvero IAS 38.

Compito del redattore, quindi, rispettare le decisioni dell'IC per i bilanci successivi non classificando più le criptovalute come attività finanziarie ma come attività immateriali.

Le criptomonete, quindi, del bilancio Oraclize dovranno essere sottoposte a un cambiamento del principio contabile, tale modifica è regolamentata dall'OIC 29.

### **Trattamento Fiscale**

L'Agenzia delle Entrate in conformità alla sentenza 22 ottobre 2015, causa C-264/14 della Corte di Giustizia Europea reputa le operazioni con criptovalute ai fini fiscali operazioni in valute estere.

Sono soggette quindi a un trattamento fiscale di imposte dirette e indirette.

L'Agenzia delle Entrate in conformità alla sentenza 22 ottobre 2015, causa C-264/14 della Corte di Giustizia Europea reputa le operazioni con criptovalute ai fini fiscali operazioni in valute estere.

Sono soggette quindi a un trattamento fiscale di imposte dirette e indirette.

### **Imposte dirette**

Il trattamento ai fini IVA per le criptovalute è disciplinato dalla direttiva IVA 2006, in quanto vi sono in oggetto strumenti di pagamento e quindi indirettamente le valute virtuali.

Le criptovalute assimilate come valute estere, sono esenti IVA, in quanto ritenute operazioni di prestazioni di servizi a titolo oneroso.

Conseguenza di ciò è che gli exchanger non potranno dedurre IVA sostenuta su acquisti di beni e servizi relativi al loro business.

### **Imposte dirette**

Ai sensi dell'art.67, comma 1 lett.c-ter e comma 1 ter del TUIR, le operazioni di criptovalute detenute al di fuori del regime di impresa generano redditi imponibili ai fini fiscali.

Ai fini IRPEF, ogni conversione di criptovaluta in altra valuta virtuale o a corso legale è rilevabile per:

1. cessioni a termine
2. cessioni a pronti

Il contribuente dovrà dichiarare nel quadro RT dell'UNICO le plusvalenze ottenute dall'operazione di cambio valuta.

La loro classificazione e qualificazione contabile come immobilizzazione immateriale o rimanenza, comporta effetti positivi/negativi a livello di base imponibile IRAP

Soggette al monitoraggio fiscale sono le attività finanziarie estere, quindi per analogia iuris anche le Criptovalute.

Per il monitoraggio fiscale è necessario compilare il quadro RW, dichiarando il valore delle criptovalute detenute.

Per quanto riguarda l'IVAFE i wallet delle criptovalute sono esenti, in quanto l'imposta è applicabile ai solo depositi di natura "bancaria"

### **Le criptovalute e l'ordinamento USA**

L'ordinamento statunitense ha avuto una reazione più decisa nei confronti della regolamentazione delle criptovalute rispetto a quello europeo e, quindi, italiano.

La guida fiscale statunitense è stata emessa nel 2019 da parte dell'International Revenue service (IRS), il corrispettivo della nostra Agenzia delle entrate.

L'IRS definisce i bitcoin e le restanti criptovalute come valute virtuali convertibili, definizione che risulta estremamente corretta, in quanto ormai è certo che le criptovalute assolvono funzione di unità di pagamento

per beni e servizi ma anche come forma di investimento, essendo possibile la negoziazione digitale fra utenti, tramite il cambio criptovaluta/criptovaluta o criptovaluta/valuta legale.

L'IRS ha stabilito di tassare le criptovalute come un bene immobiliare quindi ai fini fiscali federali, le valute virtuali sono trattate come una proprietà, non come una valuta.

Conseguenza di tale assunzione è che alle transazioni in valuta virtuale si applicano i principi generali di tassazione applicate alle transazioni di proprietà.

## **Controversie**

Le criptovalute presentano comunque dei lati negativi per via della loro natura digitale e per le caratteristiche intrinseche che possiedono:

Sono *una fonte di inquinamento ambientale*: Una singola transazione in Bitcoin consuma quanto 1 122 196 pagamenti con una carta Visa, equivalenti a 36 giorni di consumo elettrico di una casa di una famiglia media. Secondo digiconomist, sito citato da diverse testate giornalistiche, una singola transazione in Bitcoin consuma quanto 1 122 196 pagamenti con una carta Visa, equivalenti a 36 giorni di consumo elettrico di una casa di una famiglia media americana e pari a guardare youtube per 84 388 ore. Si stima, secondo diverse testate indipendenti, tra cui cbs che solo il 40% dell'energia consumata dalle criptovalute sia da fonti rinnovabili, e il restante 60% provenga da combustibili fossili.

Una svolta alla lotta all'inquinamento delle criptovalute però, può provenire dagli Accordi Climatici Crypto, ispirati a quelli di Parigi del 2015.

Questa iniziativa parte dal presupposto di rendere le criptovalute "green",

Favoriscono il *riciclaggio di denaro*: il sistema della blockchain e, quindi, le criptovalute permettono l'uso dell'anonimato all'interno delle loro transazioni, tramite l'uso di pseudonimi e il celare l'indirizzo IP

Possono essere fonti di *finanziamento al terrorismo*: Il mercato delle criptovalute presenta una percentuale di domanda proveniente proprio dalle organizzazioni terroristiche. Il flusso di capitali dovuto ad operazioni che coinvolgono come una delle parti i terroristi consiste almeno l'1% delle transazioni totali all'interno della blockchain, che espresso in termini monetari, si aggira intorno a 500 milioni di dollari. Molti sono stati i casi di fundraising al terrorismo tramite criptovalute, grazie ai vari cambi di valuta e le propagande lanciate dalle organizzazioni terroristiche al fine di ricevere donazioni ai propri wallet

Si stanno comunque mettendo in atto contromisure a questi aspetti negativi

## **Conclusioni**

Al fine di semplificare la rappresentazione contabile delle criptovalute e attribuire una determinata sfera fiscale, è necessario l'inserimento di una nuova voce di bilancio che vada a comprendere tutti i nuovi, o potenziali, assets digitali.

La ricerca di una forte sostenibilità da parte delle nuove tecnologie blockchain e criptovalute, potrebbe rivelarsi una rampa di lancio per un nuovo sistema economico-finanziario

●