LUISS

Dipartimento
di Impresa e Management

Cattedra di Economia dei Mercati e degli Intermediari Finanziari

# BLOCKCHAIN E CRIPTO-ASSET: CONTESTO E SCENARIO EVOLUTIVO

Prof. Francesco Cerri

RELATORE

Filippo Petrone Mat. 231421

CANDIDATO

Anno Accademico 2020/2021

*Ai miei genitori,*

*Alla mia famiglia.*

**ABSTRACT**

L'obiettivo della tesi è quello di condurre un'analisi nell'ambito della Blockchain e dei "cripto-asset", due tematiche di grande interesse al giorno d'oggi, data la loro crescente diffusione. Nello specifico si analizzerà innanzi il funzionamento della tecnologia *Blockchain* e delle infrastrutture DLT, individuando i campi applicativi dove questa potrà risultare un'invenzione essenziale. In seguito si delineerà l'inquadramento di quei cripto-asset chiamati comunemente "criptovalute", evidenziando i rischi connessi ad un loro utilizzo diffuso. Infine, si farà riferimento alla necessità di regolamentazione della materia da parte delle Autorità Centrali con un focus sulle proposte nell'area Euro, in cui oggi la normativa si esaurisce a livello dei singoli ordinamenti nazionali. Si cercherà inoltre di valutare il posizionamento degli Intermediari Finanziari in relazione alla loro necessità di supportare questa innovazione sfruttandone i possibili benefici e presidiando i rischi nell'ambito del futuro scenario regolamentare.

**INDICE**

# INTRODUZIONE

La tecnologia *Blockchain* (letteralmente "catena di blocchi") rappresenta una delle innovazioni informatiche più rivoluzionarie degli ultimi anni, che permette, tra l'altro, la creazione e il trasferimento dei c.d. cripto-asset. In generale, essa appartiene alla classe tecnologica DLT (*Distributed Ledger Technology*): un DLT è assimilabile ad un registro mastro condiviso in grado di memorizzare in modo univoco (tramite crittografia) delle informazioni, che appena vengono correttamente validate saranno poi accessibili e verificabili da tutti i soggetti che partecipano alla rete. Su un DLT è registrata immutabilmente tutta la cronologia di informazioni (che nel caso dei cripto-asset sono dati di transazioni) relativamente alle operazioni compiute da tutti i nodi della rete.

In questo modo, la *Blockchain*, consente lo scambio di beni (nella forma di cripto-asset) in modo sicuro, anonimo, inalterabile ma soprattutto decentrato, cioè senza la necessità di ricorrere a un soggetto terzo che verifichi l'effettività della transazione. La decentralizzazione è l'elemento fondante e veramente innovativo incorporato in questa tecnologia. Potenzialmente l'utilizzo di "registri distribuiti" può aprire la strada ad una prospettiva futura in cui la circolazione di beni e lo scambio di ricchezza tra privati avvenga senza il bisogno di un soggetto intermediario che svolga la funzione di vigilanza e controllo.

Dopo aver analizzato il funzionamento e i potenziali benefici che la tecnologia DLT può apportare al sistema economico e al mercato, si prova ad analizzare l'inquadramento, teorico ed effettivo, di queste "monete digitali" (tipo Bitcoin, Ethereum…) esaminando quello che è ad oggi, il loro utilizzo da parte dei privati (molti dei quali si sono interessati al mondo *crypto* solo perché attirati dalle considerevoli oscillazioni di prezzo e dalla prospettiva di realizzare utili immediati). In questo ambito si confrontano le funzioni monetarie tipiche assolte dalle valute a corso legale (mezzo di pagamento, unità di conto, riserva di valore) con le proprietà delle "criptovalute".

Approfondiremo l'analisi parlando di *Stablecoin*, le criptovalute il cui valore è ancorato a una moneta fiat o a un determinato paniere di beni per conseguire la stabilità di prezzo nel tempo. Si esaminano i caratteri di queste valute virtuali a limitata volatilità, citando i progetti più rilevanti in termini di capitalizzazione di mercato e portata geografica (cd. *Global Stablecoin*).

Per concludere, cercheremo di evidenziare quindi i molteplici rischi che possono emergere da una crescente diffusione di tutti questi strumenti digitali: dai rischi sistemici e per la sovranità monetaria connessi ad un probabile ingresso delle *Big Tech* nel settore finanziario, ai rischi correlati alla difficoltà nel tracciamento delle transazioni (riciclaggio, finanziamento della criminalità); dai rischi prettamente "cyber" fino a quelli più "comuni" connessi alla necessità di assicurare la protezione dei consumatori.

Dopo aver condotto quindi un *trade-off* tra benefici e rischi derivati da questa tecnologia e dalle sue prime implementazioni pratiche, vedremo come le Autorità Monetarie Centrali stanno cercando di regolare la materia rispondendo al contesto che è in rapida evoluzione, anche al fine di evitare una progressiva obsolescenza degli intermediari finanziari tradizionali.

In questo ambito si tracciano le linee generali riguardo la regolamentazione nelle principali giurisdizioni del mondo, quella Americana e Cinese, per poi condurre un'analisi approfondita riguardo l'approccio regolamentare in corso di definizione nell'Unione Europea. Si analizzano le proposte di regolamento contenute nel *Digital Finance Package* emanato dalla Comunità Europea e la proposta relativa all'introduzione della CBDC (digital euro) evidenziandone i motivi e le finalità.

Nelle conclusioni si tirano le fila dell'analisi svolta, per capire se davvero è possibile un futuro in cui la circolazione di ricchezza prescinda dall'attività delle Autorità Centrali e degli Intermediari Finanziari, o se, al contrario, il sistema bancario tradizionale incorporerà o stabilirà dei collegamenti con questa frontiera tecnologica, al fine di sfruttarne le opportunità, sostenere l'innovazione e guidare il più ampio processo di transizione digitale.

# 1. BLOCKCHAIN E CRIPTO-ASSET

## 1.1 Definizioni, funzionamento e finalità

Prima di iniziare ad analizzare una delle tecnologie più innovative e rivoluzionare degli ultimi anni, la *Blockchain*, non si può non citare il suo ideatore: Satoshi Nakamoto, pseudonimo al quale è attribuita la paternità dell'invenzione. Al giapponese, la cui identità rimane ancora oggi ignota, va riconosciuto il pregio di aver elaborato la *Blockchain*, il sistema informatico su cui si basa il Bitcoin, la criptovaluta più famosa al mondo. Era il 31 ottobre 2008, quando lo sconosciuto giapponese annunciava in un sito di crittografia di aver creato una moneta elettronica che non avesse bisogno di una parte terza fiduciaria per circolare o essere scambiata. Inoltre, affermava che il sistema era solido e non presentava rischi di *double spending,* un fattore di importanza cruciale nell'ambito dei pagamenti elettronici. A dimostrazione di ciò che affermava, il giapponese presentò un documento intitolato *Bitcoin, a peer-to-peer electronic cash system*, dove spiegava tecnicamente l'operatività della tecnologia sottostante.

La Blockchain è un'infrastruttura informatica che permette la creazione e il trasferimento di asset crittografici a condizioni tali da rendere il processo di scambio sicuro, trasparente e immutabile. Gli asset in parola, anche noti come "cripto-asset", sono delle rappresentazioni digitali di valore rese univoche tramite l'impiego della crittografia, che possono quindi essere trasferiti da un soggetto all'altro senza correre il rischio di venir replicati (evitando il rischio di doppia-spesa). Il concetto di "unicità" dell'asset scambiato è una caratteristica fondante di questa tecnologia e consente di trasferire nel "mondo virtuale" il concetto di scarsità dei beni del mondo reale.

Per capire come ciò sia possibile occorre introdurre il concetto di *registro distribuito*, ovvero della *Distributed Ledger Technology* (DLT). Con DLT si intende un'infrastruttura digitale basata su un algoritmo che consente alle parti di giungere al consenso per apportare modifiche ad un registro che è per l'appunto *distribuito* tra gli utenti, senza un ente centrale che faccia da garante.

Un registro altro non è che un insieme di dati legati da regole, che normalmente si usa per avere un consenso sui fatti; così abbiamo registri per le proprietà immobiliari, per le auto e via di seguito. Possono essere cartacei o digitali, ma la loro caratteristica nel mondo ante-blockchain, è che sono gestiti da una parte terza nella quale riponiamo fiducia. Viceversa, i "cripto-asset" pur essendo beni "al portatore", quindi non legati ad un fattore identitario trascritto, funzionano tramite il DLT che è gestito contemporaneamente da tutti coloro che ne hanno interesse e che condividono lo stesso sistema di regole, in questo caso un protocollo che ne permette il funzionamento.

Uno dei protocolli del DLT è la blockchain (letteralmente "catena di blocchi") dove il registro è strutturato in blocchi concatenati tra loro. Ogni blocco contiene l'*hash* del blocco precedente (per questo parliamo di catena in cui ogni blocco è collegato al precedente e al successivo). Nei blocchi sono registrate in modo crittografico

e irreversibile le transazioni validate, che sono accessibili e verificabili da tutti i soggetti che condividono il registro.

Ogni blocco di transazioni, per essere aggiunto alla catena, deve essere validato dai *miners* tramite risoluzione di algoritmi complessi. I *miners* sono dei partecipanti alla rete che mettono a disposizione la propria potenza di calcolo per "risolvere" i blocchi di informazioni che devono essere validati. Questo lavoro, che comporta un consumo considerevole di energia elettrica, viene compensato con criptovaluta di nuova emissione. Il *mining* è il processo che consente di giungere al consenso distribuito e verificare i blocchi di transazioni senza il bisogno di ricorrere a un garante terzo. Per verificare la veridicità della transazione (ossia verificare che il mittente sia nelle disponibilità che promette di trasferire) si ricorre alla verifica della storia dei saldi del soggetto coinvolto, registrata eternamente sulla blockchain. In questo modo ogni nodo può verificare la disponibilità dell'asset della controparte. Al termine del processo che conduce al *consenso distribuito*, il blocco di dati verrà aggiunto alla catena preesistente e infine i nodi aggiorneranno la propria copia del registro.

Sintetizzando, la blockchain è una struttura che consente lo scambio di beni nella forma di cripto-asset, tra soggetti anche sconosciuti o meglio che godono del c.d. *pseudonimato*, in modo sicuro, inalterabile ma soprattutto decentrato: in assenza cioè di un soggetto garante che svolga la funzione tradizionale di controllo della correttezza della transazione. In questo ambito si riscontra la finalità del suo creatore[1]: creare un sistema di pagamento elettronico assolutamente sicuro sostituendo il sistema della fiducia nel terzo garante ed eliminando completamente i costi relativi all'intermediazione.

## 1.2 Proof of Work vs Proof of Stake

In un contesto di pagamenti elettronici, uno dei rischi principali è costituito dal fenomeno del "double spending" nel quale, un soggetto in malafede, potrebbe alterare volontariamente la storia delle transizioni per commettere un'azione fraudolenta utilizzando la stessa valuta più volte. Satoshi Nakamoto pensò che l'unico modo per avere sicurezza riguardo l'effettiva disponibilità delle parti in una transazione, senza doversi affidare a una terza parte fiduciaria, fosse quello di verificare la storia dei saldi dei soggetti in questione. Per questo motivo, ebbe l'idea di creare un registro distribuito, visibile a tutti i nodi della rete, che contenesse dal principio tutta la storia delle transazioni.

Il protocollo *Blockchain* prevede la complicazione del processo di validazione del blocco, inserendo un puzzle crittografato al suo interno. Ogni nodo che si offre volontario per validare un blocco di transazioni cercherà di trovare la soluzione del relativo puzzle crittografico. Il primo nodo che risolve l'algoritmo avrà diritto a validare il blocco di transazioni e a ricevere una ricompensa in nuova criptovaluta emessa (entra così in gioco l'incentivo economico). Una volta che il nodo presenta la *Proof of Work*, tutti gli altri nodi ne verificano in modo semplice la correttezza, senza dover risolvere nuovamente il puzzle. Quando gli altri nodi esprimono "il

[1] S. Nakamoto (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online] PDF disponibile al sito: https://bitcoin.org/bitcoin.pdf;

consenso", il blocco di transazioni così validato verrà aggiunto alla catena esistente e la copia della blockchain presente in ogni nodo verrà aggiornata. A questo punto, gli altri nodi smettono di lavorare quel "messaggio" e lo sostituiscono con la catena di blocchi aggiornata che sarà più lunga e a cui corrisponderà un *puzzle* da risolvere più complesso.

Questo appena descritto è il processo di *Proof of Work*, il criterio per la determinazione del consenso che caratterizza il funzionamento della Blockchain di Bitcoin, ma non è l'unico criterio di consenso esistente sulle piattaforme DLT. Un altro criterio diffuso su DLT, è la *Proof of Stake*, secondo cui un minatore di criptovalute ha diritto a convalidare le transazioni proporzionalmente alla quantità di cripto-asset posseduta. La *Proof of Stake* è stata creata come alternativa alla *Proof of Work*, probabilmente per i motivi di consumo energetico che quest'ultima comporta. Il mining, infatti, richiede una grande potenza di calcolo per risolvere gli algoritmi e la potenza di calcolo si traduce in un elevato consumo di energia elettrica. La *Proof of Stake*, invece, assegna il "potere di mining" in base alla valuta detenuta dal soggetto sul presupposto che più grande è la partecipazione ("stake"), ovvero la quantità di token posseduti da un utente, maggiori sono le probabilità che non si stia violando il sistema. Ancora, più un individuo è esposto ad una criptovaluta, più è probabile che questi si comporti in modo ottimale. I blocchi della *Proof of Stake*, a differenza dei blocchi della *Proof of Work*, non vengono *minat*i, ma coniati. I partecipanti che possiedono una partecipazione significativa nei sistemi *Proof of Stake* vengono selezionati su base pseudocasuale per coniare i blocchi e aggiungerli alla blockchain. La *Proof of Stake* viene applicata generalmente alle criptovalute pre-minate, così da consentire all'utente di accedervi attraverso la partecipazione. Ciò significa che l'offerta complessiva delle criptovalute *Proof of Stake* viene fissata sin dall'inizio e che non vi è alcun premio per la creazione dei blocchi, come avviene invece nella *Proof of Work*. L'unico incentivo per i miners in questo sistema è rappresentato dalle commissioni delle transazioni associate allo specifico blocco.

In tema di rischi, la *Proof of Stake* è considerata meno rischiosa dal punto di vista di possibili frodi. Infatti, con la *Proof of Work* si potrebbe verificare un problema riconducibile al fenomeno noto come "La Tragedia dei Beni Comuni[2]" (William Forster Lloyd, 1833) ossia una situazione nella quale, in un momento futuro, il numero dei miners si potrebbe ridurre considerevolmente in seguito alla riduzione del *premio* per aver risolto un blocco di transazioni. Infatti, il protocollo di Bitcoin prevede un processo di *halving*, ovvero ogni 210 mila blocchi minati la quantità di nuova criptovaluta emessa viene dimezzata e contemporaneamente è previsto un quantitativo massimo di bitcoin esistenti, pari a 21 milioni. Considerando che il processo di risoluzione dei blocchi diventa progressivamente più dispendioso, questo potrebbe giustificare la possibile progressiva riduzione dei miners. In un contesto simile, il miner o gruppo di miners che riuscisse a concentrare su di sé una potenza di calcolo pari al 51% della potenza di calcolo totale della rete, potrebbe facilmente attaccarla per commettere azioni fraudolente di *double.spending*: dopo aver approvato col 51% del consenso i blocchi fraudolenti, le transazioni comprese in quei blocchi scompariranno e il denaro tornerà nel portafoglio del

[2] Investopedia.com (2021) *Proof of Stake (PoS)* [Online] Disponibile al sito: https://www.investopedia.com/terms/p/proof-stake-pos.asp;

mittente. Tuttavia, un'ipotesi del genere su reti di criptovalute ormai affermate come Bitcoin o Ethereum è improbabile in quanto le dimensioni del fenomeno renderebbero comunque l'azione nel suo complesso sconveniente; viceversa, una simile fattispecie di attacco potrebbe essere possibile sulle piattaforme di criptovalute minori.

La *Proof of Stake* è considerata generalmente più sicura per due motivi: il primo è che il miner dovrebbe arrivare ad accumulare una quantità di criptovaluta pari al 51% del totale, un processo evidentemente lungo e costoso; il secondo è che da quel momento non sarebbe più nel suo interesse attaccare la rete di un cripto-asset che già possiede in grande quantità.

## 1.3 Token e Coin

La cripto-valuta nativa che dispone di un proprio registro condiviso è anche detta *"coin"* per distinguerla dai c.d. *"token"* che sono una sorta di gettone emesso e scambiato appoggiandosi ad una rete DLT e che legittima il possessore a diritti correlati al cripto-asset in questione. La necessità di questa distinzione sorse da quando, grazie agli *Smart Contracts* di Ethereum, è stato possibile per tutti emettere token tramite *Initial Coin Offering* (ICO) senza creare una blockchain sottostante, ma solo sfruttandone una già esistente. Le transazioni in token tra gli utenti vengono infatti comunque memorizzate sul registro condiviso e la validità della transazione è verificata sia dal protocollo blockchain che da questi *Smart Contracts,* che sono contratti che permettono di eseguire in modo automatico determinate azioni all'avverarsi di determinate condizioni. L'utilità dei token si ravvede nel fatto che sono estremamente frazionabili. Il token Bitcoin, per esempio, può essere frazionato fino a un centomilionesimo di unità, consentendo lo scambio di cifre anche molto esigue. Ad oggi la maggior parte dei token sono emessi sulla blockchain di Ethereum.

## 1.4 Chiavi di autenticazione, wallet ed exchange

### 1.4.1 Chiavi di autenticazione

La crittografia asimmetrica è l'elemento fondante che permette il funzionamento sicuro delle transazioni in cripto-valuta. Di seguito descriverò in termini il più possibile semplici il processo di crittografia e in particolare il modo di utilizzo che se ne fa nell'ambito della Blockchain.

Crittografia è un termine che deriva dal greco: κρυπτός [kryptós] che significa «nascosto», e γραφία [graphía] che significa «scrittura» e nasce per rendere comprensibile un messaggio solo a chi è effettivamente "autorizzato" a leggerlo.

La crittografia può essere semplice o asimmetrica; nella semplice esiste una sola chiave crittografica e il mittente, dopo averla usata per codificare il messaggio dovrà trasmetterla al destinatario per permettergli di decifrarlo, sperando che la chiave non venga intercettata da terzi non autorizzati.

La crittografia asimmetrica viceversa prevede l'utilizzo di due chiavi distinte: il soggetto che vuole inviare un messaggio cifrato possiede una coppia di chiavi legate tra loro, una privata, da conservare segretamente, e una pubblica, visibile a tutti e lo stesso avviene per il destinatario. In questo modo il processo è più sicuro perché non c'è bisogno di scambiarsi le chiavi private.

Facciamo un esempio per capirne meglio il funzionamento: ci sono due soggetti: A, il mittente, e B, il destinatario, che possiedono entrambi la coppia di chiavi di cifratura. A cripterà il messaggio che vuole inviare utilizzando la chiave pubblica di B e lo firmerà utilizzando la propria chiave privata. B, per decifrare il messaggio, dovrà usare la propria chiave privata che corrisponde univocamente alla sua chiave pubblica, che è la stessa usata da A per indirizzare il messaggio. Nel contempo, sarà sicuro della correttezza del messaggio perché questo è firmato digitalmente da A (con la sua chiave privata). Se B volesse in seguito replicare, userà la chiave pubblica di A per criptare il messaggio, la propria chiave privata per firmarlo e così di seguito

Vediamo ora l'utilizzo che se ne fa nell'ambito della blockchain.

Cominciamo col dire che nel protocollo Bitcoin la crittografia viene utilizzata solo come sistema di «Firma Digitale» e non di crittografia del messaggio, i dati delle transazioni sono infatti liberamente consultabili nella blockchain.

Ogni soggetto che vuole eseguire transazioni sulla blockchain deve possedere due chiavi crittografiche: una chiave pubblica e una privata che sono generate da un algoritmo molto complesso partendo da una stringa casuale. Tra le due chiavi vi è una relazione algoritmica in base alla quale dalla chiave privata si ricava la chiave pubblica; non è però possibile il procedimento inverso: dalla chiave pubblica non è possibile cioè risalire alla chiave privata.

La chiave pubblica serve per ottenere il recapito (*bitcoin address*, una sorta di IBAN di un conto corrente) a cui trasferire la somma desiderata, nella forma di asset digitali. La chiave privata, invece, serve per disporre il trasferimento di questi asset. Quindi, per poter eseguire una transazione in Bitcoin, il mittente deve possedere la propria chiave privata e la chiave pubblica del destinatario. Ma affinché la transazione possa efficacemente trasferire la titolarità di bitcoin, dovrà essere verificata. La verifica consiste nel dimostrare il collegamento tra la firma e la chiave privata utilizzata per produrla; questo, senza rivelare la chiave privata, che deve rimanere inaccessibile.

A tal fine, l'algoritmo che verifica la firma prenderà in considerazione: la transazione, la firma, la chiave pubblica del firmatario; la firma risulterà verificata ove si accerti la sua relazione con la chiave privata che ha prodotto la chiave pubblica presa in considerazione per la verifica: la firma risulta verificata ove si accerti che questa non può che provenire dalla chiave privata che ha generato quella pubblica "fornita" per la verifica.

Ma come vengono create le coppie di chiavi? Senza addentrarsi in un percorso matematico particolarmente complesso accenniamo soltanto al fatto che il processo parte dalla generazione della chiave privata da una stringa casuale di caratteri (c.d. entropia iniziale), dalla quale viene derivata tramite una funzione irreversibile

(*Elliptic Curve Digital Signature Algorithm*) la relativa chiave pubblica e, da quest'ultima, viene generato un indirizzo bitcoin.

Il tutto in maniera unidirezionale e irreversibile, ovvero dalla chiave privata si ricava quella pubblica, ma dalla chiave pubblica è impossibile ottenere la chiave privata.

### 1.4.2 Wallet ed exchange

Dal momento che è necessario conservare la chiave privata in massima sicurezza, esistono delle piattaforme che servono essenzialmente per la custodia delle chiavi crittografiche. Questi servizi sono chiamati *wallet* (anche se la parola "portafoglio" può far fraintendere il servizio effettivo dei *wallet,* che è solo di custodia). I fornitori di servizi *wallet* sono dei soggetti terzi (*Custodial Wallet Providers*) che conservano le chiavi crittografiche di soggetti operanti su DLT, sulla base della fiducia che questi ultimi ripongono nel servizio. Possiamo distinguere due macrocategorie di *wallet* in base alla tecnologia implementata: *hot wallet* e *cold wallet*. Gli *hot wallet* sono software che consentono di ricevere e inviare criptoasset tramite applicazioni connesse al web. I *cold wallet* invece consentono solo di custodire le chiavi crittografiche in un luogo fisico sicuro (noto come *cold storage*) non connesso direttamente alla rete.

Appare evidente come il servizio offerto dai *Custodial Wallet Providers* presenti un punto di debolezza. Dal momento che detengono le chiavi pubbliche e private di una grande quantità di soggetti, questi "custodi" potrebbero essere esposti ad attacchi informatici che potenzialmente potrebbero privare gli utenti delle proprie "cripto-disponibilità".

I *Custodial Exchange Provider* (noti comunemente come *exchange*) sono dei soggetti terzi che oltre a fornire il servizio di custodia delle chiavi crittografiche, forniscono la conversione di monete *fiat* in criptoasset, secondo il rapporto di cambio valido in quel preciso momento. Questi Exchange operano come dei tradizionali cambia-valute, con la differenza che questi ultimi non hanno la possibilità di disporre delle quantità detenute dai propri clienti, cosa che gli *exchange* potrebbero teoricamente fare.

In questo ambito, si possono distinguere i *Centralized Exchange Provider* e i *Decentralized Exchange Provider*. I primi, per attuare una qualsiasi conversione (fiat-cripto, cripto-cripto, cripto-fiat) trattengono fondi dei clienti su un *conto escrow*, fino al momento in cui il processo di conversione non sia terminato. Un *conto escrow* è un conto derivante da un accordo commerciale, in base al quale delle somme di denaro vengono trattenute a titolo di garanzia. Al giorno d'oggi, i principali *Centralized Exchange Provider* prevedono a titolo di garanzia il deposito di collaterali costituiti da criptoasset. Questi collaterali sono costituiti dalle cosiddette fiat *pegged token* (o *"asst-backed token*), asset digitali il cui valore è ancorato al valore di una moneta fiat e per questo sono caratterizzati da un tasso di volatilità molto ridotto. I *Decentralized Exchange Provider*, sono invece dei soggetti che non trattengono i fondi dei clienti, ma si limitano a lasciar gestire, in modo interamente autonomo (grazie a opportuni *Smart Contract*) il trading fra gli utenti della piattaforma. "Possono essere

considerati come dei market-place decentralizzati[3] che permettono ai partecipanti della piattaforma di gestire l'incontro fra domanda e offerta, automaticamente". Come per i *Centralized Exchange*, a garanzia delle transazioni vi sono dei *collateral* costituiti da *fiat-backed token* o particolari conti escrow basati su sistemi di multi-firma.

## 1.5 Tipologie di DLT

Dopo aver delineato un inquadramento di base riguardo la tecnologia blockchain e i cripto-asset, possiamo ora classificare le tipologie di reti DLT. In questo senso distinguiamo le DLT in due macrocategorie: *permissionless ledger* e *permissioned ledger.* Per entrambe le tipologie di rete vi è un registro distribuito che tiene traccia di ogni transazione, i nodi sono collegati tra loro in modalità *peer-to-peer* (i nodi non sono organizzati secondo strutture gerarchiche "server-client" in quanto possono svolgere entrambi i ruoli) e le transazioni sono immutabili.

Le reti DLT *permissionless* sono caratterizzate da una completa decentralizzazione: manca la terza parte fidata (*Trusted Third Party*) e l'accesso al registro condiviso non è condizionato in alcun modo. La validazione delle transazioni avviene tramite l'attività di *mining* del blocco e la presentazione della soluzione del puzzle crittografico (*proof of work*) o attraverso altri criteri di consenso. Al termine di questo processo i *miners* vengono ricompensati tramite emissione di nuove criptovalute. Inoltre, gli attori che operano su DLT *permissionless* non possono essere identificati in maniera diretta, in quanto si può risalire solo allo pseudonimo con cui il soggetto si è autenticato per la prima volta (in questo senso viene usato il termine "pseudonimato" cui si accennava all'inizio del capitolo). In questo modo si ha la sicurezza riguardo l'indirizzo che ha originato la transazione, ma non può essere identificata la persona fisica che possiede la chiave privata di quell'indirizzo.

Al contrario, le reti DLT *permissioned* sono governate da un'Autorità Centrale alla quale è affidata il compito di validare le transazioni e di governare l'accesso al registro distribuito. In questo modo l'accesso al ledger viene ristretto e la validazione delle transazioni è affidata ad entità appositamente incaricate che vengono ricompensate tramite condivisione di ricavi. Gli attori che operano su DLT *permissioned* sono necessariamente noti in quanto identificati a priori dalla terza pare fidata. Queste entità non devono presentare alcuna proof-of-work, non avendo bisogno di competere al fine di pervenire a un consenso distribuito, poiché la fiducia di cui essi godono è riconosciuta per "investitura" (Banca d'Italia, 2019). Questo tipo di configurazione può rilevarsi

[3] Banca d'Italia Eurosistema (2019) *Quaderni di Ricerca Giuridica della Consulenza Legale Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* n.87 a cura di Fabrizio Maimeri e Marco Mancini [PDF] disponibile al sito: qrg-87.pdf (bancaditalia.it);

utile per quelle organizzazioni (aziende, istituzioni finanziarie, banche…) che vogliono sfruttare i benefici di efficienza della blockchain, senza però cedere in termini di *governance.*

Alla luce di questa prima distinzione, si possono ulteriormente classificare le DLT in reti pubbliche, private o ibride. Le reti pubbliche seguono il funzionamento delle DLT *permissionless*: chiunque può partecipare alla rete e le transazioni vengono validate secondo il processo di *proof of work* precedentemente descritto. Nelle DLT *permissioned* pubbliche, tutti i partecipanti alla rete (precedentemente identificati ed autorizzati ad accedere alla stessa) sono in grado di verificare i dati ed eseguire transazioni. Nelle *permissioned* private, invece, l'ente centrale che si occupa della governance della rete può limitare queste azioni ai soli utenti da lui stesso autorizzati. Nelle DLT ibride, invece, il solo processo di validazione viene assegnato ad una parte terza fidata. In questa configurazione, l'ente centrale può distribuire responsabilità e poteri ai partecipanti alla rete secondo le esigenze specifiche della DLT, riuscendo così a moderare l'accentramento di poteri e funzioni tipico delle DLT private.

## 1.6 Benefici blockchain

Dopo aver introdotto i concetti chiave riguardo al funzionamento della *blockchain* e dei *criptoasset*, passerò ad esaminare nel dettaglio in che modo le caratteristiche innovative di questa tecnologia sono destinate ad influenzare in maniera permanente il nostro futuro.

Decentralizzazione e disintermediazione sono i primi due elementi che consideriamo; sono quelli che determinano il carattere *trustless* della piattaforma. Abbiamo quindi un'infrastruttura digitale dove la sicurezza e la resilienza delle operazioni è garantita tramite distribuzione dei ruoli tra una pluralità di nodi e non da una terza parte fidata che viene sostituita da meccanismi crittografici che conducono al consenso distribuito. Il terzo carattere fondamentale è la programmabilità della piattaforma. Alcuni sistemi blockchain, infatti, possono essere utilizzati come "fondamenta" per programmare determinati servizi o implementare specifiche innovazioni. Il tutto gestito da opportuni *Smart Contracts* che permettono la conclusione di veri e propri contratti al verificarsi di determinate condizioni. Quindi, ritroviamo nella blockchain il carattere di *generativity*, considerato come il valore aggiunto apportato da piattaforme digitali open-source utilizzate come base per ulteriori sviluppi tecnologici. Di seguito, la blockchain si differenzia per il carattere di immutabilità, in quanto una volta che vengono inseriti i dati, questi diventano pressoché immodificabili, e di verificabilità, ossia la facilità con cui qualunque nodo può accertarsi della veridicità delle informazioni e la relativa marcatura temporale. Infine, gli ultimi elementi, strettamente connessi tra loro, caratterizzanti della blockchain, sono la tracciabilità e la trasparenza. Infatti, ogni transazione è tracciabile nel senso che è possibile ricostruire la storia dell'asset e il contenuto del registro distribuito è visibile da ogni nodo, quindi è trasparente.

Alla luce delle caratteristiche presentate, è facile capire il motivo per cui l'invenzione di questa tecnologia abbia suscitato un grande e diffuso interessamento, nei primi tempi solo tra gli addetti al settore, ma

progressivamente sempre più su larga scala, fino a diventare, ad oggi, un "fenomeno" globalmente riconosciuto.

## 1.7 Applicazioni tecnologia settore bancario

Tradizionalmente, il controllo sulle transazioni di un certo rilievo è affidato ad un'entità terza (*Trusted Third Party*) che esegue il compito di vigilanza al fine di garantire la consistenza delle stesse. Intermediari come banche, assicurazioni o notai presiedono allo scambio commerciale e annotano su un registro i movimenti dei dati dei soggetti coinvolti in esso. Questo scenario è indicato con l'appellativo *trust-based*, in quanto, queste terze parti sono dotati di una fiducia generale e fanno da garanti per il corretto svolgimento di registrazione e validazione della transazione. La custodia delle informazioni da parte di un unico ente centrale però espone l'utente a dei rischi, tra i quali la perdita parziale o totale delle informazioni conservate. Adottando un sistema blockchain viene meno la necessità della terza parte fidata, in quanto il registro dei dati non è più gestito da un ente unico, bensì è distribuito digitalmente tra tutti i nodi della rete, che lo aggiornano alle condizioni di operatività viste prima. Come detto in precedenza, la consistenza dello scambio viene garantita da un algoritmo che conduce al consenso distribuito (come abbiamo visto in precedenza, il più diffuso è quello basato sulla *proof-of-work*). Si configura quindi uno scenario *trust-less*, la sicurezza della transazione e quella generale del sistema non è garantita da una TTP, bensì dallo stesso protocollo di funzionamento della blockchain. Sebbene il carattere *trust-less* sia il vero elemento innovativo del paradigma, si osserva come le principali iniziative avviate dalle banche si basino su reti DLT *permissioned*, comunemente note come blockchain private[4].

I vantaggi dell'applicazione di un sistema blockchain piuttosto che un sistema basato sulla fiducia, possono essere sintetizzati in una maggiore resilienza della struttura e una maggiore efficienza negli scambi. La resilienza, definita come la capacità del sistema di far fronte ad eventi negativi è garantita dalla crittografia alla base della piattaforma e dalla tracciabilità e verificabilità delle transazioni, in modo che sia possibile risalire a ritroso all'esatto indirizzo di provenienza. La possibilità di perdere le informazioni custodite è limitata dall'aggiornamento delle copie del registro da parte di numerosi nodi. Inoltre, il carattere decentrato della DLT permette di inibire qualsiasi comportamento opportunistico da parte di un utente a scapito degli altri. In termini di efficienza i vantaggi invece sono riscontrabili nell'eliminazione o comunque nella riduzione dei costi di transazione, nel processo di disintermediazione e nell'efficientamento dei processi di aggiornamento del registro.

[4] ABILab (2021) *Spunta Banca DLT,* Rapporto ABILab. [Online] PDF disponibile al sito: https://www.abilab.it/documents/20124/0/Descrizione+iniziativa+Spunta+Banca+DLT.pdf/1a458e5c-29d7-cdbc-2bda-554ea70bd3e8?t=1590615492283;

La tecnologia basata su blockchain/reti DLT offre un ampio spettro di applicazioni nel settore bancario. Al giorno d'oggi la maggior parte delle banche e degli intermediari finanziari hanno reagito a questa innovazione implementando un dipartimento c.d. "fintech" che si occupi di studiare quali sono gli ambiti che maggiormente potrebbero sfruttare i miglioramenti in termini di efficienza e sicurezza nei processi operativi. Gran parte delle iniziative sono ancora in fase di studio e sperimentazione, ma già sono state individuate le possibili macroaree di applicazione: pagamenti, finanza, credito e Know Your Customer. Tra questi, l'ambito finanziario (nelle attività di trading e collateral management) è quello a cui si è rivolta la maggiore attenzione, come riporta il Rapporto ABILab 2021, che indica come a livello globale, 67 dei 158 progetti in esecuzione basati su DLT, appartenga al settore finanziario.

Anche in Italia, i principali intermediari finanziari stanno attuando una fase di sperimentazione su progetti basati su DLT: dai dati forniti dal rapporto ABI LAB, *Rivelazione sulle priorità ICT delle Banche Italiane*, si evince che circa il 50% dei rispondenti considera la tecnologia DLT una priorità d'indagine, ma se l'analisi si circoscrive alle banche di maggiori dimensioni, la percentuale sale fino al 70%. Inoltre, dal rapporto emerge che il settore in cui si è investito di più, è quello dei trasferimenti interbancari. Infine, circa il 60% delle istituzioni esaminate utilizzano una rete permissioned, solo il 10% di questi ha adottato una rete permissionless (mentre il restante 30% non ha scelto ancora la configurazione preferita).

### 1.7.1 Progetto Spunta Interbancaria DLT

Il settore bancario italiano si è sempre dimostrato particolarmente dinamico nell'adattamento all'innovazione e non a caso è all'avanguardia anche in ambito blockchain/DLT. Infatti, una delle prime iniziative concrete destinata a coinvolgere l'intero settore nazionale è stata la c.d. "Spunta Banca DLT". Il progetto in questione, promosso da ABILab[5] si pone l'obbiettivo di innovare e ridisegnare il processo di spunta interbancaria, definito come "un processo di verifica della corrispondenza delle attività che interessano due banche diverse". Il processo di spunta riguarda il regolamento dei conti reciproci e la gestione dei sospesi, un'attività di carattere amministrativo tradizionalmente a carico del *back office.*

Il processo di spunta interbancaria era precedentemente regolato da un accordo interbancario del 1978, aggiornato in seguito nel 1987 e ulteriormente modificato nel 1991 e nel 1994. Quindi, il Progetto Spunta, ha rappresentato anche un'occasione per aggiornare una normativa ormai datata. Nel maggio 2019 il Comitato Esecutivo ABI ha approvato l'aggiornamento dell'accordo interbancario, inserendo il capitolo 18-bis, in cui

[5] ABI sito web (2019) *Spunta Project avvia test blockchain su operatività a regime* [Online] Disponibile al sito: https://www.abi.it/Pagine/news/Spunta-project- -test.aspx#:~:text=La%20spunta%20%C3%A8%20un%20processo%20interbancario%20basato%20su,standardizzazione%2C%20%C3%A8%20caratterizzato%20da%20modalit%C3%A0%20operative%20non%20avanzate.;

viene descritta la nuova operatività del processo basato su DLT. In particolare, il progetto "Spunta Banca DLT" si pone un duplice obiettivo: quello di sperimentare una tecnologia innovativa capace di apportare notevoli benefici in termini di efficienza, e quello di creare un'infrastruttura digitale (l'ABILabChain) capace di ospitare, in un futuro prossimo, nuovi progetti basati su DLT. L'ABILabChain rappresenta il network, basato su un sistema DLT privato, delle banche aderenti al progetto, con regole di governance comuni a tutti i partecipanti. Nel corso del 2019 si sono tenute delle fasi di prova e sperimentazione del progetto per testare la capacità e la sostenibilità della piattaforma in termini di volume di dati delle banche dell'intero settore italiano. Dopo il successo dei test tecnici, nel periodo compreso tra marzo e ottobre 2020, sono state attuate, con esito positivo, le tre "onde di migrazione" delle banche aderenti al progetto. I principali vantaggi per il settore nell'adozione della tecnologia DLT per il processo di spunta sono: una maggiore e immediata trasparenza riguardo i movimenti propri e della controparte, una riconciliazione dei flussi su base giornaliera, invece che mensile, e una riduzione del rischio operativo attraverso l'applicazione di regole comuni ad ogni nodo della rete. L'effetto finale è quello di un incremento generale della qualità del processo di spunta, ottenuto attraverso un efficientamento delle operazioni e una maggiore velocità nella gestione dei conti.

È evidente come il valore aggiunto di questa iniziativa pioneristica e circoscritta vada ben al di là del miglioramento qualitativo dello specifico processo di spunta e "si sostanzia nell'opportunità di sperimentare e utilizzare sul campo una tecnologia innovativa e soprattutto realizzare un'infrastruttura capace di abilitare ulteriori casi d'uso, anche più orientati verso un'ottica business" (ABILab, 2021). Infatti, il processo di spunta interbancaria non porta elevati benefici in termini economici; il surplus apportato dall'iniziativa è quello di aver creato una piattaforma DLT capace di ospitare ulteriori *use case*, che contribuiranno al processo di rinnovamento del settore bancario, particolarmente vulnerabile alle forze innovative esterne soprattutto pensando che l'innovazione di cui trattasi volge all'eliminazione delle terze parti e potrebbe influire in maniera drastica nella governance dei processi che hanno da sempre costituito l'attività *core* del sistema bancario.

# 2. CRIPTOVALUTE

## 2.1 Bitcoin

### 2.1.1 Cenni Storici

Era il 31 ottobre 2009, quando il dominio *bitcoin.org* compariva per la prima volta in una mailing list di un sito di crittografia (metzdowd.com). Un utente della piattaforma, usando lo pseudonimo di Satoshi Nakamoto, asseriva di aver creato un sistema di pagamenti virtuali incensurabile e decentrato, che quindi non avesse bisogno di una terza parte fiduciaria. Il *white paper*, allegato dal giapponese, si diffuse molto velocemente tra i membri delle community di siti di crittografia, che ne avevano riconosciuto immediatamente l'appetibilità e il potenziale di un sistema monetario *trust-less*. Si rese dunque subito disponibile una rete di programmatori e informatici pronti a sperimentare questo sistema *peer-to-peer* (P2P) di pagamenti virtuali. Dopo alcune settimane, il 3 gennaio 2009, venne generato il *genesis block*, il primo blocco di Bitcoin. Nel blocco 0 venne trascritta la celebre frase "*The Times 03/Jan/2009 Chancellor on brink of second bailout for bank*" ossia "Il cancelliere è in procinto di effettuare un secondo salvataggio per le banche". Il messaggio di testo cita il titolo del quotidiano americano *New York Times* che alludeva alle numerose e ingenti operazioni bancarie messe in atto dalle Federal Reserve (e da tutte le Banche Centrali) al fine di salvare le numerose banche condotte sull'orlo del fallimento in seguito alla crisi finanziaria del 2008. Appare fin da subito chiaro il fine ultimo dello sconosciuto giapponese: creare un sistema di pagamenti virtuali incensurabile e incorruttibile con "l'obiettivo di minare il sistema oligopolistico delle banche al fine di rendere irrilevante il ruolo degli intermediari finanziari[6]". Bitcoin nasce quindi con un duplice fine: quello di sostituirsi al sistema finanziario tradizionale, che secondo il creatore della rete sarebbe stato soggetto negli anni a numerose altre crisi finanziarie, e quello di creare un network di pagamenti completamente decentralizzato, nel quale la trasmissione di ricchezza tra individui possa avvenire senza ricorrere a una terza parte fiduciaria, e quindi senza incorrere nei rischi ad essa collegati.

Pochi giorni dopo che fu rilasciato il primo client Bitcoin Open Source, il 12 gennaio 2009 venne effettuata la prima transazione, consistente in 10 bitcoin. Da questa data iniziò la diffusione virale di bitcoin, tramite la creazione del forum *BitcoinTalk* e la nascita delle prime piattaforme operanti come *exchange*. Ad ottobre dello stesso anno, venne stabilito il prezzo di mercato del bitcoin, originariamente pari a 0,0007 dollari. Nell'anno seguente, il 22 maggio 2010, venne effettuato il primo acquisto in bitcoin, nel quale un uomo americano, per dimostrare l'efficacia del sistema, pagò due pizze, dal valore di 25 dollari, con 10.000 bitcoin (che al tasso di cambio attuale corrispondono a circa 560 milioni di dollari). Tra il 2013 e il 2015 la criptovaluta fu soggetta ad una serie di eventi negativi che portarono il valore della stessa ad una drastica riduzione. Tra questi possiamo ricordare nel 2013, l'arresto del fondatore di Silk Road, una piattaforma illegale per lo scambio di armi e droga che utilizzava il bitcoin come moneta principale. Successivamente, a dicembre dello stesso anno,

[6] Comandini G. (2020) *Da zero alla Luna: quando, come, perché la Blockchain sta cambiando il mondo,* Palermo: Dario Flaccovio Editore;

Cina e Norvegia proibirono l'impiego del bitcoin, il che causò la chiusura di uno dei mercati più estesi al mondo. Infine, nel febbraio 2014, Mt. Gox, una dei primi *exchange* mai creati, annunciò la perdita di 850.000 bitcoin, in seguito ad un attacco hacker, dichiarò fallimento e non riuscì a rimborsare i clienti delle quantità rubate. Questa serie di eventi impattò fortemente sulla fiducia che gli investitori riservavano nella criptovaluta, causando una simultanea riduzione nel suo valore (una perdita di oltre 80%). La fiducia verso la criptovaluta si trovò allora ai minimi storici, tanto che la dottrina prevalente ne sancì (ancora una volta) la morte prematura. Tuttavia, tra il 2015 e il 2017, tornò a crescere l'interessamento verso bitcoin e per la prima volta anche verso la tecnologia sottostante: la blockchain. Il prezzo riprese a crescere e a raggiungere cifre considerevoli, anche grazie al *fork*[7] della blockchain, avvenuto in agosto 2017, che portò alla creazione di Bitcoin Cash, una variante di Bitcoin, con la dimensione dei blocchi estesa da 1 a 8 MB. Nel novembre 2017, il valore della criptovaluta arrivò a toccare il picco dei 10.000$. Ciò portò alla nascita di alcuni contratti derivati (*futures*) che avevano come sottostante Bitcoin. Dal 2017 a fine 2020, il valore della criptovaluta è oscillato tra i 4.000 e 13.000 dollari; dall'ottobre 2020 fino al momento in cui si scrive, il valore del Bitcoin ha seguito una crescita vertiginosa, riuscendo a superare la soglia dei 60.000$ nel marzo 2021. Questo drastico incremento lo si può ricondurre a diversi fattori. Il principale è sicuramente un aumento dell'interessamento e del coinvolgimento generale sulla materia da parte sia dei piccoli risparmiatori, ma anche da parte di investitori istituzionali e grandi aziende.

Satoshi Nakamoto decise di dare alla sua moneta virtuale una natura deflattiva controllata. Il sistema su cui si basa Bitcoin è regolato da un algoritmo secondo il quale ogni quattro anni, la ricompensa in bitcoin (o *reward*) per il *mining* del blocco, si dimezza. Il processo appena descritto, noto come *Halving* (letteralmente "dimezzamento") è un evento che conduce alla riduzione programmata della criptovaluta emessa ogni 210.000 blocchi minati, fino al momento in cui i bitcoin in circolazione raggiungeranno numericamente i 21 milioni (si stima nel 2136 circa). La natura deflattiva del bitcoin potrebbe, negli intenti del suo creatore, rappresentare un meccanismo interno al protocollo, volto a sostenere nel tempo il valore della valuta virtuale. Una curiosità: i minatori del gruppo F2Pool, che hanno validato il blocco numero 629.999 (ossia l'ultimo blocco prima del terzo *halving*) hanno voluto omaggiare Satoshi Nakamoto trascrivendo all'interno del blocco il titolo del *New York Times* del 9 aprile 2020: *With $2.3T Injection, Fed's Plan Far Exceeds 2008*. Il titolo si riferisce alle operazioni bancarie condotte dalla Fed (pesanti iniezioni di liquidità sul mercato) in risposta alla crisi economica causata dalla Pandemia. Appare chiaro il riferimento al titolo del quotidiano statunitense trascritto da Satoshi Nakamoto sul blocco genesi, per ribadire, 12 anni dopo, una critica diretta ad un sistema finanziario obsoleto e prossimo al collasso.

[7] Un *fork* si genera quando viene creata una versione di protocollo differente da quella originale. I fork servono per risolvere problemi che affliggono il protocollo base, o comunque per aggiornarlo e inserire nuove funzionalità. Si parla di *hard fork* quando il nuovo software non presenta soluzioni di retrocompatibilità con quello originale, ed entrambi continuano ad operare indipendentemente l'uno dall'altro. Al contrario è definito *soft fork* un aggiornamento del software retrocompatibile con la versione precedente. In seguito ad un *soft fork* anche gli utenti che non hanno eseguito l'upgrade potranno continuare ad operare sulla rete insieme a quelli che lo hanno eseguito.

Ad oggi, riguardo il futuro di Bitcoin, si dividono due ideologie predominanti e diametralmente opposte. La prima è costituita da tutti quei soggetti che ritengono che il Bitcoin sia una bolla speculativa a fronte di un valore del criptoasset troppo distante dai fondamentali tipici di una valuta e che quindi se acquistano cripto-valuta lo fanno solo per realizzare un profitto immediato con uno spread positivo. La seconda, minoritaria, si compone di tutte quelle persone che invece "credono nel progetto", ossia chi ha investito nella criptovaluta in un'ottica di medio periodo (*buy-and-hold*), cioè senza fini speculativi nel breve termine. Solo il tempo potrà stabilire chi dei due abbia ragione.

### 2.1.2 Utilizzo effettivo e limiti pratici

A fronte delle proprietà chiave di Bitcoin, intese come l'insieme delle caratteristiche (quali decentralizzazione, sicurezza, trasparenza e velocità) che lo rendono un sistema di scambio innovativo e per certi versi appetibile a confronto dei canali tradizionali, bisogna tenere presente l'esistenza di un certo numero di elementi che invece sono portatori di esternalità negative. I principali fattori, intrinsechi al protocollo Blockchain, che rendono l'utilizzo quotidiano della criptovaluta non sostenibile sono: la volatilità, la limitata scalabilità e il consumo energetico.

Il primo limite che si contrappone ad un utilizzo quotidiano dello strumento è l'elevata volatilità, ossia la tendenza dell'asset digitale a subire variazioni di prezzo accentuate e imprevedibili. Le criptovalute sono asset altamente volatili: non avendo un'attività reale come sottostante ed essendo prive di valore intrinseco, il loro valore è determinato essenzialmente dalle aspettative razionali degli investitori. Inoltre, il BTC non è una passività di alcun ente emittente e non c'è nessuna autorità competente volta a garantirne la stabilità del valore. I caratteri enunciati in precedenza, uniti ai profili di rischio in tema di *cyber-security* e alla mancanza di una regolamentazione ufficiale, fanno sì che il BTC sia scambiato tra un numero ancora ristretto di investitori. Tutto ciò rende il suo mercato altamente illiquido. È ravvisabile, negli intenti dello sconosciuto giapponese, la previsione di una progressiva riduzione della volatilità, come conseguenza all'incremento di numero degli attori operanti nella rete e una sua più ampia diffusione globale. Tuttavia, oggi, l'utilizzo dell'asset digitale come mezzo di pagamento risulta marginale, a fronte del basso grado di accettazione. Dunque, tra i motivi delle scelte di investimento in BTC, rientrano marginalmente il fine precauzionale, ossia la detenzione di valuta virtuale come riserva di valore nel tempo e principalmente il fine speculativo, inteso come la ricerca di un profitto nel breve termine dato dalla differenza tra prezzo di acquisto e di vendita.

Oltre alla volatilità, uno dei problemi principali di Bitcoin è rappresentato dalla sua ridotta scalabilità. Una blockchain risulta scalabile, se è in grado di gestire un progressivo aumento nel volume delle transazioni. L'unità di misura della scalabilità di una piattaforma è misurata in TPS (*Transaction Per Second*), ossia dal numero di transazioni al secondo. In tal senso, la Blockchain non è scalabile, a causa della limitata grandezza dei blocchi (1MB), cui corrisponde un limitato numero di transazioni, il che allunga considerevolmente i tempi di elaborazione e di conferma delle transazioni. Il tempo impiegato per generare un nuovo blocco (*Block Time*)

è fissato pari a 10 minuti, mentre è stimato che all'interno di un singolo blocco rientrano solo circa 2000 transazioni. Ciò significa che la Blockchain è in grado di processare dalle 4 alle 7 transazioni al secondo, dei numeri troppo esigui rispetto a quelli di circuiti come VISA o Mastercard, che processano in media 150 milioni di transazioni al giorno, ad una velocità di circa 2000 TPS. Se il numero di transazioni supera il massimo gestibile dalla Blockchain, vengono messe in coda ed elaborate successivamente, creando un congestionamento dell'intera rete. Come risultato avremo quindi un rallentamento nella capacità di elaborazione e un aumento delle commissioni pagate dagli utenti. Si genera questo circolo vizioso in quanto i *miner* danno priorità di validazione alle transazioni che offrono commissioni più elevate mettendo in coda quelle con commissioni ridotte. La scalabilità di Bitcoin rappresenta un ostacolo all'impiego di tutti i giorni della valuta virtuale, in particolare per le transazioni più esigue. Per risolvere questo problema, nell'agosto del 2017, la rete di programmatori di Bitcoin decise di dare avvio a un *hard fork* della Blockchain, sviluppando un software non retrocompatibile con il protocollo originale (*Bitcoin Cash*) che prevede l'aumento della dimensione dei blocchi a 8 MB.

L'elettricità che viene consumata nel processo di estrazione di Bitcoin è diventato un argomento molto dibattuto negli ultimi anni, in quanto l'impatto ambientale di un'attività è una variabile che ormai deve essere considerata da ogni operatore economico al fine di ridurre le esternalità negative. Come abbiamo visto precedentemente il processo di *Proof of Work* (PoW) è essenziale per l'attività di validazione delle transazioni e per risolvere il problema di *double spending*, elemento critico nei pagamenti digitali. Tuttavia, è la stessa PoW che rende Bitcoin estremamente dispendioso dal punto di vista energetico, poiché richiede una potenza di calcolo direttamente proporzionale al numero di *miner* che competono per la validazione del blocco. Questi competono per l'elaborazione del blocco al fine di ricevere criptovalute di nuova emissione. Maggiore è la potenza di calcolo apportata, maggiore sarà la probabilità di validare per primo il blocco. Quindi più aumenta il numero di *miner* (e quindi la potenza computazionale apportata al protocollo), maggiore sarà la difficoltà dei puzzle crittografici che essi dovranno risolvere. La Blockchain richiede quindi un aumento di energia proporzionale alla diffusione della valuta virtuale sul globo. Secondo il *Cambridge Bitcoin Electricity Consumption Index*[8] è stimato che la rete Bitcoin sia passata da un consumo annuo medio pari a 30 Terawatt orari di elettricità nel 2018, rendendola paragonabile a paesi come l'Irlanda, fino ad arrivare, nel 2021, ad un consumo medio annuo pari a 140 Terawatt orari[9], più di quella consumata da nazioni come la Norvegia (124

[8] Cambridge Bitcoin Electricity Consumption Index, 2021. [Online] Disponibile al sito: https://cbeci.org/;

[9] Il Cambridge Bitcoin Electricity Consumption Index (CBECI) fornisce una stima in tempo reale del consumo totale di elettricità della rete Bitcoin. Il modello si basa su un approccio bottom-up sviluppato inizialmente da Marc Bevand nel 2017 che prende come punto di partenza diversi tipi di hardware di mining disponibili. Dato che il consumo esatto di elettricità non può essere determinato, il CBECI fornisce una gamma di possibilità che consiste in una stima del limite inferiore (floor) e superiore (ceiling). Entro i confini di questo intervallo, viene calcolata una stima di massima per fornire una cifra più realistica del consumo annuale di elettricità di Bitcoin. La stima del limite inferiore corrisponde al minimo assoluto della spesa totale di elettricità basata sull'ipotesi migliore che tutti i minatori usino sempre l'attrezzatura più efficiente, dal punto di vista energetico, disponibile sul mercato. La stima del limite superiore specifica la spesa totale di elettricità massima, basata sull'ipotesi peggiore, in cui tutti i

TWh) o l'Argentina (121 TWh). È innegabile che l'*energy footprint* rilasciata da Bitcoin stia diventando problematica dal punto di vista dell'inquinamento ambientale, soprattutto dal momento che i paesi dove si concentrano le maggiori attività di "estrazione" della valuta virtuale sono Cina e USA, due paesi che ricavano il proprio fabbisogno energetico tramite la combustione di carbone e altre energie fossili.

## 2.2 Altcoin

Sono definite *Altcoin* tutte le criptovalute diverse dal Bitcoin. Il termine deriva da *alternative coin* ed è utilizzato per individuare tutti le criptovalute nate dopo il Bitcoin. La loro diffusione è iniziata circa due anni dopo la pubblicazione del *white paper* da parte di Satoshi Nakamoto, dal momento che una pluralità di soggetti si era resa conto delle enormi potenzialità della tecnologia alla base.

La struttura di base delle *altcoin* è simile a quello del Bitcoin: sono basate sulla stessa tecnologia *peer-to-peer*, ma differiscono da essa per gli obiettivi per cui sono progettate. Generalmente le *altcoin* sono sviluppate dallo stesso codice sorgente di Bitcoin, al quale vengono successivamente sostituite alcune variabili al fine di modificare delle specifiche funzionalità. Molte delle *alternative coin* infatti hanno lo scopo di migliorare o sostituire alcuni aspetti critici del Bitcoin.

A maggio 2021, si stimano poco meno di 10.000 *altcoin* in circolazione, con una capitalizzazione di mercato pari al 60% del mercato criptovalutario totale[10]. Poichè sono derivate dal Bitcoin, i movimenti dei prezzi tendono a imitare la traiettoria del Bitcoin. Tuttavia, gli analisti sostengono che una volta raggiunta la maturità degli ecosistemi su cui sono basate, i movimenti di prezzo delle *altcoin* risulteranno indipendenti dalle fluttuazioni della "criptovaluta madre".

### 2.2.1 Ethereum

Se la Blockchain di bitcoin rappresenta un sistema *peer-to-peer* che mira a decentralizzare il modello tradizionale di pagamenti virtuali, quella di Ethereum ha lo scopo di creare un sistema contrattuale parallelo a quello tradizionale al fine di sostituire le terze parti di Internet che memorizzano i dati (Comandini, 2020).

Ethereum è una specifica piattaforma open-source basata su blockchain, ideata nel 2013 e lanciata nel 2015 da Vitalik Buterin, uno sviluppatore russo ventenne. Ethereum viene spesso descritto con il termine "computer mondiale", in relazione alle sue funzionalità. La peculiarità di tale piattaforma è quello di essere una *programmable blockchain*: Ethereum fornisce un linguaggio di programmazione completo di Turing che consente agli utenti di realizzare svariate tipologie di applicazioni decentralizzate, non necessariamente

minatori usino sempre l'hardware meno efficiente dal punto di vista energetico, finché il funzionamento dell'attrezzatura è ancora redditizio in termini di elettricità.

[10] Coinmarketcap.com (2021) *Cryptocurrencies Capitalization* [Online] Disponibile al sito: https://coinmarketcap.com/it/;

circoscritte alla sola attività di scambio di ricchezza tipica di Bitcoin. Le *Decentralized Applications Apps* (DApps) sono applicazioni implementate su una rete decentralizzata (tramite opportuni *smart contract*) che per tale motivo, non hanno necessità della supervisione da parte di un entità centrale di vigilanza. Un'ulteriore utilità pratica fornita dalla piattaforma, è quella di consentire agli utenti di costituire delle *Initial Coin Offering* (ICO). Le ICO rappresentano un meccanismo ibrido di finanziamento, a metà tra *Crowdfunding* e *Initial Public Offering* (IPO). Le ICO permettono di effettuare una raccolta fondi che prevede lo scambio di token dell'emittente a fronte di una certa quantità di moneta *fiat* o di altre valute virtuali. Le ICO rappresentano un metodo di finanziamento alternativo per aziende o Startup, nelle quali gli investitori scelgono di partecipare al fine di ottenere un profitto sull'eventuale vendita futura dei token ottenuti.

Uno *smart contract* è definito come "la trasposizione in codice di un contratto in grado di verificare automaticamente il realizzarsi di determinate condizioni e quindi di eseguire in automatico le azioni previste dal contratto" (Comandini, 2020). Nonostante gli *smart contract* esistessero già agli inizi degli anni '90, è solo tramite l'avvento della blockchain che questi ultimi hanno acquisito rilevanza, rendendo possibile l'esecuzione automatizzata del contratto senza ricorrere ad una terza parte fiduciaria. Una volta che il codice del contratto viene inserito nella rete decentralizzata, quest'ultimo viene replicato immutabilmente su tutti i nodi della rete, in modo da non poter essere modificato ulteriormente. Quando le parti giungono all'accordo, sono consapevoli che non c'è alcuna possibilità di violarlo: "*Ethereum is a decentralized platform that runs programs exactly as programmed without any possibility of downtime, fraud, censorship and third-party interference*[11]"

La valuta virtuale nativa della blockchain di Ethereum è chiamata Ether (ETH), la quale, ad oggi, è l'*altcoin* più diffusa al mondo (seconda solo a bitcoin per capitalizzazione di mercato). L'Ether, come Bitcoin, è una vauta virtuale decentralizzaa che utilizza metodi crittografici per essere creata e scambiata. Tuttavia, a differenza di Bitcoin, ha una "valenza binaria" (Comandini, 2020) poiché viene utilizzata sia come risorsa computazionale per produrre gli *smart contract*, sia come compenso per gli sviluppatori per la loro realizzazione. Ogni operazione che viene svolta su ethereum, come le transazioni o la creazione di *smart contract*, ha un costo noto come Ethereum Gas. Questo rappresenta un *Internal Transaction Pricing Mechanism*, ovvero un meccanismo interno adibito alla determinazione del prezzo da pagare per svolgere delle operazioni su Ethereum. Questo prezzo ha un valore fisso ed è pagato in Ether. Il Gas rappresenta l'energia che serve a far funzionare l' *Ethereum Virtual Machine* (EVM) intesa come "motore" della piattaforma (centro di calcolo), che garantisce la corretta esecuzione degli *smart contract* e l'implementazione del meccanismo di consenso che governa la rete.

Anche ethereum si basa sull'attività di *mining* per l'emissione di nuovi Ether e sul meccanismo di consenso di *Proof of Work* (anche se si stà progettando un meccanismo per passare alla *Proof of Stake* in relazione agli

[11] Coinbase.com (2021) *Cos'è Ethereum?* [Online] Disponibile al sito: https://www.coinbase.com/it/learn/crypto-basics/what-is-ethereum;

alti costi energetici della PoW) . Anche per quest'ultima è stata stabilita una fornitura massima annuale, pari a 18 milioni di unità, mentre il tempo di elaborazione di un singolo blocco è pari a 12 secondi.

In relazione alla sua programmabilità ed elasticità, Ethereum è considerato uno dei progetti più importanti in ambito Blockchain date i numerosi ambiti applicativi.

### 2.2.2 Ripple

Ripple (XRP) è una criptovaluta ideata e sviluppata nei Ripple Labs di San Francisco nel 2013, ad opera dei co-fondatori Chris Larsen e Jed McCaleb. Il termine Ripple indica sia il nome della valuta virtuale sia la piattaforma *open-source* decentralizzata su cui viene scambiata.

Al contrario di Bitcoin, Ripple ha una natura finanziaria: nasce cioè per soddisfare specifiche esigenze delle banche e degli intermediari finanziari, garantendo velocità, sicurezza e tracciabilità delle transazioni. Definita come la criptovaluta delle banche, Ripple si propone come una piattaforma scalabile che può essere usata per facilitare gli scambi interbancari con bassi costi di commissione. Ripple si configura come un network di pagamenti governato da uno specifico algoritmo di consenso basato sulla presenza di un soggetto validatore (*Ripple Consensus*), e un registro distribuito (*Ripple Consensus Ledger*) su cui vengono archiviate immutabilmente tutte le informazioni. Il sistema virtuale di pagamenti si basa sulla circolazione di crediti IOU ("I Owe You") denominati in XRP, che definiscono la situazione dei saldi tra gli utenti. Attraverso questo network di pagamenti digitali si possono effettuare trasferimenti di denaro "senza continuità di forma" (Comandini, 2020). In questo modo, gli utenti possono eseguire transazioni in qualsiasi valuta (monete *fiat* o altre criptovalute in loro possesso) che verranno convertite in Ripple, tramite appositi *gateway*. Questi intermediari hanno diverse funzioni: innanzitutto si occupano di definire l'identità degli utenti, in accordo con le disposizioni di antiriciclaggio; successivamente si occupano di accettare i depositi da parte degli utenti e di tracciare gli spostamenti di denaro utilizzando il registro condiviso.

Un'altra figura di notevole importanza per il funzionamento dell'ecosistema Ripple, è quella dei *market maker*. Questi ultimi sono solitamente grandi aziende che si occupano di garantire che il mercato sia sufficientemente liquido, cosicchè sia sempre possibile scambiare la quantità di valuta desiderata. Essi detengono una certa quantità di asset con cui possono fare *trading* sul mercato, garantendo un continuo flusso di cassa agli investitori che vogliono partecipare. I *market maker* definiscono quindi il prezzo di acquisto (*bid price*) e il prezzo di vendita (*ask price*) conseguendo un profitto dato dal differenziale tra questi.

Come accennato precedentemente, la criptovaluta nativa della piattaforma è il Ripple, indicata con il simbolo XRP. Ripple si differenzia dalla maggior parte delle criptovalute per il fatto di essere ad emissione centralizzata, ad opera dei *Ripple Labs*. Il quantitativo massimo di criptovaluta emessa, è fissato ad oggi a 100 miliardi di unità (di cui 99 già generati e 55 già distribuiti). Per questo motivo, gli XRP non possono essere

estratti tramite *mining*, così come avviene per Bitcoin o Ethereum. In questo caso, la valuta virtuale viene distribuita agli utenti che mettono a disposizione del sistema i propri computer e la propria potenza di calcolo. Nata anche per risolvere le criticità di Bitcoin, Ripple si caratterizza per un'elevata scalabilità (riesce a gestire 1500 transazioni al secondo) e un'elevata velocità delle transazioni (dai 2 ai 5 secondi per transazione), due fattori che insieme permettono di mantenere a un livello esiguo i costi di commissione.

## 2.3 Stablecoin

Per stablecoin si intende una particolare tipologia di cripto-attività che mira a garantire un valore stabile e a diminuire la volatilità dei prezzi mediante l'ancoraggio ad altre attività finanziarie e non (es. altre valute fiat, commodities, altre cripto-attività).

Le *stablecoin* nascono per unire i benefici delle valute virtuali basate su DLT con la stabilità propria di valute *fiat* o asset comunque più stabili. Le *stablecoin* cercano di risolvere la criticità relativa all'elevata volatilità di prezzo delle criptovalute, che ne ostacola l'impiego quotidiano come mezzo di scambio ancorando il loro valore ad una o più valute fiat (come il dollaro o l'euro), o a un determinato paniere di beni (come l'oro o altri metalli preziosi) tramite un tasso di cambio fisso. In pratica per assicurare un valore stabile, queste iniziative si impegnano a tenere dei fondi e/o altre attività come *collateral* contro cui le stablecoin possono essere riscattate o scambiate. Le stablecoin possono essere distinte in relazione allo strumento usato per mantenere stabile il valore o in base alla loro portata geografica: le *Global Stablecoin* sono iniziative diffuse a livello mondiale che comprendono più giurisdizioni in termini di utenti ed entità partecipanti. L'asset di riferimento più comune utilizzato come "ancora" per le Global S*tablecoin* è il dollaro USA, che è generalmente accettato come valuta di riserva globale.

Sulla base dello strumento usato possiamo distinguere sostanzialmente tre categorie di Stablecoin: 1)le valute virtuali ancorate a valute *fiat*: a fronte dell'emissione di questo tipo di *stablecoin* sono detenute delle riserve della valuta *fiat* utilizzata come forma di garanzia. Le *stablecoin* più diffuse sono ancorate al dollaro, come Tether (USDT) e USD Coin (USDC) che occupano rispettivamente la prima e seconda posizione per capitalizzazione di mercato. La seconda categoria si compone delle *stablecoin* il cui valore è ancorato ad altre criptovalute. Dato che in questo caso il loro valore è legato a quello di asset molto volatili, molto spesso le riserve sono "sovra-collateralizzate", ossia contano un maggior numero di unità rispetto al numero delle *stablecoin* emesse. La terza tipologia invece è costituita dalle *stablecoin* algoritmiche. Il loro valore è dettato da un algoritmo che contrae o espande la quantità emessa in base al prezzo della criptovaluta. Il funzionamento di questo tipo di valute virtuali trae origine dalla Teoria Quantitativa della Moneta in base alla quale il prezzo di un determinato bene o servizio è determinato dalla quantità di moneta in circolazione in quel dato momento. Quindi viene fissato un prezzo di equilibrio, se il valore della valuta virtuale si riduce rispetto al prezzo di equilibrio l'algoritmo ridurrà la quantità emessa, e viceversa. Il numero di progetti basati su *stablecoin* algoritmiche risulta ancora esiguo a fronte del carattere fortemente innovativo e delle complessità tecniche.

### 2.3.1 Tether

Tether (indicata con simbolo USDT) è una *stablecoin* che utilizza come valore di riferimento il prezzo del dollaro statunitense (con un tasso di cambio alla pari) ed è emessa da Tether Holdings Limited con sede a Hong Kong. L'ancoraggio del token al dollaro è ottenuto attraverso il mantenimento di riserve in dollari, in modo che la somma depositata sia pari al numero di USDT in circolazione.

Originariamente lanciato nel luglio 2014 come Realcoin, un token non nativo, sviluppato sopra la blockchain di Bitcoin attraverso l'uso della piattaforma Omni, è stato poi rinominato in USTether, e poi, infine, in USDT. Oltre a quello di Bitcoin, USDT è stato successivamente aggiornato per funzionare sulle blockchain di Ethereum, EOS, Tron, Algorand e OMG.

Lo scopo dichiarato di USDT è quello di combinare la natura senza restrizioni delle criptovalute - che possono essere inviate tra gli utenti senza un intermediario terzo di fiducia - con il valore stabile del dollaro USA.

Secondo quanto dichiarato da Tether, ogni volta che vengono emessi nuovi token USDT, la società deposita la stessa quantità di dollari nelle proprie riserve, assicurando così che USDT sia completamente supportato da contanti ed equivalenti. La *stablecoin* si propone come una criptovaluta affidabile per essere utilizzata come mezzo di scambio e riserva di valore, risolvendo due delle criticità che affliggono da sempre il settore *crypto*. Inoltre, USDT fornisce un modo rapido ed economico per effettuare transazioni potenzialmente *borderless* (senza confini) tramite blockchain, senza dover fare affidamento sui servizi prestati da un intermediario terzo, come una banca o un fornitore di servizi finanziari.

Tuttavia, nel corso degli anni, ci sono state numerose controversie riguardanti la veridicità delle affermazioni di Tether riguardo le riserve di dollari mantenute dalla società, che hanno provocato la riduzione del prezzo di USDT, che è arrivato a toccare il valore di 0,91 dollari il 24 aprile 2017 (Coinmarketcap, 2021). I dubbi riguardavano l'effettiva presenza di fondi in dollari sufficienti per coprire la somma di USDT in circolazione e il fatto che le riserve stesse non erano mai state verificate da una *Trusted Third Party*. Nel 2018 il procuratore di New York ha citato in giudizio Bitfinex, una delle maggiori piattaforme *exchange* a livello mondiale, per frode, in quanto la società avrebbe nascosto agli investitori la dissipazione di 850 milioni di dollari per delle transazioni con una società panamense. Questa somma di denaro fungeva da riserva per gli USD Tether scambiati su Bitfinex e l'accusa si riferiva al fatto che l'*exchange* aveva prelevato oltre 700 milioni di dollari dalla tesoreria di Tether per coprire delle ingenti perdite non rilevate in bilancio. Tutto ciò era stato nascosto agli investitori, mentre la società Tether Limited continuava a dichiarare la presenza di riserve in dollari tali da coprire i token con rapporto 1:1. La causa si è chiusa nel febbraio 2021, con la conferma delle accuse riguardo le false dichiarazioni rilasciate da Bitfinex e Thether Limited e un'ammenda da pagare pari a 18,5 milioni di dollari. Il procuratore di New York, Letitia James, attraverso una nota pubblicata sul proprio sito ufficiale, ha dichiarato che: "Bitfinex e Tether hanno coperto sconsideratamente e illegalmente enormi perdite

finanziarie per mantenere il loro piano in corso e proteggere i loro profitti. L'affermazione di Tether, secondo cui la sua criptovaluta era sempre completamente sostenuta da dollari Usa è falsa. Queste società oscuravano il vero rischio che gli investitori dovevano affrontare ed erano gestite da persone ed entità prive di licenza e non regolamentate, che operavano negli angoli più oscuri del sistema finanziario". A seguito delle indagini portate avanti dalla procura di New York, Tether ha modificato il disclaimer sul proprio sito, che precedentemente affermava la copertura totale degli USDT tramite dollari, mentre oggi recita che i token sono coperti da denaro e equivalenti insieme a titoli di credito.

### 2.3.2 Diem-Libra

Alla crescente diffusione delle *stablecoin* come mezzo di scambio o riserva di valore ha sicuramente contribuito il progetto Libra, ora noto come Diem che è stato il primo caso di *global stablecoin,* ovverosia di una valuta virtuale con prezzo stabile, che nasce con l'ambizione di essere un mezzo di scambio/pagamento su scala globale e come tale ha influenzato in maniera rilevante la definizione del quadro regolamentare internazionale ed europeo applicabile a questa categoria di valute virtuali.

Possiamo riassumere la storia di Diem nei seguenti passi: il 18 giugno 2019 c'è l'annuncio formale del progetto Libra, sistema di pagamenti basato su *multi-currency stablecoin* a bassa volatilità e blockchain *permissioned*. Durante il luglio 2019 ci sono le prime reazioni negative di governi e banche centrali: non si parte senza l'approvazione di tutti i regolatori e le Autorità di supervisione competenti. Ad aprile 2020, l'autorità svizzera (FINMA) dichiara di aver avviato un procedimento autorizzativo per la gestione di un sistema di pagamento DLT basato su *stablecoin*. A dicembre dello stesso anno viene modificato il nome (da Libra a Diem) e vengono annunciate le principali caratteristiche del progetto. Infine, a maggio 2020 vi è il ritiro definitivo della richiesta autorizzativa in Svizzera e ripartenza del progetto negli Stati Uniti.

Il progetto Diem ha colto impreparati regolatori e supervisori di tutto il mondo e ha certamente influenzato i successivi lavori sul trattamento prudenziale delle cripto-attività, la proposta della Commissione Europea sul Regolamento dei mercati di cripto-attività (MICAR) nonché i lavori del FSB sulle Global Stablecoins (*regulation, Supervision and oversight of "global stablecoin" arrangements*).

Diem nasce per essere un sistema di pagamento basato sull'utilizzo di un'infrastruttura DLT e, almeno nella prima fase, su un single-currency stablecoin il cui valore è ancorato al dollaro su base 1:1 (USD Diem). Il sistema di pagamento e l'infrastruttura tecnologica sottostante saranno aperti e vi potranno aderire, con diversi ruoli e responsabilità, sia intermediari finanziari sottoposti a regolamentazione e vigilanza (es.banche) sia soggetti non regolamentati, quali:

- Designated Dealers o DDs: intermediari, dotati di licenza bancaria, che svolgono l'attività di distribuzione degli USD Diem ai VASPs;

- Virtual Asset Service Providers o VASPs: soggetti, vigilati e non, che prestano l'attività di vendita/acquisto degli USD Diem dagli utenti finali e adempiono agli obblighi di tutela della clientela e di conformità con il quadro regolamentare applicabile;

- Reserve Custodians o RCs: intermediari, dotati di licenza bancaria, che detengono e gestiscono le attività oggetto della riserva sulla base delle regole del sistema di pagamento;

- Unhosted wallets: in prospettiva potrebbe partecipare anche ogni altra persona fisica o giuridica che vuole fare transazioni sul sistema Diem.

I rischi che i regolatori hanno visto in questo progetto attengono innanzi tutto al rischio di sostituzione tra *global stablecoin* e valute fiat e quindi di sovranità monetaria. Rischio che un *global stablecoin* possa acquisire una dimensione monetaria alternativa a quella di alcune valute fiat (soprattutto in piccole economie aperte e instabili), con conseguente perdita di «sovranità monetaria» da parte delle banche centrali di questi Stati. Rischi connessi alla maggiore interconnessione tra i nuovi prestatori di servizi crypto e gli intermediari tradizionali, con la necessità di definire nuove forme di vigilanza per attività che prescindono dalla natura del soggetto che le esercita. Ultimo, ma non meno importante, il rischio di concorrenza tra Big Tech vs incumbents: la possibilità da parte di colossi informatici (come Google, Facebook, Alibaba…) di sfruttare il bacino di utenti e/o i dati generati dai consumatori durante l'utilizzo delle piattaforme digitali (ruolo di Facebook nel progetto Libra/Diem) a beneficio dell'offerta dei servizi finanziari e di pagamento, col rischio di sostituzione dei diversi attori del sistema dei pagamenti con un'unica infrastruttura sotto il controllo/influenza di una Big Tech.

## 2.4 Definizioni e inquadramento giuridico

A causa degli elementi fortemente innovativi incorporati nella tecnologia blockchain e dal fatto che essa costituisce un'invenzione relativamente recente, ad oggi non vi è ancora un quadro regolamentare unico che disciplini la materia. La regolamentazione dei cripto-asset rimane pertanto un elemento critico per le autorità competenti, che si trovano costrette a risolvere dispute giurisprudenziali in assenza di un quadro normativo di riferimento. Le criptovalute ad oggi non hanno una definizione positiva nel diritto, in quanto costituiscono una categoria nuova non identificabile con quelle esistenti. La regolamentazione, almeno in Unione Europea, si esaurisce infatti a livello dei singoli ordinamenti nazionali. A seguito di questa frammentazione normativa, molte attività che hanno deciso di implementare uno o più servizi relativi all'intermediazione e scambio di valute virtuali (come *wallet* ed *exchange),* sono soggette a disposizioni differenti in base allo specifico ordinamento vigente. Nel corso dell'ultimo decennio, si sono succedute diverse sentenze, decreti legislativi e altri provvedimenti giuridici che hanno fornito delucidazioni più o meno contrastanti in materia.

Analizzando il profilo fenomenico, i cripto-asset sono rappresentati da documenti elettronici che rispondono a una serie di caratteristiche: vi è menzionato un dato numerico che incorpora un valore, sono suscettibili di appropriazione esclusiva (in base all'unicità delle chiavi di autenticazione), sono trasferibili e non rappresentano un diritto di credito. Infatti, a circolare non è un contratto di tipo obbligazionario, bensì un bene valore contabilizzato dal relativo documento elettronico (c.d. moneta-segno).

In base al quadro normativo attuale, il d.lgs. n. 90 del 2017, a seguito del recepimento della IV Direttiva Antiriciclaggio, ha modificato il d.lgs. n. 231 del 2007 ed ha individuato per la prima volta a livello legislativo una definizione di valuta virtuale: "una rappresentazione digitale di valore, non necessariamente collegata ad una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento, trasferita, archiviata e negoziata elettronicamente" Ad oggi, il legislatore riconosce quindi l'utilizzo di valute virtuali come strumento di pagamento alternativo a quelli tradizionalmente accettati nello scambio di beni e servizi.
Il decreto n.90 ha inserito gli *Exchange* tra i soggetti destinatari delle normative antiriciclaggio e ha introdotto l'obbligo di iscrizione di tali "cambiavalute virtuali" in un registro specifico, rimandando al Ministero dell'Economia e delle Finanze (MEF) l'emanazione di appositi decreti per la sua applicazione. Il MEF, a tal riguardo, ha disposto il decreto per cui si prevede nei confronti di "chiunque sia interessato a svolgere sul territorio italiano l'attività di prestatore di servizi relativi all'utilizzo di valuta virtuale" l'obbligo di comunicazione al Ministero dell'Economia e delle Finanze. L'iniziativa, come specificato dal MEF stesso, "mira a realizzare una prima rilevazione sistematica del fenomeno, a partire dalla consistenza numerica degli operatori del settore che, a regime, saranno tenuti ad iscriversi in uno speciale registro tenuto dall'OAM, l'Organismo degli Agenti e dei Mediatori, per poter esercitare la loro attività sul territorio nazionale".

Tra le valute virtuali, la criptovaluta è "definibile come rappresentazione digitale di valore, decentralizzata, basata sul *peer-to-peer*, su una blockchain condivisa il cui trasferimento si fonda sulla crittografia e le cui regole di emissione sono basate su un algoritmo open-source[12]". Tale concetto è stato poi ripreso da Banca d'Italia che ha fornito una prima delucidazione riguardo i criptoasset, ossia qualsiasi attività di natura digitale il cui trasferimento è basato su meccanismi crittografici e su DLT.

È lecito domandarsi se le criptovalute possano considerarsi strumenti finanziari in quanto il loro valore è determinato da domanda e offerta nel mercato. Allo stesso tempo, ci si chiede se sia possibile definire il servizio di intermediazione nello scambio di valute *fiat* in valute virtuali (servizio prestato dagli *Exchange*) come servizio di investimento. Ad oggi, la fattispecie giuridica nega l'equiparazione tra strumenti di pagamento e strumenti finanziari e sottolinea che, per essere considerato servizio di investimento, l'asset in

[12]Comandini G. (2020) *Da zero alla Luna: quando, come, perché la Blockchain sta cambiando il mondo: Cosa dice il fisco* a cura di Capaccioli Stefano, Palermo: Dario Flaccovio Editore;

oggetto deve essere qualificato come strumento finanziario. Per strumento finanziario si intende una sottospecie della più vasta categoria dei prodotti finanziari, definita come l'insieme di tutti gli strumenti finanziari e di ogni altra forma di investimento di natura finanziaria. L'insieme degli strumenti finanziari è elencato nell'articolo 1, comma 2 del Testo Unico della Finanza, a cui appartengono i valori mobiliari (azioni, obbligazioni e tutti quei prodotti che possono essere scambiati sul mercato dei capitali), strumenti del mercato monetario, quote di investimento in organismi di investimento collettivo (Fondi Comuni) e contratti su strumenti finanziari derivati. Le criptovalute, essendo riconosciute come mezzi di pagamento, non possono qualificarsi come strumenti finanziari.

Emblematico a riguardo, è il verdetto della Cassazione Penale n. 28607/2020[13], riguardo un procedimento in tema di riciclaggio di denaro tramite compravendita di criptovalute. In particolare, la Cassazione si interrogava sul quesito chiedendosi se la compravendita di valute virtuali potesse essere soggetta alle disposizioni del Testo Unico della Finanza in materia di prodotti finanziari. La sentenza dichiarava che era infondato il motivo di ricorso secondo cui le criptovalute, non essendo veri e propri prodotti di investimento, sarebbero sottratte alla normativa in materia di prodotti finanziari. La vendita di bitcoin in questione, "veniva reclamizzata come una vera e propria proposta di investimento, tanto che sul sito ove veniva pubblicizzata si davano informazioni teoricamente idonee a mettere i risparmiatori in grado di valutare se aderire o meno all'iniziativa, affermando, tra l'altro, che - chi ha scommesso in bitcoin in due anni ha guadagnato più del 97% -". In definitiva, le criptovalute sono da considerarsi al pari di prodotti finanziari, laddove, la loro vendita sia pubblicizzata dal soggetto offerente come una vera e propria proposta d'investimento ed esista un regolare prospetto informativo per la clientela. Nel caso si verifichino tali condizioni, l'attività di compravendita è soggetta agli adempimenti previsti dal T.U.F.

In generale peraltro, ai fini del T.U.F., le criptovalute sono considerate strumenti di pagamento in quanto non rileva il movente personale del soggetto che investe (anche chi acquista valute fiat lo può fare per finalità di investimento) ma la funzione oggettiva del "bene", che è di intermediazione negli scambi, non permette di per sé di maturare un rendimento. Quello che appare certo è che le criptovalute non possono considerarsi "denaro". Ai sensi dell'art. 1277 c.c. "i debiti pecuniari si estinguono con moneta avente corso legale al tempo del pagamento per il suo valore nominale." In materia di conferimenti, invece, ai fini degli artt. 2342 ss. c.c., rappresentano conferimenti in denaro solo quelli nella stessa moneta in cui è espresso il capitale, dunque l'euro. Tutti i conferimenti diversi dal denaro sono invece conferimenti "in natura". I conferimenti in criptoasset sono perciò da considerarsi al pari di conferimenti in valuta estera (quindi in natura) data le necessità di stima e di immediata liberazione.

[13] Corte di Cassazione, sez. II, sentenza 25 settembre 2020, n.26807 *Titoli di credito, utilizzo, carta di credito, acquisto di criptovalute, terzo, autorizzazione del titolare, irrilevanza, ad eccezione, considerazione del terzo come longa manus o mero strumento esecutivo,* [PDF] disponibile al sito: https://www.altalex.com/massimario/cassazione-penale/2020/26807/titoli-di-credito-titoli-di-credito-in-genere-reato;

In definitiva, le criptovalute sono dei beni-valori trasferibili che possono essere utilizzate come strumenti di pagamento. Possiamo considerare questi asset digitali nell'accezione di "monete complementari" alla moneta avente corso legale nello stato. Le monete complementari operano al fianco della valuta a corso legale e non "competono" con essa. In questo ambito occorre evidenziare un aspetto fondamentale delle criptovalute, che le differenzia dalle valute *fiat* tradizionali. Una *fiat money*, o valuta a corso legale di Stato, è "una moneta dotata del potere di estinguere le obbligazioni in denaro, riconosciuta come tale dall'ordinamento giuridico[14]". Le *fiat money* sono prive di valore intrinseco, ma sono dotate di potere liberatorio per legge, in base alla fiducia generale di cui sono investiti i soggetti emittenti, ossia le Banche Centrali. In Europa, la Banca Centrale Europea (BCE) si occupa di gestire e amministrare il processo di emissione tramite complesse procedure volte a garantire la stabilità del valore nel tempo e la fiducia generale nel sistema. Ogni euro emesso, così come ogni unità di qualsiasi moneta *fiat*, rappresenta un titolo di credito (passività) verso una Banca Centrale. Al contrario, le criptovalute, in relazione alla specifica natura informatica dei protocolli su cui si basano, non rappresentano un titolo di credito nei confronti di alcun ente emittente (che, nel caso di reti pubbliche come Bitcoin, neanche esiste). Per questo motivo le criptovalute non sono assimilabili nemmeno come forma di moneta elettronica (*e-money*) in quanto quest'ultima rappresenta comunque un titolo di credito verso il soggetto emittente, a fronte dei fondi depositati. L'emissione di criptoasset è invece governata da regole dettate dai rispettivi protocolli, non dipende da politiche monetarie o da variabili macroeconomiche esterne, e il loro valore è determinato dal mercato, in base alle quantità domandate e offerte dai partecipanti alla rete.

## 2.5 Criptovalute e valute a corso legale

### 2.5.1 Cenni storico-evolutivi

La moneta rappresenta da sempre lo strumento volto a regolare i rapporti economici tra due o più individui. Originariamente, lo scambio di ricchezza tra due soggetti avveniva tramite baratto (scambio di un bene con un altro) che però presentava ostacoli dal punto di vista della diversità dei beni scambiati. Si rese subito evidente la necessità di un bene intermedio largamente accettato che mantenesse un valore stabile nel tempo. Nelle civiltà più antiche e primordiali allora vennero impiegati come prima forma di moneta dei beni che acquisivano valore in funzione della loro utilità e della loro domanda, come sale, tabacco, conchiglie e infine metalli preziosi come oro e argento. Questi ultimi si prestavano particolarmente alla funzione monetaria in quanto non deperibili e provvisti di valore intrinseco, il che ne legittimò l'accettazione su larga scala. I beni, come metalli preziosi, che avevano una propria domanda e un proprio valore di mercato acquisirono lo status di moneta merce. Successivamente, a causa dei rischi e delle scomodità derivanti dal trasporto delle monete metalliche, emerse l'esigenza di una forma di moneta cartacea. Una prima forma di moneta rappresentativa nacque con l'introduzione delle "lettere di cambio" emesse da mercanti o orefici italiani nel 1300. Questi ultimi, a fronte dei depositi in oro dei clienti cominciarono ad emettere titoli rappresentativi del credito nei loro confronti, attribuendo al possessore del titolo la facoltà di scambiarlo con un altro mercante, in funzione

[14] Banca d'Italia Eurosistema (2017) *La moneta legale e la moneta scritturale* [Online] Disponibile al sito: https://www.bancaditalia.it/servizi-cittadino/cultura-finanziaria/informazioni-base/moneta-legale-scritturale/index.html;

degli specifici legami economici (Comandini, 2020). In seguito, le prime banche iniziarono ad emettere le banconote, fogli cartacei privi di valore intrinseco ma diffusamente accettate in quanto rappresentanti la promessa della banca a convertire, in un qualsiasi momento successivo, le banconote con una determinata quantità di oro, su richiesta del possessore. Questo sistema entrò in crisi nel ventesimo secolo successivamente alle guerre mondiali, quando le diverse condizioni dei paesi attori, resero imprescindibile un cambio del sistema. Si passò agli accordi di Bretton-Woods nel 1944 che hanno governato il sistema valutario mondiale fino al 1971: secondo il sistema definito a Bretton Woods il dollaro era l'unica valuta convertibile in oro in base al cambio di 35 dollari contro un'oncia del metallo prezioso. Il dollaro poi venne poi eletto valuta di riferimento per gli scambi. Alle altre valute erano consentite solo oscillazioni limitate in un regime di cambi fissi a parità centrale.

Oggi, le economie moderne hanno abbandonato il "sistema aureo" e si basano su un concetto di moneta fiduciaria, una moneta priva in sé di valore intrinseco e non coperta da riserve in oro (quindi inconvertibile), ma accettata in cambio di beni e servizi. Il termine "moneta fiduciaria" deriva dalla fiducia che gli utilizzatori riservano nella promessa di solvibilità dell'emittente. Oggi il denaro emesso da Autorità Centrali è definito "a corso legale" in quanto è la legge a decretarne il potere liberatorio (potere di estinguere obbligazioni pecuniarie) e l'obbligo di accettazione (difatti costituisce reato non accettarlo) all'interno del territorio dello Stato.

### 2.5.2 Differenze e funzioni principali

Anche se i termini "valuta virtuale" e "criptovalute" conducono ad un accostamento naturale con il concetto di denaro, le banche centrali dell'Eurosistema e l'attuale ordinamento giuridico non riconoscono le criptoattività come una forma particolare di denaro, né da una prospettiva economica, né tantomeno da una legale.

Secondo la dottrina economica prevalente, le funzioni tipiche del denaro sono: mezzo di scambio, ossia il denaro è riconosciuto come mezzo intermedio nel commercio poiché rappresentativo di un valore in cui tutti confidano; riserva di valore, poiché il denaro non utilizzato istantaneamente può essere detenuto al fine di trasferire il potere di acquisto in un momento futuro; e unità di conto, in quanto il denaro funge da unità numerica standard per la misurazione del valore e dei costi di beni e servizi, così da agevolare decisioni economiche riguardo beni diversi tra loro. Tuttavia, il concetto di moneta non si esaurisce con le funzioni che essa svolge, ma implica l'insieme di convenzioni, oggetti e procedure che rendono possibile l'estinzione delle obbligazioni rilevanti dell'attività di scambio.

Le valute virtuali attualmente conosciute non soddisfano pienamente tutte e tre le funzioni. Andiamo ad analizzarne le ragioni.

Svolgere tecnicamente il ruolo di mezzo di scambio è un requisito piuttosto semplice, di cui qualsiasi bene (digitale o fisico) è dotato, una volta che viene acquistato o venduto da qualcuno allo scopo di essere scambiato con un altro bene. A questo proposito, le criptovalute possono soddisfare questa funzione in quanto possono essere facilmente trasferite attraverso piattaforme online e possono essere oggetto di migliaia di transazioni al giorno. Tuttavia, le valute digitali hanno una lunga strada da percorrere per diventare un mezzo di scambio ampiamente accettato, in particolare se paragonate alle valute nazionali basate sulle proprie infrastrutture finanziarie statali. Sebbene la natura prettamente digitale delle criptovalute si presti decisamente al ruolo di mezzo di scambio, è improbabile che la loro accettazione si diffonda nel caso in cui non vengano risolvano le criticità legate all'estrema volatilità che pone un limite inevitabile in tal senso.

Un confronto con le valute tradizionali è utile per fornire un quadro di riferimento per l'analisi delle criptovalute in tema di funzione di riserva di valore e unità conto. Sebbene le valute digitali non siano supportate da banche centrali, e quindi non prevedano nessun meccanismo per fissare i tassi d'interesse e i rapporti di riserva obbligatoria, la maggior parte di esse sono dotate di protocolli informatici che ne prestabiliscono le quantità future di emissione. Una caratteristica chiave che caratterizza le valute a corso legale di Stato è quella di avere un certo grado di prevedibilità nella loro offerta. Infatti, le Banche Centrali, perseguendo i propri obiettivi di politica monetaria, limitano e modificano l'offerta di moneta al fine ultimo di conseguire la stabilità dei prezzi. Questo serve a rendere la valuta in questione una riserva di valore più o meno affidabile e quindi a proteggere i possessori da rapidi e imprevisti cali nel potere d'acquisto. Prendendo come esempio Bitcoin, è risaputo che la quantità di criptovaluta emessa diminuirà progressivamente fino a quando non saranno raggiunti i 21 milioni in circolazione. L'offerta di bitcoin diventerà progressivamente più rigida mentre la domanda rimarrà puramente determinata dal mercato, cosicché un aumento nell'adozione della valuta virtuale ne determinerà un aumento di valore, mentre grandi liquidazioni della stessa ne determineranno una significativa riduzione. È presumibile, come risultato della progressiva espansione del mercato Bitcoin, che il valore del token aumenterà nel medio periodo e quindi sarà più conveniente per gli investitori detenerlo (come una sorta di investimento finanziario) piuttosto che utilizzarlo come mezzo di pagamento quotidiano. Si potrebbe pensare, allora, che le criptovalute rappresentino un valido strumento per svolgere la funzione di riserva di valore nel tempo. Tuttavia, la prevedibilità dell'offerta non si traduce in una pari prevedibilità del potere d'acquisto, a fronte della volatilità della domanda. Inoltre, in assenza di una Autorità Centrale dotata del potere di regolare l'offerta di valuta e mantenere stabile il suo valore nel tempo, appare evidente che le criptovalute non possano svolgere la funzione di riserva di valore

Tutte le criptovalute hanno fluttuato significativamente dalla loro introduzione, e ci si può aspettare che continuino a farlo indefinitamente. L'unico momento futuro in cui il valore di una criptovaluta potrebbe plausibilmente raggiungere la stabilità, sarà solo quando la domanda dell'asset digitale come riserva di valore non varierà più in modo significativo. Questo obiettivo potrà essere raggiunto solo quando le valute virtuali non saranno più prevalentemente oggetto di attività speculative e quando il loro mercato diventerà

sufficientemente liquido. Infine, in mancanza di una regolamentazione specifica della materia, che garantisca al consumatore una tutela per rischi operativi e informatici, correlati alla natura estremamente variabile di questa categoria di asset digitali, appare altamente improbabile (se non impossibile) che in un futuro prossimo le criptovalute possano sostituirsi alle valute a corso legale di Stato. Per lo stesso motivo, elevata volatilità anche nel corso della stessa giornata, sarebbe altamente inefficiente, per non dire impossibile, prezzare beni e servizi in criptovalute. Riteniamo quindi che, al momento, i cripto-asset non possano assolvere nemmeno alla funzione di unità di conto.

# 3. RISCHI CONNESSI E REGOLAMENTAZIONE

## 3.1 Rischi connessi

A fronte dei vantaggi e benefici che la tecnologia blockchain può apportare ad un ampio spettro di settori (bancario, assicurativo, trasporti…) bisogna riconoscere, allo stesso tempo, i numerosi rischi che contraddistinguono la categoria di asset digitali (cd. criptoattività) implementate su strutture DLT. Proprio per il carattere decentralizzato di cui è emblema Bitcoin, il sistema creato dal giapponese non mette a disposizione dell'utente alcuna "tutela" in caso di malfunzionamenti, smarrimento delle chiavi o in caso di altri errori operativi che si possono verificare durante l'utilizzo della piattaforma. Non c'è alcun servizio clienti da contattare poiché non c'è alcuna istituzione pubblica o privata a cui rivolgersi, che sia responsabile del funzionamento delle blockchain *permissionless*. In questo senso, l'onere della prova è a carico dell'utente finale, in quanto essere in possesso delle chiavi pubbliche e private è sufficiente per essere legittimato a ricevere o inviare criptoattività. A fronte delle opportunità che un sistema decentralizzato e disintermediato può mettere a disposizione, ci sono altrettanti rischi che devono quindi essere considerati.

I rischi connessi all'utilizzo delle valute virtuali si possono ripartire in più macroaree. Innanzitutto, possiamo classificare come rischi prettamente "finanziari" (controparte, liquidità, mercato) quelli consessi all'attività di investimento in valute virtuali da parte del singolo utilizzatore. Insieme a questi bisogna tenere conto anche della categoria di rischi in termini di *cyber-security* in relazione ai frequenti attacchi informatici che hanno colpito le piattaforme *exchange* nel corso degli ultimi anni e in termini di tutela della privacy e protezione dei dati. Successivamente, troviamo dei rischi correlati a possibili attività illecite che possono essere condotte e mascherate tramite l'utilizzo delle criptovalute, come il riciclaggio del denaro e il finanziamento del terrorismo. In ultima analisi, bisogna considerare i rischi a livello strutturale, per la stabilità finanziaria e la sovranità monetaria (soprattutto in relazione alla natura delle valute virtuali cd. *stablecoin* e alla loro potenziale propagazione *cross-border*).

Appare evidente la necessità da parte dei Governi e delle Autorità Centrali di regolare la materia al più presto, per fornire una forma di tutela per gli utilizzatori finali e per preservare la stabilità economica e finanziaria degli Stati. Allo stesso tempo, in relazione alla velocità con cui si propaga l'innovazione finanziaria nel settore digitale, emerge l'esigenza degli Intermediari Finanziari di rinnovarsi per evitare di l'obsolescenza che porterebbe ad un progressivo processo di disintermediazione.

### 3.1.1 Rischi finanziari

Fare *trading* con asset criptovalutari è considerata un'attività molto rischiosa: rischio e rendimento sono spesso due elementi strettamente collegati fra loro e infatti nel corso dell'ultimo decennio, come si può notare analizzando le curve di mercato, le criptoattività con maggiore capitalizzazione di mercato (Bitcoin, Ether,

XRP, Binance Coin…) hanno conseguito rendimenti molto elevati, il che ha attratto un gran numero di investitori verso questo nuovo tipo di mercati non regolamentati.

Le Banche Centrali e le Istituzioni di Vigilanza hanno ribadito più volte le insidie congenite nell'investimento in criptoattività, mettendo in guardia soprattutto i piccoli risparmiatori dai rischi relativi al collocamento dei propri risparmi in questo tipo di asset digitali "che possono comportare la perdita integrale delle somme di denaro utilizzate[15]". Questi rischi sono accentuati dalla natura digitale delle criptovalute, e quindi dalla relativa facilità con cui chiunque può accedere alle piattaforme di *exchange* e convertire il proprio denaro fiat.

Dal punto di vista dell'utente finale, tali rischi possono essere ricondotti prevalentemente a tre specie: rischi di liquidità, di controparte e di mercato. Il rischio di liquidità è definito come "rischio che un titolo non possa essere venduto a un prezzo equo con bassi costi di transazione e in breve tempo[16]". E' evidente, analizzando il rapporto tra la capitalizzazione di mercato e il volume di transazioni delle criptoattività più diffuse, che i mercati delle criptovalute sono ancora essenzialmente illiquidi. Ciò espone l'investitore al rischio che non riesca a vendere l'asset digitale al prezzo o nel momento desiderato. Il secondo tipo è quello connesso al rischio di controparte, nel caso in cui siano negoziati in mercati OTC strumenti derivati aventi come sottostante una o più criptovalute. Dal momento che non c'è nessuna organizzazione esterna che garantisca il contratto, le parti devono accertarsi della reciproca solidità finanziaria e di riuscire ad assolvere gli obblighi contrattuali previsti. Attualmente, tale rischio di controparte viene gestito o attraverso l'uso di modelli interni, o tramite tre metodi standardizzati, rispettivamente, mark-to-market method, original exposure method, standardised method (Banca d'Italia, 2019).
In questa sede, l'ultimo profilo di rischio è quello correlato alla natura variabile del mercato delle criptovalute. Il rischio di mercato espone l'investitore a rilevanti e impreviste variazioni nel prezzo dell'attività su cui ha investito. Questo è strettamente legato all'estrema volatilità di prezzo delle valute virtuali e riflette il fatto che la formazione dei prezzi sia determinata essenzialmente dal mercato (incontro tra una domanda fluttuante e un'offerta semi rigida) e perciò risulti essere poco trasparente al singolo risparmiatore.

### 3.1.2 Rischi per attività illecite

Un altro profilo di rischio connesso alla natura digitale e deregolamentata delle criptovalute è rappresentato da una serie di attività criminali che possono essere condotte utilizzando questi strumenti. Tra il 2019 e il 2020

[15] Consob, Banca d'Italia (2021) *Consob e Banca d'Italia mettono in guardia contro I rischi insiti nelle crypto-attività*, Comunicato Stampa, [PDF] disponibile al sito: https://www.consob.it/documents/46180/46181/cs_20210428.pdf/ca5fec2f-36fb-4677-8292-e40bb0d7a597;
[16] Borsaitaliana.it (2021) *Rischio di Liquidità – Glossario Finanziario,* [Online] Disponibile al sito: https://www.borsaitaliana.it/borsa/glossario/rischio-di-liquidita-.html#:~:text=Glossario%20finanziario%20%2D%20Rischio%20di%20Liquidit%C3%A0&text=Rischio%20che%20un%20titolo%20non,transazione%20e%20in%20breve%20tempo;

è stato rilevato un aumento considerevole di attività sospette connesse all'utilizzo delle criptovalute[17]. In questo ambito, i profili di rischio più pericolosi sono costituiti da attività illecite in materia di riciclaggio del denaro e finanziamento del terrorismo, ossia conversione del denaro illecito in valute virtuali o vendita di merci illecite con pagamento in criptovalute. In questo modo la criminalità organizzata potrebbe mascherare i profitti illeciti come proventi derivanti da attività di trading o simili.

Il sistema blockchain e le criptovalute, per motivi legati alle caratteristiche naturali di decentralizzazione e pseudo-anonimità, vengono percepiti dalla criminalità organizzata come interessanti strumenti per condurre attività illecite di riciclaggio, in particolare considerando la loro natura *cross-border* e deregolamentata. Inoltre, anche se la blockchain permette la tracciabilità a ritroso di tutte le transazioni, rende complicato, rispetto ai mezzi di pagamento tradizionali, identificare il reale possessore del *wallet*, a cui sono intestate le valute virtuali. Infatti, è possibile identificare il reale proprietario del portafoglio virtuale solo se quest'ultimo si rivolge ad un *exchange* centralizzato, che quindi fa capo ad una società specializzata e regolata. Al contrario, se l'utente decide di gestire il *wallet* in autonomia, comprando criptovalute direttamente da un *miner* o utilizzando una piattaforma *exchange* decentralizzata, l'identificazione del soggetto risulta più complicata dato che sarebbe possibile esclusivamente tramite investigazioni della polizia postale sugli indirizzi IP, ma anche queste spesso si rivelano infruttuose. Non essendo possibile ricondurre le singole transazioni ai possessori dei wallet, risulta difficile l'assolvimento degli obblighi previsti dalla normativa antiriciclaggio in materia di "titolare effettivo" (Galmarini et al., 2018).

A questo proposito, come esposto in precedenza, in Italia è stata introdotta una normativa *ad hoc* per gli esercenti di servizi connessi alle criptoattività, volta a presidiare i profili di antiriciclaggio (*Anti Money Laundering*, AML) e finanziamento del terrorismo (*Counter Terrorist Financing*, CFT). La normativa in parola prevede obblighi di registrazione in una sezione speciale del registro dell'Organismo degli Agenti e dei Mediatori (OAM) per i prestatori di servizi connessi alle criptovalute. Questi ultimi sono quindi vincolati al rispetto della disciplina antiriciclaggio tramite identificazione dei soggetti che intendono fare trading attraverso le loro piattaforme. Tuttavia, l'utilizzo di siti web e di applicazioni decentralizzate rende l'elusione delle disposizioni in parola non controllabile da parte delle autorità competenti, in relazione alla difficile l'identificazione del titolare effettivo delle criptovalute.

### 3.1.3 Rischi informatici

Nella categoria di rishi connessi all'utilizzo di tali strumenti digitali rientrano anche il rischio prettamente *cyber* (relativo ad attacchi hacker) con finalità illecite connesse a furti o estorsioni.

[17] IASSP website (2021) *Il ruolo delle criptovalute nel riciclaggio di denaro.* [Online] Disponibile al sito: Il ruolo delle Criptovalute nel Riciclaggio di Denaro | IASSP;

Come esposto in precedenza, chi vuole investire in criptovalute ha la necessità di conservare e gestire le chiavi private in uno specifico *wallet*. In alcuni casi le chiavi di autenticazione non sono nemmeno rivelate al soggetto, in quanto sono conservate e gestite in modo automatico dall'*exchange* che si utilizza. Quest'ultima circostanza espone l'investitore a rilevanti rischi informatici, nel caso in cui la piattaforma venga presa di mira da attacchi *hacker* con lo scopo di rubare le chiavi private. Se questo rischio si dovesse verificare, come accaduto diverse volte in passato, vi potrebbe essere la perdita anche totale dei fondi investiti.

A titolo di esempio si riportano alcuni dei più famosi attacchi informatici. Come accennato in precedenza, nel 2013 la piattaforma giapponese Mt. Gox (uno dei primi *exchange* della storia, inizialmente specializzato in giochi online) ha subìto un attacco *cyber* che ha comportato la perdita di 850 mila bitcoin (per un corrispettivo, all'epoca, di 450 milioni di dollari) e la chiusura della piattaforma. Nel 2016, l'*exchange* della società di Hong Kong, Bitfinex, coinvolta anche in successivi scandali relativi alle riserve di Tether, ha subito un attacco *hacker* con una perdita di 72 milioni di dollari. Nel gennaio 2018, Coincheck, un'altra piattaforma giapponese, ha annunciato di aver subìto il furto di 260 mila chiavi private corrispondenti ad altrettanti *hot wallet* custoditi all'interno della piattaforma stessa, per un controvalore di circa 530 milioni di dollari. Coinvolta in attacchi informatici anche l'*exchange* italiano BitGrail, che ha subito un furto di 11 milioni di Nano (criptovaluta nata negli USA), per un valore pari a 170 milioni di dollari. Per concludere, durante l'agosto 2020, la criptovaluta Ethereum Classic ha subito un attacco informatico del 51% che ha causato la sottrazione di 800 mila Ether (di un valore pari a 5,6 milioni di dollari). Un *51% attack* si verifica quando una parte dei *miner* guadagna più potere di *hashing* (potenza di calcolo) rispetto al resto dei minatori. Chi ha attaccato la rete può allora "riscrivere" la storia della catena di blocchi e spendere due volte la valuta. Successivamente all'attacco gli sviluppatori di Ethereum hanno esortato tutti i nodi della rete a implementare dei nuovi software ritenuti più sicuri per sostituire quello precedente, OpenEthereum, divenuto immediatamente obsoleto.

Appare evidente che quella informatica sia una componente di rischio rilevante e molto frequente nel settore delle valute virtuali. Questo è dovuto alla natura prettamente digitale delle criptovalute e ancora una volta alla mancanza di regolamentazione che tuteli il consumatore finale da questo tipo di rischi. Per questo motivo, oltre all'utilizzo di canali autorizzati e affidabili, si ritiene che il modo più sicuro ed efficace per conservare la chiave crittografica privata sia il c.d. *cold wallet*, che non è connesso alla rete, cosi che il consumatore possa conservarla in un luogo fisico sicuro da lui scelto.

### 3.1.4 Rischi per la stabilità economica e sovranità monetaria

Come accennato precedentemente, in relazione al progetto Libra-Diem di Facebook, si può affermare che gli *stablecoin* vengono visti dai regolatori come un fattore destabilizzante per il sistema economico e finanziario globale. Secondo un rapporto della BCE, solo nel 2020 sono state annunciati più di 200 progetti di questo tipo. Inoltre, il G7 e la Banca dei Regolamenti Internazionali di Basilea hanno definito questi accordi come "una crescente minaccia alla politica monetaria, alla stabilità finanziaria e alla concorrenza". Le preoccupazioni

sono rivolte in particolare verso i *global stablecoin*, ossia monete virtuali stabili che vengono definite "globali" in ragione della loro potenziale capacità di raggiungimento di elevati volumi e la loro possibile propagazione senza confini.

Nello specifico, i regolatori hanno avanzato le loro perplessità nel caso in cui, ad emettere queste valute virtuali stabili, siano le *Big Tech*, ossia i colossi del web come Amazon, Google e Facebook che vantano un enorme bacino di utenza, e che già stanno diversificando la loro attività in diversi settori. I problemi emergono nel caso in cui questi giganti informatici si mettano ad offrire servizi finanziari o di pagamento a titolo gratuito, sfruttando l'abbondanza di liquidità e il controllo delle piattaforme social, in cambio della gestione delle informazioni e dei dati dei clienti.

Per le loro caratteristiche, gli *stablecoin* potrebbero essere vulnerabili a una situazione di *liquidity run*, con la quale si intende una corsa al rimborso degli utenti finali che si confrontino con la prospettiva di una abbattimento del valore della stablecoin: una *liquidity run* si potrebbe verificare nel caso in cui l'emittente della valuta virtuale sia percepito dagli utenti come privo di sufficiente capacità di assorbimento delle perdite, oppure nel caso in cui quest'ultimo rilasci notizie false sullo stato delle riserve (come accaduto per Tether) che faccia perdere la fiducia degli investitori. In un simile scenario, la liquidazione delle attività per coprire i rimborsi potrebbe avere effetti di contagio negativi sul sistema finanziario, risultando un fattore critico per la stabilità finanziaria internazionale[18].

Un altro aspetto critico per le Autorità di Vigilanza e per le Banche Centrali deriva dal fatto che l'emissione di *stablecoin* da parte di emittenti privati andrebbe ad espandere il cosiddetto *shadow banking system*. Il "sistema bancario ombra" comprende tutti quegli intermediari finanziari che permettono metodi alternativi di finanziamento, rispetto ai canali ufficiali e per questo motivo nella maggior parte dei casi non sono soggetti a regolamentazione. Nel 2008, lo *shadow banking system* giocò un ruolo fondamentale nell'esplosione di erogazione del credito verso soggetti con rating inadeguati tramite l'offerta di prodotti finanziari quali i mutui sub-prime la cui diffusione tra il grande pubblico è stata considerata uno dei fattori determinanti della crisi finanziaria globale.

Le dimensioni dello *shadow banking system* hanno superato da molti anni quelle dei tradizionali canali bancari, e una diffusione di strumenti come gli *stablecoin* porterebbe ad un'espansione ancora maggiore di questo mercato non regolamentato. L'industria bancaria ombra gioca da tempo un ruolo critico negli Stati Uniti riuscendo a soddisfare la crescente domanda di credito. Anche se in alcuni casi è stato sostenuto che il processo di disintermediazione dai canali tradizionali così operato possa migliorare l'efficienza economica tramite un

[18] ECB Crypto-Assets Task Force (2020) *Occasional paper series Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area,* Eurosystem [PDF] disponibile al sito: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf;

taglio dei costi, la sua operatività che sfugge alla regolamentazione continua a sollevare molte preoccupazioni in termini di rischio sistemico per la stabilità dei sistemi finanziari. Inoltre la propagazione di *stablecoin* avrebbe effetti destabilizzanti per i mercati, perché riducendo le tradizionali attività bancarie (e i loro profitti) porterebbe ad una inevitabile contrazione del numero degli operatori.

## 3.2 Finalità di tutela

A fronte dei numerosi profili di rischio connessi con un utilizzo diffuso delle valute virtuali, appare chiaro il motivo per cui le Banche Centrali e gli Intermediari Finanziari autorizzati si siano da sempre rivolte verso questo nuovo settore con sospetto e diffidenza. Considerando tuttavia le numerose opportunità offerte e l'ampio spettro di *use case* che possono essere implementati tramite l'utilizzo di DLT o blockchain, emerge l'esigenza da parte degli Intermediari Finanziari di cogliere i risvolti positivi di questa tecnologia al fine di un efficientamento generale del settore, ma allo stesso tempo di arginare, per quanto possibile, i fattori di rischio che potrebbero determinare l'obsolescenza dello stesso. In particolare, il pericolo maggiore per il settore bancario tradizionale è costituito dalla possibilità che in un futuro prossimo si possa formare un canale finanziario alternativo nel quale la trasmissione di ricchezza avvenga senza l'intervento degli intermediari.

I regolatori hanno iniziato a fornire differenti risposte normative in materia, accomunate tutte dal fatto di trovarsi ancora ad uno stato embrionale. Il settore delle valute virtuali rimane un settore difficile da regolamentare nel suo complesso, considerando la sua natura transfrontaliera e l'assenza di una istituzione responsabile. Per questo motivo, gli approcci implementati dalle varie giurisdizioni sono volti *in primis* a far acquisire esperienza nell'operatività e nel funzionamento dei criptoasset, al fine di comprenderne meglio rischi ed opportunità. Come risultato, ad oggi la maggior parte di prestatori di servizi connessi al settore rimangono non regolamentati.

In conclusione, è auspicabile che le autorità competenti forniscano al più presto un quadro regolamentare completo che consegua molteplici finalità: da una parte la tutela a livello del consumatore finale, dall'altra quella a livello sistemico, riuscendo a far confluire in un'unica normativa la regolamentazione sulla privacy e sui rischi *cyber* con le disposizioni in tema di riciclaggio di denaro e finanziamento del terrorismo. Alle autorità competenti è lasciato il compito, non banale, di fornire risposte adeguate a numerose sfide derivanti da un settore in rapida evoluzione riuscendo a "calibrare il contenuto dei futuri regolamenti in modo da affrontare adeguatamente i rischi senza, tuttavia, soffocare l'innovazione" (Consob, 2021).

## 3.3 Approcci implementati

In questa sede si vogliono esaminare gli approcci regolamentari connessi ad attività concernenti le valute virtuali nelle due principali giurisdizioni del globo (USA e Cina) per poi andare ad analizzare nei prossimi paragrafi, la normativa e le proposte regolamentari in Unione Europea. Per la complessità di identificazione della categoria, i principali approcci si sono limitati a regolamentare i soggetti che operano sul mercato ed i

servizi da loro offerti (*Wallet* e *Echange providers*) senza concentrare gli sforzi sulla creazione di una categoria di strumenti separata. Comunque, l'idea comune alla maggior parte delle autorità nei vari paesi è quella di operare una separazione normativa tra le criptoattività (es. Bitcoin, Ethereum, Theter…) e la tecnologia sottostante (DLT, blockchain…) allo scopo di analizzarne i rischi e identificarne le opportunità. Nel corso degli anni sono state date svariate definizioni normative in materia, spesso discordanti tra loro, che hanno contribuito a formare un quadro regolamentare opaco e frammentato a livello globale. Nel complesso, non vi è ancora un'uniformità di vedute e rimangono ancora molte perplessità in merito a quale sia l'approccio "migliore" a cui fare riferimento.

In questo ambito, sono stati considerati generalmente tre approcci regolamentari alternativi: "isolare", "regolare" e "integrare"[19]. La prima soluzione, più drastica, consiste nell'imposizione del divieto di svolgimento di attività connesse alle criptovalute, sia a livello del singolo utilizzatore sia a livello istituzionale. La seconda alternativa consiste prevalentemente nel fornire una definizione giuridica specifica e nell'emanazione di un apposito regolamento per questa classe di asset digitali. L'ultima soluzione invece consiste nell'integrare appunto le disposizioni vigenti ed applicarle, dove sia possibile, ai servizi connessi a una o più attività in valute virtuali.

Gli Stati Uniti, in particolare il Dipartimento dello Stato di New York, sono stati il primo paese ad aver cercato di regolare appositamente i servizi connessi alle criptovalute. Nel 2015 è stata introdotta la norma secondo cui i prestatori di servizi relativi allo scambio di criptovalute sono obbligati ad ottenere una licenza specifica. Quest'ultima viene rilasciata se vengono rispettati determinati standard prudenziali in materia di *governance*, capitale minimo e presidi per rischi operativi.
Anche se ancora oggi manca una definizione univoca riguardo lo status giuridico delle criptovalute, il Dipartimento del Tesoro USA ha fornito in questo senso una prima esplicitazione definendole "*medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency*".
A livello fiscale, invece, l'autorità competente ha inquadrato le valute virtuali nella classe di *commodities*, poiché sono suscettibili ad appropriazione esclusiva (*property*) e ricadono sotto le norme generali del *Commodity Exchange Act* in materia di frodi e manipolazioni del mercato, ma non sono soggette alle norme della SEC (*Security Exchange Commision*) in materia di tutela dell'investitore. Tuttavia la SEC, il 25 luglio 2017, ha dichiarato nell'Exchange Act n. 81207 che il processo di raccolta di fondi tramite *Initial Coin Offering* può essere accostato, in particolari condizioni, a una reale proposta d'investimento. In particolare, per verificare se tale processo si configura come proposta di investimento, viene effettuato l'*Howey Test* nel quale si ricercano tre condizioni sufficienti: un investimento iniziale, una proposta concernente un progetto di

[19] A. Caponera, C. Gola (2019) *Aspetti economici e regolamentari delle «cripto-attività» - Questioni di Economia e Finanza (Occasional Papers) Numero 484* - Banca d'Italia Eurosistema [Online] Disponibile al sito: Banca d'Italia - N. 484 - Aspetti economici e regolamentari delle «cripto-attività» (bancaditalia.it);

tipo imprenditoriale e l'aspettativa dell'investitore di conseguire un profitto. Se tutte e tre le condizioni sono soddisfatte è necessario qualificare i token emessi tramite ICO, come strumenti finanziari e conseguentemente applicare l'apposita normativa in materia di antiriciclaggio e registrazione delle offerte.

In Cina l'approccio regolamentare al settore delle criptovalute è stato fondamentalmente diverso da quelli implementati negli Stati Uniti e in Unione Europea. Infatti, il Governo e la Banca Centrale Cinese hanno manifestato fin da subito la loro avversione alle criptovalute ed hanno avvertito i consumatori e le istituzioni finanziari dei potenziali rischi derivanti da un utilizzo diffuso delle stesse. Per questo motivo, nel 2017, sono state imposte delle norme che vietano, a società private o statali, qualsiasi attività di scambio di valuta legale con criptovalute, comprese le raccolte di fondi tramite *Initial Coin Offering*. In quest'ambito, le ICO sono state definite dalle Autorità Cinesi come "attività di finanziamento pubblico non autorizzata e illegale, che comporta reati finanziari come la distribuzione illegale di token finanziari, l'emissione illegale di titoli e la raccolta illegale di fondi, la frode finanziaria e lo schema piramidale." Per questo motivo, dal 2017 in poi, numerose piattaforme di *exchange* o che fornivano prestiti in forma P2P hanno ricevuto l'ordine di chiudere. Non è una sorpresa che le ICO, a causa dell'aumento, sia nel numero che nella quantità di fondi raccolti, abbiano ricevuto la "*condanna a morte"* dalla People's Bank of China (PBOC). Nonostante ciò, nessuna legge o regolamento proibisce agli investitori cinesi di detenere o scambiare criptovalute, in quanto Bitcoin è stato classificato come una merce virtuale e non come una valuta. Inoltre, analizzando i dati del *Cambridge Bitcoin Electricity Consumption Index*, si evince che proprio la Cina è il paese dove è concentrata la maggior parte dell'attività di *mining* di Bitcoin e dove sono collocate le più importanti *mining pool* a livello globale. Per questo motivo, è possibile che la scelta di un approccio regolamentare essenzialmente proibitivo possa fornire agli utenti sufficienti incentivi per mettere in atto forme di elusione o di arbitraggio regolamentare. Sebbene la PBOC e altre agenzie governative hanno manifestato il loro dissenso in materia di ICO o di servizi connessi all'attività di *exchange*, le stesse autorità cinesi hanno elogiato più volte la tecnologia blockchain sottostante, purché il suo obiettivo sia quello di servire "l'economia reale" e non di promuovere attività finanziarie illegali.

## 3.4 Quadro Regolamentare UE

Nella maggioranza dei paesi dell' Unione Europea è stato deciso di applicare un approccio regolamentare riconducibile al concetto di *soft regulation* (A. Caponera, C. Gola, 2019). Quest'ultimo prevede principalmente di mettere in guardia i consumatori dai rischi derivanti dall'utilizzo delle criptovalute, che per questo motivo sono coscienti di non essere tutelati, e di stabilire determinati meccanismi volti a presidiare i rischi di riciclaggio del denaro e di finanziamento del terrorismo (AML/CFT). Per raggiungere questo fine, è stato imposto alle autorità competenti dei paesi membri di registrare in un apposito registro i soggetti che intendono operare come *exchange* e *wallet providers*.

In merito allo status giuridico delle criptovalute, le normative emanate dai paesi membri si sono limitate a definire cosa non sono le valute virtuali. In questo ambito è stato stabilito che certamente non sono: denaro, fondi, depositi, moneta elettronica o valute di gioco utilizzate in piattaforme apposite. A livello fiscale, per determinare se i proventi derivanti da *trading* in criptovalute siano soggetti a tassazione, ci si affida alla sentenza della Corte di Giustizia dell'UE in merito a un caso amministrativo sottoposto alla corte svedese. In quest'ultimo ci si interrogava sul quesito circa il pagamento dell'IVA sui proventi effettuati tramite *trading*. La Corte di Giustizia Europea ha risolto il caso identificando il bitcoin come "mezzo di pagamento contrattuale" in relazione alla finalità di utilizzare le criptovalute in questione come mezzo di pagamento o simili. Conseguentemente è stato stabilito che l'attività di *trading* in valute virtuali è esente dall'imposizione IVA. In seguito, la disposizione è stata recepita anche dalla normativa italiana con la risoluzione 72/E del 2016 da parte della Agenzia delle Entrate, nel quale è stato ribadito come "lo scambio di valute virtuali con valute a corso legale" sia esente dal pagamento dell'imposta sul valore aggiunto.

### 3.4.1 Digital Finance Package

Sulla base di ampie consultazioni pubbliche e dei rapidi sviluppi nel settore digitale, il 24 settembre 2020 la Commissione Europea ha deciso di adottare il *Digital Finance Package*, un "pacchetto" normativo che comprende vari documenti: in primis, un testo riguardante la *Digital Finance Strategy*, che funge da linea guida e pone gli obiettivi che devono essere conseguiti da tutti i paesi membri. In seguito troviamo diverse proposte legislative in materia di cripto-asset e resilienza digitale, al fine di formare un settore finanziario europeo competitivo, che offra ai cittadini l'accesso a prodotti finanziari innovativi, garantendo al contempo la tutela degli stessi e preservando la stabilità finanziaria dell'Unione. Il *Digital Finance Package* ha l'obbiettivo di sostenere il processo di transizione digitale e di modernizzare il settore finanziario europeo al fine di rendere l'Unione un "attore digitale globale"[20].

La *Digital Finance Strategy*[21] definisce, perciò, le linee generali su come l'Europa può sostenere la trasformazione digitale della finanza nei prossimi anni, regolandone al contempo i rischi. Il documento individua quattro obiettivi prioritari: rimuovere la frammentazione regolamentare nel mercato unico, adattare il quadro normativo dell'UE per favorire l'innovazione digitale, promuovere una strategia in materia di protezione dati e infine, promuovere lo sviluppo della resilienza operativa digitale del sistema finanziario.

[20] Ec.europa.eu (2020) *Digital Finance Package* [Online] Disponibile al sito: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en;

[21] European Commission (2020) *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on a Digital Finance Strategy for the EU. COM/2020/591 final* [Online] Disponibile al sito: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0591&from=EN;

In materia di criptoasset, la Commissione Europea propone un quadro regolamentare che ha l'obiettivo di promuovere l'innovazione e allo stesso tempo di preservare la stabilità finanziaria e proteggere gli investitori. In tal senso la Commissione propone un regime pilota per le infrastrutture di mercato (*Pilot Regime for Market Infrastructures based on DLT*[22]) che desiderano operare tramite sistemi DLT e regolare le transazioni in criptoasset. Negli intenti della CE, il regime pilota dovrebbe permettere ai soggetti operanti sul mercato e alle autorità di regolamentazione di acquisire esperienza operativa nel settore, al fine di individuare i possibili casi d'uso e di presidiare i rischi correlati. Difatti, riuscendo a stimolare la sperimentazione di sistemi DLT sul campo, si auspica di rendere il mercato *crypto* più contendibile, favorendo un accesso più ampio da parte di consumatori e fornitori.

Per i cripto-asset precedentemente non regolamentati, compresi gli *stablecoin*, la CE propone un regolamento apposito: il MiCAR (*Markets in Crypto-assets Regulation*[23]*)*. La regolamentazione proposta segue l'esigenza di supervisionare a livello unico europeo, superando la frammentazione normativa attuale, il funzionamento e i rischi insiti nel mercato *crypto*. La centralità della normativa è rivolta agli *stablecoins* (nelle accezioni di *Asset Referenced Token* e *E-Money Token*), in particolare quelli emessi dalle *BigTech*. Emerge chiaramente la finalità della CE di presidiare ogni possibilità che questi asset digitali possano minare i principi di stabilità finanziaria e sovranità monetaria. In questo ambito, il regolamento stabilisce standard rigorosi per gli emittenti e per i fornitori di servizi (*Crypto-asset Service Provider)* che desiderano operare all'interno del mercato unico europeo. Gli standard preposti includono requisiti in materia di capitale minimo, custodia dei beni e gestione della liquidità. Inoltre sono previste delle procedure volte a far valere i diritti dell'investitore contro l'emittente. Oltre alla fissazione di requisiti minimi da rispettare, il MiCAR ha la finalità di accrescere la trasparenza nel mercato *crypto*, stabilendo dei presidi informativi volti ad ampliare la conoscenza, da parte del pubblico e delle autorità, circa le caratteristiche e l'utilizzo dei criptoasset.

L'ultima proposta contenuta nel *Digital Finance Package* è il DORA (*Regulation on Digital Operational Resilience for the Financial Sector*[24]), una proposta normativa che mira ad aumentare la resilenza del settore finanziario digitale in relazione ai rischi cyber e alle minacce informatiche. La crescente dipendenza del settore finanziario dai processi digitali comporta l'assunzione dei rischi derivanti dall'utilizzo di tecnologie dell'informazione e della comunicazione. La Commissione Europea propone quindi un regolamento che si

---

[22] European Commission (2020) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology. COM/2020/594 final.* [Online] Disponibile al sito: EUR-Lex - 52020PC0594 - EN - EUR-Lex (europa.eu);

[23] European Commission (2020) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM/2020/593 final.* [Online] Disponibile al sito: EUR-Lex - 52020PC0593 - EN - EUR-Lex (europa.eu);

[24] European Commission (2020) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. COM/2020/595 final*. [Online] Disponibile al sito: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020PC0595;

pone l'obiettivo di garantire le imprese e gli altri soggetti economici da tutti i tipi disfunzioni e pericoli legati alle ICT (*Information Communication Technology*). Il regolamento prevede il rispetto di standard rigorosi da parte di banche, casse di compensazione ed altre istituzioni finanziarie al fine di prevenire o limitare l'impatto degli incidenti informatici. In particolare, sono previsti requisiti più rigorosi per quelle aziende (come le *Big Tech*) che forniscono servizi di cloud computing alle istituzioni finanziarie.

La Commissione Europea sostiene che l'attuazione del *Digital Finance Package* sia propedeutica per il raggiungimento di molteplici obiettivi. Innanzitutto, quello di sostenere l'innovazione sviluppando prodotti finanziari più facilmente accessibili ai consumatori e ai soggetti che attualmente non usufruiscono dei servizi finanziari. Inoltre, con la transizione digitale, si aprirebbero nuovi canali di finanziamento alle imprese dell'UE, in particolare alle PMI. Inoltre, dato il carattere *cross-border* della finanza digitale, quest'ultima può offrire validi strumenti per ottimizzare l'integrazione dei mercati finanziari e dei mercati dei capitali, all'interno dell'unione bancaria. In questo modo, il "pacchetto della finanza digitale" ha l'obiettivo di sostenere il progetto più ampio di ripresa economica e di consolidamento dell'unione economica e monetaria europea.

### 3.4.2 Digital Euro

Come accennato in precedenza, la strategia di diversificazione delle linee di business attuata negli ultimi cinque anni dalle c.d. *BigTech*, ha fatto si che improvvisamente non sembri più tanto remota l'ipotesi di un loro ingresso anche nel settore finanziario.

Tutto ciò, insieme alla progressiva digitalizzazione dei beni e servizi, ha innescato una discussione sempre più ampia riguardo la necessità degli intermediari finanziari di rinnovarsi per continuare ad essere competitivi nell'offerta ai propri clienti di prodotti e servizi finanziari. L'obiettivo è quello di limitare il progressivo fenomeno di disintermediazione scaturito dalla declinante fiducia del sistema finanziario tradizionale. La perdita di fiducia è stato uno dei fattori che ha contribuito alla rapida crescita e diffusione di Bitcoin e di tutto il settore crypto.

Tra le possibili strategie di contrasto alla diffusione delle valute virtuali private messe in atto dalle autorità monetarie centrali di numerosi stati, una delle soluzioni individuate riguarda la possibilità, da parte degli Stati e delle Banche Centrali, di emettere una propria moneta digitale basata su DLT  progetto che si inquadra perfettamente con il graduale processo di digitalizzazione di beni e servizi.

Attualmente, la maggior parte degli Stati sta conducendo delle consultazioni pubbliche e delle sperimentazioni tecniche per valutare gli effetti  di una eventuale introduzione delle proprie CBDC (*Central Bank Digital Currencies*), ossia delle valute virtuali a corso legale di Stato emesse dalla Banca Centrale attraverso sistemi DLT. I motivi principali per l'adozione delle CBDC variano generalmente in base alle caratteristiche

economico-sociali dello Stato di appartenenza. Nelle economie avanzate, le ragioni principali sono riconducibili al progressivo declino nell'uso del contante e al contrasto alla diffusione di sistemi di pagamento privati più rischiosi (es. *stablecoin*). Nelle economie emergenti invece, l'introduzione di una valuta virtuale di Stato velocizzerebbe il processo di digitalizzazione e condurrebbe a una maggiore inclusione finanziaria, raggiungendo i segmenti non "bancarizzati" della popolazione.

Anche la BCE e le Banche Centrali dei paesi membri dell'Unione Europea stanno conducendo degli studi per avviare il progetto relativo ad un Euro Digitale, che potrebbe essere introdotto già nella seconda metà del 2021. Nel *Report on a Digital Euro*[25], pubblicato ad ottobre 2020 dalle Banche dell'Eurosistema, si evincono sia le possibili proprietà tecniche, sia i motivi principali per l'adozione di un Euro Digitale. Molto probabilmente il progetto delle CBDC funzionerebbe al meglio nell'ambito di un sistema DLT *permissioned*, in un network di soggetti pre-identificati e usando un algoritmo di consenso efficiente dal punto di vista energetico, come la *proof of authority*. La Banca Centrale Europea si riserverebbe il compito di emettere l'euro digitale, come avviene propriamente in un sistema centralizzato. Il compito di validazione delle transazioni, invece, potrebbe essere svolto in modo decentralizzato o meno. La Banca Centrale potrebbe decidere se lasciare il processo di validazione decentrato, che quindi verrà eseguito dai nodi in base alla specifica regola di consenso istituita, oppure potrebbe riservarsi anche il ruolo di unico nodo validatore.

Le caratteristiche tecniche del token virtuale sarebbero innanzitutto la programmabilità, la convertibilità alla pari con il contante fisico (che non verrà in alcun modo sostituito) o con altre forme di denaro (depositi, riserve…), e il fatto di essere una passività della BCE. Qui si ravvisa la prima differenza fondamentale con le valute virtuali private tipo Bitcoin: l'affidabilità della moneta per gli utenti finali. In tal senso, l'Euro Digitale rappresenterebbe una forma risk-free dell'Euro, rimanendo una passività della BCE in qualsiasi momento. Dunque, l'Eurosistema sarebbe responsabile nei confronti dei cittadini europei, sia della solvibilità dell'Euro Digitale, sia della stabilità di valore nel tempo dello strumento emesso. Inoltre, la valuta virtuale dell'Unione sarebbe ampiamente accessibile in tutta l'area EU, per conseguire una maggiore inclusione finanziaria e rimarrebbe comunque neutrale al mercato, non escludendo le soluzioni private.

Le Autorità Europee prevedono che l'Euro Digitale sarà uno strumento monetario utile a sostenere gli obiettivi di medio termine dell'Eurosistema, fornendo ai cittadini l'accesso a una forma di denaro che unisce i benefici di sicurezza dovuti al corso legale di Stato, a quelli di velocità ed efficienza apportati dalla natura digitale. L'adozione di un Euro Digitale comporterebbe contestualmente sia il sostenimento del processo di transizione digitale, sia la riduzione dei rischi collegati alla diffusione delle valute virtuali private. Come risultato dell'efficientamento dei processi di gestione del contante avremmo, inoltre, una riduzione dei costi di transazione. Di seguito, una simile valuta virtuale offrirebbe un metodo più rapido per eseguire pagamenti

[25] ECB Eurosystem (2020) *Report on a digital Euro.* [Online]. PDF disponibile al sito: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf;

giornalieri, sia una valida soluzione per i pagamenti transfrontalieri, sfruttando la velocità dei registri distribuiti e i bassi costi di transazione.

Il fine ultimo della BCE e degli Stati che stanno sperimentando progetti basati sulle CBDC è quello di implementare un mezzo di pagamento digitale, sfruttando i benefici della tecnologia DLT, contrastando lo sviluppo delle valute private e mantenendo al contempo la Vigilanza sugli intermediari. In ogni caso qualsiasi soluzione adottata e che implichi l'utilizzo di sistemi DLT deve riuscire a garantire una serie di requisiti minimi in termini di robustezza, scalabilità, sicurezza e interoperabilità della piattaforma, rispettando nel contempo la legislazione inerente per presidiare i rischi derivanti (riciclaggio di denaro/finanziamento del terrorismo, rischi correlati a ICT e protezione della privacy).

# CONCLUSIONI

Nell'ultimo decennio, un periodo contraddistinto da due pesanti crisi economiche (2008 e 2020) che hanno fortemente scosso gli equilibri economico-finanziari dell'economia globale, Bitcoin e successivamente tutto il settore *crypto*, si è proposto come un alternativo sistema di trasferimento di ricchezza basato su logiche *peer-to-peer*. Bitcoin si presenta quindi come uno strumento per minare il sistema bancario oligopolistico tradizionale, colpevole, secondo il suo creatore, di aver intossicato i principi economici fondamentali tramite una manipolazione inefficiente dell'offerta di moneta, guidata essenzialmente da logiche egoistiche a beneficio di pochi. In un'era caratterizzata da forti incertezze e dalla mancanza di fiducia nel sistema finanziario tradizionale, il protocollo informatico creato da Nakatomo si propone di dar vita ad un sistema monetario parallelo, completamente decentralizzato e incensurabile dalle istituzioni tradizionali (Stati, governi e Banche Centrali) con l'obiettivo di raggiungere una piena democrazia nel controllo della moneta, trasferendolo dalle banche ai nodi della rete e quindi, nelle mani del popolo e della gente comune.

Tuttavia, la realizzazione di tale progetto, ad oggi, sembra molto complicata, per non dire utopica. Sia perché il controllo della moneta appartiene storicamente ad un sistema bancario/governativo difficilmente spodestabile, sia perché Bitcoin e la maggior parte delle *cryptocurrencies* non presentano in pieno le proprietà per assolvere le tradizionali funzioni monetarie (mezzo di scambio, riserva di valore, unità di conto) soprattutto in relazione alla loro natura volatile e alla mancanza di tutela per l'utente. Il dilemma è di difficile soluzione: il popolo non vuole sentirsi controllato…ma senza un controllore non si sente sicuro.

Attualmente le criptovalute non sono considerate strumenti affidabili agli occhi del grande pubblico; anche le *stablecoin*, che si presentano come valute virtuali con la promessa di stabilità di valore nel tempo, presentano diversi profili di rischio che le rendono attualmente inadatte per essere usate come mezzo di scambio globalmente accettato. Appare indubbio quindi che il valore aggiunto del settore *crypto*, non sia tanto apportato dalle criptovalute, che comunque offrono l'opportunità di ridisegnare il modo tradizionale di approccio al denaro, quanto dalla tecnologia sottostante che permette tali implementazioni: la *Blockchain*. È opinione ormai diffusa che la frontiera tecnologica costituita da sistemi *blockchain* o DLT potrà, nel breve-medio termine, rivoluzionare le attività svolte in un ampio range di settori. Per il carattere innovativo e per i relativi sviluppi recenti, le iniziative basate su queste tecnologie sono ancora poche, ma in rapido aumento. Al giorno d'oggi la tecnologia DLT ha catturato il maggior interesse in ambito bancario, "il settore che da circa 10.000 anni basa il proprio successo sulla mancanza di fiducia tra gli esseri umani" (Comandini, 2020). Negli ultimi due anni, le Banche Centrali hanno iniziato le fasi di sperimentazione riguardo ad una valuta virtuale nazionale, mentre già diverse centinaia di intermediari bancari, a livello globale, hanno investito in *blockchain* o, addirittura implementato questa tecnologia, al fine di efficientare alcune delle loro operazioni. In questo ambito, uno dei progetti italiani maggiormente degno di nota è il progetto di Spunta Interbancaria, a cui ha aderito quasi la totalità delle banche del settore italiano. Sebbene la *blockchain* rimanga ad oggi un settore

prevalentemente inesplorato, è certo che nei prossimi 5-10 anni, questa tecnologia sarà l'artefice di una crescita vertiginosa in diverse linee di business. Un ausilio a ciò verrà sicuramente dalla c.d. Sandbox Regolamentare istituita dal c.d. Decreto Crescita (D.L 39/2019). La Sandbox altro non è che un ambiente di test protetto e regolamentato, nel quale le aziende possono sviluppare soluzioni innovative a contatto con il mercato reale *"*volta al perseguimento, mediante nuove tecnologie quali l'intelligenza artificiale e i registri distribuiti, dell'innovazione di servizi e di prodotti nei settori finanziario, creditizio, assicurativo e dei mercati regolamentati[26]*"*.

Tra le infrastrutture basate su *blockchain,* quella di Ethereum è considerata dagli esperti del settore, come una delle migliori mai progettate. Come esposto in precedenza, Ethereum è una piattaforma programmabile su cui possono essere "costruite" le *DApps*, applicazioni decentralizzate che eseguono, in modo automatizzato, le azioni per cui sono state create, al verificarsi di determinate condizioni. Inoltre, Ethereum consente di mettere in atto uno dei più innovativi metodi di finanziamento per aziende e start-up: le *Initial Coin Offering*. Tutto ciò è possibile grazie ai "contratti intelligenti", trasposizioni in codice di veri e propri accordi contrattuali, che si eseguono da soli, ed una volta inseriti nel *ledger* diventano immutabili. Il codice del contratto è registrato in una sottostante blockchain e il suo comportamento è deterministico. Il concetto originale di *Smart Contract* fu coniato nel 1997 da Nick Szabo, il quale paragonò il suo funzionamento a quello di un distributore automatico di bibite, arguendo che molti accordi potevano essere *"embedded in the hardware and software we deal with, in such a way as to make a breach of contract expensive…for the breacher*[27]*"*.

Tuttavia, anche gli *smart contract* presentano dei rischi: se ci fossero errori o falle nel codice questi potrebbero permettere un attacco esterno tale da mettere a rischio i fondi o rendere inattuabile il contratto, per cui l'utente deve essere sempre a conoscenza che il protocollo è sicuro quanto lo è il codice sottostante: sfortunatamente sono pochissimi gli utenti in grado di capire e valutare il codice. E anche se i controlli, le verifiche formali e i servizi di assicurazione risolvono parzialmente il problema, un certo grado di incertezza rimane. Un altro punto di possibile debolezza concerne le fonti esterne di dati: molti *smart contract* si basano su dati che non risiedono in maniera nativa sulla blockchain. Questo può portare ad interconnessioni tali da condurre ad un'esecuzione del contratto pesantemente centralizzata. Controlli, verifiche, dati esterni…come si vede, quindi sembra esistere un trade-off molto stretto, quasi connaturato, tra decentralizzazione e sicurezza.

Proprio con l'avvento degli *smart contract*, è affiorata la possibilità trasferire i benefici della *blockchain*, circoscritti sino a quel momento ad un ambito "monetario", a numerosi altri settori, in primis quello

[26] Testo del decreto-legge 30 aprile 2019, n. 34 (in Gazzetta Ufficiale - Serie generale - n. 100 del 30 aprile 2019), coordinato con la legge di conversione 28 giugno 2019, n. 58 (in questo stesso Supplemento ordinario - alla pag. 1 ), recante: «Misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi.». (19A04303) (GU Serie Generale n.151 del 29-06-2019 - Suppl. Ordinario n. 26)

[27] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548;

contrattuale. Esempi di settori lavorativi che saranno certamente rivoluzionati dall'avvento degli Smart contract e della *blockchain*, sono il settore assicurativo e quello immobiliare. Nel settore assicurativo, l'applicazione di tale tecnologia genererà un aumento generale di efficienza nei processi di gestione del rischio, riducendo al contempo, i costi delle polizze. Grazie agli *smart contract*, si potrebbero limitare, fino ad escludere totalmente, tutti quei problemi dovuti a truffe o frodi, che da sempre affliggono le compagnie assicurative. Possiamo dire lo stesso per il settore immobiliare, nel quale un sistema DLT consentirebbe di velocizzare i processi transattivi, di evitare errori nel titolo di proprietà e di limitare truffe e frodi, il tutto pagando dei costi di commissione molto minori. Un' altra utilità, la possiamo ritrovare nel processo di "tokenizzazione" dei beni fisici, in questo caso di immobili. La tokenizzazione di asset immobiliari consentirebbe di democratizzare la proprietà dei beni, offrendo agli investitori la possibilità di partecipare ad un progetto imprenditoriale tramite acquisto di uno o più gettoni digitali memorizzati sulla *blockchain*. In tal senso, la tokenizzazione degli asset permette di aumentare l'inclusione finanziaria: l'investitore, dovunque esso si trovi, potrà svolgere attività di *trading* con quote di proprietà immobiliari, rappresentate da token, o frazioni di esso.

In conclusione, possiamo dire che la creazione di *blockchain*, DLT e *smart contract* ha sicuramente scatenato un'ondata innovativa, che partendo dall'obiettivo iniziale di scardinare il sistema finanziario tradizionale, porterà nel breve termine a vantaggi concreti in un largo range di settori. Tuttavia, il grande potenziale di questa tecnologia non deve portare a sottovalutare i rischi in essa insiti (in particolare se circoscritti all'ambito finanziario) e non bisogna dimenticare che il termine "decentralizzato" può, in alcuni casi, risultare ingannevole. Si rende quindi necessaria una normativa che regoli l'attività di investimento nelle criptoattività, in quanto non si conoscono ancora gli effetti sistemici connessi ad una loro propagazione. In ogni caso, se verranno quanto meno arginati i principali problemi che la affliggono, la *Blockchain*, potrà senza dubbio rivoluzionare l'operatività di numerose attività e servizi, che al giorno d'oggi nemmeno si conoscono. Sostituendo il paradigma *trust-based* tradizionale, con uno *trust-less* paradossalmente più sicuro e trasparente, sarà possibile attuare un processo di democratizzazione finanziaria, istituendo sistemi più aperti ed inclusivi, ma anche più efficienti e robusti.

**BIBLIOGRAFIA / SITOGRAFIA**


ABILab (2021) *Spunta Banca DLT,* Rapporto ABILab. [Online] PDF disponibile al sito: https://www.abilab.it/documents/20124/0/Descrizione+iniziativa+Spunta+Banca+DLT.pdf/1a458e5c-29d7-cdbc-2bda-554ea70bd3e8?t=1590615492283;

ABI sito web (2019) *Spunta Project avvia test blockchain su operatività a regime* [Online] Disponibile al sito: https://www.abi.it/Pagine/news/Spunta-project-_-test.aspx#:~:text=La%20spunta%20%C3%A8%20un%20processo%20interbancario%20basato%20su,standardizzazione%2C%20%C3%A8%20caratterizzato%20da%20modalit%C3%A0%20operative%20non%20avanzate.;

Altalex (2021) *L'Euro Digitale e le Central Backed Digital Currency (CBDC)* [Online] Disponibile al sito: https://www.altalex.com/documents/news/2021/01/06/euro-digitale-e-central-backed-digital-currency;

Banca d'Italia Eurosistema (2019) *Quaderni di Ricerca Giuridica della Consulenza Legale Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale* n.87 a cura di Fabrizio Maimeri e Marco Mancini [PDF] disponibile al sito: qrg-87.pdf (bancaditalia.it);

N. Branzoli (2020) *Le criptovalute: gli stablecoins e il progetto Libra*, Servizio Stabilità Finanziaria, Banca d'Italia Eurosistema;

Banca d'Italia Eurosistema (2021) *Fintech regulation in the US, in the EU and in Italy: a summary and some tentative policy considerations;*

Banca d'Italia Eurosistema (2018) *Rapporto sulla stabilità finanziaria n.1* [Online] Disponibile al sito: https://www.bancaditalia.it/pubblicazioni/rapporto-stabilita/;

Banca d'Italia Eurosistema (2017) *La moneta legale e la moneta scritturale* [Online] Disponibile al sito: https://www.bancaditalia.it/servizi-cittadino/cultura-finanziaria/informazioni-base/moneta-legale-scritturale/index.html;

Bank of England (2020) *Central Bank Digital Currency, opportunities, challenges and design* [Online] Disponibile al sito: Discussion Paper - Central Bank Digital Currency: Opportunities, challenges and design (bankofengland.co.uk);

Caetano R. (2016) *"Bitcoin. Guida all'uso delle criptovalute",* Apogeo, Milano;

Cambridge Bitcoin Electricity Consumption Index, 2021. [Online] Disponibile al sito: https://cbeci.org/;

A. Caponera, C. Gola (2019) *Aspetti economici e regolamentari delle «cripto-attività» - Questioni di Economia e Finanza (Occasional Papers) Numero 484* - Banca d'Italia Eurosistema [Online] Disponibile al sito: Banca d'Italia - N. 484 - Aspetti economici e regolamentari delle «cripto-attività» (bancaditalia.it);

Ciaian, P., Rajcaniova, M. & Kancs (2016) *"The digital agenda of virtual currencies: Can BitCoin become a global currency*?", Inf Syst E-Bus Manage (2016) 14: 883;

Comandini G. (2020) *Da zero alla Luna: quando, come, perché la Blockchain sta cambiando il mondo,* Palermo: Dario Flaccovio Editore;

Consob, Banca d'Italia (2021) *Consob e Banca d'Italia mettono in guardia contro I rischi insiti nelle crypto-attività*, Comunicato Stampa, [PDF] disponibile al sito: https://www.consob.it/documents/46180/46181/cs_20210428.pdf/ca5fec2f-36fb-4677-8292-e40bb0d7a597;

N. Cucari, V. Lagasio, G. Lia & C. Torriero (2021) *The impact of blockchain in banking processes: the Interbank Spunta case study*, Technology Analysis & Strategic Management, DOI: 10.1080/09537325.2021.1891217;

Criptovaluta.it (2020) *Criptovalute del futuro: come saranno?* [Online] Disponibile al sito: https://www.criptovaluta.it/9543/futuro-criptovalute;

Decentra Academy (2020) *MiCA: la proposta di regolamento della Commissione europea sui cripto-asset.* [Online] Disponibile al sito: https://decentra.academy/deeper-news/mica-la-proposta-di-regolamento-della-commissione-europea-sui-cripto-asset.html;

A. de Vries, *Bitcoin's Growing Energy Problem*, Joule, Volume 2, Issue 5, 2018, Pages 801-805;

EBA (2016), *"Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)*", disponibile al sito: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1547217/32b1f7f2-90ec-44a8-9aab-021b35d1f1f7/EBA%2520Opinion%2520on%2520the%2520Commission%25E2%2580%2599s%2520proposal%2520to%2520bring%2520virtual%2520currency%2520entities%2520into%2520the%2520scope%2520of%25204AMLD.pdf?retry=1;

ECB Eurosystem (2020) *Report on a digital Euro.* [Online]. PDF disponibile al sito: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf;

ECB Eurosystem (2020) *Digital Euro* [Online]. Disponibile al sito: https://www.ecb.europa.eu/euro/digital_euro/html/index.en.html;

ECB Crypto-Assets Task Force (2020) *Occasional paper series Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area,* Eurosystem [PDF] disponibile al sito: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf;

European Commission (2020) *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on a Digital Finance Strategy for the EU. COM/2020/591 final* [Online] Disponibile al sito: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0591&from=EN;

European Commission (2020) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. COM/2020/593 final.* [Online] Disponibile al sito: EUR-Lex - 52020PC0593 - EN - EUR-Lex (europa.eu);

European Commission (2020) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a pilot regime for market infrastructures based on distributed ledger technology. COM/2020/594 final.* [Online] Disponibile al sito: EUR-Lex - 52020PC0594 - EN - EUR-Lex (europa.eu);

European Commission (2020) *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. COM/2020/595 final*. [Online] Disponibile al sito: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020PC0595;

European Commission (2016) *"Proposta di Direttiva del Parlamento Europeo e del Consiglio che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica la direttiva 2009/101/CE",* Strasburgo, COM (2016) 450 final, 2016/0208 (COD);

European Parliament (2018) *Competition issues in the Area of Financial Technology (FinTech)* [PDF] disponibile al sito: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU(2018)619027_EN.pdf;

IASSP website (2021) *Il ruolo delle criptovalute nel riciclaggio di denaro.* [Online] Disponibile al sito: Il ruolo delle Criptovalute nel Riciclaggio di Denaro | IASSP;

N. Mainieri (2020) *La Cassazione penale esamina le valute virtuali sotto il profilo del Testo Unico della Finanza – le precedenti qualificazioni e i richiami della Direttiva penale sulla lotta al riciclaggio mediante l'uso del penale (n. 2018/1673 UE)* Giurisprudenza Penale Web 10 [Online] Disponibile al sito: https://www.giurisprudenzapenale.com/2020/10/20/la-cassazione-penale-esamina-le-valute-virtuali-sotto-il-profilo-del-testo-unico-della-finanza-le-precedenti-qualificazioni-e-i-richiami-della-direttiva-penale-sulla-lotta-al-riciclaggio-med/;

Nakamoto S. (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online] PDF disponibile al sito: https://bitcoin.org/bitcoin.pdf;

ValuteVirtuali (2017) *Bitcoin: che cosa sono i BTC e come funziona la valuta virtuale più utilizzata* [Online]. Disponibile al sito: https://valutevirtuali.com/bitcoin-cosa-btc-funziona-la-valuta-virtuale-piu-utilizzata/;

Shen. W. (2021) *New development on regulation of cryptocurrency in China*, Journal of Investment Compliance [Online] Disponibile al sito: https://doi.org/10.1108/JOIC-11-2020-0045;

Szabo, N. (1997). *Formalizing and Securing Relationships on Public Networks*. First Monday, *2*(9). Disponibile al sito: https://doi.org/10.5210/fm.v2i9.548.