LUISS Guido Carli, Roma (RM)

2021

MONETA DIGITALE, CRIPTO-VALUTE & CBDC

UN APPROCCIO MACROECONOMICO, INFORMATICO E FINANZIARIO AI SISTEMI DI PAGAMENTO DIGITALI DECENTRALIZZATI

JACOPO BRACALONI

Relatore: Salvatore Nisticò
Corso: Macroeconomia ed economia politica
Dipartimento: Impresa & Management

SOMMARIO

RINGRAZIAMENTI

A mia Mamma Silvia, per aver garantito per me sempre il meglio
A mio Babbo Andrea, per avermi insegnato che il lavoro e il rispetto sono virtù importanti
A mio Fratello Tommaso, dato che la famiglia è un bene prezioso e che va protetto, sempre
A mia Nonna Grazia, perché i valori della vita non hanno né tempo, né età

Ad Adele per aver sempre creduto in me ed aver guardato oltre ciò che io mi limitavo a vedere

A Francesco, dato che Via Acherusio rimarrà sempre la Nostra casa
A Lorenzo e Marco, da voi ho capito il vero significato dell'amicizia
Ad Alessia e Cesare, per aver reso tutto questo un viaggio e non una semplice esperienza

A tutti i miei cari amici, compagni di avventure e di sventure, a voi devo tutti i miei risultati e il mio futuro. Un giorno faremo la storia

A Roma, dove sono rinato

Grazie.

INTRODUZIONE

La tecnologia indica l'insieme di tecniche utilizzate dall'Uomo per produrre oggetti altrimenti non reperibili in natura, per risolvere problemi e per migliorare le proprie condizioni di vita. La tecnologia è, quindi, l'impronta di una civiltà in un dato momento e in un dato luogo: la società contemporanea ha a disposizione i prodotti di quel processo, avviatosi nei Paesi industrializzati di metà Novecento, che ha portato ad una digitalizzazione della tecnologia meccanica e che prende il nome di rivoluzione informatica; questa, può ragionevolmente essere considerata come una declinazione dell'innovazione tecnologica nell'ambito dei processi informatici, ovvero l'elaborazione computerizzata di programmi ed algoritmi con lo scopo di trasformare informazioni input in soluzioni atte a soddisfare determinate necessità.

Ciò che rende la rivoluzione informatica tale è da un lato l'eterogeneità dei bisogni che contraddistinguono i diversi ambiti della società contemporanea, a fronte dei quali sono state prodotte diverse soluzioni, alcune più complesse di altre a seconda dell'esigenza che sono chiamate a soddisfare, dall'altro i notevoli benefici che la tecnologia digitale presenta rispetto a quella meccanica in termini di versatilità, di velocità e di universalità.

La rivoluzione informatica ha generato prodotti particolarmente interessanti e discussi all'interno dell'ambito finanziario, in particolare, all'interno del settore degli strumenti di pagamento: l'introduzione delle c.d. monete digitali, chiamate così dato che la loro creazione ed il loro scambio virtuale sono resi possibile grazie a processi informatici, non sta solo rivoluzionando il modo con cui i soggetti detengono liquidità, ma sta anche generando nuove opportunità di investimento e di finanziamento, prima del tutto sconosciute, beneficiando il sistema economico nel suo complesso grazie sia ad un maggior grado di diversificazione delle attività, sia ad un più elevato livello sicurezza durante le transazioni.

In questo studio verrà analizzato il fenomeno dell'introduzione della moneta digitale, distinguendo le caratteristiche dei nuovi strumenti informatici rispetto ai metodi di pagamento tradizionali. Da questo spettro generale, particolare attenzione sarà rivolta all'ambito delle cripto-valute e dei nuovissimi sistemi di finanza decentralizzata, nati dallo sviluppo della tecnologia *blockchain*. In ultima analisi verrà valutata l'ipotesi riguardo l'adozione di un sistema di pagamento digitale centralizzato, c.d. *CBDC* (*Central Bank Digital Currency*), studiando il suo eventuale funzionamento, i rischi ed incertezze connesse con la sua introduzione, ed il suo impatto sul sistema bancario, finanziario e sull'offerta di moneta.

CAPITOLO 1. LE VALUTE DIGITALI

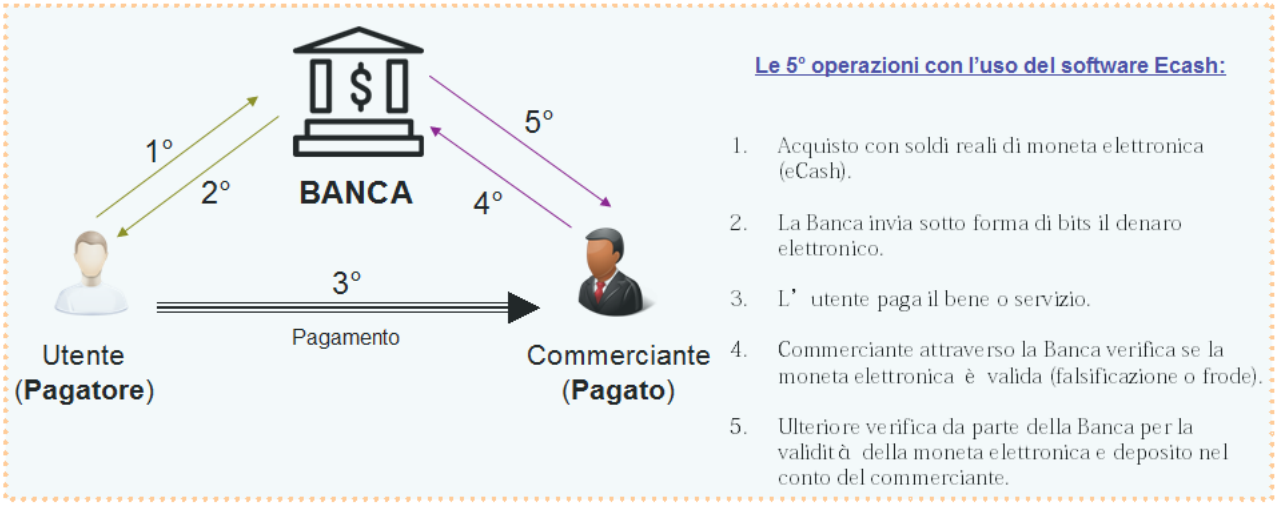
1.1 STORIA DELLA MONETA DIGITALE

È il 4 Aprile del 1994, James H. Clark e Mark Andreessen fondano la Netscape Communications Corporation, la società proprietaria del *web browser* Netscape Navigator (Wikipedia, l'enciclopedia libera 2021). A quattro mesi dal lancio, il motore di ricerca aveva già conquistato tre quarti del mercato dei *web browsers*: il suo successo era dovuto essenzialmente a quello raggiunto dai prodotti complementari al *browser* come i sistemi operativi - Windows ed OSX -, i computer - PC, Mac o Workstation - e la vasta gamma di *plug-in* ed applicazioni in esclusiva - ShockWave, Media Player, ToolBox, … -, attivabili dall'interfaccia *user-friendly* e che permettevano l'esecuzione di funzioni multimediali al tempo avanzate come la riproduzione video-audio, le animazioni e la realtà virtuale (University of California, Bakerley n.d.). È quindi il 1994 la data che segna il passaggio dalla *Old Economy*, basata sul settore manifatturiero, alla *New Economy*, improntata sul digitale e slanciata verso il futuro della rivoluzione informatica.

Grazie al successo di Netscape si assistette alla sconcertante proliferazione di aziende operanti nei settori Internet e informatico che, sfruttando l'euforia generale derivante dai concetti di "sviluppo", "crescita" e "progresso", riuscirono ad alimentare le aspettative di continui aumenti futuri dei prezzi dei titoli azionari, generando una marcata sopravvalutazione degli stessi rispetto al loro valore fondamentale: si generò, così, la prima bolla speculativa che interessò il mondo dell'Internet e che prese il nome di *Dot-com Bubble*. Agli inizi degli anni 2000 alcune imprese pubblicarono bilanci che indicavano una performance deludente: il calo della quotazione di molte imprese iniziò ben presto a preoccupare gli azionisti che iniziarono a chiudere in massa le loro posizioni (c.d. *panic selling*) con la speranza di rientrare nei loro investimenti prima che i titoli stessi si svalutassero ulteriormente, così da limitare le perdite. A partire dal 2001 molte società operanti nel settore informatico furono costrette a dichiarare fallimento e molte altre furono soggette ad operazioni di acquisizione o fusione. Nel 2004 solo la metà delle aziende che si erano quotate ad inizio millennio era ancora attiva (CONSOB, Commissione Nazionale per le Società e la Borsa s.d.).
Sebbene da un lato quella della *Dot-com Bubble* si è rivelata essere un'esperienza fallimentare per molte imprese e *start-ups* che si affacciavano al mondo dell'informatica, dall'altro è innegabile l'importanza del ruolo che ha giocato in qualità di propulsore dell'innovazione tecnologica avviatasi già a partire degli anni '50-'60: è grazie sia al clima riformista che le nuove generazioni stavano respirando a scapito del conservatorismo relitto delle generazioni precedenti, sia alla "*trust in the machine*" che fomentava l'emergere di nuove professionalità ed affascinava gli investitori, sia all'*American Dream* che si perpetuava tra le aziende della Silicon Valley, sia all'innovazione dei processi tecnologici per la produzione di componenti sempre più *smart* ed efficienti che la rivoluzione informatica ha piantato le sue radici così a fondo nella società contemporanea (Castells 2001).

È figlio di questo periodo lo scritto "*Blind Signatures for Untracble Payments*", di David Chaum, datato 1983, in cui si muovono i primi passi verso un sistema di pagamento del tutto virtuale che utilizzasse un nuovo sistema di crittografia asimmetrica – il c.d. *Blind Signature Crypto-System* –, nell'esecuzione molto simile al tradizionale algoritmo di firma *RSA*, che da un lato rendesse impossibile a terze parti sia di risalire all'identità dei beneficiari, sia di stabilire il momento o l'ammontare dei pagamenti effettuati da un individuo; dall'altro fornisse ai pagatori sia la prova dell'avvenuta transazione – grazie alla firma digitale apposta da un intermediario fiduciario –, sia la possibilità di stabilire l'identità dei beneficiari in determinate circostanze (Chaum 1983). Lo schema inventato da Chaum, che comunque presentava rischi di doppia spesa e problemi relativi al fatto che l'intermediario fiduciario venisse tratto in inganno e finisse col validare pagamenti inverosimili (Goldwasser 2008), fu effettivamente implementato nel 1989 con la moneta digitale ECash, di proprietà della DigiCash, società di cui Chaum ne era il fondatore. Il funzionamento dello strumento di pagamento richiedeva l'apertura di un conto corrente presso una delle banche convenzionate con il circuito ECash – come Deutsche Bank o Mark Twain Bank –, e il deposito di valute a corso legale (*fiat*) su tale conto. La banca provvedeva successivamente alla certificazione dell'ammontare depositato e all'emissione di equivalente denaro digitale, di cui il depositario poteva disporre su tutte le piattaforme, virtuali e non, aderenti al circuito ECash, mantenendo la sicurezza e la riservatezza delle transazioni grazie all'uso della firma digitale (portafoglioelettronicomigliore.com 2019).

Funzionamento del sistema di pagamento eCash



Fonte: http://www.portafoglioelettronicomigliore.com/digicash.asp

Il periodo che intercorre tra la fine degli anni '90 e la prima metà degli anni 2000 vide la nascita di un numero significativo di imprese la cui *core-activity* si basava sull'offerta di strumenti di pagamento digitale; questo fu reso possibile sia grazie alla risonanza della *wave of innovation* generata da scritti come quelli di Chaum e dall'invenzione della tecnologia ECash, sia grazie al fervore degli investitori durante il periodo della *Dot-com Bubble.* Infatti questi investitori, imitando i *trends* e le prassi maggiormente diffuse (*hearding behaviour*),

avevano fatto confluire gran parte della loro ricchezza sui settori dell'informatica e dell'Internet (CONSOB, Commissione Nazionale per le Società e la Borsa s.d.). Oggigiorno, la maggior parte di queste compagnie o ha cessato la propria attività o è stata al centro di operazioni di acquisizione o fusione da parte di altre imprese più solide; questa sorte nefasta è imputabile ad una serie di ragioni: alcune aziende non sono state in grado di interpretare correttamente i bisogni di un mercato così mutevole e in rapida espansione, a volte antecedendo la domanda effettiva – è questo il caso di DigiCash, la quale è stata acquisita nel 2009 (Pitta 1999) –; altre sono rimaste vittime della *Dot-com Bubble bust* – questa la sorte di Flooz.com, impresa con sede legale a New York, fondata nel Febbraio 1999 e fallita nel 2001 a causa di una svalutazione eccessiva delle attività causata dal drastico deprezzamento sul mercato secondario dei titoli emessi (Rossen 2017) –; altre ancora, ree di attività illecite come il riciclaggio di danaro sporco o di fatti che costituiscono reato cibernetico – come lo sviluppo e la messa in rete di *malwares* e/o *phishing scams* –, sono state sottoposte a particolari procedure di liquidazione forzata da parte delle Autorità di Vigilanza Statunitensi: a tal riguardo, di particolare rilievo sono gli scandali della e-Gold Ltd e del Liberty Dollar (White 2014).

e-Gold Ltd, fu fondata da Douglas Jackson e Barry Downey nel 1996. e-Gold è stata la prima piattaforma *software* di pagamento che abbia permesso agli utenti di eseguire complicate transazioni finanziarie globali al di fuori del sistema bancario regolamentato, il tutto a commissione zero. L'e-Gold è stato anche il primo sistema di pagamento monetario sicuro al mondo basato su *account* ad aver consentito l'uso dell'oro e di altri metalli preziosi come valuta. A partire dagli anni 2000, si registrava una proliferazione di servizi di cambio indipendenti che hanno segnato la prima apparizione di un'industria che fornisse scambi tra monete *fiat* e una marca di denaro emessa da privati. Nel 2001, diverse dozzine di aziende e individui in tutto il mondo offrivano servizi di scambio di terze parti tra valute nazionali ed e-Gold, ampliando ulteriormente la base di utenti internazionali e consentendo alla piattaforma, che permetteva l'esecuzione di transazioni fino a un decimillesimo di grammo d'oro, di diventare l'unico sistema di micro-pagamenti di successo al mondo (Wikipedia, l'enciclopedia libera 2016).

e-Gold è tristemente ricordata per la frode adoperata da vari soggetti in grado di trarre vantaggio dalla piattaforma per finanziare uno schema Ponzi di dimensioni internazionali: uno schema Ponzi è una truffa sugli investimenti che coinvolge il pagamento di presunti rendimenti agli investitori esistenti da fondi forniti da nuovi investitori ((Securities & Exchange Commission 2018). L'intervento delle Autorità di Vigilanza degli Stati Uniti d'America, a fronte delle molteplici denunce presentate da proprietari di conti truffati, ha rivelato che gli schemi Ponzi erano un *driver* sostanziale del *business* di e-Gold per il riciclaggio di denaro sporco (Mullan 2014). A ciò si aggiungono gli innumerevoli attacchi cibernetici – come *malware* e *phishing scams* – adoperati da criminalità organizzate ed *hacker* che, sfruttando il successo della piattaforma, sono riusciti a raccogliere i dati di milioni di *account* e-Gold. A nulla è servito effettuare controlli più stringenti sugli utenti da parte della società - basti pensare che nel 2006 e-Gold è stata parte attiva nell'intercettazione dell'*hacker* che si era illegittimamente impossessato del codice *firewall* di Cisco Systems, a fronte di un pagamento in oro

digitale (Meek 2007) -, la valuta aveva ormai la triste fama di essere “il metodo di pagamento prediletto dai criminali”.
È il 2011, il Governo degli Stati Uniti estende gli effetti del Patriot Act del 2008 - che considera reato federale la gestione di un'attività di trasmissione di denaro senza licenza statale in uno Stato che richieda tale licenza - non più alle valute, ma a qualsiasi bene che abbia un valore intrinseco quantificabile: e-Gold, non potendo ottenere nessuna licenza statale, fu costretta a cessare la propria attività.

L’episodio del Liberty Dollar fu l’ulteriore dimostrazione di quanto alacremente e sconsideratamente la società del nuovo millennio stesse muovendo i suoi passi in un ambito che il procuratore Jonathan W. Haray, riferendosi al caso e-Gold Ltd, ha definito essere “il *Far West*” dei sistemi di pagamento, dove “le persone stanno cercando quali siano le regole e quali le conseguenze” (United States Distrisct Court for the District of Columbia 2008).
Il Liberty Dollar è stato progettato da Bernard von NotHaus e lanciato nell'ottobre 1998. Al suo inizio, von NotHaus ha annunciato che il suo obiettivo era quello di fornire una valuta di baratto volontario privato come alternativa alla valuta della Federal Reserve. Il nuovo Liberty Dollar doveva essere basato principalmente sulle monete d'oro e d'argento, fornendo, grazie alla sua preziosa base metallica, protezione contro l'inflazione a cui è incline l'inconvertibile dollaro tradizionale (Stanford Computer Science 2010), la coniazione fu adoperata da Sunshine Minting Inc., attualmente operante in Idaho, USA.
Il Liberty Dollar era costituito principalmente da tre componenti: la prima consisteva in monete d’oro e d’argento; la seconda consisteva in certificati rimborsabili su richiesta detenuti in un magazzino in Idaho; mentre la terza componente, il c.d. 'eLibertyDollar', consisteva in ricevute di pagamento digitali, pertanto il Liberty Dollar esisteva in carta e in forma digitale, e tutte le forme del Liberty Dollar erano denominate in unità di dollari, cioè l'unità di conto era il dollaro. Anche se l’intento era competere con la valuta statunitense, il Liberty Dollar non venne mai rappresentato come una valuta ufficialmente riconosciuta dal governo degli Stati Uniti, anzi, tutto il successo e la campagna *marketing* ruotavano attorno al fatto che non fosse una valuta ufficiale degli Stati Uniti, ma che fosse superiore a quest’ultima.
Il Liberty Dollar ebbe un grande successo e divenne la seconda valuta più popolare negli Stati Uniti.
Sebbene all’inizio l’atteggiamento del governo degli Stati Uniti verso la valuta fu permissivo, nel 2006 la zecca di stato, tramite comunicato stampa, dichiarò la creazione, fisica e digitale, del Liberty Dollar come un reato federale (United States Mint 2006). Sebbene più e più volte il fondatore von NotHaus abbia rimarcato quanto il Liberty Dollar non costituisse una moneta a corso legale, né abbia mai avuto l’intenzione di farlo, ma fosse in realtà una valuta di permuta tra due *assets*, ossia il dollaro tradizionale ed i metalli preziosi, nel 2011 la giuria di StatesVille, North Carolina, ordinò la cessazione immediata della coniatura, fabbricazione e/o creazione del Liberty Dollar, accusando il fondatore di “fare, possedere e vendere le proprie monete”, in concorrenza con il dollaro americano.

Il corso degli eventi non solo ha dimostrato quanto l'innovazione tecnologica ed informatica abbiano rivoluzionato il settore degli strumenti di trasferimento del danaro, ponendo le basi per lo sviluppo del *FinTech* e creando nuove opportunità di successo; ma ha anche messo in evidenza le debolezze di governi ed Autorità di Vigilanza, impreparati nell'affrontare un cambiamento di tale portata ed indolenti nell'emanare un *corpus* normativo atto a regolamentare il settore, scegliendo, purtroppo spesso, di ostacolare il progresso piuttosto che indirizzarlo sapientemente a beneficio dell'interesse collettivo.
I primi anni 2000 sono stati caratterizzati da una profonda incertezza da parte delle imprese che si affacciavano al mondo informatico le quali, spesso, avviavano la propria attività senza una strategia di successo ben precisa perché sospinte dai *trends*, dai comportamenti degli investitori che avevano devoluto ingenti capitali nel settore, e, di conseguenza, dalle prospettive di alti rendimenti ottenibili in lassi di tempo ridotti. Per queste *start-ups*, trovatesi in pochissimo tempo agli apici delle quotazioni borsistiche e prive dell'esperienza necessaria per mettere in atto soluzioni in grado di salvaguardare la propria posizione gli effetti dello scoppio della bolla finanziaria si sono fatti sentire maggiormente e per un periodo di tempo prolungato. Tuttavia, le innovazioni e le scoperte tecnologiche se da un lato sono state una condanna per molte neo-imprese, dall'altro si sono rivelate essere il punto di partenza per la scalata al successo di altre che hanno sia saputo affrontare con cautela i tempi che stavano attraversando, sia mettere in atto le giuste scelte di investimento e finanziamento: è questo il caso di PayPal, Payoneer e della più recente Stripe.

Tuttavia, l'innovazione informatica non si è limitata esclusivamente a generare nuove occasioni di riuscita per le imprese, ma ha rivoluzionato completamente un settore che, solo a partire da Bretton Woods, aveva raggiunto un sistema di scambi fluttuante, libero dalla convertibilità in oro e che, per garantire bassi tassi di inflazione, era posto sotto il controllo e la regolamentazione verticale delle Banche Centrali; un sistema, questo, che Satoshi Nakamoto definì essere come una vittima " […] delle debolezze intrinseche ad un modello basato sulla fiducia" e a cui Bitcoin si presentava come migliore sostituto.

Bitcoin nasce dal *paper* "Bitcoin: un sistema di moneta elettronica *Peer-to-Peer*", pubblicato nel 2008 dalla figura leggendaria di Satoshi Nakamoto[1]. Lo scritto riprende le pubblicazioni di David Chaum riguardo l'introduzione di uno strumento di pagamento digitale che utilizzasse il sistema della crittografia asimmetrica distribuito all'interno di una rete *Peer-to-Peer*[2] per l'esecuzione del *software* Bitcoin, a sua volta incentrato sulla attività di *mining*, ossia la risoluzione algoritmica di problemi computazionali (*Proof-of-Work*) per la validazione delle transazioni registrate e la conseguente creazione di nuova valuta Bitcoin (Nakamoto 2008).

[1] Seppure la reale identità di Satoshi Nakamoto rimannga ancora oggi avvolta nel mistero, è ragionevole credere che un protocollo come quello di Bitcoin, che ha rivoluzionato la finanza odierna, nasce dal lavoro congiunto delle più grandi imprese operanti nel settore *tech* orientali: Samsung, Toshiba, Nakamichi e Motorola.

[2] *Peer-to-Peer* è un concetto della teoria delle reti informatiche che caratterizza un network di calcolatori in cui la totalità delle funzionalità richieste è distribuita tra singoli nodi client/server, in maniera omogenea e paritaria, senza ricorso ad infrastrutture centrali, in modo che tali singoli nodi concorrano alla realizzazione di tutte le funzioni del network.

Già da questa prima definizione è possibile comprendere la caratteristica più rilevante della valuta di Nakamoto, la decentralizzazione: Bitcoin, infatti, non è sottoposta al controllo di nessuna Autorità Centrale, né dipende, quindi, dalla "fiducia" di nessuna particolare Istituzione; vuole essere, invece, una moneta *open-source*, in cui chiunque possa essere in grado di implementare la sua progettazione, pur nel rispetto del protocollo stabilito da Nakamoto.

In breve tempo Bitcoin, grazie anche alla caratteristica di rendere estremamente complicato risalire all'identità delle controparti delle transazioni – questo perché viene utilizzato il sistema della crittografia asimmetrica – ha ottenuto, a partire dalla sua introduzione, un successo sempre maggiore, ne è testimonianza non solo la quotazione che ha raggiunto recentemente i suoi massimi storici, grazie agli ingenti investimenti effettuate da imprese di grandi dimensioni come Tesla o PayPal (Tepper 2021), ma anche per la proliferazione di nuove cripto-valute come Ethereum, Cardano o Libra, per citarne solo alcune, che si appoggiano a sistemi informatici e tecnologici che riprendono i protocolli utilizzati da Bitcoin e che, per questo motivo, col tempo hanno preso il nome di AltCoin, abbreviazione per "*Alternative Coins*" (Torchiani 2018).

Quotazione Bitcoin/EURO

Fonte: Yahoo! Finance https://it.finance.yahoo.com/quote/BTC-EUR/

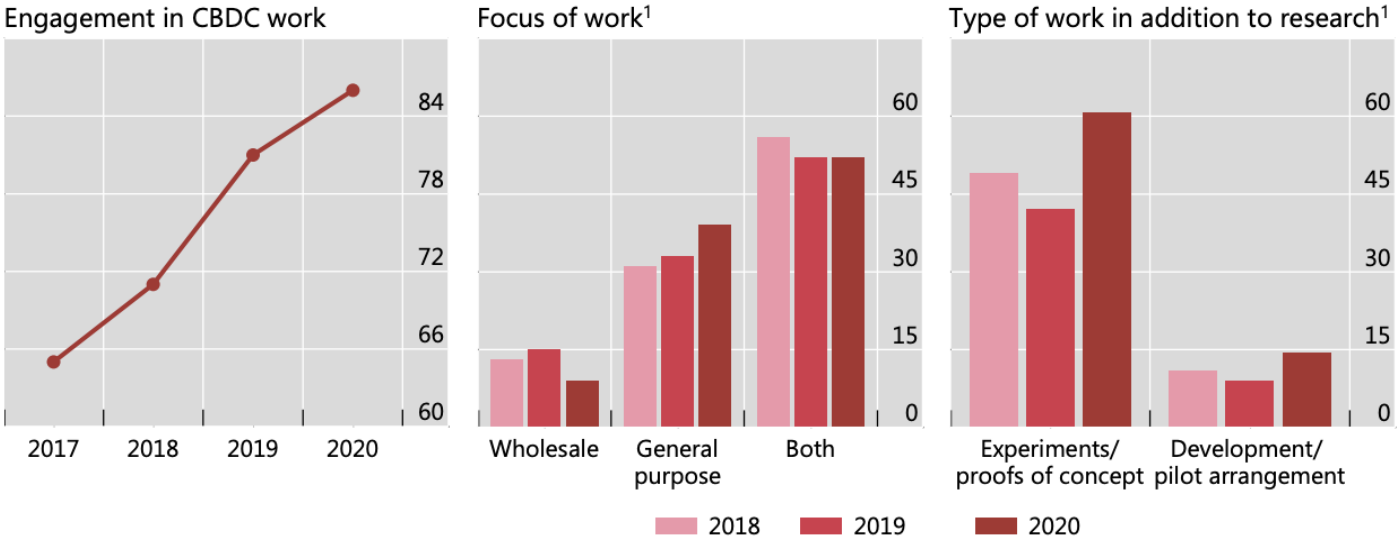
È innegabile l'importanza del ruolo che le cripto-valute hanno giocato nel porre le basi per lo sviluppo del *FinTech* e dei più recenti sistemi di finanza decentralizzata, segnando così l'inizio di un nuovo periodo storico caratterizzato dalla presenza di nuove tecnologie informatiche come il *WEB3* o gli *smart contracts*[3].

Dato che le valute digitali stanno ricoprendo un ruolo sempre più rilevante all'interno del sistema economico contemporaneo, coinvolgendo soggetti privati, famiglie, imprese, intermediari finanziari e banche, ecco che le principali autorità incaricate dell'attuazione della politica monetaria, come la Federal Reserve, la Banca Centrale Europea o la Bank of England, hanno recentemente rivolto il loro interesse verso l'introduzione di una valuta digitale (c.d. *CBDC* o "*Central Bank Digital Currency*") – vedere grafico relativo a: "Coinvolgimento delle Banche Centrali riguardo l'introduzione di una *CBDC*" – che mantenga in tutto e per tutto le caratteristiche della moneta tradizionale: rimanga sotto il controllo verticale della Istituzione di

[3] Affronteremo questi temi in modo più approfondito nei capitoli relativi alla cripto-valuta e ai sistemi di *De-Fi*

riferimento, la quale ne garantirà il corretto funzionamento, e riesca soprattutto a mantenere la stabilità monetaria e bassi tassi di inflazione[4].

Coinvolgimento delle Banche Centrali riguardo l'introduzione di una CBDC



[1] Share of respondents conducting work on CBDC.

Fonte: C Boar and A Wehrli, "Ready, steady, go? Results of the third BIS survey on central bank digital currency ", BIS Papers, no 114, January 2021.

[4] A scapito delle cripto-valute, le quali, spesso, vengono apostrofate come *assets* troppo volatili (Draghi 2021)

1.2 MONETA DIGITALE: CHE COS'È? IN COSA È DIVERSA RISPETTO ALLA VALUTA TRADIZIONALE?

La valuta digitale, per essere considerata tale, svolge le tre funzioni caratteristiche della moneta tradizionale: è considerata a tutti gli effetti un'unità di conto, in quanto può essere utilizzata per confrontare in maniera omogenea il valore di prodotti e servizi molto diversi tra loro, agevolando così le decisioni economiche e gli accordi contrattuali; è una riserva di valore, dal momento che permette di spostare nel tempo la quota di reddito che non viene utilizzata immediatamente per consumare beni e servizi ed è, infine, un mezzo di pagamento, in quanto può essere scambiata istantaneamente con beni e servizi (Banca d'Italia 2017).

Stando a quanto appena esposto, la valuta digitale può essere intesa come una rappresentazione informatica della moneta "*fiat*", ossia la valuta fiduciaria a corso legale come l'Euro, il Dollaro o lo Yen: in questo caso, la definizione di valuta digitale è assimilabile al concetto di moneta elettronica, o *E-Money*, intesa come il valore monetario memorizzato elettronicamente, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento e che sia accettato da persone fisiche e giuridiche diverse dall'emittente. L'emissione di moneta elettronica è rimessa in via esclusiva alle banche ed agli istituti di moneta elettronica; sotto questo profilo, di particolare rilevanza è la veste formale che le Autorità Centrali, come la BCE, la FED o le Banche Centrali Nazionali, assumono nell'emissione di moneta elettronica: tali Istituzioni, non possono agire in qualità di autorità monetaria[5] (TUB - Testo unico delle leggi in materia bancaria e creditizia 1993).

La definizione di valuta digitale coincideva perfettamente con la descrizione appena fornita di moneta elettronica fino al 2008, anno a partire dal quale le cripto-valute hanno iniziato a diventare uno strumento di pagamento sempre più utilizzato e rilevante: per questa ragione, è opportuno attribuire al concetto di valuta digitale un senso ancora più ampio di quanto inizialmente inteso, che possa includere al suo interno non solo la nozione di cripto-valuta, ma anche quella relativa ai più recenti sistemi di finanza decentralizzata risultanti da quest'ultima: infatti, si intende valuta digitale o moneta digitale qualsiasi valuta, denaro o a*sset* simile al denaro che venga principalmente gestito, archiviato o scambiato su sistemi informatici digitali, in particolare su Internet. I tipi di valute digitali sono: cripto-valuta, valuta virtuale[6] e valuta digitale della Banca Centrale (*CBDC*). La valuta digitale può essere registrata su un *database*[7] distribuito su Internet, un *database* elettronico centralizzato di proprietà di una società o di una banca, all'interno di file digitali o anche su una carta a valore memorizzato come carte di credito/debito (Carstens 2015).

[5] La *ratio* dietro a questo vincolo è individuabile nella volontà di tenere il canale riservato alla valuta tradizionale ben distinto da quello della moneta elettronica onde evitare che variazioni nel valore di quest'ultima possano produrre effetti inflazionistici sulla prima. Questa scelta è stata fatta anche nell'ottica di riuscire a valutare gli effetti degli esperimenti sull'introduzione di una *CBDC*, senza che questi risultati vengano viziati dalla presenza di situazioni di un alto profilo di inflazione della moneta *fiat*, per cui le persone considererebbero un *asset* più sicuro della seconda e renderebbero i dati raccolti privi di significato statistico.

[6] La letteratura si dimostra ambigua riguardo l'inclusione della definizione di "valuta virtuale" all'interno del più ampio concetto di "moneta digitale". Il punto verrà approfondito nel capitolo "Valute a confronto: digitale vs. virtuale".

[7] Tecnicamente chiamato "*ledger*".

La differenza principale tra la valuta digitale e quella tradizionale risiede nella natura dematerializzata della prima, ottenuta per mezzo dell'esecuzione di processi informatici che da un lato garantiscono l'unicità della neo-moneta, proteggendola dalla contraffazione, dall'altro sostengono la sicurezza durante le transazioni non solo per mezzo di una connessione di tipo SSL[8], ma anche attraverso l'uso di una "*ledger*"[9], ossia un registro digitale, che tenga traccia dei movimenti delle controparti (Shin 2021): il problema della doppia spesa viene risolto attraverso il processo della validazione della transazione, che può essere effettuato o centralmente da parte delle Istituzioni emittenti della moneta, oppure, come nel caso delle cripto-valute, in maniera decentralizzata da parte dei partecipanti al *network* della valuta.

La moneta digitale, intesa nel suo concetto più ampio di valute che assolve alle sue funzioni all'interno di un ambiente informatico, da un lato presenta gli indubbi vantaggi di trasportabilità e di rapidità nel completamento delle transazioni, evitando, per giunta, l'usura fisica dovuta al tempo, dall'altro può restare vittima di attacchi cibernetici che minino o il corretto funzionamento del sistema di pagamento o la sicurezza dei *wallets*[10] di danaro digitale detenuti dagli utenti (Candiloro 2015).

1.3 VALUTE A CONFRONTO: VIRTUALE VS. DIGITALE

Per valuta virtuale si intende quel metodo di pagamento digitale di tipo decentralizzato, privo di corso legale, emesso e controllato direttamente dai suoi sviluppatori ed accettato dai membri di una determinata *community* virtuale. Il metodo più veloce per ottenere valuta virtuale è attraverso lo scambio con moneta "reale" ad un tasso di conversione prefissato dagli sviluppatori della prima. Inoltre, gli utenti possono aumentare l'ammontare di valuta virtuale in loro possesso raggiungendo determinati obiettivi stabiliti o dagli sviluppatori o dalla *community* stessa.

Esistono diversi tipi di schemi di valute virtuali, di seguito sono riportate le principali:

1. **Schemi chiusi di valuta virtuale**: questi programmi non hanno quasi alcun legame con l'economia reale e a volte sono chiamati schemi "solo *in-game*". Gli utenti di solito pagano una quota di abbonamento e possono guadagnare denaro virtuale in base alle loro prestazioni online. La valuta

[8] Per maggiori informazioni riguardo la connessione SSL, consultare il testo, a cura di P. Peer: Privacy, Diritto e Sicurezza Informatica, Milano, Giuffrè 2007, paragrafo 8.5.

[9] Con la parola ledger, lett. "libro mastro", si intende il record pubblico ed impermutabile di transazioni contenente le "impronte temporali", c.d. timestamp, sotto forma di funzioni hash, generate da algoritmi informatici al completamento dell'operazione commerciale, ed inviate tramite liste broadcast ai nodi del network. La ledger può essere posta sotto il controllo diretto di un'autorità centrale, come nel caso di una CBDC, o può essere decentralizzata, come nel caso della BlockChain.

[10] Difatti, spesso si ricorre all'uso di *hardware wallets*, ossia *hard-drives* dove sono contenute le valute al pari delle tradizionali cartelle di lavoro.

virtuale può essere spesa solo acquistando beni e servizi virtuali offerti all'interno della comunità virtuale e, almeno in teoria, non può essere scambiato al di fuori della comunità stessa[11].

2. **Schemi di valuta virtuale con flusso unidirezionale**: in questo caso la valuta virtuale può essere acquistata utilizzando direttamente la valuta reale a un tasso di cambio specifico ma non può essere effettuato il procedimento inverso. Le condizioni di conversione sono stabilite dal proprietario dello schema. Questi modelli consentono sia di utilizzare la valuta per acquistare beni e servizi virtuali, sia di utilizzare le proprie valute per acquistare beni e servizi reali[12].

3. **Schemi di valuta virtuale con flusso bidirezionale**: in questo modello gli utenti possono acquistare e vendere denaro virtuale sulla base di determinati tassi di cambio con la loro valuta. La valuta virtuale è simile a qualsiasi altra valuta convertibile per quanto riguarda la sua interoperabilità con il mondo reale. Questi schemi consentono l'acquisto di beni e servizi sia virtuali che reali[13].

La valuta virtuale può essere considerata come uno specifico tipo di moneta digitale. Tuttavia, tra le due è possibile identificare alcune differenze *in primis* il fatto che la valuta virtuale sia espressa esclusivamente nella propria unità di conto[14]: la nozione di valuta digitale, infatti, proprio per la sua caratteristica di raggruppare strumenti di pagamento elettronico che presentino caratteristiche tra loro differenti, può essere espressa sia nell'unità di conto della moneta a corso legale (come USD, EUR, ecc.), sia in unità di conto, appunto, "virtuali" (come L$, BTC, ADA, ecc.); in quest'ultimo caso l'*asset* fa affidamento su un tasso di cambio fluttuante, dato che il suo valore è determinato dalle leggi di domanda ed offerta.
Inoltre, il controllo completo della valuta virtuale è rimesso al suo emittente, che di solito è una società non finanziaria, mentre, nel caso della moneta digitale, è rimesso o ad un'autorità centrale (come nel caso della *Central Bank Digital Currency, CBDC*), o ad un *network* di utenti *DLT – Decentralized Ledger Technology –* (come nel caso delle cripto-valute) che regolano le transazioni. Per questo motivo, le valute virtuali, al contrario di quelle digitali che presentano rischi connessi esclusivamente con l'eventuale interruzione del funzionamento dei rispettivi sistemi di regolazione – centralizzati o decentralizzati che siano –, sono affette

[11] Esempio: World of Warcraft Gold (WoW Gold) è una valuta virtuale utilizzata nel famoso gioco di ruolo sviluppato dalla Blizzard Entertainment. I giocatori, che possono guadagnare valuta o comprandola o raggiungendo determinati obiettivi di gioco, usano questa valuta come un metodo di pagamento all'interno del videogame. Lo scambio di WoW Gold è proibita al di fuori del gioco.

[12] Esempio: i Nintendo Points erano punti speciali, ottenibili in vari modi, che permettevano di acquistare giochi e Apps scaricabili da internet per le console Wii e Nintendo DSi. Il metodo principale per ottenere Nintendo Points era mediante o l'acquisto delle Wii Points Card, ossia carte prepagate contenenti un diverso ammontare della valuta di Nintendo, oppure pagando sul Canale Wii Shop. I Punti non potevano essere convertiti in valuta a corso legale.

[13] Esempio: Linden Dollars (L$) è la valuta virtuale utilizzata da Second Life, una piattaforma digitale dove gli utenti possono creare il proprio "avatar". Second Life ha una propria economia dove gli utenti possono scambiare ed acquistare beni e servizi vicendevolmente. Per fare ciò, è necessario disporre di Linden Dollars, acquistabili online attraverso PayPal o opagamento con carta di credito/debito.

[14] Sotto questo punto di vista, la nozione di moneta virtuale si avvicina molto a quello di cripto-valuta: infatti assets come Bitcoin, Ethereum, Ripple, ecc., sono espresse in una loro specifica unità di conto (rispettivamente: BTC, ETH, XRP, ecc.).

da rischio di credito, di liquidità ed operativo, non appoggiandosi ad un solido *framework* (legale e/o informatico) sottostante.

Nel novero di valute virtuali non rientrano i sistemi di pagamento quali PayPal, Satyspay o Revolut, dato che, seppure venga creato un *account*, finanziato attraverso trasferimenti di fondi da un conto corrente bancario o da una carta di credito/debito, nessuna valuta virtuale viene creata dai loro sistemi; inoltre, sono strumenti di pagamento sottoposti alla supervisione di Autorità settoriali quali, nel caso di PayPal, la Banca Centrale del Lussemburgo e la Commissione di Sorveglianza del Settore Finanziario del Lussemburgo (European Central Bank 2012).

CAPITOLO 2. LE CRIPTO-VALUTE

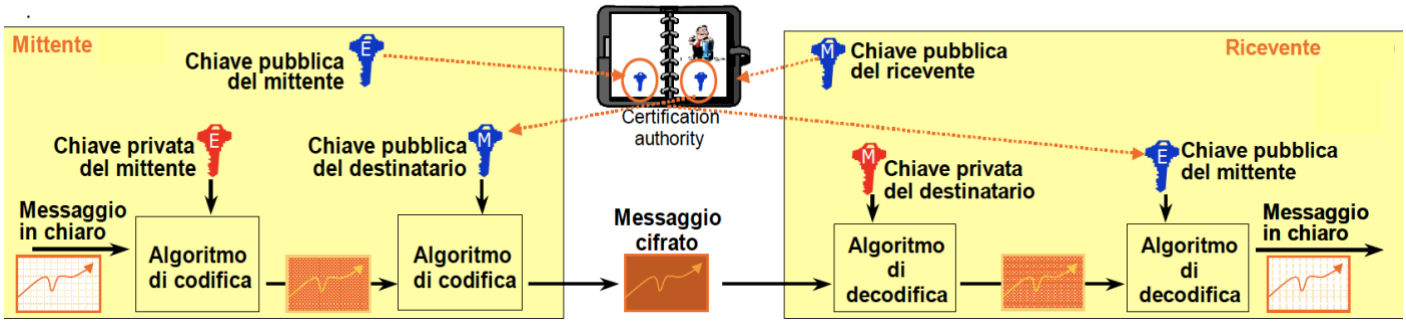
2.1 CRIPTO-VALUTE: CHE COSA SONO ED IN COSA SONO DIVERSE RISPETTO ALLA VALUTA TRADIZIONALE

Dare una definizione di "cripto-valute" non è semplice. Ad oggi, il termine cripto-valuta include un ampio *range* di innovazioni tecnologiche che si appoggiano a sistemi avanzati di crittografia.

La crittografia, in breve, è una tecnica attraverso cui si proteggono informazioni e dati sensibili, codificando il messaggio all'interno del quale sono contenuti in un formato che sia estremamente difficile da leggere per tutti coloro che non possiedano una specifica chiave di decifrazione.

I sistemi di crittografia utilizzati da valute come Bitcoin sono riconducibili ai sistemi di crittografia a chiave asimmetrica.

Sistema di crittografia a chiave asimmetrica



Fonte: Sistemi di sicurezza informatica, LUISS, corso di informatica 2018/2019, prof. Massimo Bernaschi

Il sistema di crittografia a chiave asimmetrica (detta anche a chiave pubblica/privata) prevede l'utilizzo di una coppia di chiavi, distinte ma legate fra loro nel senso che, mentre una è usata per codificare, l'altra è usata per decifrare il messaggio, ma i ruoli sono tra loro interscambiabili. Più nello specifico le chiavi sono:

1. Una chiave pubblica, divulgabile a tutti;
2. Una chiave privata, conosciuta e custodita del mittente del messaggio.

L'algoritmo, che garantisce i principi eIDAS[15] quali confidenzialità, autenticazione ed integrità del messaggio, rende impossibile a chi conosce solo la chiave pubblica risalire a quella privata. Inoltre, un messaggio cifrato con la chiave pubblica è decifrabile solo con la corrispondente chiave privata e viceversa.

L'algoritmo alla base del sistema di crittografia a chiave asimmetrica, benché più complesso della tecnica a chiave simmetrica, in quanto prevede l'utilizzo di una coppia di chiavi piuttosto che di una soltanto, è molto semplice:

---

[15] Il Regolamento europeo per l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (abbreviato in eIDAS, acronimo di *electronic IDentification, Authentication and trust Services*, ufficialmente regolamento (UE) n. 910/2014), è un regolamento dell'Unione europea, che riguarda l'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel Mercato europeo comune. Il regolamento sostituisce la precedente direttiva 1999/93/EC.

1. Il destinatario divulga la propria chiave pubblica[16], mantenendo segreta la chiave privata. Il mittente cifra il messaggio usando prima la sua chiave privata, e poi la chiave pubblica del destinatario: in questo modo si applica una doppia crittografia del messaggio.
2. Il messaggio cifrato, una volta ricevuto dal destinatario, può essere decodificato utilizzando prima la propria chiave privata, e dopo la chiave pubblica resa disponibile dal mittente.

In questo modo si garantisce l'autenticazione del messaggio in quanto il ricevente è sicuro che ad aver inviato il messaggio è stato quello specifico mittente dato che è l'unico a conoscenza della propria chiave privata; viceversa, si garantisce pure la confidenzialità in quanto il mittente è sicuro che a leggere il messaggio sia colui e a cui è effettivamente destinato dato che è il solo a conoscere la propria chiave privata.

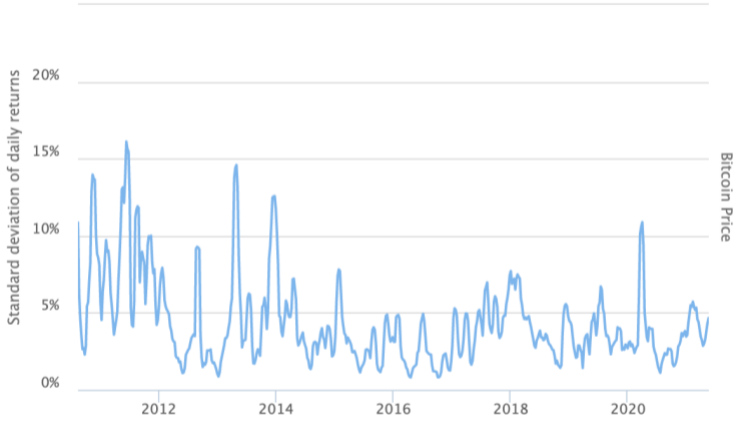
Nel definire il concetto di valuta virtuale, è stata presa in considerazione l'enunciazione fatta dalla Banca Centrale Europea la quale considera la nozione di cripto-valuta al pari di uno schema di valuta virtuale (o "valuta elettronica", i termini sono interscambiabili, come spiegato al cap.1, paragrafo 1.2) a flusso bidirezionale[17]. Tuttavia, riallacciandosi alla letteratura in materia[18], il concetto di valuta virtuale è stato considerato al pari di un "sottoinsieme" del più ampio *cluster* di valute che prende il nome di moneta digitale: emerge dunque una mancata convergenza da parte delle varie Autorità settoriali riguardo ad una definizione *standard* delle suddette valute.
Nel sintetizzare le varie interpretazioni in materia, ecco che una buona definizione di cripto-valuta può essere la seguente: "la cripto-valuta è un sottoinsieme delle valute digitali, per tali si intendono tutte quelle rappresentazioni, ottenute mediante l'esecuzione di processi informatici, della moneta a corso legale. Specificatamente, la cripto-valuta costituisce un'alternativa *Peer-to-Peer* (*P2P*) alle monete a corso legale "*fiat*": è usata come un mezzo di scambio non regolato centralmente da nessuna Autorità o Governo, è protetta dal sistema di crittografia a chiave asimmetrica e può essere convertita in moneta a corso legale e viceversa." (Parlamento Europeo 2018)

[16] Solitamente le chiavi pubbliche sono create e distribuite da una Autorità di Certificazione all'interno di e solo per uno specifico circuito. In questo modo gli utenti hanno la garanzia sia che la chiave pubblica associata al loro account venga ricevuta esclusivamente dai soggetti interessati, sia che la chiave pubblica che ricevono non sia stata contraffatta o non esegua correttamente l'algoritmo di decodifica del messaggio.

[17] Vedere capitolo 1, paragrafo 1.2.

[18] Autorità come la *World Bank* o la *FATF* hanno considerato i concetti di valuta virtuale e di cripto-valuta al pari di *assets* riconducibili alla più generale nozione di moneta digitale.

Volatilità BTC/USD 30-giorni



Fonte: https://www.buybitcoinworldwide.com/volatility-index/

Le cripto-valute non possono essere considerate come strumenti di pagamento stabili, bensì come *assets* speculativi (Spagnolo 2021). La cripto-valuta, infatti, non soddisfa le tre funzioni necessarie a definire una moneta come tale: infatti, non costituisce una riserva di valore, in quanto l'accentuata volatilità (grafico sopra riportato) del tasso di cambio con valute a corso legale può erodere nel tempo il reddito non destinato al consumo, piuttosto che garantirlo; inoltre, cripto-valute come Bitcoin o Ethereum, non possono essere considerate unità di conto in quanto non permettono di confrontare in maniera omogenea il valore di beni o servizi diversi tra loro, sempre a causa della accentuata volatilità del tasso di cambio; infine, le cripto-valute costituiscono un mezzo di pagamento "ambiguo": fino a poco tempo fa, infatti, figuravano come sistemi di pagamento accettati esclusivamente da un numero piuttosto limitato di piattaforme per l'acquisto di beni e servizi[19], solo recentemente giganti come PayPal, Goldman Sachs o Revolut hanno iniziato ad utilizzare Bitcoin e/o altre cripto-valute come strumenti di pagamento[20].

I vantaggi attribuiti alle cripto-valute, piuttosto che alle monete a corso legale, sono legati principalmente alla loro decentralizzazione: difatti, esse non dipendono dalla fiducia di una particolare istituzione regolatrice, per questo sono teoricamente[21] immuni al fallimento di banche ed altri intermediari finanziari. Inoltre, rispetto ad altri strumenti al portatore, essendo completamente digitalizzate, le cripto-valute sono più facili da trasportare e da rendere sicure grazie ai sistemi di crittografia a chiave asimmetrica precedentemente esposti.

[19] I siti del c.d. *Deep Web* e *Dark Web* sono stati tra i primi ad accettare pagamenti con Bitcoin appunto perché la protezione derivante dalla crittografia a chiave asimmetrica rende difficile (ma non impossibile) risalire all'identità di coloro che portano a termine transazioni "maliziose" come l'acquisto di armi o droghe online.

[20] Tesla ha dato la possibilità di acquistare i suoi modelli di automobili con un pagamento in Bitcoin, conseguentemente agli ingenti investimenti che l'impresa ha effettuato sulla cripto-valuta e che hanno portato ad un "boom" rialzista sul tasso di cambio BTC/fiat.

[21] È chiaro che, qualora una banca o intermediario che sia di grandi dimensioni dichiarasse fallimento come Lehman Brothers nel 2009, il tasso di cambio delle cripto-valute subirebbe delle forti oscillazioni dato che è un mercato altamente inefficiente dove i *drivers* principali sono gli *hypes* di mercato. Inoltre, le cripto-valute vengono percepite come *inflation hedges*, per cui i depositari che non rientrino all'interno del sistema di copertura dei propri depositi della banca in dissesto finanziario sarebbero incentivati a ritirare la loro liquidità e ad investirla in *assets* come anche più aleatori e speculativi (come le cripto-valute) piuttosto che subire un decurtamento certo, dovendo partecipare al rischio operativo della banca stessa qualora si aprisse la procedura di ricapitalizzazione.

La volatilità di una cripto-valuta è spiegata dall'incertezza normativa, dalla bassa liquidità, da una bassa capitalizzazione di mercato, da un accesso limitato al mercato e così via.
Alcune proposte avanzate per ridurre la volatilità di una cripto-valuta come Bitcoin sono:

- Creare un ciclo di *feedback* nell'algoritmo della valuta in modo tale che, se il prezzo aumentasse verrà creata più valuta come premio per i *miners*, viceversa qualora il prezzo diminuisse. La difficoltà sta nel modo con cui inserire un flusso di dati dei prezzi della valuta all'interno della *blockchain*: infatti, se i dati venissero introdotti dai *miner*s, questi avrebbero un incentivo a tenere comportamenti scorretti (Buterin 2013).

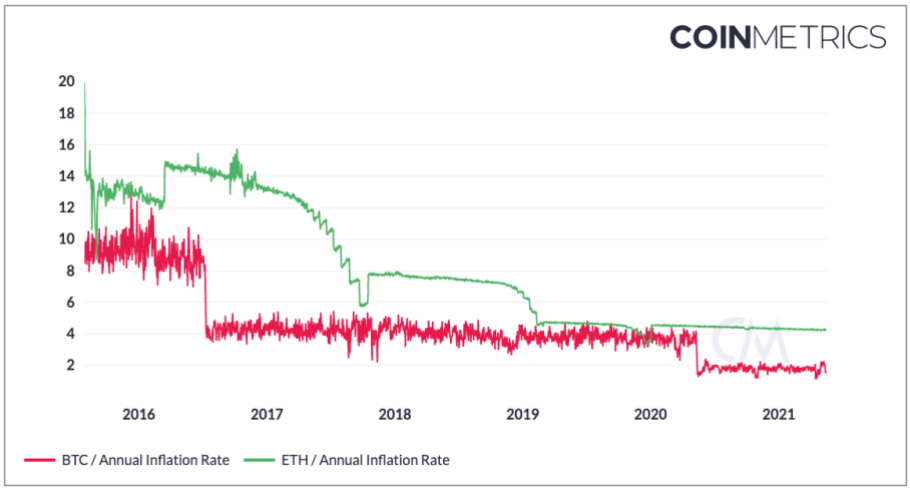
- Regolare la quantità di fondi in ogni *wallet* in base al potere d'acquisto della valuta (Ametrano 2016). Se il potere d'acquisto aumentasse, la quantità di fondi in ogni portafoglio dovrebbe essere regolata di conseguenza per far sì che il potere d'acquisto della valuta rimanga inalterato. Anche in questo caso, i *miners* potrebbero barare dichiarando un quantitativo di valuta da loro detenuto più basso di quello effettivo in modo da non risentire di questo effetto.

- Affidare la politica monetaria della cripto-valuta ad un'Autorità centrale piuttosto che lasciare l'offerta monetaria nelle mani di un algoritmo.

In tema di inflazione[22] le cripto-valute si distinguono in due tipologie a seconda del modello adottato nel rispettivo protocollo: infatti, da un lato vi sono cripto-valute come Bitcoin o Litecoin che hanno stabilito sin da subito un *hard cap* (21 milioni nel caso di Bitcoin, 84 milioni nel caso di Litecoin) che rappresenta un limite asintotico dell'emissione di nuova moneta, la quale viene dimezzata (c.d. funzione di *halving*) circa ogni quattro anni in entrambi i casi; dall'altro lato vi sono, invece, cripto-valute come Ethereum che non hanno stabilito, nel loro protocollo, alcun limite all'emissione; tuttavia, Ether è attualmente emesso ad un tasso annuale pari a 2 ETH/Blocco estratto (ossia il *reward* per i *miners*), il che rende il modello adottato disinflazionistico, ossia di rientro dell'inflazione, mentre quello adottato da Bitcoin/Litecoin è deflazionistico, ossia di abbassamento del livello generale dei prezzi tale da generare un incremento del potere d'acquisto di una moneta .

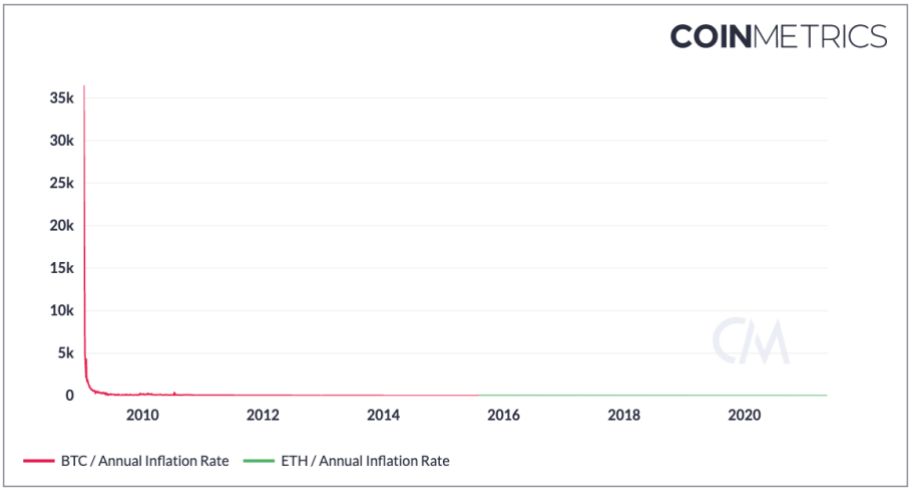
[22] Il termine inflazione ha due significati: il primo legato al tema di inflazione dei prezzi, il secondo legato all'ammontare totale di moneta in un sistema economico – la base od offerta monetaria –. In questa analisi verranno distinte le due voci anche perché spesso, ma non sempre, l'inflazione monetaria è un effetto di quella dei prezzi.

Tasso di inflazione della base monetaria annuale Bitcoin (rosso), Ethereum (verde)



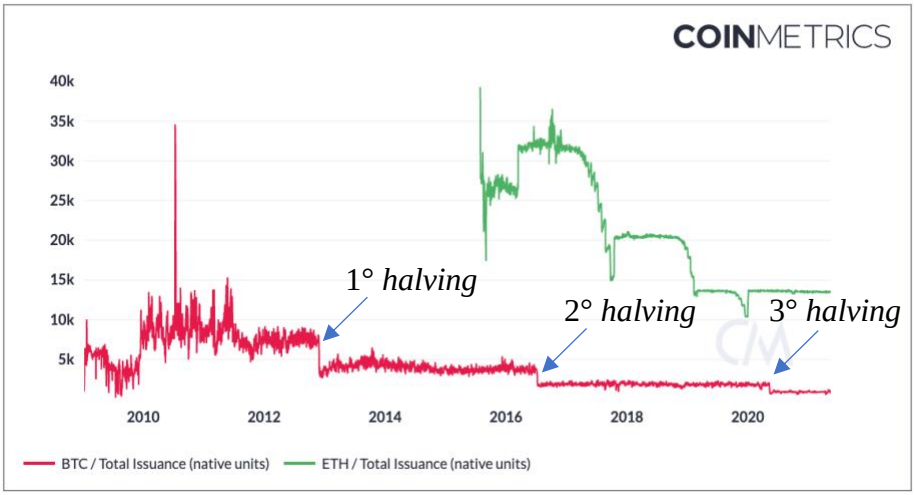
Fonte: https://charts.coinmetrics.io/network-data/

Tasso di inflazione della base monetaria *ALL-TIME* Bitcoin (rosso), Ethereum (verde)



Fonte: https://charts.coinmetrics.io/network-data/

Emissione totale/*Mining-Reward* di Bitcoin ed Etherem



Fonte: https://charts.coinmetrics.io/network-data/

Come si evince dal secondo grafico, Bitcoin ha attraversato un periodo di altissima inflazione della base monetaria in concomitanza con il suo lancio, proprio perché la funzione di *halving* non aveva ancora prodotto alcun effetto. Solo dopo quattro anni (2013), a seguito del primo *halving*, si è passati ad un modello deflazionistico ed il livello di emissione si è mantenuto entro un *range* moderato e decrescente (come dimostrato dal terzo grafico). Quando l'*hard cap* verrà raggiunto, l'inflazione della base monetaria si annullerà al pari dell'emissione di nuova moneta.
Per quanto riguarda Ethereum, invece, il livello di emissione è cambiato più volte nel tempo[23] (attualmente il tasso di emissione è di 2ETH/Blocco estratto, mentre tre anni fa era di 3 ETH/Blocco e ancora prima 5 ETH/Blocco estratto) ma, visto che il protocollo non impone né un'*hard cap*, né una funzione di *halving*, l'inflazione della base monetaria si muove esattamente al pari del livello di emissione in quel dato momento[24]. In questo caso, possiamo intendere il tasso di emissione al pari di una valvola della politica monetaria di Ethereum per regolare la quantità di circolante, seguendo il principio

Intendendo l'inflazione come la variazione percentuale del livello generale dei prezzi, all'offerta monetaria si aggiunge il livello di domanda di cripto-valuta come variabile *driver* del prezzo della stessa in un dato momento: se la domanda di una cripto-valuta, che adotti uno schema di emissione a tasso fisso come Bitcoin ed Ethereum, continuasse a crescere grazie ad un'economia in espansione, il relativo prezzo entrerebbe in un regime deflazionistico. Fintantoché il tasso di deflazione del prezzo si mantenga entro un *range* moderato, i meccanismi di fissazione dei prezzi si adegueranno ed il sistema funzionerà senza intoppi. La tradizionale obiezione alle economie deflazionistiche, ossia la viscosità salariale, probabilmente non sarà un problema poiché tutti i sistemi di pagamento saranno fluidi. Se, inoltre, il regime deflazionistico fosse persistente e le aspettative non subissero significative variazioni nel tempo, anche i termini di prestito e di rimborso di un finanziamento potranno essere regolati di conseguenza con un buon grado di certezza. Il modello deflazionistico può quindi diventare una sorta di riparo dall'inflazione (c.d. *inflation hedge*) delle monete *fiat* in periodi di regressione economica.
Il modello deflazionistico di una cripto-valuta è rifiutato dagli economisti tradizionali, i quali sostengono che, se questa dovesse affermarsi come alternativa alle valute *fiat*, ciò potrebbe impedire le banche centrali dall'attuazione della politica monetaria, ridurrebbe le entrate generate dai governi con la stampa di denaro, portando ad una destabilizzazione del sistema finanziario nel suo complesso. Fatto sta che cripto-valute come Bitcoin o Litecoin, una volta raggiunto il livello di *hard cap*, vedranno schizzare il loro prezzo a fronte di una domanda insoddisfatta, rendendo la valuta un *asset* meramente speculativo.

[23] La fluttuazione del premio per l'attività di *mining* e, quindi, il livello generale di emissione è avvenuta in concomitanza con i principali *hard forks* della *blockchain* di Ethereum ed Ethereum Classic.

[24] La linea del livello di emissione di Ethereum (linea verde nel 3° grafico) ha lo stesso andamento della linea di inflazione (linea verde nel 1° grafico).

2.2 L'EFFETTO DELLE CRIPTO-VALUTE SULL'ECONOMIA FINANZIARIA E L'INTERMEDIAZIONE BANCARIA

L'introduzione delle cripto-valute ha permesso a piccole *start-ups* di partecipare al settore finanziario, aumentando la pressione competitiva delle aziende, amplificando il ritmo dell'innovazione tecnologica e costringendo le istituzioni finanziarie a rivedere la loro infrastruttura per raggiungere un maggiore livello di sicurezza fornito dalla crittografia asimmetrica.

Un rischio per le attuali istituzioni finanziarie è la disintermediazione qualora gli utenti preferiscano detenere una percentuale maggiore dei propri risparmi in cripto-valute. Questo potrebbe accadere a seguito di un aumento delle imposte sui depositi, del fallimento di un grande istituto finanziario o qualora i governi decidano di applicare scarti di garanzia sui depositi stessi.

È oggetto di dibattito se sia possibile creare una riserva frazionaria con cripto-valute come Bitcoin: la riserva frazionaria allude al fatto che le banche mantengono solo una frazione dei depositi dei loro clienti in riserva, immettendo il resto sull'economia reale sotto forma di prestiti e finendo per aumentare l'offerta monetaria attraverso l'effetto del moltiplicatore della moneta. Sebbene nulla impedisca ad un'istituzione di praticare attività bancarie a riserva frazionaria con una o più cripto-valute, non è ancora possibile stabilire con certezza se gli utenti preferirebbero rendersi parte attiva di questo processo o meno. Permarrebbe comunque il rischio di controparte per l'ente che pratichi la riserva frazionaria, non esistendo un'assicurazione sui depositi o un prestatore di ultima istanza per le cripto-valute che possa limitare questo rischio.

D'altra parte, una criptovaluta potrebbe essere creata, gestita e controllata da un'Autorità monetaria che funga da prestatore di ultima istanza. Una simile cripto-valuta presumibilmente dovrebbe competere con le cripto-valute esistenti per aggiudicarsi una più ampia quota di mercato.

Tuttavia, la base monetaria delle cripto-valute, ad oggi, è ancora molto bassa rispetto alle monete *fiat*: Bitcoin, infatti, ha una dimensione due volte inferiore rispetto al circolante delle valute a corso legale.

Si ritiene ancora che le valute digitali siano troppo piccole per avere un impatto sulla politica bancaria. Tuttavia, i governi e le banche centrali stanno iniziando a prestarvi un'attenzione maggiore con la *CBDC* (*Central Bank Digital Currency*).

L'equazione quantitativa della moneta viene utilizzata per argomentare che se sia la velocità del denaro, sia la produzione reale di un'economia rimangono costanti, un aumento nell'offerta monetaria produce un aumento del livello dei prezzi, ossia dell'inflazione, senza qualsiasi effetto sull'economia reale. Un recente rapporto (Elwell et al., 2013) ha esplorato i possibili effetti di Bitcoin sulla politica monetaria del dollaro USA. Usando la teoria quantitativa della moneta si sostiene che se i bitcoin vengano ampiamente utilizzati, si potrebbe generare un aumento della velocità delle valute legali, poiché la necessità di detenerle, a parità di condizioni, diminuirebbe. Un tale aumento della velocità di denaro a corso legale potrebbe aumentare il livello generale dei prezzi, costringendo le banche centrali a diminuire l'offerta di moneta, ad es. attuando un inasprimento della politica monetaria. Alcuni economisti vedono l'uso diffuso di Bitcoin e del suo potenziale effetto sulla

politica monetaria delle valute legali come un evento positivo per l'economia nel suo complesso: per questi economisti, tale sviluppo sarebbe simile a un ritorno al *Gold Standard*.
Infine, alcuni economisti sostengono che Bitcoin e le cripto-valute in generale potrebbero far aumentare la resilienza dell'economia in quanto creano un sistema di pagamento alternativo che potrebbe essere utile in caso di turbolenze o malfunzionamenti delle strutture finanziarie esistenti.

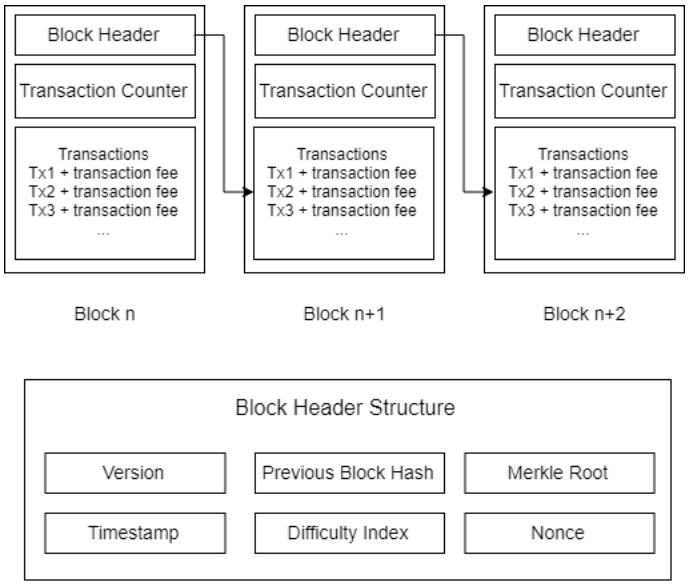
2.3 LA TECNOLOGIA BLOCKCHAIN

La *blockchain* fu introdotta per la prima volta da Satoshi Nakamoto nel 2008 con l'obiettivo di costruire una tecnologia solida su cui si potesse appoggiare la valuta di sua invenzione: Bitcoin. La *block chain* (Nakamoto si riferiva ad essa mantenendo le parole *block* e *chain* distinte nel suo *paper* originale) può essere intesa come un libro mastro pubblico, un *record* di tutte le transazioni effettuate suddivise in catene di blocchi. La catena continua a crescere non appena viene aggiunto un nuovo blocco[25]. La *blockchain* presenta le seguenti caratteristiche: decentralizzazione, persistenza, anonimità ed udibilità. La *blockchain* funziona in un ambiente decentralizzato, creato dall'integrazione di alcune tecnologie fondamentali come le funzioni crittografiche "*hash*", la firma digitale (basata sulla crittografia asimmetrica) ed una metodologia di consenso (c.d. *Proof-of-Work* o *Proof-of-Stake*) distribuita in un network di utenti. La tecnologia *blockchain* permette di ridurre drasticamente i costi e le tempistiche di una qualsiasi transazione dal momento che ovvia all'intermediazione effettuata da soggetti specializzati (come banche o intermediari finanziari) la quale richiede costi nettamente superiori in termini di tempo e danaro: questa caratteristica della *blockchain*, oltre che a rendere più efficiente il sistema che la utilizzi, permette di implementare un'innumerevole serie di servizi finanziari che vanno ben oltre le funzionalità delle cripto-valute.
La *blockchain* è intesa come una serie di "blocchi", ognuno dei quali contiene una serie storica di transazioni, al pari dei tradizionali libri mastri. Ogni blocco richiama quello precedente utilizzando il valore *hash* di quest'ultimo come referenza: un valore *hash* è il risultato dell'esecuzione di un algoritmo[26] (chiamato così perché responsabile dell'esecuzione della c.d. "funzione *hash*") che, a partire da un blocco di dati iniziale di lunghezza variabile (in *bit*), genera una stringa di lettere e numeri di lunghezza fissa (detta *digest* o *fingerprint*), più corta di quella del blocco di partenza e "relativamente" univoca: la probabilità che due diversi blocchi di dati producano la stessa serie numerica deve essere virtualmente nulla.

[25] Inizialmente la *block chain* di Nakamoto pesava solo 10 GB mentre, ad oggi, pesa oltre 162 GB.

[26] I più famosi algoritmi per l'esecuzione delle funzioni di *hash* sono il *Message Digest 5* (o MD5), lo *SHA-256* (usato dalla *blockchain* di Bitcoin) e il *RIPEMD-160*.

Composizione della *blockchain*



Ogni blocco di una *blockchain* può suddiviso in due parti: la "testata" (o *block header*) ed il "corpo" (o *block body*). La "testata", come mostrato anche in figura, è a sua volta composta dai seguenti elementi:

- **La versione del blocco** (o *block version*): indica la versione che un particolare blocco sta utilizzando, al momento esistono quattro tipologie di versioni della *blockchain*, ciascuna delle quali rende possibile lo svolgimento di particolari attività digitali in un modo completamente decentralizzato:
  - **Versione 1.0**: usata per raccogliere dati, proprio come un libro mastro. La versione 1.0 (o prima generazione) è la forma di *block chain* implementata da Nakamoto per il funzionamento di Bitcoin. La forma di consenso a cui si appoggia la *blockchain* di prima generazione è quella del *Proof-of-Sork* (*PoW*). I codici di implementazione delle *blockchain* di prima generazione sono tutti scritti con il linguaggio di programmazione C++ e fanno quasi tutti riferimento al protocollo di Nakamoto.
  - **Versione 2.0**: usata per rendere possibile, attraverso la raccolta dei dati, non solo l'esecuzione dei c.d. "*smart contracts*[27]", ossia programmi digitali e dinamici autorealizzanti, ma anche la creazione di *assets* digitali unici, i c.d. "*tokens*". La versione 2.0 (o seconda generazione) è propria della *blockchain* di cripto-valute come Ethereum. La forma di consenso a cui si appoggia la *blockchain* di seconda generazione è quella del *Proof-of-Stake* (*PoS*). I codici della *blockchain* 2.0 sono scritti utilizzando un nuovo linguaggio di programmazione, sviluppato da Ethereum, chiamato Solidity (nella pratica è il risultato di una mescolanza tra vari linguaggi di programmazione quali C++, JavaScript e Python).
  - **Versione 3.0**: usata per ovviare a quelle problematiche risultanti dalle versioni precedenti (quindi 1.0 e 2.0), come la lentezza di processo e la ridotta funzionalità e scalabilità, attraverso

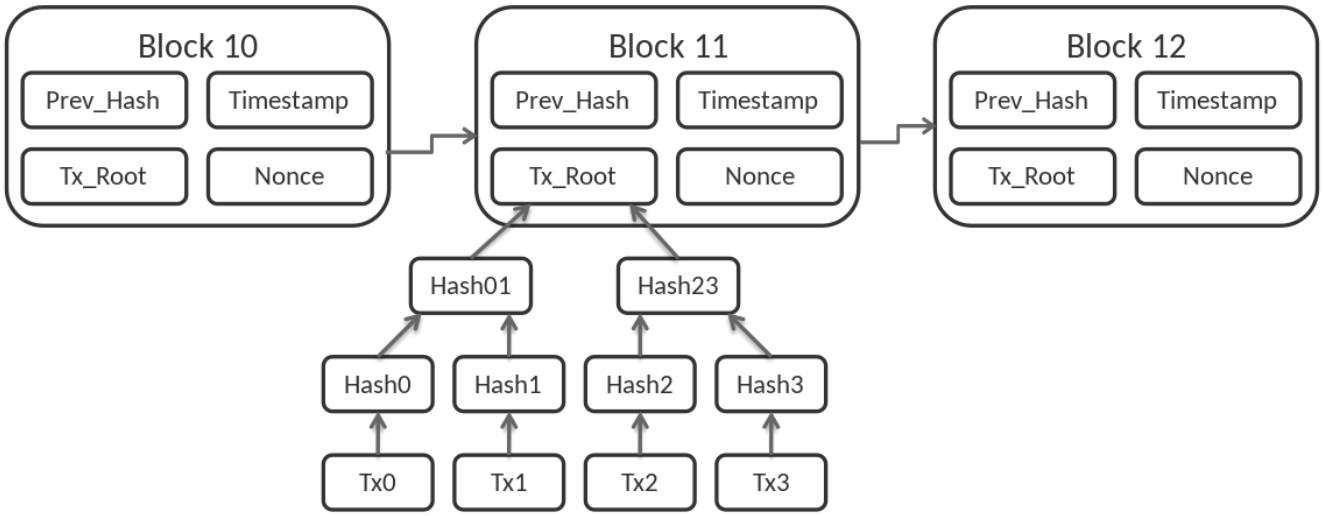
[27] La libreria più utilizzata per la distribuzione (c.d. *deployment*) di *smart contracts* è Open Zeppelin. Maggiori informazioni al seguente link: https://openzeppelin.com/

l'ideazione di nuove forme di consenso come la *Proof-of-Activity* (*PoA*) o la *Proof-of-Burn* (*PoB*). La caratteristica principale della *blockchain* di terza generazione è la possibilità di processare transazioni c.d. *cross-chain*, ossia tra *assets* (come le cripto-valute o i *tokens*) realizzati rispettivamente su *blockchain* differenti: i protocolli di *cross-chain trading* di maggiore rilevanza sono *Atomic Swap* e *P2PTradeX*. La *blockchain* 3.0 è adottata da cripto-valute come Cardano (ADA) o IOTA.

- **Versione 4.0**: attualmente non ancora sviluppata. Oggigiorno si pensa che la quarta generazione di *blockchain* verrà realizzata soltanto quando sarà correttamente applicata ai sistemi di Intelligenza Artificiale: a tal riguardo sono molto interessanti i progetti portati avanti da DeepBrain Chain, o da SingularityNET sulla creazione di una rete neurale decentralizzata modellata sul sistema nervoso umano.

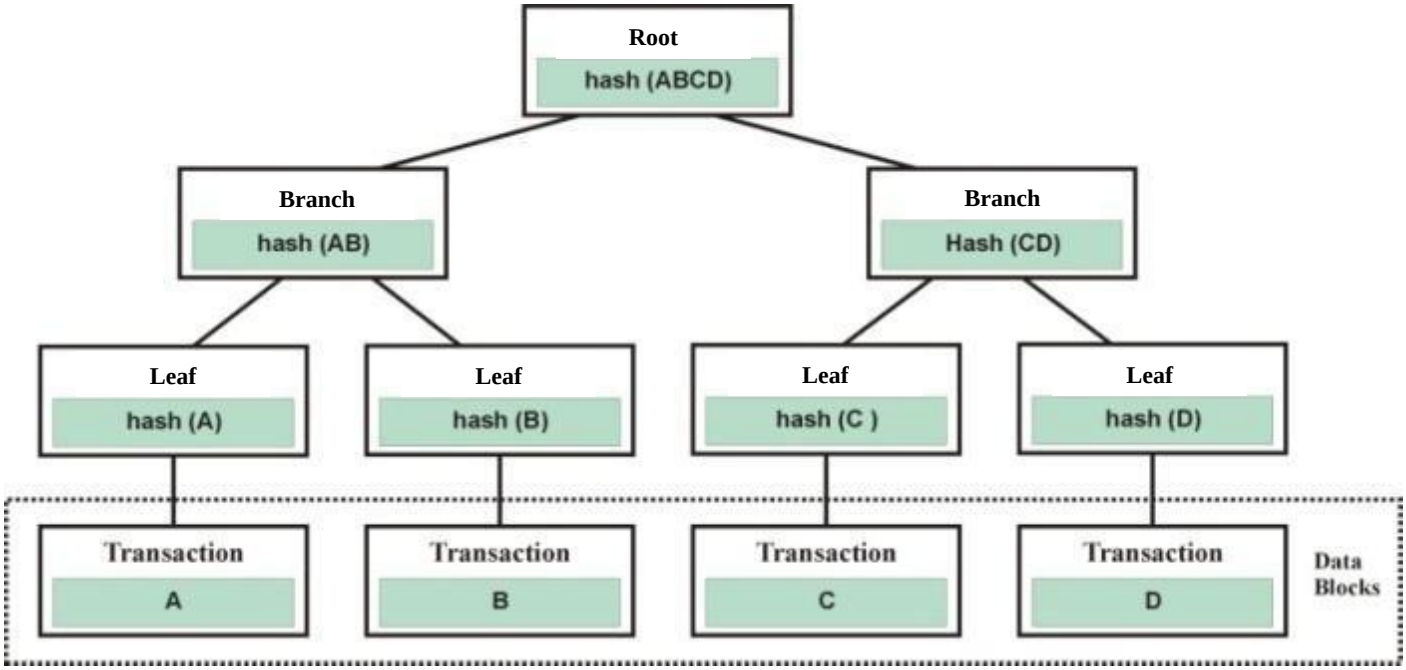
- **Valore *hash* del blocco precedente** (o *previous block hash*): si tratta valore *hash* del blocco validato precedentemente. Questo valore viene usato come referenza per il blocco successivo nell'ottica di dare continuità all'intera *blockchain*.

Scomposizione di una blockchain nei vari elementi. Il Merkle tree root è messo in evidenza



- **Valore *hash* dell'albero di Merkle** (o *Merkle tree root*): si tratta del valore *hash* ottenuto a partire da quelli associati a ciascuna transazione contenuta nel *block body*. Il *Merkle Tree* è una funzione matematica che dispone i valori *hash* di una grossa mole di dati in uno schema piramidale tale da permettere la generazione di un singolo valore *hash* (la "radice" dell'albero, o *root*), rappresentativo di tutti i singoli valori *hash* associati a ciascun dato contenuto nel blocco (le cosiddette "foglie", o *leaves*, ossia le unità della funzione), raggruppati per macro-classi (i "rami", o *branches*). Lo schema piramidale è riportato qui sotto. Nel caso in cui la serie di dati (o transazioni, nel caso della *blockchain*) sia dispari, una di queste (generalmente l'ultima) viene ripetuta per raggiungere un numero pari.

Struttura del Merkle tree

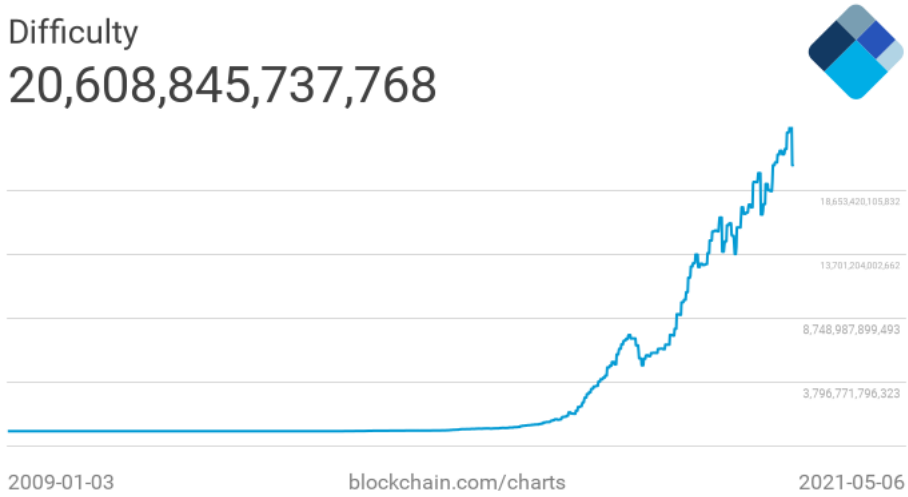


- **Marca temporale** (o *timestamp*): si tratta del numero di secondi trascorsi da una data convenzionale chiamata *Unix Epoch* corrispondente al 1° gennaio 1970. La marca temporale serve a certificare l'orario cui effettivamente è avvenuta una transazione e a garantirne sia la validità nel tempo, sia l'opponibilità a terzi. Nel caso della *blockchain*, la transazione cui si associa il *timestamp* è l'estrazione (o *minaggio*) del blocco.

- **Indice di difficoltà** (o *difficulty index*): L'indice di difficoltà è una misura di quanto sia difficile trovare un valore *hash* per un determinato livello obiettivo: nella pratica, il c.d. *puzzle* crittografico che i *miners* sono chiamati a risolvere consiste nella sostituzione dei primi "n" termini esadecimali della stringa *hash* di ogni blocco di una *blockchain* con degli 0; il valore "n" è stabilito dalla *difficulty* attraverso un algoritmo decentralizzato che tiene conto della frequenza con cui vengono estratti nuovi blocchi ed aggiunti alla *blockchain* (come si evince dal grafico, nel caso di Bitcoin, ad oggi il livello di difficoltà è individuato ai primi 20 *digits* esadecimali della stringa *hash* da convertire in zero: questo è il c.d. *puzzle* crittografico che i *miners* devono risolvere per estrarre i singoli blocchi che andranno ad aggiungersi alla *blockchain*). Una difficoltà elevata significa che sarà necessaria più potenza di calcolo per estrarre lo stesso numero di blocchi, rendendo la rete più sicura. La regolazione della difficoltà è direttamente correlata alla potenza di *mining* (o di estrazione). Secondo l'algoritmo di Bitcoin, l'indice di difficoltà viene regolato ogni 2016 blocchi (ogni 2 settimane circa) in modo che il tempo medio per la validazione di ogni blocco sia di 10 minuti. Ethereum, appoggiandosi ad una *blockchain* di seconda generazione che sfrutti il protocollo *PoW GHOST*[28], ha un tempo di estrazione dei blocchi molto più veloce, pari a 12 secondi.

[28] *Greedy Heaviest Observed Subtree* (o *GHOST*) è il protocollo introdotto da Yonatan Sompolinsky e Aviv Zohar nel dicembre 2013 e utilizzato dalla *blockchain* di Ethereum. *GHOST* si promuovere di rendere più efficiente e sicuro il processo di *mining* di

Andamento del livello di difficoltà di Bitcoin nel tempo



- ***Nonce***: *nonce* è l'abbreviazione per "*number only used one*" (ossia "numero usato solo una volta"). Il *nonce* è un parametro numerico di lunghezza variabile che, una volta individuato, permette all'intero blocco di essere valido: solo i blocchi con un *nonce* valido possono essere aggiunti alla *blockchain*. Degli elementi componenti il blocco di transazioni, il *nonce* è l'unico su cui il *miner* può agire direttamente: è infatti il *miner* a selezionare il *nonce-range*[29] oggetto dell'esecuzione dell'algoritmo di *re*-hashing. Un *nonce* può essere classificato in base a come viene selezionato il suo *range*: in modo casuale o sequenziale. Un *nonce* casuale viene prodotto mettendo insieme numeri arbitrari mentre un *nonce* sequenziale viene prodotto in modo incrementale. L'utilizzo del metodo "*nonce* sequenziale" garantisce che i valori individuati non si ripetano, non possano essere riprodotti e non occupino spazio non necessario. Tuttavia, l'utilizzo del metodo "*nonce* casuale" protegge da eventuali aggressori ed è quindi più sicuro in quanto non se ne può tenere traccia.

In sintesi, la *blockchain* presenta le seguenti caratteristiche chiave:

- **Decentramento**. Diversamente, una transazione nella rete *blockchain* può essere condotta tra qualsiasi nodo della rete *peer-to-peer* (*P2P*) senza necessità di autenticazione da parte di un'infrastruttura centrale. In questa maniera, la *blockchain* può ridurre significativamente i costi del server (incluso il costo di sviluppo e il costo operativo) e mitigare i colli di bottiglia delle prestazioni sul server centrale.

- **Persistenza**. Poiché ad ogni transazione è associato uno specifico valore *hash* che ne garantisce l'unicità, anche la più piccola manomissione del dato comporterebbe una stringa *hash* completamente

nuovi blocchi. Per maggiori informazioni, seguire il seguente link: https://ethereum.org/en/whitepaper/#modified-ghost-implementation.

[29] Il ruolo del *nonce-range* verrà approfondito nel capitolo 2.3 "*Mining* e algoritmi di connsenso". Per il momento, basti sapere che per *nonce-range* si intende quell'intervallo numerico selezionato arbitrariamente dal *miner* sulla base della sua potenza di calcolo computazionale al di indivuare il *nonce*, ossia quel numero unico che, aggiunto al *merkle tree root*, renda una stringa *hash* che abbia il termine 0 come primi *n* termini.

differente: questo significa che, visto che il valore *hash* di un blocco (ossia il suo *Merkle tree root*) deriva da quegli delle singole transazioni contenute nel *block body*, le possibilità di manomissione delle informazioni contenute senza cambiare l'intera struttura del blocco sono pari a zero. Inoltre, ogni blocco verrà validato da altri nodi della rete (questo accade durante una *mining pool*), quindi ogni transazione in esso contenuta sarà verificata ed eventuali falsificazioni saranno rintracciate.

- **Anonimato**. Ogni utente può interagire con la rete *blockchain* attraverso un indirizzo generato dalla rete. Inoltre, un utente potrebbe generare molti indirizzi per evitare l'esposizione dell'identità. Non esiste più una parte centrale che conserva le informazioni private degli utenti. Questo meccanismo preserva una certa riservatezza sulle transazioni incluse nella *blockchain*.

- **Auditabilità**. Poiché ciascuna delle transazioni sulla *blockchain* è convalidata e registrati con un *timestamp*, gli utenti possono facilmente verificare e tracciare i record precedenti accedendo a qualsiasi nodo della rete distribuita. Nella *blockchain* di Bitcoin, ciascuno la transazione potrebbe essere ricondotta a transazioni precedenti in modo iterativo. Questo migliora la tracciabilità e la trasparenza.

Le *blockchain*, oltre che suddivise in base alla propria versione, possono essere a loro volta distinte in tre tipologie: pubbliche, private e consortili. La distinzione è effettuata sulla base dei seguenti parametri:

- **Determinazione del consenso**, ossia chi può partecipare al processo di estrazione del blocco e chi no: nel caso di una *blockchain* pubblica, a farlo possono essere tutti i nodi della rete; invece, nel caso di una *blockchain* consortile, solo un *range* selezionato di utenti può partecipare al processo di validazione; infine, in una *blockchain* privata, il processo è interamente riservato ad uno specifico utente, che solitamente è l'impresa sviluppatrice e proprietaria della *blockchain* stessa.

- **Permessi di lettura**, ossia chi può avere accesso alle transazioni e chi non: in *blockchain* pubbliche, chiunque può leggere i dati contenuti nei singoli blocchi; invece, in *blockchain* consortili o private, la lettura può essere riservata solo a nodi selezionati, mentre proibita ad altri.

- **Immutabilità**, ossia chi può manomettere i dati di una *blockchain* e chi no: in una *blockchain* pubblica, essendo i dati condivisi tra più nodi di una rete, è quasi impossibile manomettere i dati senza cambiare completamente la struttura dell'intera *blockchain*. Tuttavia, nelle *blockchain* di tipo consortili gli utenti "maggioritari" possono riservarsi la facoltà di riscrivere i dati contenuti in ogni blocco; lo stesso avviene in una *blockchain* privata.

- **Efficienza**, ossia il tempo, la latenza e le restrizioni che riguardano un tipo di *blockchain* piuttosto che un altro: nelle *blockchain* pubbliche, le liste *broadcast* contenenti le transazioni impiegano molto tempo a raggiungere ogni nodo della rete, questo comporta una più alta latenza, e, visto il numero elevato di utenti che solitamente ha una *blockchain* privata, maggiori restrizioni. Le *blockchain* consortili e private, invece, avendo un numero inferiore di nodi, possono operare più efficientemente ed essere più flessibili di quelle pubbliche.

- **Centralizzazione**. La principale differenza tra i tre tipi di *blockchain* sta nel fatto che quella pubblica è decentralizzata, la *blockchain* consortile è parzialmente centralizzata e la *blockchain* privata è completamente centralizzata in quanto controllata da un singolo gruppo.

- **Autorizzazione**. Tutti potrebbero partecipare al processo di consenso di una *blockchain* pubblica. Diversamente, sia la *blockchain* consortile, sia la *blockchain* privata richiedono un'autorizzazione per poter operarvi in qualità di nodo: ogni richiedente deve essere certificato per aderire a processo di consenso.

	BLOCKCHAIN PUBBLICA	*BLOCKCHAIN CONSORTILE*	*BLOCKCHAIN PRIVATA*
DETERMINAZIONE DEL CONSENSO	Tutti i nodi della rete	*Set* selezionato di nodi	Un'organizzazione soltanto
PERMESSI DI LETTURA	Pubblica	Pubblica o ristretta	Pubblica o ristretta
IMMUTABILITÀ	Manomissione quasi impossibile	Può essere manomessa	Può essere manomessa
EFFICIENZA	Bassa	Alta	Alta
CENTRALIZZAZIONE	Decentralizzata	Parzialmente centralizzata	Completamente centralizzata
AUTORIZZAZIONE	Senza autorizzazione	Con autorizzazione	Con autorizzazione

2.4 MINING E ALGORITMI DI CONSENSO

L'attività di *mining* (o di "estrazione") è quel processo di validazione di un determinato *set* di informazioni per la generazione di una serie storica di dati su cui costruire apparati e servizi esterni.
Il processo di validazione è la risposta al problema della doppia spesa, ossia una truffa consistente nello spendere lo stesso ammontare di risorse due o più volte per ricevere un solo bene/servizio in contropartita: questa situazione può occorrere tipicamente durante una transazione virtuale, in cui non si verifica uno scambio di *asset* fisici ed il luogo dove questo avviene è completamente dematerializzato, incentivando l'adozione di comportamenti truffaldini qualora non vi sia un'Autorità (o di un algoritmo in questo caso) a vigilare sul corretto svolgimento della transazione stessa.
L'attività di *mining*, quindi, si occupa di risolvere questo problema senza ricorrere ad alcuna Istituzione, ma solo ad un *network* distribuito di utenti.

Validare un *set* di informazioni, o di transazioni come nel caso della *blockchain*, è un'attività costosa in termini di calcolo: la spesa in termini computazionali che un *miner* deve sostenere per operare su una *blockchain* è direttamente proporzionale al suo *difficulty level*, il quale varierà a sua volta in base al numero di *miners* attivi. La *ratio* dietro il costo intrinseco allo svolgimento del processo di validazione è quella sia di disincentivare l'adozione di comportamenti opportunistici da parte dei *miners*, sia di favorire la competizione tra gli stesso: ogni *miner*, infatti, opera su una *blockchain* attraverso una *mining pool*, ossia un gruppo congiunto di *miners*, che rappresentano i nodi del *network P2P*, e che condividono su di esso la propria potenza di calcolo individuale. Infatti, la probabilità di validare un blocco, risolvendo un *puzzle* crittografico, è direttamente proporzionale al livello di difficoltà della *blockchain*: condividere risorse su una stessa rete contribuisce a ridurre questa probabilità.
Ogni qualvolta si validi un blocco di transazioni, i *miners* vengono remunerati con valuta di nuova emissione proporzionalmente a quanto contribuito individualmente con la propria potenza di calcolo per risolvere il *puzzle* crittografico. Esistono diversi schemi di remunerazione dei *miners*, tutti basati sul concetto di "quota di partecipazione" (o *share*) al processo di validazione, e che presentano i seguenti elementi in comune:

- B = "*Block reward*", ossia il premio per aver validato un blocco, a questo va sottratto una commissione (*fee*), o *f*, che ciascun *miner* deve pagare per iscriversi alla *pool*.
- p = probabilità di estrarre un blocco.
- D = Difficoltà della *blockchain*.
- R = "*Revenue*", ossia il guadagno per il singolo *miner*.

Essendo p inversamente proporzionale a D, vale la seguente equazione:

$$p = \frac{1}{D}$$

Ogni *pool* permette al *miner* di selezionare *ex-ante* un livello *target* di difficoltà il quale rappresenta la quota di partecipazione con la propria potenza di calcolo al processo di validazione: la probabilità, quindi, si aggiusta

proporzionalmente alle risorse che il *miner* possiede: più capacità computazionali significa poter selezionare un più alto livello *target* di difficoltà e quindi dover sopportare una minore probabilità di estrarre un blocco autonomamente; se questo però accadesse sarà maggiore il premio che si riceverà.

I diversi schemi di *mining pool* sono i seguenti:

1) ***Pay-per-Share*** (o schema *PPS*): offre un pagamento istantaneo al *miner* che si iscriva alla *pool* sulla base del livello medio di potenza di calcolo richiesta ad ogni *miner* per validare un blocco. Il compenso viene prelevato direttamente da un saldo gestito dall'operatore della *pool*. Questo modello consente la minima variazione possibile nel pagamento per i minatori, trasferendo anche gran parte del rischio in capo all'operatore della *pool* stessa. Nello schema *PPS* il guadagno è proporzionale sia al *Block reward* (*B*), sia alla probabilità di estrarre un blocco con successo: $R = B \cdot p$
2) ***Schema proporzionale***: ogni *miner* è libero di partecipare alla *pool* condividendo arbitrariamente la propria potenza durante il processo di validazione. Il livello di difficoltà è suddiviso in *n* segmenti uguali, che rappresentano le quote di partecipazione alla *pool*. Una volta che il blocco è stato validato, il premio è ridistribuito in base alla potenza di calcolo condivisa: più questa è stata alta, più il *miner* detiene quote di partecipazione sul totale (che verrà chiamato N) e maggiore sarà il suo guadagno. L'equazione del *Reward* è data da: $R = \frac{n}{N}$
3) ***Pay-per-last-N-shares*** (o schema *PPLNS*): lo schema è molto simile a quello proporzionale nella sua fattispecie, l'unica differenza è che il premio è calcolato non sul numero totale di quote, ma solo sulle ultime *N*: questo significa che, quando un blocco è estratto, si calcola il guadagno del *miner* solo sulla sua partecipazione al segmento finale della *pool*. Questo garantisce maggiori guadagni quando la *pool* è breve.
4) ***Solo Pools*** (o schema solitario): in questo caso l'intero guadagno della validazione del blocco è conferito al *miner* che abbia risolto il *puzzle* crittografico.
5) ***Score Pools*** (o schema del punteggio): ogni *miner* ha un punteggio che varia a seconda sia della quota di risorse computazionali condivise sulla *pool,* sia del momento in cui le condivide: rispetto al momento di inizio della *pool,* quote inviate più in lá nel tempo garantiranno uno *score* maggiore per il *miner*. Questo rende le quote condivise per ultimo molto più preziose di quelle condivise per prima, quindi il premio per il *miner* inizia a decadere dall'istante in cui smette di condividere potenza di calcolo sulla *pool*. I premi sono calcolati in base allo *score* che del *miner* al momento in cui il blocco viene estratto. Questo metodo garantisce che i *miners* partecipino sempre attivamente alla *pool*.
6) ***Schema Geometrico***: si basa sempre sul concetto di "punteggio" del *miner,* tuttavia, a differenza del precedente metodo, lo schema geometrico prevede che tutte le quote non varino in base al tempo, quindi non c'è nessun vantaggio nel partecipare alla *pool* o all'inizio o in un momento protratto della stessa. Il metodo geometrico permette da un lato di godere di un tasso di decadenza del premio che non sia correlato al tempo ma al numero di quote di risorse computazionali condivise dal numero totale dei *miners*, dall'altro di beneficiare di un sistema del tutto *anti-hopping*, impendendo ai *miners* di

attuare comportamenti opportunistici partecipando alla *pool* solo al suo inizio, quando il suo guadagno atteso è sproporzionato in confronto al contributo effettivo reso alla *pool*.

7) ***Peer-to-Peer Mining Pool*** (o schema *P2Pool*): questo schema permette di ridistribuire i rischi su una rete di nodi, evitando sia che il *server* su cui si appoggia la *pool* si sovraccarichi divenendo un *Single Point Of Failure* (o *SPOF*), pregiudicando il corretto funzionamento del sistema, sia che un singolo operatore, il quale si accolla tutti i rischi in un protocollo *PPS*, possa mettere in atto comportamenti opportunistici a scapito dei *miners*. Lo schema *P2Pool* prevede che ogni *miner* esegua un nodo *P2Pool* che vada a formare una rete P2P. I partecipanti, quindi, condividono la propria potenza di calcolo connettendosi al nodo *P2Pool*, operando ad un basso livello di difficoltà. Nel *network P2Pool* si tiene traccia di coloro che iniziano a condividere risorse computazionali in modo che, qualora il livello di difficoltà raggiunga quella del *network target* (come nel caso di Bitcoin), il blocco validato sarà convertito sulla *blockchain* di riferimento e la relativa ricompensa sarà distribuita tra tutti coloro che hanno partecipato attivamente sulla *share-chain.* Lo svantaggio di questo metodo è che tutti i *miners* devono gestire un nodo completo di una nuova *blockchain* sopportando ingenti costi in temi di *server* ed unità computazionali.

Il processo di *mining* cambia sulla base del protocollo di consenso stabilito: sebbene il *Proof-of-work* (*PoW*) sia il più famigerato, perché adottato da Bitcoin, altri protocolli, come il *Proof-of-Stake* (*PoS*), il *Proof-of-Burn* (*PoB*), il *Proof-of-Activity* (*PoA*) e l'algoritmo *Obelisk*, si sono dimostrati nel tempo come valide alternative al *PoW*, pur presentando pregi e difetti.

- ***Proof-of-Work***: il protocollo della "prova di lavoro", creato da Satoshi Nakamoto per risolvere il problema della doppia spesa, richiede ai *miners* di sostenere un lungo processo di tentativi ed errori per identificare un valore *nonce* tale da rendere un blocco valido. Il protocollo *PoW* prevede che la stringa *hash* di un blocco di transazioni, ottenuta dalla combinazione dei vari elementi caratteristici (ossia il suo numero nella *blockchain*, la stringa *hash* del blocco precedente validato, il *Merkle-tree root* delle transazioni ed infine il *range* del *nonce* selezionato dal *miner ex-ante*), sia l'input per l'esecuzione dell'algoritmo iterativo di *re-hashing*, il quale tenta di identificare un valore *nonce* che generi una stringa *hash* che presenti il numero zero come primi "*n*" termini esadecimali (il valore di "*n*" è stabilito dal livello di difficoltà della *blockchain*). Qualora questo *puzzle* crittografico venga risolto, i *miners* che hanno partecipato alla *pool* di validazione riceveranno un premio sulla base della potenza di calcolo condivisa sul *network.*

  Come si può ben capire, l'algoritmo di *PoW* si caratterizza per un elevato grado di aleatorietà dato che il *nonce* identificato sarà l'*n*-esima combinazione che l'algoritmo di *re-hashing* ha eseguito per estrarre il blocco. *Ex-ante*, il *miner* potrà selezionare, in base alla potenza di calcolo di cui dispone, un *range* di combinazioni che l'algoritmo di *re-hashing* potrà eseguire per identificare il *nonce*: più il *miner* dispone di risorse computazionali, più ampio sarà il *range* selezionato, maggiore sarà il numero di iterazioni svolte dall'algoritmo di *re-hashing* per identificare il *nonce* e quindi più elevata sarà anche

la probabilità di risolvere prima il *puzzle* crittografico. La cripto-valuta Bitcoin è stata la prima ad adottare un protocollo di consenso basata sul *PoW* (il sistema utilizzato è quello Hashcash[30]). Attualmente, il tempo di validazione di un blocco sulla *blockchain* di Bitcoin è di dieci minuti, con un livello di difficoltà pari a 20 zeri come primi "n" termini esadecimali.

Il premio che i *miners* ricevono dall'aver estratto un blocco è pari a 6,25 BTC, ossia € 259136,125 (13/05/2021), un premio che va dimezzandosi ogni quattro anni fino al raggiungimento del limite dei ventuno milioni di Bitcoin in circolazione (che, attualmente, si aggira intorno a diciannove milioni).

L'algoritmo di *PoW* può essere riassunto nel seguente *code snippet*[31]:

```
import hashlib
from hashlib import sha256
import random as r
import time
import uuid

#Defining the hashing function

def SHA256(text):
    return sha256(text.encode("ascii")).hexdigest()

#Defining the mining function

def Mine(block_number, merkle_tree_root, previous_hash, difficulty_lvl):
    difficulty = '0'*difficulty_lvl
    for nonce in range(int(MAX_NONCE)):
        block_info = str(block_number) + merkle_tree_root + previous_hash +
str(nonce)
        new_hash = SHA256(block_info)
        if new_hash.startswith(difficulty):
            print(f"Block was mined successfully with this nonce value:{nonce}")
            return new_hash

    raise BaseException(f"Stop mining: after {nonce} combinations mining will
become too much expensive if compared with the reward ")

#Defining the Merkle-tree

class MerkleTreeRoot(object):
    def __init__(self):
        pass
    def find_merkle_hash(self, file_hashes):
        blocks=[]
        if not file_hashes:
            raise ValueError('Missing files required to generate the Merkle tree
root')
        for m in sorted(file_hashes):
            blocks.append(m)
        list_len=len(blocks)
        while list_len%2!=0:
            blocks.extend(blocks[-1:])
            list_len=len(blocks)
```

[30] Hashcash è un sistema *PoW* introdotto da Adam Back nel 1997 come meccanismo per porre un freno alle e-mail di *spam* ad alto contenuto di pericolosità: Hashcash si propone di aggiungere un *token* nell'intestazione di un'e-mail. Questo *token* è il risultato dell'esecuzione di alcune funzioni informatiche di *hashing*. La funzione di *proof-of-workl* utilizzata in Hashcash consiste in una parziale inversione *hash*, utilizzando lo SHA-1 come algoritmo di *hashing*.

[31] Il seguente codice è stato creato per mostrare un algoritmo di *mining*, con un basso livello di difficoltà (da 1 a 8 zero randomicamente), di un solo blocco di una *blockchain* (il numero 2 in questo caso). Il processo può essere reso iterativo in modo tale da costruire un'intera *blockchain* con il relativo algoritmo di *PoW* automatizzato.

```
        secondary =[]
        for k in [blocks[x:x+2] for x in range(0, len(blocks), 2)]:
            hasher=hashlib.sha256()
            hasher.update((k[0]+k[1]).encode('utf-8'))
            secondary.append(hasher.hexdigest())
        if len(secondary) == 1:
            return secondary[0][0:64]
        else:
            return self.find_merkle_hash(secondary)


#Test the values...


if __name__=='__main__':

    block_number = 2

    #Supposing the block number does not change: the whole algorithm is based on
just one block, and not on the entire blockchain

    previous_hash =
'0ee359f06f39167a279742e7c3f677d7e853ff378579ea1de47869db615f2144'

    #The difficulty level was 1: you can see it by the zeros at the beginning of
the hash
    #Since the block number selected is 2, this means that this hash comes from
the originator block (the first block in the blockchain)
    #The originator block has a previous hash string of 256 hexadecimal 0s

    #testing the Merke_tree

    file_hashes = []
    for i in range(0,10):
        file_hashes.append(str(uuid.uuid4().hex))
    print('Generating the Merkle tree root of the following {0}
transactions:'.format(len(file_hashes)))
    cls=MerkleTreeRoot()
    merkle_tree_root = cls.find_merkle_hash(file_hashes)
    print(*file_hashes, sep = "\n")
    print('...')
    print('Merkle tree root is: {0}'.format(merkle_tree_root))

    print('...')

    #The difficulty level is a random value selected everytime the mining
process starts

    difficulty=r.randint(1,8) #The random value is selected in this range: if it
is close to 8, the cimputational power required will be higher and so the
timestamp
    print("The actual difficulty level is:", difficulty)

    print('...')

    MAX_NONCE = input("Select a range of combinations to try in order to get the
nonce ")

    start = time.time()
    print("Start mining...")

    new_hash = Mine(block_number, merkle_tree_root, previous_hash, difficulty)
```

Due tipologie di attacchi possono mettere in pericolo il sistema di *PoW*:

1. L'attacco *Sybil*: l'aggressore tenta di riempire la rete con dei client sotto il suo controllo. Se così fosse, egli potrà effettivamente controllare od ottenere un monopolio sulla rete, in quanto questi client possono eseguire diversi tipi di azioni in base alle istruzioni dell'aggressore: possono rifiutarsi di trasmettere i blocchi validi o possono solo trasmettere i blocchi generati dagli attaccanti, portando a un problema di doppia spesa.
   In altri termini, l'attaccante può includere più nodi nella rete che possano compromettere collettivamente il meccanismo *Proof of Work*.
2. Attacchi *Denial of Service* (*DOS*): l'attaccante trasmette un flusso enorme di dati con lo scopo di saturare la backlog queue di uno o più nodi in modo che questi non siano più in grado di elaborare le normali transazioni Bitcoin. Di conseguenza, il metabolismo della procedura di mining verrà ritardato, sprecando risorse di calcolo. Nel frattempo, l'attaccante può creare nuovi nodi sulla rete, sostituendo quelli che hanno subito l'attacco e generando un monopolio di controllo del network.

- ***Proof-of-Stake***: Il protocollo *PoS*, ideato dallo sviluppatore Sunny King, è probabilmente la migliore alternativa a quello *PoW* in quanto permette di ridurre sensibilmente i rischi di un attacco informatico. Infatti, il protocollo *PoS* prevede che la probabilità di estrarre un blocco con successo sia correlata non con la potenza di calcolo del *miner* ma con il quantitativo di valuta che esso effettivamente detiene: in altri termini, chi possiede l'1% del circolante di Bitcoin, potrà estrarre l'1% dei blocchi di nuova generazione. Il protocollo *PoS* permette anche a chi non partecipa attivamente al processo di validazione di farlo passivamente, delegando una quantità arbitraria di valuta ad un *miner* di fiducia con la promessa di ricevere in cambio una quota del premio qualora quest'ultimo riesca ad estrarre un blocco con successo. Infine, il protocollo *PoS* riduce drasticamente il rischio che qualcuno possa truffare gli altri utenti: i *miners* sono disincentivati a mettere in atto comportamenti opportunistici dato che la quantità di valuta in loro possesso, dichiarata per partecipare al processo di validazione, rimane "ferma" per tutto il periodo dello stesso, rischiando di perderla definitivamente qualora la truffa venga scoperta dagli altri utenti della rete. Il problema di fondo legato al protocollo di consenso *PoS* può essere sintetizzato con la seguente affermazione: "i *miners* più ricchi, si arricchiscono ancora di più"; infatti, più un validatore (o *miner*) dispone di circolante, più ha probabilità di estrarre un blocco con successo, ricevendo il premio del *mining*. Ragionando al limite, questa situazione può generare un monopolio che tagli fuori dalla rete coloro che detengono minori percentuali di valuta. Il protocollo *PoS* è stato attualmente adottato da cripto-valute come Cardano e Dash, mentre Ethereum promette di ricorrervi nel prossimo futuro con il prossimo *hard-fork*[32] della *blockchain*.

[32] Un *hard-fork* è un cambiamento radicale di una *blockchain* ad un nuovo protocollo di rete che estragga blocchi o transazioni prima considerate invalidi, o viceversa. Un *hard-fork* richiede a tutti gli utenti di quella *blockchain* di aggiornare il *software* di

- ***Proof-of-Burn***: il protocollo *PoB* cerca di risolvere il problema dell'elevato consumo di energia di un sistema *PoW*. Il *PoB* è spesso definito un sistema *PoW* senza spreco di energia. Funziona in base al principio di consentire ai minatori di "bruciare" gettoni di valuta virtuale. Viene quindi concesso loro il diritto di scrivere blocchi in proporzione alle monete bruciate. Il protocollo *PoB* prevede che le monete "bruciate" servano per ottenere una possibilità maggiore per estrarre un blocco con successo: più si "bruciano" monete, più questa probabilità diventa elevata. In questo senso, il protocollo *PoB* è molto simile a quello *PoS*.

  Per bruciare le monete, i *miners* inviano un ammontare di moneta pari al livello di difficoltà della *blockchain* ad un indirizzo verificabile non-spendibile. Questo processo non consuma molte risorse (oltre alle monete bruciate) e garantisce che la rete rimanga attiva. A seconda dell'implementazione del protocollo, i *miner* possono bruciare la valuta nativa o la valuta di una catena alternativa, come Bitcoin. In cambio, ricevono una ricompensa in *token* di valuta nativa della *blockchain*.

  Una volta che un utente abbia bruciato moneta, si generano transazioni che possono essere aggiunte ai blocchi anche di altri *miners* per effettuare l'estrazione.

  Per prevenire la possibilità di comportamenti opportunistici da parte degli utenti che abbiano "bruciato" moneta per primi, il protocollo POB prevede che periodicamente si debba "bruciare" moneta per poter operare in qualità di *miner*: questa facoltà "decade" o si riduce parzialmente ogni volta che viene estratto un nuovo blocco. Ciò promuove un'attività regolare da parte dei *miners*, invece di un investimento iniziale e *una tantum*. Per mantenere un vantaggio competitivo, i *miners* potrebbero anche dover investire periodicamente in attrezzature migliori man mano che la tecnologia avanza.

  Attualmente, il protocollo *PoB* è implementato dalla cripto-valuta Slimcoin.

- ***Proof-of-Acticity***: il protocollo di consenso *PoA* può essere inteso come l'unione dei protocolli *PoW* e *PoS*, tentando di ridurne le specifiche problematiche. Secondo il protocollo *PoA*, il processo di *mining* inizia allo stesso modo di un processo *PoW*, con vari *miners* che cercano di competere tra di loro con una maggiore potenza di calcolo per trovare un nuovo blocco. Quando viene trovato (o estratto) un nuovo blocco, il sistema passa al protocollo *PoS*, con il blocco appena trovato contenente solo un'intestazione e l'indirizzo di ricompensa del minatore.

  In base ai dettagli dell'intestazione, viene selezionato un nuovo gruppo casuale di *miners* dalla rete *blockchain* che dovranno a convalidare o firmare il nuovo blocco. Più monete possiede un validatore, maggiori sono le possibilità di essere selezionato come firmatario.

  Una volta che tutti i validatori firmano il blocco viene aggiunto alla rete *blockchain* e le transazioni iniziano a essere registrate su di esso. Nel caso in cui alcuni dei firmatari selezionati non siano disponibili per firmare il blocco fino al completamento, il processo passa al blocco successivo vincente

esecuzione del protocollo all'ultima versione. Di particolare rilevanza è l'*hard-fork* "*Serenity*"che porterà Ethereum ad abbandonare il protocollo di consenso *Proof-of-work* e ad adottare quello *Proof-of-Stake*.

con una nuova serie di validatori scelti a caso (a seconda della loro puntata di monete). Questo processo continua fino a quando un blocco riceve il numero richiesto di firmatari e diventa un blocco completo. Le commissioni / ricompense *mining* sono suddivise tra il minatore e i vari validatori che hanno contribuito nei rispettivi ruoli a firmare il blocco.

Il problema relativo a questo protocollo di consenso è che, proprio come coniuga gli aspetti positivi di entrambe i protocolli *PoW* e *PoS*, non riesce ad eliminare del tutto i rischi ed i costi connessi con i due sistemi: la potenza di calcolo richiesta per estrarre i blocchi rimane sempre troppo elevata e *miners* sono ancora di più incentivati ad accumulare moneta avendo più possibilità di entrare nella lista dei firmatari ed ottenere più premi di validazione.

La prima cripto-valuta ad aver adottatto il protocollo di consenso *PoA* è Decred (DCR).

- ***Algoritmo di consenso Obelisk***: L'algoritmo di consenso Obelisk, di proprietà della cripto-valuta SkyCoin, si pone l'obiettivo di ovviare alle problematiche che i protocolli *PoW* e *PoS* presentano, distribuendo l'influenza esercitata da ciascun nodo su una "rete di fiducia": ogni nodo dovrà, infatti, votare un numero selezionato di altri nodi, andandone a riconoscere la propria influenza esercitata sul *network*.

  Secondo l'algoritmo Obelisk, esistono due tipologie di nodi:

  1. Nodi generatori di blocchi, ossia gli utenti che raccolgono le transazioni, le autenticano, generando un blocco e trasmettendolo al *network*;
  2. Nodi di consenso, ossia coloro che in un primo momento raccolgono i blocchi trasmessi dai nodi generatori, in un secondo momento, invece, verificano quale, tra questi blocchi, sia quello che è stato creato dal maggior numero di nodi generatori: tale blocco, chiamato "vincitore locale", forma la *blockchain*. Quando i "vincitori locali" sono stati segnalati dalla maggioranza dei nodi di consenso, si qualifica come "vincitore globale" e continuerà a restare sulla *blockchain*.

2.5 TOKENS, ICOs, STOs, IEOs & METODI DI VALUTAZIONE

La prima cripto-valuta, Bitcoin, fu creata nel 2009 da Satoshi Nakamoto come metodo di pagamento alternativo alla moneta *fiat*. Ethereum è una valuta alternativa (c.d. *AltCoin*) a Bitcoin, creata nel 2014 da Vitalik Buterin che permetta l'elaborazione automatica dei c.d. *smart contracts* ossia set di codici e dati associati ciascuno a specifici indirizzi di una *blockchain*. I *tokens* sono creati come *smart contracts* sulla *blockchain* di Ethereum. Esistono tre macro-categorie di *tokens*:

1. ***Utility Tokens***: *tokens* che confermano i diritti di accesso a prodotti, servizi o altro. Generalmente richiedono l'uso di un'infrastruttura di tipo *blockchain*. Gli *Utility Tokens* sono utilizzati come mezzi di scambio all'interno di un determinato eco-sistema: l'esempio più illustre di *Utility Token* è il *Basic Attention Tokens (BAT)*, sviluppato dal *browser* Brave, che viene distribuito sia agli utenti in base alla loro attività *on-line*, sia ai creatori in base alla capacità di catturare l'attenzione dell'utente. *BAT* è quindi un *token* utilizzato per monetizzare l'attenzione, incentivando da un lato gli sviluppatori di contenuti multimediali ad acquistare spazio *on-line* e a pubblicare contenuti attrattivi, dall'altro gli utenti che ricevono *Brave Rewards*, che possono essere scambiati in moneta *fiat* sulla piattaforma *Binance*: più tempo di visualizzazione è stato dedicato ad un *banner* pubblicitario, più l'utente ed il creatore riceveranno *tokens* in cambio.

2. ***Security Tokens***: *tokens* negoziabili il cui scopo principale è quello di conferire ai propri titolari diritti amministrativi, come il diritto di voto in un'assemblea, e/o diritti patrimoniali, come la partecipazione agli utili societari. I *Security Tokens* rappresentano solitamente diritti connessi con gli *assets* sottostanti, quali: *cash-flows*, proprietà immobiliari od oggetti da collezione come le opere d'arte. Rispetto alle azioni o alle obbligazioni i *Security Tokens* presentano i seguenti vantaggi:
   - Maggiore frazionalizzazione, anche di *assets* di grandi dimensioni;
   - Nessuna limitazione geografica e/o temporale in quanto possono essere liberamente scambiati su mercati *Over-The-Counter* o su piattaforme di *exchange* di cripto-valute;
   - Maggiore liquidità, in quanto è molto più semplice dismettere questi *tokens* rispetto ad azioni od obbligazioni.
   - Minori costi di emissione rispetto alla sottoscrizione di azioni od obbligazioni;
   - Minore connessione con i mercati dei capitali.

   Il *security token* si può distinguere nelle seguenti categorie:

   a) *Equity Token*: detenendo questa tipologia di *token* si possiede una quota di proprietà dell'impresa emittente o di interesse nel progetto di finanziamento. L'*equity token* conferisce gli stessi diritti patrimoniali e/o finanziari di una azione tradizionale.

b) *Debt Token*: detenendo questa particolare tipologia di *token* si ha diritto a ricevere in un dato istante una quota di interessi sull'importo conferito all'azienda, al pari di una obbligazione tradizionale.

c) *Asset Backed Token*: detenendo questa forma di *security token*, si riceve il diritto a possedere uno specifico *asset* ed una quota dei ricavi che esso genera; questo *asset* solitamente è un bene fisico altamente illiquido, come un'opera d'arte o una proprietà intellettuale che viene reso digitale attraverso il processo di *tokenizzazione.*

d) *StableCoin Token*: lo *StableCoin Token* ha la stessa natura di un *Asset Backed Token* ma presenta delle garanzie sottostanti (o *collateral*) come monete *fiat* o altre cripto-valute. Gli *StableCoin Tokens*, dato che mantengono un rapporto fisso con il relativo *collateral* sottostante, sono *tokens* che non risentono di un'elevata volatilità nel tempo. USDT (Tether) è lo *StableCoin Token* con il più alto *market cap* nel 2021, creato per avere un valore che si mantenga entro il rapporto 1:1 con il dollaro americano. Altri *StableCoin Tokens*, come Dai, sono supportate da cripto-valute che possono essere soggette ad alta volatilità; per questo motivo, questa tipologia di *StableCoin Token* è "sovra-collateralizzata": ciò significa che è supportata da una riserva che conta un numero maggiore di unità di cripto-valuta rispetto agli *StableCoin Tokens* emessi (ciò significa che il rapporto di cambio sarà, per esempio 1:1,15 ossia un DAI per ogni 1,15 ETH). Esistono, inoltre, altre tipologie di *StableCoin Tokens* che adottano nella loro struttura concetti finanziari come l'investimento composto o gli indici: ciò significa che, per ogni unità di *token* detenuto, si ha diritto a percepire un paniere di cripto-valute.

e) *Rebase Tokens*: Un *token* ad offerta elastica è un particolare tipo di *asset* crittografico che varia algoritmicamente e periodicamente la sua offerta sulla base dei cambiamenti del prezzo in un dato momento. Sotto questo punto di vista, i *rebase tokens* sono molto simili agli *StableCoin Tokens*, in quanto si prefissano di mantenere un livello di prezzo obbiettivo che, tuttavia, è raggiunto non variando il tasso di cambio ma modificando l'offerta: all'aumentare del prezzo, l'offerta diminuirà e viceversa. Per questo motivo, i *rebase tokens* sono investimenti altamente rischiosi e pericolosi.

3. ***Crypto-currency Tokens***: *tokens* accettati come mezzi di pagamento per l'acquisto di prodotti o servizi o per trasferire valore nel tempo. Bitcoin, Bitcoin Cash e Litecoin sono esempi di *tokens* su cripto-valute. I *cripto-currency tokens* sono indipendenti da qualsiasi piattaforma e possono essere usati come valute al di fuori del loro ambiente d'origine, mentre gli *utility tokens*, al pari dei *security tokens* esistono su una piattaforma creata generalmente dal loro emittente.

Un elemento di particolare rilievo per poter definire la natura di un *token* dal punto di vista della regolamentazione da applicare è il test di Howey, che definisce i quattro seguenti criteri: 1) avviene un investimento di denaro; 2) ci si aspetta di ricevere profitti; 3) c'è attività di impresa; 4) qualsiasi profitto

proviene dal lavoro di un terzo soggetto. Secondo questi criteri, la maggior parte dei *tokens* in circolazione sono associabili ai *security tokens*, la cui disciplina, negli Stati Uniti, è rimessa alla Regulation D, alla Regulation S ed alla Regulation A+.

La comparsa dei *tokens* ha permesso agli investitori di poter godere di un meccanismo che da un lato incentivi la partecipazione all'ecosistema della *blockchain* e ad il processo di informazione del *FinTech*, dall'altro garantisca un *funding* di risorse anche a livelli di sviluppo di un progetto non avanzati.

Le *Security Token Offerings* (o *STOs*) sono raccolte di capitali (*crowdfunding*) avviate da *smart contracts* con lo scopo di finanziare progetti basati sulla *blockchain*. Lo standard condiviso per le STOs e la creazione di nuovi *tokens* è stato inizialmente l'ERC-20[33], già ampiamente adottato durante le prime ICOs (*Initial Coin Offerings*) del 2015. Tuttavia, oggigiorno sono disponibili altri protocolli, come l'ERC-721 e l'ERC-1155, nati per rispondere ad esigenze che vanno oltre il puro e semplice finanziamento, come l'implementazione di *tokens* non fungibili (o *NFT*), ossia *tokens* che hanno la peculiarità di non essere reciprocamente interoperabili, cosa che accade invece con l'adozione del protocollo ERC-20.
Altro schema di raccolta del capitale è attraverso il ricorso ad una ICO, o *Initial Coin Offering*, ossia un modello (piuttosto recente) che prevede la distribuzione di *tokens* o di cripto-valute per ricevere monete *fiat* in contropartita, senza dover necessariamente garantire *equity* (e quindi *ownership*) agli investitori o a coloro che comprano i *tokens*.
Le *STOs*, al contrario delle *ICOs*, distribuiscono titoli finanziari fungibili e negoziabili *tokenizzati* con un valore monetario annesso, come una quota del capitale sociale aziendale, e che garantiscono diritti patrimoniali e/o finanziari al loro detentore. Per questo motivo le *STOs*, essendo sottoposte ad una regolamentazione *ex-ante* adoperata da figure di intermediazione finanziaria come *dealers*, *brokers* e/o sottoscrittori del collocamento, forniscono maggiori garanzie al pubblico di investitori che la raccolta non si riveli uno *scam* (come è accaduto nei 2/3 dei casi di *ICOs*). Per di più, gli investitori che partecipano all'operazione di *STO* sono accreditati dai regolatori e presentano un elevato *standing* creditizio.
Lanciare una *STO* richiede però maggiore tempo e risorse rispetto ad una *ICO* in quanto richiede *ex-ante* la presentazione di un *business model* che convinca i regolatori ad autorizzare l'operazione.
Ricorrere ad una *ICO*, d'altro canto, riduce drasticamente le tempistiche ed i costi connessi con la raccolta dei capitali in quanto non si fa ricorso ad un intermediario finanziario, né si è obbligati ad attendere il permesso di nessuna autorità di regolazione; inoltre, non si pongono vincoli in termini temporali e all'operazione può partecipare chiunque indistintamente.
Sia le *ICOs*, sia le *STOs* sono validi sostituti dei più tradizionali metodi di *Initial Public Offering* (o *IPO*), in quanto contribuiscono a ridurre i rischi di azzardo morale e di selezione avversa pur non ricorrendo

[33] ERC-20, ERC-721 ed ERC-1155 sono protocolli (c.d. *standards*) per l'emissione di *utility* e *security tokens* sulla *blockchain* di Ethereum. Mentre l'ERC-20, lo *standard* più antiquato tra i tre, descrive le funzioni *core* degli *utility tokens* mentre l'ERC-721 e l'ERC-1155 descrive quelle dei *security tokens* o *NFTs*. Recentemente, si sta implementando un nuovo *standard*, l'ERC-1404, che permetta di raggiungere un *framework* traversale all'emissione di tutti i *tokens*.

direttamente alla figura dell'intermediario finanziario dato che i progetti di investimento vengono presentati on-line o comunque su piattaforme digitali, garantendo così un maggior afflusso di informazioni sulla rete, riducendo le asimmetrie informative. Sia le *ICOs*, sia le *STOs* permettono inoltre all'impresa che le metta in atto di raccogliere capitali anche in una fase iniziale dell'implementazione del progetto di investimento, piuttosto che in fasi finali come nel caso delle tradizionali *IPOs*, questo rende le prime metodologie le migliori per finanziare progetti di *start-ups* o di piccole imprese native digitali.
Ultimamente sta raccogliendo un sempre maggiore interesse il metodo di raccolta *IEO*, o *Initial Exchange Offering*, molto simile alle *ICOs* dal momento che prevede la distribuzione di *tokens* di nuova emissione, ma si differenzia da quest'ultima per il fatto che le risorse raccolte dagli investitori sono costituite da cripto-valute o da altri *tokens*, per cui questo metodo di *funding* deve necessariamente avvenire su piattaforme di *exchange* specializzate, come Binance, Bitfinex o OnEx, che fungono da *middle-man*, agendo da sottoscrittori della raccolta e fornendo l'accesso alla start-up ai mercati di compratori di *tokens*. L'attività di *IEO*, può, tuttavia, generare situazioni di conflitti di interesse tra la compagnia emittente e la piattaforma *exchange*: basti pensare che Binance ha cancellato la *IEO* del videogioco RAID: Shadow Legends poche ore prima dell'apertura dell'operazione per un "difetto" riscontrato nel *business model*.

Lo studio condotto da Burniske e Tatar è il primo che affronta il tema della valutazione dei *tokens* attraverso l'uso di indici e metriche tradizionali. Le metodologie di valutazione sono diverse a seconda della natura del *token*: i primi 3 schemi (Velocità, Curva J e NVT) prendono in esame la valutazione degli *utility tokens*, mentre gli ultimi 3 (Crypto-CAPM, DFC e le Valutazioni comparative sul prezzo) studiano il prezzo dei *security tokens*.

1. **Velocità del *Token***

   Questa metodologia prevede l'applicazione della Teoria Quantitativa della Moneta ad un'economia basata sullo scambio di *tokens*. La Teoria Quantitativa della Moneta (TQM) definisce il seguente rapporto:

   $$M^S V = PQ$$

   Dove:

   M^S = *Money Supply*, ossia l'offerta di moneta. In condizione di equilibrio si avrà che M^S=M^D, ossia che l'offerta di moneta è pari alla sua domanda. In un'economia basata su *tokens*, M rappresenta la quantità di *tokens* in circolazione in un dato periodo.

   V = *Velocity of Money*, la velocità di circolazione della moneta è un indice che rappresenta quante volte una moneta, o in questo caso il *token*, passa di mano.

   P = *Price Level*, ossia il livello generale dei prezzi espresso nella valuta adottata o, come in questo caso, in *tokens*. Il prezzo dei *tokens* sarà quindi pari all'inverso di questa grandezza (1/P)

Q = *Quantity of Output*, ossia il livello di beni e servizi generati in quell'economia (spesso questa grandezza è associata al PIL dell'economia considerata). Considerando i *tokens*, Q rappresenta il valore economico delle transazioni che avvengono quotidianamente.
Dalla relazione si evince che il prezzo del *token* di quell'economia è pari a:

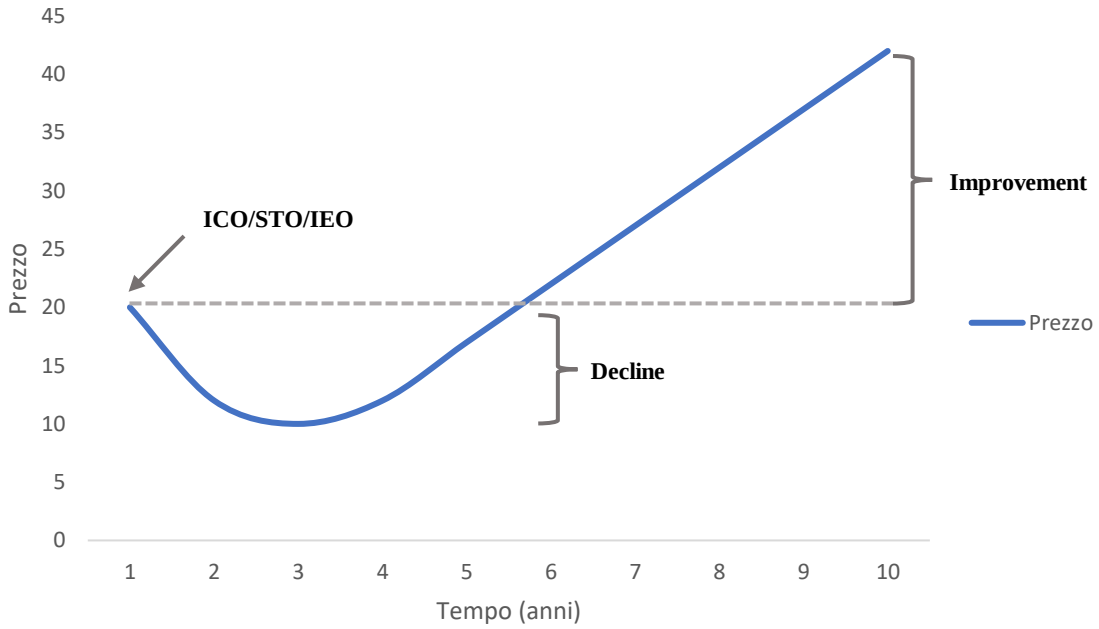
$$Prezzo\ token = \frac{1}{P} = \frac{Q}{M^S V}$$

La variabile critica di questa relazione è sicuramente la velocità di circolazione dei *token*: più questo viene tenuto come *asset* speculativo, più il prezzo è destinato a crescere. Il *focus* finale di questa metodologia di valutazione porta ad affermare che qualora un *token* inizi ad essere utilizzato con un'alta frequenza, questo può diventare una valuta indipendente, al pari delle monete tradizionali.
Esistono delle forme di *StableCoin* che, per contenere la volatilità, contraggono o aumentano l'offerta del *token* sulla base del prezzo del collaterale (che sia esso una moneta *fiat*, o una cripto-valuta), generando delle pressioni al rialzo o al ribasso del prezzo del *token* a seconda delle necessità. Questi *StableCoin*, chiamati "algoritmici" in quanto si appoggiano agli *smart contracts* per regolare istantaneamente il prezzo del primo al variare di quello del collaterale sottostante, sono ancora poco diffusi: il progetto del LUNA Coin (italiano, tra le altre cose) è quello più promettente e che sta riscuotendo notevole attenzione.
La difficoltà di applicazione di questa metodologia di valutazione sta nel reperimento dei dati: mentre il lato sinistro dell'equazione, quindi l'offerta di moneta e la sua velocità di circolazione, sono relativamente più facili da calcolare rispetto a quanto si possa fare con la moneta *fiat* in quanto le *blockchain* di molte cripto-valute (tra cui Bitcoin) sono pubbliche (anche se nel computo di M^S potrebbero o non potrebbero comparire valute non-minate o perse, basti pensare che circa il 4% di Bitcoin ogni anno viene perso su *wallet* di cui vengono dimenticate le chiavi di accesso); il lato destro è formato da una grandezza in particolare, ossia Q, che è quasi impossibile da identificare in quanto l'uso di queste valute incide relativamente poco sul PIL di un qualsiasi Paese occidentale e le realtà che le accettano come mezzi di pagamento, seppure stiano proliferando a ritmi sostenuti, impattano marginalmente sull'economia reale attuale.

2. **Curva-J**

La curva *J* è tradizionalmente utilizzata per studiare la svalutazione di una moneta in relazione al deficit nazionale di un Paese che la adotti; tuttavia, recenti studi, come quelli condotti da Burniske e Tatar, hanno dimostrato l'efficacia di questo parametro anche nel valutare il prezzo dei cripto-*assets*.
Infatti, si può pensare al prezzo di un *token* come l'unione di due componenti, uno operativo, chiamato "valore utile corrente", che rappresenta la valutazione dell'utilità del *token* sulla base di una media di transazioni quotidiane, ed uno speculativo, chiamato "valore utile atteso scontato" (molto simile, nella sua accezione, al concetto di *Discounted Cash-Flows*), che rappresenta il valore dell'investimento per il futuro.

Il valore di queste due voci cambia nel tempo a seconda degli sviluppi della *blockchain* su cui si appogia il *token* e di come il mercato recepisce queste informazioni: infatti, al lancio del *token* (tramite ICO, STO o IEO) il valore speculativo del prezzo sarà preponderante rispetto a quello operativo, in quanto il mercato è in fermento. Una volta che il mercato ha scontato l'*hype* iniziale, il prezzo scende, appoggiandosi per la maggior parte sulla sua componente operativa. Man mano che gli sviluppatori migliorano la tecnologia *blockchain* sottostante, il *token* raggiungerà un più vasto utilizzo: il mercato interpreterà positivamente queste informazioni e la domanda del *token* aumenterà, generando un apprezzamento. In ultima istanza, il valore operativo dovrebbe essere l'elemento guida del prezzo del *token* piuttosto che la componente speculativa.



3. ***Network Value-to-Transaction* (*NVT*)**

L'analisi di Willy Woo su Forbes del 2017, ha introdotto l'indice Price-to-Equity, utilizzato per lo studio del Patrimonio Netto di un'azienda e per indicarne la crescita futura, al mondo delle cripto-valute, prendendo in esame, essenzialmente, due elementi: il *market cap* (o il valore del *network* in un dato momento) ed il volume delle transazioni giornaliere in USD (definendo così un rapporto chiamato *Network Value-to-Transaction, NVT*). Questo indice serve a stimare se il valore del *network* è sotto o sopra valutato rispetto al volume delle transazioni giornaliere di quella rete, il quale rappresenta l'utilità che gli utenti traggono dal ricorso al *network*. Quando il valore *NVT* è molto elevato, è sinonimo di sopravvalutazione del *network*; viceversa, un basso indice significa svalutazione della rete. L'NVT è utilizzato nei più recenti algoritmi di *trading* automatizzati o *crypto-trading bots*, che sfruttano questo indice assieme ad alcuni concetti di analisi tecnica per aprire/chiudere posizioni sula cambio con moneta *fiat* quasi istantaneamente.

$$Network\ Value - to - Transaction\ (NVT) = \frac{Market\ Cap}{Volume\ delle\ transazioni\ giornaliere\ in\ USD}$$

Bitcoin NVT Ratio (Woo 2017)

Fonti: https://charts.woobull.com/bitcoin-nvt-ratio/

4. *Spent Output Profit Ratio* (*SOPR*)

L'indice *SOPR* (*Spent Output Profit Ratio*) fornisce informazioni sulle aspettative di mercato, sulla redditività e sulle perdite di un *asset*, rilevate in un determinato *frame* temporale.

Il *SOPR* è un indicatore molto semplice: è il valore di realizzo (in USD) diviso per il valore di creazione (sempre in USD) di una moneta in un giorno. In altri termini, è il rapporto tra prezzo di vendita di una moneta e prezzo pagato per aggiudicarsela in quel dato giorno (in quanto il valore di creazione di una moneta rappresenta il suo costo che un soggetto è disposto a pagare per aggiudicarsela).

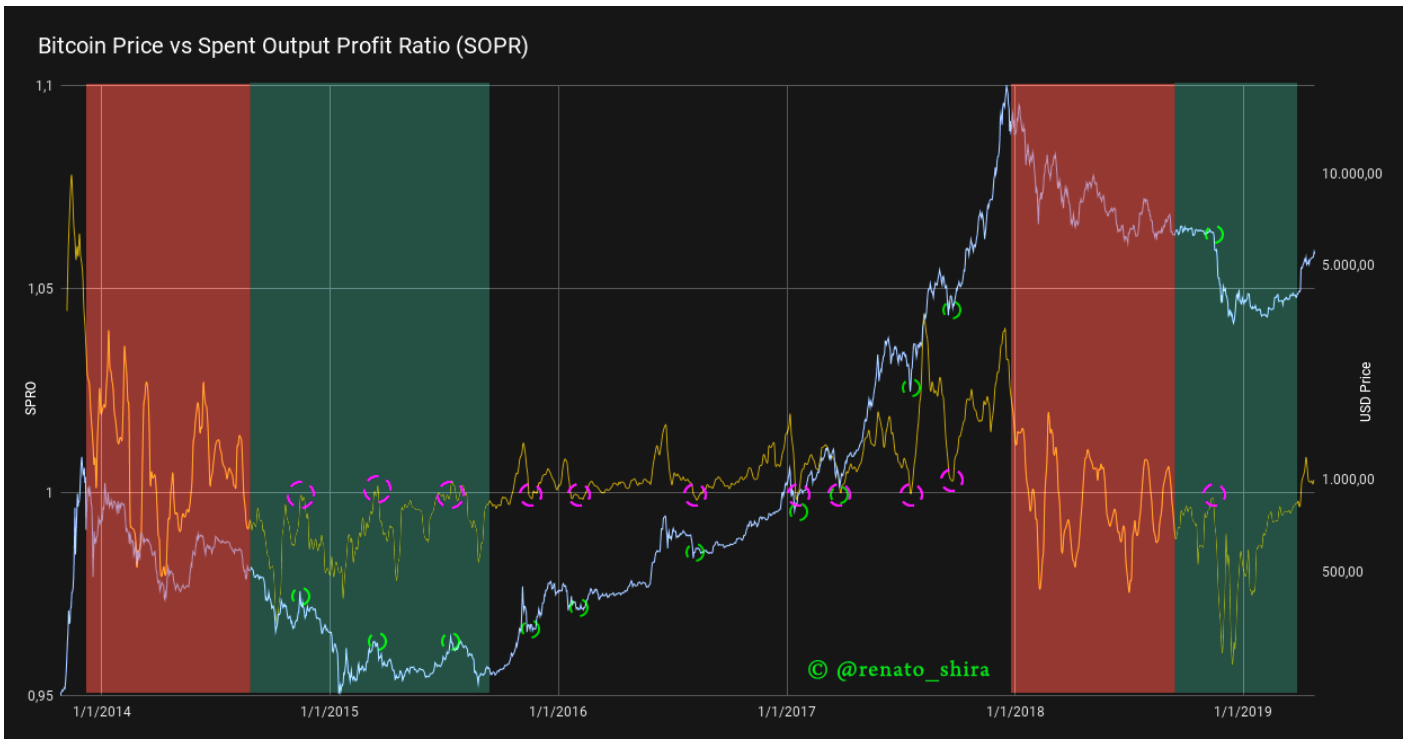
$$Spent\ Output\ Profit\ Ratio\ (SOPR) = \frac{prezzo_{vendita}\ [USD]}{prezzo_{creazione}\ [USD]}$$

L'indicatore SOPR può essere considerato nel seguente quadro:

- SOPR > 1: significa che le monete in quel giorno sono state vendute, in media, in profitto (il prezzo di vendita è superiore a quello di acquisto per quel giorno);
- SOPR < 1: le monete in quel giorno sono state, in media, vendute in perdita (il prezzo di vendita è inferiore a quello di acquisto per quel giorno).
- SOPR = 1: il valore di creazione di nuova moneta è, in media, pari al valore di realizzo (il prezzo di vendita è esattamente pari a quello di acquisto per quel giorno).

In un mercato rialzista, se l'indice *SOPR* scende sotto l'unità significa che gli utenti venderebbero in perdita ma che sarebbero riluttanti nel farlo. Questo spinge al ribasso l'offerta che produce un effetto rialzista sul prezzo.

In un mercato ribassista, invece, tutti vendono o aspettano il punto di pareggio per vendere. Quando l'indice *SOPR* è vicino o maggiore all'unità, significa che le persone iniziano a vendere ancora di più, man mano che raggiungono il pareggio. Con un'offerta più alta, il prezzo precipita.



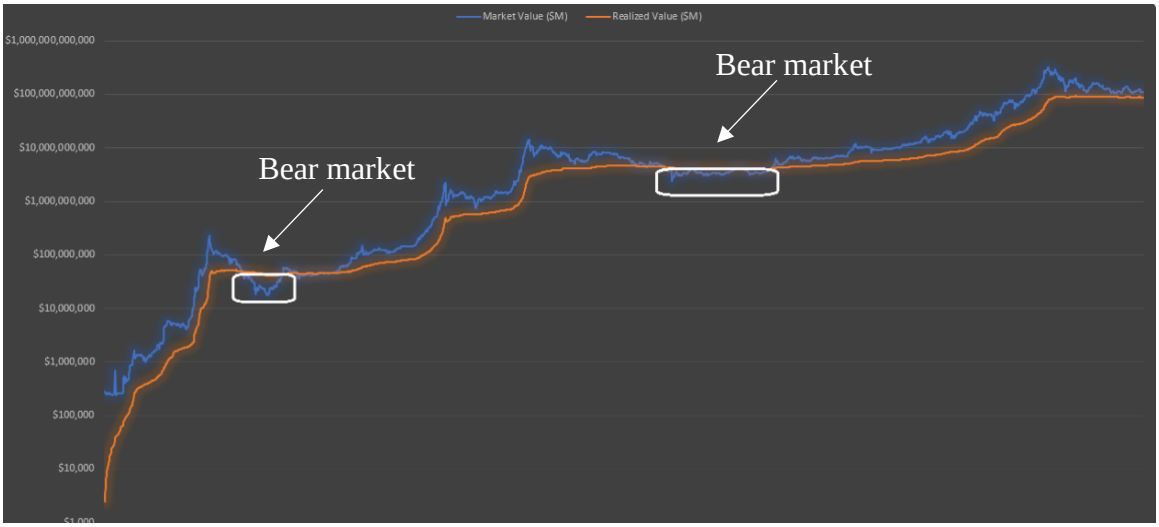
(Shirakashi 2019)

Fonte: https://medium.com/unconfiscatable/introducing-sopr-spent-outputs-to-predict-bitcoin-lows-and-tops-ceb4536b3b9

5. *Market-Value-To-Realized-Value (MVRV)*

L'indice MVRV è calcolato semplicemente come la divisione tra la capitalizzazione di mercato di un *asset* in un dato momento e il suo prezzo realizzato, ossia il valore medio a cui ciascuna unità di quell'*asset* si è mossa l'ultima volta (ossia l'ultima transazione di un blocco) sul relativo *network*. (Murad Mahmudov 2018)

Capitalizzazione di mercato (blu) ed indice MVRV (arancione) di Bitcoin a confronto



Fonte: https://medium.com/@kenoshaking/bitcoin-market-value-to-relized-value-mvrv-ratio-3ebc914dbaee

L'indice MVRV è utile a spiegare le fasi di boom & bust del mercato delle cripto-valute: fasi, queste, che sono trainate da un "meccanismo di gossip virale" e che portano rispettivamente ad una espansione e contrazione della rete. L'indice MVRV riesce quindi a ponderare l'esuberanza del mercato delle cripto-valute: in termini di analisi tecnica, la metrica serve a stabilire il *fair value* di una cripto-valuta, il quale è calcolato a partire dalle fasi in cui il prezzo non subisce eccessive variazioni e rimane stabile; sotto questo punto di vista si può quindi considerare il funzionamento dell'indice MVRV al pari di quello di una media mobile: quando la capitalizzazione di mercato scende al di sotto dell'indice si è davanti a situazioni di mercato *bear*, generalmente caratterizzati da *panic selling* (questi sono i migliori momenti in cui accumulare attività), viceversa, quando il valore di mercato rimane al di sopra di quello identificato dal rapporto MVRV significa che il mercato è ottimista riguardo l'andamento prezzo dell'*asset*, identificando situazioni di mercato *bull*, molto più durature nel tempo (come si evince dal grafico sovra riportato).

Quando si tratta di *security tokens* i modelli di valutazione sono più tradizionali in quanto si tratta di titoli finanziari, che forniscono una serie di diritti finanziari agli investitori come azioni, dividendi, diritti di partecipazione agli utili, diritti di voto, ecc. (Koffman 2018).
Quindi, i modelli di valutazione dei titoli tradizionali, come la valutazione DCF, i metodi relativi (ad esempio, P/E) o il modello di determinazione del prezzo delle opzioni, possono essere applicati alla valutazione dei *security tokens*:

1. ***Crypto-CAPM***
   Il modello a quattro fattori del *Capital Asset Pricing Model* (*CAPM*), sviluppato da Mark Carhart nel 1995, tenta di spiegare la persistenza a breve termine nei rendimenti azionari dei fondi pensione, aggiungendo al modello a tre fattori di Fama-French, l'elemento del *momentum*, ossia la tendenza di un prezzo di un'azione a continuare a crescere se già sta salendo, viceversa se già sta scendendo: se la media dei prezzi nei 12 mesi precedenti è positiva, allora il titolo è caratterizzato da fattore *momentum*. A questo si aggiungono gli altri tre fattori già considerati nel modello di Fama-French, ossia:
   a) Un premio per il rischio dato dalla differenza tra il rendimento del portafoglio ed il rendimento dei titoli privi di rischio.
   b) L'eccesso di rendimento storico di azioni a bassa capitalizzazione di mercato rispetto a *stock* di più grandi dimensioni.
   c) L'eccesso di rendimento storico di azioni ad elevato rapporto *book-to-market* rispetto a titoli a più basso indice.

   Il modello del *CAPM* pensato da Carhart può essere efficacemente adottato per lo studio del prezzo di *security tokens* se venissero considerati i seguenti fattori:
   - Momentum;
   - Fattore di liquidità del *token* (misurato dal volume di *trading* o attraverso gli *spread bid/ask*);

- Frizioni nello scambio e nella detenzione del *token* (date dalla qualità del *wallet* o dalla convenienza all'acquisto, etc.)
- Dimensioni/forza della comunità su cui si appoggia il *token*;
- Valore (dato dall'indice NVT);
- Fattore "FOMO" (ossia la diffida verso la multicollinearità con gli altri fattori);
- Incertezza politica/economica globale.

2. ***Discounted Cash-Flows* (*DFC*)**

   Il metodo dei flussi di cassa attualizzati è applicabile esclusivamente ai *security tokens* in quanto, chi li possiede, ha diritto a percepire anche diritti patrimoniali come la partecipazione agli utili/dividendi o agli aumenti di capitale sociale. Inoltre, i *security tokens* permettono a chi li possiede di percepire una rendita costante direttamente correlato col valore intrinseco dell'*asset.*

3. ***Approccio di valutazione comparabili***

   Nella valutazione azionaria tradizionale, i rapporti finanziari e i multipli di società comparabili possono essere utilizzati per ricavare i prezzi delle azioni di una società target. Possiamo applicare questo approccio agli *assets* crittografici?

   Sostituendo metriche tradizionali come l'*Enterprise Value/EBITDA*, l'*Enterprise Value/Sales* e altre ancora con metriche adatte ai *tokens*, tra cui l'indice *NVT*, sarà possibile attuare un approccio di valutazione *multi-token*.

2.6 APPLICAZIONI DI FINANZA DECENTRALIZZATA

Per finanza decentralizzata, o *Decentralized Finance* (*De-Fi*) si intende quell'ecosistema di applicazioni decentralizzate (*DApps*[34]) finanziarie costruite sfruttando sia la tecnologia *blockchain* di seconda o terza generazione, sia il *WEB3*[35], ossia quell'insieme di protocolli che rendono possibile una interconnessione dei dati tra varie piattaforme, piuttosto che essere archiviate in *repositories* centralizzate e resi disponibili a pagamento.

La finanza decentralizzata ha l'obiettivo di creare dei servizi finanziari *open-source*, senza permessi, trasparenti ed alla portata di chiunque senza ricorrere ad Autorità centrali. Gli utenti potranno interagire su *networks P2P* e su piattaforme decentralizzate (*DApps*), la cui modularità del *framework* permette l'interoperabilità tra varie applicazioni, creando dei nuovi mercati, nuovi prodotti e nuovi servizi finanziari.

I potenziali utilizzi delle applicazioni di *De-Fi* riguardano:

- **Mercati**: l'uso della *blockchain* permette agli utenti di beneficiare di un sistema di validazione a costi ridotti e crittograficamente sicuro, che metta istantaneamente in contatto un più vasto pubblico di soggetti in *surplus* finanziario e soggetti in *deficit* pur mantenendo un livello di fiducia tale da garantire un realistico funzionamento del mercato.
- **Banche ed offerta di moneta**: Poiché le applicazioni DeFi sono, per definizione, applicazioni finanziarie, i servizi bancari e monetari ne sono un ovvio caso d'uso. Questi possono includere l'emissione di *stablecoin*, mutui e assicurazioni:
    a. Poiché i prezzi delle cripto-valute possono variare rapidamente gli *StableCoins* potrebbero essere adottati per un uso quotidiano delle prime in veste di denaro digitale che non venga emesso e regolato da un'Autorità centrale.
    b. Soprattutto a causa del numero di intermediari che devono essere coinvolti, il processo per ottenere un mutuo è costoso e richiede tempo. Con l'uso degli *smart contracts*, le spese legali e di sottoscrizione possono essere ridotte in modo significativo.
    c. L'assicurazione attraverso la *blockchain* potrebbe eliminare la necessità di intermediari e allo stesso tempo consentire la distribuzione del rischio tra molti partecipanti. Ciò potrebbe comportare premi inferiori con la stessa qualità del servizio.

[34] Per *DApp* (*Decentralized App*) si intende quell'applicazione si appoggia ad una rete *blockchain*. Le tre caratteristiche di una applicazione decentralizzata sono le seguenti: ***Open-source***, chiunque può leggere, verificare ed implementare il codice sorgente, nel rispetto del protocollo di pubblicazione; ***Decentralizzate***, i nodi del *network* sono gli unici a garantire il funzionamento dell'App, senza ricorrere a nessuna autorità centrale; ***Crittograficamente sicure***, tutti i dati vengono raccolti e mantenuti all'interno di una *blockchain* che sfrutta le proprietà della crittografia asimmetrica.

[35] Poiché le reti Web 3.0 opereranno attraverso protocolli decentralizzati saranno interoperabili, perfettamente integrate, automatizzate tramite *smart contracts* ed utilizzate per alimentare qualsiasi cosa, dalle micro-transazioni all'archiviazione di file di dati su *repositories* resistenti alla censura e alla condivisione con applicazioni, come FileCoin, per cambiare completamente ogni condotta aziendale e gestire la propria attività. L'attuale serie di protocolli *De-Fi* è solo la punta dell'*iceberg*.

Esiste una molteplicità di servizi resi possibili dalle applicazioni di finanza decentralizzata. Di seguito ne verranno riportati i principali:

DECENTRALIZED EXCHANGES & AUTOMATED MARKET MAKERS

Le piattaforme di scambio decentralizzate sono *DApps* che sfruttano una connessione *P2P* per eseguire operazioni di *swapping* tra cripto-valute: un protocollo molto interessante è il c.d. *Atomic Swap*, ossia un sistema di *cross-chain trading* che permetta di effettuare una conversione istantanea tra due *assets* crittografici differenti (come Bitcoin e Litecoin) che si appoggiano rispettivamente a *blockchains* distinte. L'*Atomic Swap* si basa sia su di un sistema di crittografia asimmetrica per la creazione di due *wallets* crittografati contenenti valuta, sia su di un contratto *Hash Timelock*[36] che permetta l'esecuzione dello scambio tra gli indirizzi dei *wallets* in completa sicurezza. Altri protocolli per il *P2P swapping* sono P2PTradeX e 0x.
Le transazioni su una piattaforma *DEX* possono avvenire *on-chain* o *off-chain*:

- Transazioni *on-chain*: ogni ordine viene registrato su un'unica *blockchain*. Questo è il metodo più trasparente in quanto non c'è bisogno di appoggiarsi a terze parti per inoltrare gli ordini, grantendo così il maggior grado di decentralizzazione. Tuttavia, il metodo *on-chain* è il più costoso in quanto l'operazione di registrazione della transazione sulla *blockchain* richiede il pagamento di alcune commissioni[37] ai *miners*. Il problema che comunemente viene associato al modello *on-chain* è il *front-running*, ossia una situazione in cui un *insider runner* è al corrente di una transazione in fase di registrazione e compie scambi prima che questa venga elaborata, beneficiando di un'informazione che non è nota (ancora) al pubblico. Un altro tipo di attacco può essere rappresentato dai *miners* che, al corrente delle transazioni in corso di approvazione, aggiungano le loro transazioni alla *blockchain* prima delle altre.

- Transazioni *off-chain*: ordini che si verificano su una determinata rete *blockchain*, che possono essere successivamente segnalate o raggruppate insieme su di un *book* controllato e gestito da un'Autorità centrale prima di essere inoltrate alla *blockchain* principale. Diventa di fondamentale importanza il concetto di *2nd-layer chain*, ossia un *framework* di protocolli che tentano di risolvere il problema della scalabilità di una *main blockchain* (come quella di Bitcoin o di Ethereum) che non riesce a processare migliaia di transazioni al secondo (*TPS*, o *Transactions Per Second*). Esempi di *2nd-layer chains* sono Bitcoin Lightining Network ed Ethereum Plasma: il primo sfrutta i c.d. *state channels*, ossia canali di

[36] Un *Hash Timelock Contract* (*HTC*) è un particolare tipo di *smart contract* che si basa su due funzioni:
1. **Hashlock**, ossia una funzione che limita la spesa di fondi fino a quando una certa informazione parziale non venga resa pubblica (come prova crittografica). Tale prova può anche essere indicata come la pre-immagine dell'hashlock. La pre-immagine è semplicemente l'informazione parziale che viene utilizzata per generare l'hashlock e per sbloccarne successivamente i fondi.
2. **Timelock**: è una funzione che limita la spesa di fondi fino a un tempo specifico (o altezza del blocco) in futuro. Può essere ottenuto in Bitcoin, ad esempio, utilizzando funzioni come *CheckLockTimeVerify* o *CheckSequenceVerify*.

[37] Il c.d. *gas price* di Ethereum.

comunicazione bidirezionali tra utenti e nodi di una rete per elaborare le transazioni e riportarle sulla *main blockchain*; il secondo sfrutta il concetto di *sidechains*, ossia *blockchains* di dimensioni contenute, a difficoltà limitata, che si legano alla *main blockchain* secondo una struttura a *Merkle tree*. Il beneficio della metodologia *off-chain* è che non c'è necessità di eseguire nessun *hard fork* della *main blockchain* garantendo comunque l'elaborazione di un alto volume di transazioni, senza appesantire la catena principale.

Un *Automated Market Maker* (o *AMM*) è un protocollo di scambio decentralizzato (*DEX*) che non si appoggia ad un *order book*[38] come nel caso di operazioni di *P2P swapping*, ma crea automaticamente un mercato ogni qualvolta venga inoltrata un'offerta: le transazioni, infatti, non richiedono la presenza di una controparte in quanto lo scambio avviene tra utenti e *smart contracts* (l'operazione prende appunto il nome di *P2C swapping*) attingendo alle risorse di una *pool* di liquidità creata ed alimentata da utenti (c.d. *liquidity providers*) che vi depositano cripto-valute e/o *tokens* ricevendo in cambio delle commissioni sulle operazioni che avvengono nella loro *pool* (Uniswap, per esempio, applica una *fee* pari allo 0,3% delle operazioni di *trading*).
Esistono due rischi connessi con l'*Automated Market Maker*:

1. **Rischio di *slippage***, ossia la differenza tra il prezzo di esecuzione di un ordine dal prezzo di apertura inserito nella offerta. Questo rischio può essere molto elevato nel caso in cui l'offerta sia di dimensioni notevoli: più liquidità è presente sulla *pool*, più contenuto sarà lo *slippage* di tale offerta.
2. **Rischio di perdita non-permanente**: ossia la perdita derivante da un cambiamento nel prezzo dei *tokens*/cripto-valute dopo il loro deposito nella *pool* di liquidità. La perdita non-permanente è relativamente trascurabile quando il rapporto di prezzo tra i due *assets* si mantiene entro un *range* ridotto. Per questo motivo, gli *AMM* funzionano al meglio quando gli *asset* depositati sono *StableCoins* o *Asset Backed Tokens*. Qualora, invece, il rapporto subisca una variazione notevole, i fornitori di liquidità potrebbero guadagnare di più semplicemente conservando i *tokens* invece che di aggiungerli in una *poo*l. Nonostante ciò, le *pools* di Uniswap come ETH/DAI, che sono piuttosto esposte alla perdita non-permanente, sono redditizie grazie alle commissioni di *trading* accumulabili.

YIELD FARMING

Per *Yield Farming* si intende un'operazione attraverso cui si generano guadagni in base all'ammontare di *tokens* e/o cripto-valute depositate in una *pool* di liquidità. Al contrario degli *AMM*, lo *yield farming*, anziché pagare commissioni ai *liquidity providers* sulla base del volume di operazioni effettuate nella loro *pool*, concede loro *tokens* di nuova emissione relativamente all'ammontare di depositi in un'unica *pool*. Lo *yield farming*, in questo senso, è molto simile all'attività di *staking*.
I fondi depositati sono solitamente *StableCoins* ancorati all'USD.

[38] Un *order book* è un elenco di ordini di acquisto e di vendita attualmente aperti per un asset, organizzati per prezzo.

Una metrica di verifica della salute di un'applicazione di *yield farming* è il c.d. *Total Value Locked*[39] (o *TVL*) il quale misura il livello di depositi di una *pool* di liquidità: più è grande l'ammontare di depositi, più attività di *yield farming* è in corso quindi più sicura è quella piattaforma.

I ricavi dello *yield farmer* possono essere calcolati utilizzando metriche tradizionali come il rendimento percentuale annuo il quale tiene conto dell'interesse composto, ossia il rendimento derivante dal reinvestimento continuo dei profitti per generare maggiori ritorni a scadenza. Tuttavia, la pratica dello *yield farmer* è molto difficile nella sua applicazione in quanto richiede una profonda conoscenza dei mercati ed il possesso di grandi quantitativi di valuta (c.d. *whales*) per attuare strategie *ad-hoc* che comunque possono attirare altri *yield farmers* finendo per annullare, così facendo, qualsiasi opportunità di guadagno di breve termine; ecco perché i rendimenti fluttuano rapidamente e spesso riguardano ingenti somme di danaro[40].

L'attività di *yield farming* è comunque rischiosa anche per i *liquidity providers* in quanto, spesso, i protocolli d'implementazione dell'applicazione sono stati sviluppati da *teams* amatoriali e con *budget* ridotti, rendendo l'intera struttura vulnerabile a *bugs* e ad attacchi informatici che possono portare alla completa perdita de depositi.

DECENTRALIZED AUTONOUMUS ORGANIZATIONS

Una Organizzazione Autonoma Decentralizzata o (*DAO*, in inglese) è un'azienda il cui sistema di *governance* si appoggia interamente sull'esecuzione di *smart contracts*: in tali forme di *governance*, non esiste una struttura gerarchica, bensì le decisioni sono prese da algoritmi che lavorano su informazioni e dati esterni ed eseguono automaticamente comandi generando *records* pubblici che vengono registrati sulla *blockchain*. Le regole della *DAO* vengono implementate durante le assemblee ordinarie con voto a maggioranza: le proposte che ricevono più voti vengono "tokenizzate" ed archiviate sulla *blockchain*, implementando il codice sorgente dell'applicazione. Questo processo garantisce trasparenza e fornisce un *set* più ampio di informazioni con cui l'algoritmo può lavorare al verificarsi di determinati fattori esogeni.

I soci di una *DAO* non sono legati da alcun vincolo contrattuale, bensì sono mossi esclusivamente da un obiettivo comune e da incentivi di diversa natura: solitamente la partecipazione al capitale sociale avviene attraverso l'emissione, tramite *STO* o *IEO*, di *security tokens* che garantiscono ai loro proprietari diversi diritti amministrativi/patrimoniali all'interno dell'azienda emittente.

In una *DAO* nessuna autorità può prendere il controllo una volta che il protocollo sia stato distribuito: questo sia garantisce la cooperazione, sia contribuisce ad allineare gli obiettivi di diversi attori aziendali, riducendo il conflitto d'interessi *principal*/*agent.*

Tre sono le problematiche che una Organizzazione Autonoma Decentralizzata si trova a dover affrontare:

---

[39] Una piattaforma on-line che si occupa di misurare questo indice è Defi Pulse https://defipulse.com/.

[40] Basti pensare che *Chef Nomi*, lo sviluppatore della piattaforma *DEX SushiSwap* in una settimana dall'apertura della piattaforma aveva già ottenuto più di 14 milioni di dollari in Ethereum. https://decrypt.co/41547/sushiswap-chef-nomi-gives-back-14-million-ethereum

1. Problema legale: Le *DAO*, per loro natura, non hanno confini geografici per questo il panorama normativo è completamente incerto e frammentato.
2. Attacchi informatici: le caratteristiche uniche di una *DAO* sono l'autonomia e la decentralizzazione, tuttavia questi elementi possono generare notevoli problemi in termini di sicurezza informatica, dati anche dalla modularità dei sistemi in essa compresi che rischierebbero di diventare così dei *Single Point Of Failure*.
3. L'effettiva decentralizzazione: La *DAO* può consentire a un più vasto pubblico di partecipare all'attività di impresa, tuttavia il protocollo che riporta le regole di *governance* rimarrà sempre un elemento di forte centralità, riducendo la partecipazione aperta.

Fun Fact: una delle prime *DAO* fu implementata da Ethereum nel 2016, con il nome di "*The DAO*", per la costituzione di un fondo di rischio autonomo. Le quote di partecipazione al fondo erano rappresentate dai *DAO tokens* che vennero distribuiti per mezzo di una ICO arrivando a raccogliere, nei soli primi giorni, un capitale pari a circa $165 mln. A poco tempo dal lancio della ICO, The DAO fu vittima di uno dei più famosi attacchi *hacker* della storia delle cripto-valute, arrivando a prosciugare circa un terzo ($55 mln) dei fondi raccolti. Questo attacco portò Ethereum ad eseguire un *hard fork* della *blockchain* in due catene: la prima in cui le transazioni fraudolente sono state annullate, la seconda in cui si è preferito mantenere l'immutabilità della *blockchain* (seguendo il principio "*Code is Law*"), lasciando quindi intatte le transazioni fraudolente: questa *blockchain* è chiamata, adesso, Ethereum Classic.

NFT & LA CRIPTO-ARTE

I *Non Fungible Tokens* sono *security tokens* unici, non-intercambiabili tra loro, creati utilizzando gli *standard* ERC-721 ed ERC-1155 (quest'ultimo, più recente, permette di raggiungere un maggior livello di standardizzazione dell'emissione del *token*, garantendo un più alto grado di interoperabilità che va a beneficiare, in ultima istanza, l'utente finale). Nessun *NFT* può essere trasferito o replicato senza il permesso del proprietario e inoltre possono essere scambiati su mercati specifici come OpenSea o su case d'asta, come Christie's, che ne formulano il prezzo in base alla loro domanda. Gli *NFT* possono essere anche rappresentare porzioni di *assets* reali che vengono *tokenizzati* e scambiati in ambienti del tutto digitali

Gli NFT possono essere utilizzati dalle *DApps* per emettere elementi digitali unici e collezionabili. A tal riguardo molto interessante è lo sviluppo che questa nuova tecnologia sta avendo in ambito video-ludico: sempre più artisti, infatti, stanno adottando un formato digitale per la pubblicazione dei propri lavori proprio per la possibilità di associare a questi un *token* non fungibile che ne garantisca l'originalità ed autenticità durante un'asta. Piattaforme come Verisart[41] si occupano della certificazione di lavori audio-visivi digitali.

[41] Per maggiori informazioni controllare la pagina sorgente di Verisart al seguente link: https://verisart.com/

CAPITOLO 3. CBDC: IL FUTURO DELLA MONETA?

Negli ultimi anni, l'avvento delle cripto-valute e dei *tokens* ha rivoluzionato le fondamenta della finanza tradizionale, creando non solo sistemi di pagamento alternativi alla moneta a corso legale, ma costruendo degli apparati digitali altamente innovativi, capaci di tracciare e validare migliaia di transazioni virtuali in un orizzonte temporale infinitesimale senza ricorrere all'intermediazione di nessuna Autorità preposta. La rivoluzione del *FinTech* (o *Financial Technology*), avviatasi con il lancio di Bitcoin nel 2009, è stata sicuramente alimentata dalle innovazioni in campo informatico e tecnologico, le quali hanno sollecitato un maggior numero di utenti sia a fruire più soventemente di servizi digitali, come i sistemi di pagamento virtuali, sia a valutare differentemente le proprie scelte di portafoglio in termini di risparmio ed investimento.

Tuttavia, se da un lato è vero che la tecnologia dietro le cripto-valute è ormai consolidata ed empiricamente efficace, dall'altro è pur vero che esistono innumerevoli fattori di incertezza che possono impattare negativamente sul corretto funzionamento della stessa e, conseguentemente, degli *assets* che la adottano. Questi fattori possono essere considerati sia dal punto di vista tecnico/operativo, considerando principalmente la tecnologia di funzionamento sottostante alla cripto-valuta, ossia: attacchi *hacker*, *bug* del sistema, sovraccarico dei *servers*, *Single Points of Failure*, etc.; sia dal punto di vista dei mercati entro cui tali *assets* vengono scambiati, si identificano allora rischi quali: alta volatilità del tasso di cambio, insufficienza dell'offerta, eccessiva deflazione, incapienza delle *pool* di liquidità, etc., finendo per incrementare ulteriormente la loro componente speculativa ed ampliando le asimmetrie informative tra gli utenti. I mercati delle cripto-valute, infatti, sono altamente inefficienti, dato che la componente irrazionale è la variabile *driver* dell'eccessiva volatilità dei prezzi, in questo modo si riduce ancora di più la possibilità di adottare tali sistemi come nuovi strumenti di pagamento: il sogno di Nakamoto sembra sempre di più irrealizzabile.

In questo panorama, nuova spinta viene data dall'introduzione degli *StableCoins*, ossia *security tokens* in grado di contenere le fluttuazioni del tasso di cambio di una o più valute. Per garantire questa caratteristica, gli emittenti di *StableCoins* detengono portafogli di attività alternative, quali cripto-valute o titoli, a valere sui quali gli *StableCoins* possono essere rimborsati e/o scambiati. Questo sistema, se da un lato può concorrere al progresso nei sistemi dei pagamenti rendendo più efficienti, per esempio, le transazioni trans-frontalieri, dall'altro presenta indubbi rischi, tra cui il rischio di liquidità, in quanto manca qualsiasi garanzia circa il valore di rimborso da parte degli emittenti i quali, in una situazione di "corsa ai (cripto)sportelli", si troverebbero costretti a liquidare gran parte delle attività alternative in possesso, innescando una crisi finanziaria. Inoltre, i rischi relativi ad una gestione inefficiente dello *StableCoin*, ad un malfunzionamento dell'algoritmo o ad un attacco informatico potrebbero impattare negativamente sul corretto funzionamento della valuta stessa. Vero è, comunque, che la dimensione del circolante di *StableCoins* è assai ridotta se confrontata con quella della moneta *fiat*, per di più gli utenti continuano a percepire quest'ultima come moneta superiore quindi, in situazioni di rischio imminente, secondo la legge di Gresham gli *StableCoins* non

produrrebbero rilevanti effetti macroeconomici e verrebbero anzi automaticamente tagliati fuori dal mercato dei sistemi di pagamento.

In questo contesto, le Autorità centrali internazionali, come la BCE, si stanno muovendo per adeguarsi alla trasformazione dei sistemi di pagamento attuata dal *FinTech* e dalla comparsa delle cripto-valute, promuovendo la concorrenza, l'innovazione, riducendo i rischi ed adattando il quadro normativo di conseguenza. Per raggiungere questi obiettivi, sempre più Istituzioni regolatrici si stanno interessando alla costituzione di una *CBDC*, o *Central Bank Digital Currency* (trad. Moneta Digitale della Banca Centrale) rendendo disponibile ai cittadini una moneta a corso legale sotto forma digitale, esente da costi, di facile utilizzo, affidabile e priva di rischi e che stimoli l'innovazione nel sistema dei pagamenti e la modernizzazione dell'intera economia.

3.1 OBIETTIVI & OPPORTUNITÀ

Per *Central Bank Digital Currency* si intende una moneta diffusa esclusivamente in formato digitale e a corso legale, in quanto viene emessa e regolata da un'Autorità centrale, come la Banca Centrale Europea o la *Federal Reserve*, e accessibile a qualsiasi cittadino o impresa. La *CBDC* non deve sostituirsi alla moneta in contante ma deve porsi come obiettivo il raggiungimento delle seguenti quattro caratteristiche:

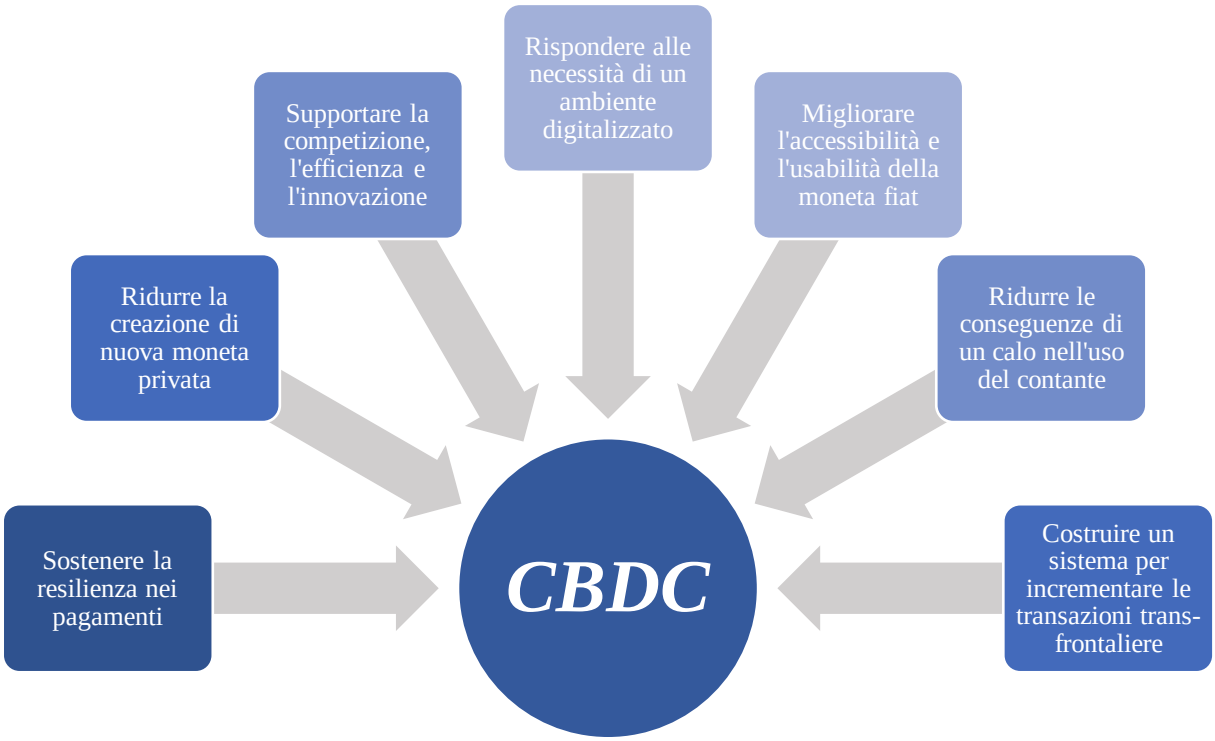
1. **Efficienza**: l'efficienza è strettamente legata alla comodità del sistema di pagamento e alla somiglianza con i pagamenti in contanti. La decisione prioritaria è quella di delineare l'infrastruttura e i ruoli della Banca Centrale e degli altri intermediari finanziari coinvolti (ad es. Banche Commerciali, PSP, ecc.). La scelta più critica da fare è quella di delineare il ruolo operativo della Banca Centrale e delle Banche Commerciali e di soppesare la collaborazione con il settore privato per garantire agli utenti un efficiente servizio di pagamento.

2. **Accessibilità**: La scelta progettuale della *CBDC* deve essere basata principalmente sull'accessibilità del sistema in modo che sia sviluppata nel modo più inclusivo possibile e comunque in grado di tutelare la *privacy* degli utenti, proprio come nelle odierne transazioni in contanti. Si delineano così due modelli distinti di accessibilità alla infrastruttura: il primo metodo basato sugli *accounts*, il secondo sui *tokens*. Questi due modelli devono rispettivamente essere analizzati per comprendere quale dei due meglio soddisfi le necessità della *CBDC*.

3. **Resilienza**: la resilienza e la robustezza delle operazioni di rete è una dimensione chiave che deve essere presa in considerazione in quanto si deve decidere se basare la *CBDC* su infrastrutture bancarie tradizionali o su una tecnologia decentralizzata come la *blockchain*. Tale scelta influenza profondamente la struttura e la gestione della *governance* dell'infrastruttura, che potrebbe essere centralizzata o decentralizzata.

4. **Interoperabilità**: tale dimensione deve essere presa in considerazione al fine di garantire la possibilità di interazione tra diversi sistemi di *CBDC*, quindi impatta un livello decisionale di livello superiore per la progettazione della *CBDC* stessa.

Il raggiungimento di queste caratteristiche obiettivo garantirebbe alla *CBDC* di sfruttare appieno le seguenti opportunità:



- **Sostenere la resilienza cibernetica ed operativa nei sistemi di pagamento tradizionali**: Seppure i sistemi di pagamento elettronici attuali siano efficaci ed efficienti, con la transizione che si sta verificando verso il digitale, l'uso di carte di debito/credito, ossia l'unico mezzo di pagamento[42] per *l'e-commerce*, sta divenendo sempre più intensivo: questa eccessiva dipendenza verso un singolo sistema di pagamento elettronico potrebbe ridurre notevolmente la resilienza a livello sistematico.

  La *CBDC* potrebbe sia condurre ad una diversificazione dei sistemi di pagamento *on-line* (dove il contante non può essere utilizzato), sia rappresentare un valido sostituto allo strumento delle carte di credito/debito qualora questo subisca un'inattesa interruzione (visto che è molto improbabile che si verifichino contemporaneamente delle disfunzioni su entrambe le infrastrutture). Tuttavia, la *CBDC* potrebbe continuare ad essere vulnerabile a situazioni di interruzione di elettricità su larga scala o di sovraccarico della rete, a meno che non venga sviluppata una funzionalità di pagamento *off-line*. *In extremis*, se la *CBDC* venisse ampiamente utilizzata, si porrebbe il rischio di concentrazione derivante da una riduzione della diversità delle opzioni di pagamento dato che questa andrebbe a sostituirsi ai sistemi già esistenti.

[42] Alcune aziende, come Amazon ad esempio, permettono a chi voglia acquistare prodotti sulla piattaforma on-line di pagare attingendo direttamente dal conto corrente, senza la necessità di dover utilizzare una carta di debito/credito.

- **Ridurre la creazione di nuova moneta privata**: la presenza da un lato di un sistema di regolamentazione e di controllo sulla gestione delle banche commerciali da parte delle Autorità centrali, dall'altro di una garanzia (o assicurazione) sui depositi[43], influisce positivamente sul sistema fiduciario nel suo complesso, riducendo al minimo sia il livello di rischio di liquidità che la banca deve sostenere, sia la possibilità che si verifichino situazioni di "corsa agli sportelli" con successiva liquidazione degli attivi di bilancio e conseguente esposizione al rischio di credito.

  Nel caso di emissione di monete "private", come le cripto-valute o gli *StableCoin tokens*, questo sistema di copertura sul rimborso non viene garantito in alcun modo. Per di più, seppure gli *StableCoins* riescano a contenere la volatilità delle cripto-valute a cui sono ancorati, in situazioni di pesanti fluttuazioni del tasso di cambio del sottostante anche il valore dello *StableCoin*, per quanto l'algoritmo riesca ad aggiustare e ponderare il rapporto con l'*asset* dipendente, ne risentirà negativamente, creando sfiducia in quanto gli utenti non saranno in grado di gestire correttamente la propria liquidità o adempiere ai propri obblighi di pagamento ed incoraggiandoli ad ripiegare su altri strumenti come il contante.

  La *CBDC*, essendo una moneta a corso legale e, quindi, garantita dalla Banca Centrale che, per sua natura, è priva di rischio, sarà un'*asset* necessariamente meno volatile dello *StableCoin token* e ancor meno delle cripto-valute, riducendo, come effetto collaterale, la domanda verso quest'ultime forme di moneta digitale.

- **Supportare la competizione, l'efficienza e l'innovazione**: Esistono opportunità di miglioramento per affrontare potenziali fallimenti del mercato nei servizi di pagamento esistenti. Per esempio: mentre i pagamenti con carta appaiono quasi istantanei per l'utente finale, il commerciante può attendere fino a tre giorni prima di ricevere i fondi. Anche se sono in corso sforzi significativi per migliorare ulteriormente i sistemi di pagamento esistenti, queste iniziative non riescono ancora a risolvere completamente tali problemi: una *CBDC* potrebbe eventualmente migliorare la velocità e l'efficienza dei pagamenti sia direttamente – offrendo un servizio di pagamento veloce ed efficiente per gli utenti – sia indirettamente – attraverso la creazione di un panorama di pagamenti più competitivo –.

  Una piattaforma *CBDC* ben progettata, robusta e aperta potrebbe consentire a un'ampia gamma di aziende di competere per offrire servizi di pagamento correlati alla *CBDC* e, soprattutto, innovare i servizi di pagamento che forniscono ai consumatori e le modalità con cui questi vengono integrati nell'economia digitale. In tal modo, l'introduzione del *CBDC* potrebbe sostenere la concorrenza sia sui costi che sulla qualità dei servizi di pagamento.

- **Rispondere alle necessità di un ambiente sempre più digitalizzato**: La prossima generazione di pagamenti dovrà supportare un'economia più digitale e consentire connessioni senza interruzioni tra i diversi servizi utilizzati sia dalle famiglie che dalle imprese.

[43] Il Fondo interbancario di tutela sui depositi garantisce una copertura sui depositi di ammontare inferiore agli €100.000.

La *CBDC* potrebbe infatti consentire alle transazioni di verificarsi in base a determinate condizioni, regole o eventi. Ci saranno molte potenziali applicazioni di queste funzionalità, inclusa l'integrazione con dispositivi fisici o applicazioni *Internet-of-Things* (*IoT*). Gli esempi potrebbero includere l'instradamento automatico dei pagamenti delle tasse alle autorità fiscali nel punto vendita, pagamento automatico delle azioni e dei dividendi direttamente agli azionisti o contatori elettrici che pagano i fornitori direttamente in base al consumo di energia. La *CBDC* potrebbe consentire l'uso di micropagamenti se esso consente di effettuare piccole transazioni a un costo inferiore rispetto a quanto avviene oggi. Ciò potrebbe aumentare il volume e la frequenza di questi pagamenti che porterebbe allo sviluppo di nuovi servizi che possono sfruttare questa capacità.

- **Migliorare l'accessibilità e l'usabilità delle monete *fiat***: Attualmente le famiglie e le imprese (non finanziarie) possono utilizzare solo denaro *fiat* sotto forma di banconote. La *CBDC* consentirebbe loro di detenere moneta a corso legale anche in formato elettronico ed usarlo per effettuare pagamenti. Ciò aumenterebbe la disponibilità e l'utilità della moneta della banca centrale, permettendo di venire utilizzato in una gamma molto più ampia di situazioni rispetto ai contanti fisici. La moneta *fiat* (contanti, riserve o potenzialmente la *CBDC*) svolge un ruolo fondamentale nel sostenere la stabilità monetaria e finanziaria agendo come una forma di denaro priva di rischi che fornisce il mezzo di regolamento definitivo per tutti i pagamenti di un'economia. Ciò significa che l'introduzione della *CBDC* potrebbe migliorare il modo in cui la Banca Centrale emette denaro e gestisce la stabilità finanziaria, fornendo una nuova infrastruttura di pagamento. Questo potrebbe avere una serie di vantaggi, compreso il rafforzamento della trasmissione delle manovre di politica monetaria producendo i suoi più ampi effetti sull'economia reale.
  Tuttavia, è comunque probabile che l'introduzione della *CBDC* porti a qualche forma di sostituzione con le forme di denaro attualmente utilizzate dalle famiglie e dalle imprese (ad es. contanti e depositi bancari). Se questa sostituzione fosse molto ampia, si genererebbe una riduzione del finanziamento delle banche commerciali, impattando negativamente sul livello di credito che le banche potrebbero fornire. Di conseguenza, CBDC deve essere attentamente progettato per gestire l'impatto sulla politica monetaria e sulla stabilità finanziaria.

- **Ridurre le conseguenze di un calo dell'uso del contante**: La liquidità fisica ha alcune caratteristiche uniche che andrebbero perse se i cittadini smettessero di utilizzarlo: il contante, ad esempio, offre un livello di *privacy* nelle transazioni che non è sempre disponibile con i sistemi di pagamento elettronico esistenti. La liquidità ha anche un ruolo importante nell'inclusione finanziaria: in un mondo in cui il contante diventa meno utilizzato, non vi è alcuna garanzia che l'attuale fornitura da parte del settore privato dei sistemi di

pagamento al dettaglio possa soddisfare le esigenze di tutti gli utenti, lasciando gli individui *underbanked*[44] particolarmente a rischio (Sveriges Riksbank (2018)).

Sebbene la *privacy* e l'inclusione finanziaria non rientrino direttamente nelle competenze della Banca Centrale, sono questioni importanti per la società nel suo insieme, di cui la Banca deve tenere conto: la *CBDC* potrebbe essere progettata in modo da proteggere la *privacy* degli utenti in misura maggiore rispetto ad alcuni sistemi di pagamento esistenti, fatto salvo il pieno rispetto di tutte le normative pertinenti, in particolare i requisiti antiriciclaggio. Una *CBDC* ben progettata può anche aiutare a promuovere l'inclusione finanziaria in un mondo sempre più digitale essendo accessibile a una gamma più ampia di persone, in formati diversi rispetto alle soluzioni del settore privato.

Comunque sia, per coloro che apprezzano la natura fisica del contante è improbabile che l'introduzione della *CBDC* influenzi il loro comportamento di pagamento, e quindi la *CBDC* probabilmente fungerà da complemento al contante piuttosto che da sostituto.

- **Costruire un sistema per migliorare le transazioni trans-frontaliere**: Per molti utenti, i pagamenti trans-frontalieri sono costosi, lenti e "opachi" (i mittenti potrebbero non essere in grado di sapere quando il pagamento verrà saldato ei destinatari non conosceranno gli addebiti che verranno detratti su un credito in entrata) (CPMI (2018)).

  Una *CBDC* può offrire un modo più sicuro per fornire migliori pagamenti trans-frontalieri: ad esempio, le Banche Centrali potrebbero essere in grado di collaborare collegare le *CBDC* nazionali in modo da consentire pagamenti transfrontalieri rapidi ed efficienti. Una *CBDC* nazionale individuale potrebbe essere progettato attorno a un insieme comune di *standard* intesi a supportare l'interoperabilità. Questo potrebbe abilitare Transazioni "atomiche" tra sistemi di *CBDC*: dove il trasferimento di *CBDC* in una valuta è collegato a un trasferimento di *CBDC* in un'altra valuta, in modo da garantire che ogni trasferimento avvenga se e solo se la controparte lo abbia effettivamente posto in essere.

3.2 L'ARCHITETTURA

La definizione della infrastruttura più adatta alla base della *CBDC* dipende principalmente dal ruolo che la Banca Centrake e gli altri intermediari finanziari vogliono assumere.

La principale differenza sottostante alle varie forme che una *CBDC* può assumere dipende sia da come la Banca Centrale si pone durante la filiera della raccolta dei dati e della loro archiviazione, sia dalle responsabilità operative di ciascun intermediario coinvolto.

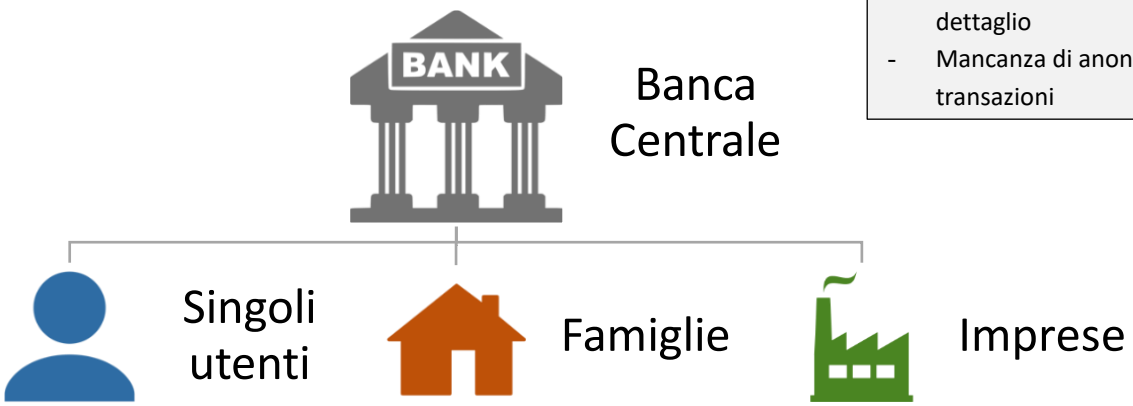
Le architetture per l'infrastruttura della *CBDC* sono:

Emissione diretta, **a due livelli** o **struttura ibrida**.

[44] Con il termine *underbanked* si fa riferimento a quegli individui o famiglie che dispongono di un conto corrente bancario ma che spesso fanno affidamento su servizi finanziari alternativi come vaglia postale, incasso di assegni e prestiti con anticipo sullo stipendio piuttosto che rivolgersi alle forme tradizionali di prestito e deposito.

1. **Emissione diretta**

- La Banca Centrale emette *CBDC* direttamente al pubblico
- La Banca Centrale si occupa delle operazioni di *KYC* e dei pagamenti al dettaglio
- Mancanza di anonimità durante le transazioni



Il modello basato sull'emissione diretta è il più semplice ed anche il più centralizzato in quanto è esclusivamente la Banca Centrale ad occuparsi sia di registrare tutte le transazioni al dettaglio, sia di controllare i bilanci di esercizio, sia di emettere la *CBDC* all'utente finale (rappresentato da singoli individui, nuclei famigliari ed imprese). Il modello ad emissione diretta, sebbene sia quello più semplice in quanto non considera il ruolo degli intermediari finanziari, è quello che pone le maggiori problematiche in termini di affidabilità, velocità ed efficienza dei sistemi di pagamento: il settore privato, infatti, potrebbe avere migliori capacità di gestione dell'infrastruttura come è dimostrato nelle reti di carte di credito odierne. Inoltre, pratiche di *Know-Your-Costumer*[45] (o *KYC*) e l'Adeguata Verifica della Clientela (*Due Diligence*[46]) potrebbero essere molto difficili da eseguire per la Banca Centrale in quanto richiederebbe investimenti massicci e sarebbe difficile concentrarsi sull'esecuzione di transazioni semplici e controllare al contempo l'emissione di più valuta.

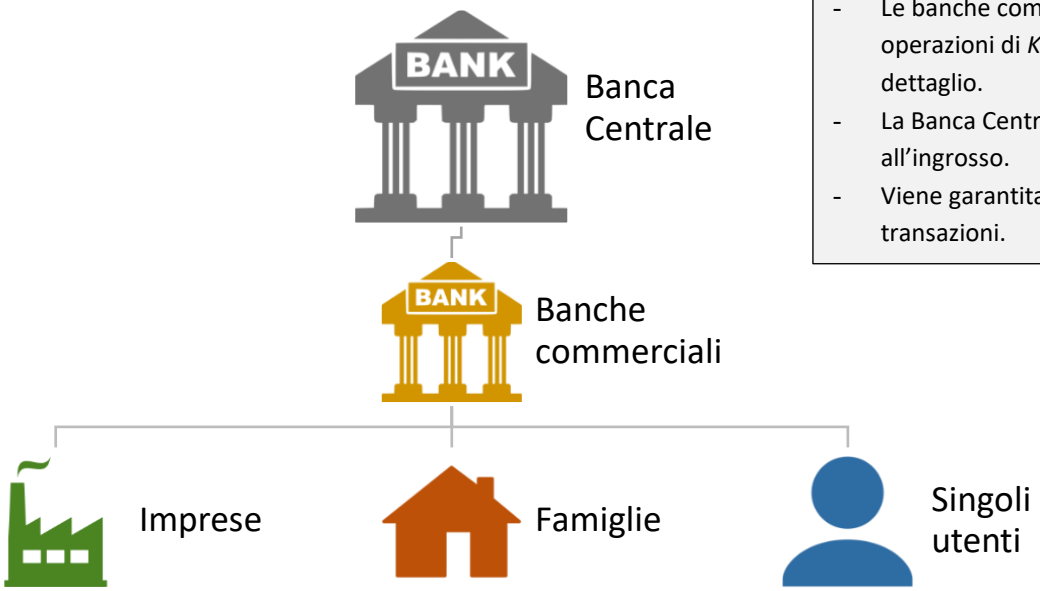
Un modello ad emissione diretta che prevede un minor impegno da parte della Banca Centrale potrebbe essere quello delegare le attività di *KYC* e *Due Diligence* al settore privato, continuando comunque a svolgere le funzioni *core*.

[45] Il *KYC*, acronimo di *Know Your Customer* (lett.: "conosci il tuo cliente"), è l'insieme di procedure che devono essere attuate da alcuni istituti e professionisti per obbligo di legge. Queste procedure servono per acquisire dati certi e informazioni sull'identità dei loro utenti e clienti.
Le procedure *KYC*, come si è detto, costituiscono obbligo di legge e sono solo una parte degli adempimenti normativi dettati dalle più ampie direttive europee antiriciclaggio

[46] Le informazioni per l'Adeguata Verifica della Clientela (*Customer Due Diligence*) comprendono una serie di dati e notizie, come le generalità del cliente, che servono alla banca per stimare quali rischi possono derivare dalle operazioni finanziarie eseguite per conto dei clienti.

2. **Emissione a due livelli**:

- La Banca Centrale emette *CBDC* alle banche commerciali.
- Le banche commerciali si occupano delle operazioni di *KYC* e dei pagamenti al dettaglio.
- La Banca Centrale si occupa dei pagamenti all'ingrosso.
- Viene garantita la p*rivacy* durante le transazioni.

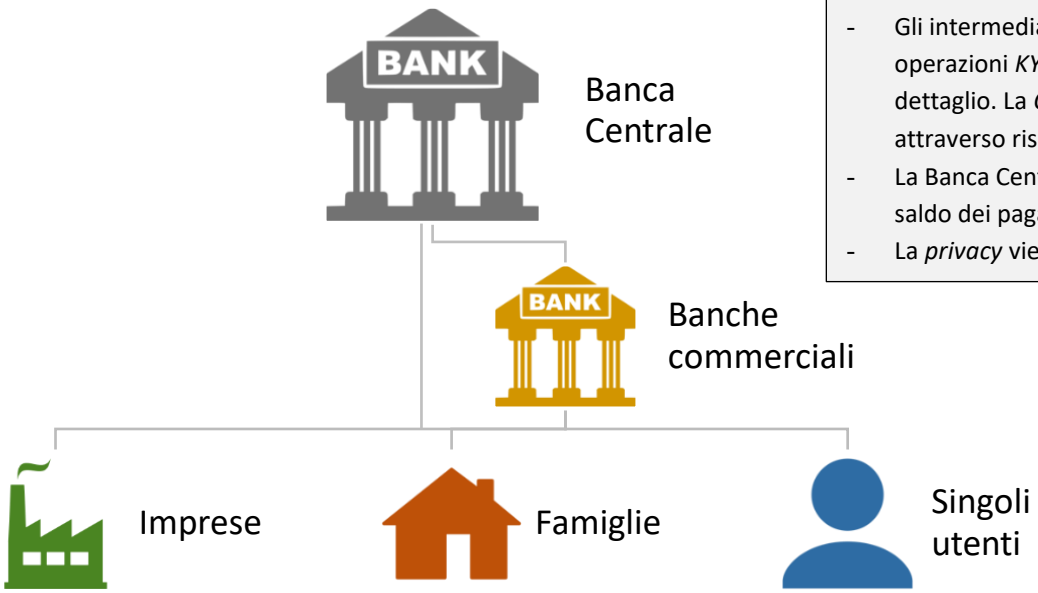


Il modello di emissione a due livelli prevede la presenza di intermediari finanziari. Questo modello presenta indubbi vantaggi in quanto la responsabilità connessa con le operazioni di interfacciamento con la clientela viene distribuita dalla Banca Centrale sugli intermediari finanziari sottostanti. Inoltre, la presenza del settore privato renderà l'infrastruttura molto più efficiente, da un lato creando una più vasta gamma di *touch-points* con una clientela che verrà sempre più *targettizzata* al fine di individuare le *personas* a cui rivolgersi con le proprie strategie; dall'altro innovando continuamente l'offerta per aggiudicarsi e per mantenere una quota sempre più rilevante di mercato.

Il modello, sebbene rispecchi fedelmente la realtà, è quello che pone il maggior freno all'operatività della Banca Centrale in situazioni di stress finanziario e di insolvenza del Settore Privato. Per questa ragione, il modello di emissione a doppio livello dovrebbe introdurre un'adeguata copertura sui depositi di *CBDC*.

3. **Modello ibrido**

- La *CBDC* è un'obbligazione che la Banca Centrale ha verso gli utenti finali;
- Gli intermediari si occupano sia delle operazioni *KYC*, sia dei pagamenti al dettaglio. La *CBDC* si crea quindi anche attraverso riserve.
- La Banca Centrale verifica puntualmente il saldo dei pagamenti *retail* e *wholesail*.
- La *privacy* viene garantita.



Il modello ibrido combina, come suggerisce il nome, gli elementi chiave dei modelli presentati in precedenza. In questo modello, infatti, da un lato la responsabilità circa la soddisfazione dei rimborsi di *CBDC* è rimessa in capo alla Banca Centrale, dall'altro è comunque presente la partecipazione di Istituzioni Private a supporto dell'operatività del sistema. L'elemento chiave di questo modello risiede nel fatto che tutta la *CBDC* emessa sull'economia può essere assimilata ad un'obbligazione che la Banca Centrale ha in essere direttamente con il cliente finale che la detiene: in questo modo non c'è alcuna necessità di istituire un sistema di copertura per rifugiarsi dal rischio di liquidità in quanto la Banca Centrale può liberamente trasferire in brevissimo tempo il rapporto che l'utente abbia in essere con un istituto privato in grave dissesto finanziario ad un altro sano che permetta di disporre della propria liquidità con continuità, efficacia ed efficienza. È quindi necessario che la Banca Centrale sia in grado di mantenere una copia aggiornata sia di tutto il saldo al dettaglio e all'ingrosso, sia del merito di credito di ogni singolo intermediario che operi nel sistema. Il modello ibrido può essere in grado di garantire una maggiore resilienza rispetto agli altri modelli, beneficiando al contempo della partecipazione del Settore Privato che rende più efficiente l'operatività della rete e assolve le responsabilità della Banca Centrale di interfacciarsi con il pubblico *retail*.

3.3 L'INFRASTRUTTURA

L'infrastruttura della *CBDC* dipende inevitabilmente dall'architettura adottata: un modello di emissione diretta meglio si addice ad un'infrastruttura centralizzata, viceversa, quando il modello è ibrido o a doppio livello, data la presenza di innumerevoli istituti privati, l'infrastruttura migliore è quella decentralizzata: quest'ultima, in particolar modo, potrebbe migliorare significativamente l'accessibilità e la resilienza del sistema, nonché la continuità nell'offerta del servizio.

Mentre la raccolta, l'aggiornamento e la condivisione dei dati, in una infrastruttura centralizzata, avvengono in collegamento con una *repository* unica, gestita esclusivamente dall'Autorità regolatrice, in un ambiente decentralizzato ogni nodo di un *network P2P* partecipa attivamente al processo di collezione delle transazioni con *CBDC*, inviandone i *records* tramite liste *broadcast* all'interno di un *Distributed Ledger* (lett. "Libro distribuito") che altro non è che la *blockchain*. In questo modo si riduce notevolmente i tempi ed i costi connessi non solo con la raccolta dei dati, ma anche con l'esecuzione degli algoritmi di *data mining* che non saranno eseguiti verticalmente dai *servers* del gestore, aumentando il rischio di *Single Point of Failure*, ma si ripartiranno sui vari nodi della rete in base al protocollo di consenso scelto.
Se da un lato la *blockchain* che con ogni probabilità verrà adottata sarà del tipo consortile, per cui i permessi di lettura dei dati verranno concessi solo a quelle infrastrutture che si occupano di gestire direttamente i pagamenti *retail*, è ancora oggetto di discussione quale sarà il protocollo di consenso da adottare: sebbene il *Proof-of-Work* consenta di operare efficacemente in un contesto in cui la *CBDC* inizia ad essere emesse e distribuita, il protocollo di *Proof-of-Stake* meglio si addice alle caratteristiche strutturali degli operatori coinvolti in quanto gli intermediari finanziari non dovranno sostenere costi elevati per risolvere un *puzzle*

crittografico (cosa che accade adottando un protocollo *PoW*), ma potranno partecipare attivamente al processo di validazione delle transazioni proporzionalmente alle "riserve digitali" di *CBDC* da loro detenute presso la Banca Centrale.

Per di più, l'uso della tecnologia decentralizzata permetterebbe di sfruttare i c.d. *smart contracts* a proprio vantaggio per ridurre le tempistiche connesse con la ricezione dei fondi sia da parte dei commercianti, sia da parte di chi emette titoli obbligazionari/azionari (c.d. *Delivery versus Payment* o Consegna contro Pagamento) grazie ad un'esecuzione automatica del trasferimento di *CBDC* dal cliente al relativo prenditore. Per di più, gli *smart contracts* renderebbero possibile lo sviluppo del c.d. "pagamento programmabile", ossia che avviene ogni qualvolta si verifichino determinate situazioni o eventi. Allo stesso modo, gli *smart contracts* garantirebbero che manovre di politiche monetaria trovino attuazione automaticamente ogni volta che vengano raggiunti determinati livelli di inflazione o del tasso di disoccupazione a partire dall'equazione della curva di *Phillips*: in questo modo non si formerebbero aspettative da parte degli operatori economico-finanziari, consentendo alla Banca Centrale di calibrare con maggior precisione gli effetti attesi dall'attuazione delle manovre di politica monetaria sull'economia reale.
Gli *smart contracts* garantirebbero, infine, l'esecuzione di micro-pagamenti, ossia pagamenti frazionati (proprio come i gwei e gli shannon nel caso di Ethereum), e pagamenti *bulk*, ossia molteplici pagamenti effettuati in un *time-range* ridotto.

Ci possono essere due modi con cui un utente può accedere alla *CBDC*:

1. Modello basato sull'*account*: in quest'approccio la proprietà è collegata ad un'identità per cui chiunque è in grado di verificare chi sia effettivamente il proprietario dell'*account* (questo tipo di accesso è molto simile al modo con cui inviamo oggi pagamenti digitali).Lo schema basato sull'*account* presuppone che il credito patrimoniale sia imputato ad un'identità certificata, al pari dei tradizionali conti corrente bancari: per effettuare una transazione sarà necessario l'utilizzo di una *password* e di un codice OTP. Quando la transazione viene verificata, il *record* viene aggiornato automaticamente e aumenta o diminuisce proporzionalmente il saldo dell'*account*.

2. Modello basato su token: in quest'approccio si registra lo stato del sistema come un elenco di singole risorse (o "token"), ciascuna delle quali ha un corrispondente "proprietario" che possa controllare la risorsa. Ciascuno di questi gettoni ha un valore specifico (es. €15), che non cambia. Per avviare un trasferimento, il titolare di un token è tenuto a dimostrare di controllare il token, solitamente firmando un'istruzione di pagamento con la chiave privata associata a quel token. I token individuali non possono essere spesi parzialmente - invece, il token trasferito viene generalmente separato in due token più piccoli di nuova creazione (con lo stesso valore totale), uno per il destinatario e l'altro restituito al mittente come resto.

Non esiste alcuna ragione intrinseca per cui i sistemi basati su token fornirebbero automaticamente l'anonimato. Sia i sistemi basati su account che quelli basati su token possono essere configurati con varie soluzioni di identità, che vanno da completamente anonimo a pseudonimo fino a una soluzione completamente trasparente e identificabile.
Inoltre, né un approccio basato su account né un approccio basato su token consentirebbero trasferimenti simili al contante, in cui un pagamento può essere effettuato senza riferimento a terzi o intermediari. In un sistema basato sull'*account*, gli *account* dei pagatori e dei beneficiari devono essere addebitati e accreditati dall'operatore o dagli operatori autorizzati del libro mastro. E in un sistema basato su token, al fine di evitare la doppia spesa, la proprietà dei token deve essere registrata in un libro mastro (*ledger*), che dovrà essere aggiornato per riflettere eventuali cambiamenti di proprietà. Pertanto, da un punto di vista operativo, un approccio basato su token o account potrebbe essere in grado di fornire la gamma di funzionalità necessaria per una CBDC. Tuttavia, potrebbero esserci alcuni casi d'uso o servizi di sovrapposizione che sono meglio supportati da una di queste strutture di dati e potrebbero anche esserci importanti implicazioni legali.

3.4 IMPATTO SUL SISTEMA BANCARIO, MONETARIO E FINANZIARIO

La *CBDC* costituisce una nuova forma di denaro che consentirebbe ad individui e ad aziende di effettuare pagamenti elettronici utilizzando valuta virtuale coniata da una Banca Centrale. Questo cambiamento di paradigma potrebbe potenzialmente influenzare la struttura del sistema bancario e il modo attraverso cui la Banca Centrale raggiunge i suoi obiettivi primari di mantenimento della stabilità finanziaria e monetaria.

La *CBDC* produrrebbe i suoi vantaggi solo se le famiglie e le imprese la detenessero e la utilizzassero per effettuare i loro pagamenti quotidiani. Se questo fosse il caso, l'introduzione di una *CBDC* genererebbe il trasferimento di alcuni dei depositi dalle banche commerciali alla Banca Centrale sotto forma di *CBDC*. Infatti, come le altre forme di moneta (contante e riserve), la *CBDC* verrebbe registrata tra le passività di bilancio della Banca Centrale a fronte delle quali vengono detenute attività tra cui figurano, *in primis*, le obbligazioni emesse dal governo o dai governi degli Stati Membri (come nel caso della BCE), ma anche i prestiti al settore bancario nonché le linee di liquidità ordinarie.
Allo stesso modo, i depositi delle banche commerciali figurano come passività nel loro bilancio e sono garantiti da attività che consistono, tipicamente, in riserve (libere ed obbligatorie), obbligazioni, prestiti (come i mutui) e altri strumenti finanziari.
Se la *CBDC* venisse ampiamente utilizzata, alcune delle famiglie e delle imprese che attualmente detengono depositi bancari commerciali potrebbero desiderare di scambiare questi depositi con *CBDC*, generando un depauperamento dalle passività di bilancio delle banche commerciali ed un innalzamento del livello del passivo di bilancio della Banca Centrale.

Presupponendo che le banche commerciali rimangano inermi di fronte a questo processo di conversione dei loro depositi in *CBDC*, si troverebbero costrette a liquidare parte delle loro attività per far fronte agli impegni contrattuali assunti sul breve termine, non disponendo di sufficiente liquidità dal lato passivo. Dopodiché si troveranno, sul medio-lungo termine, con bilanci molto più contenuti sia lato passivo, sia lato attivo: per questo motivo, per riuscire a coprirsi dal maggior rischio di credito, inizieranno a ridurre la fornitura di credito a famiglie e ad imprese le quali vedranno l'accesso agli ordinari strumenti di finanziamento (come il mutuo o l'apertura di un c/c bancario) limitato da condizioni molto più stringenti (come la richiesta di garanzie quantitativamente e qualitativamente migliori, valutazioni del merito di credito più stringenti, innalzamento degli interessi passivi sui c/c bancari, etc.); questo processo di contrazione aumenterà l'asimmetria informativa sui mercati finanziari in quanto le famiglie/imprese che non dispongano di un elevato *standing* creditizio o dovranno rivolgersi ad altri soggetti per ottenere le risorse finanziarie di cui hanno bisogno oppure non metteranno in atto alcun investimento, riducendo proporzionalmente il loro consumo di beni e servizi ed impattando negativamente sull'economia reale.
Questa contrazione del bilancio del settore bancario è nota come "disintermediazione". Un certo grado di disintermediazione è una conseguenza inevitabile di una *CBDC* di successo.

Le banche, tuttavia, non rimarrebbero inermi di fronte a questo cambiamento: infatti potrebbero o pagare un tasso di interesse attivo più elevato sui c/c bancari al fine di limitare ulteriori deflussi di depositi, o cercare di sostituire i fondi persi con finanziamenti alternativi, come depositi a più lungo termine, o ancora fornire servizi aggiuntivi per ingraziarsi i depositari e mitigare la loro migrazione verso la *CBDC*. Tuttavia, entrambe queste opzioni possono aumentare il costo complessivo di finanziamento inducendo un'emissione di un volume inferiore di prestiti. Un'altra risposta alla situazione potrebbe essere quella di rivolgersi alla Banca Centrale per sostituire i depositi persi con nuovi fondi; tuttavia, questo prestito potrà avvenire soltanto qualora le banche richiedenti dispongano di *collateral* quantitativamente e qualitativamente significativi: questo potrebbe generare, in ultima analisi, un aumento della domanda di *asset* sicuri portando al rialzo i rispettivi tassi di interesse sul mercato.
Infine, le banche che non dispongano di garanzie adeguate dovranno rivolgersi al libero mercato per l'approvvigionamento di nuovi fondi, aumentando la loro esposizione al rischio di tasso di interesse e al rischio di controparte.

Una rapida transizione dei depositi in *CBDC* potrebbe produrre, inoltre, effetti disastrosi per l'economia finanziaria e reale soprattutto se si è già avviato un periodo di stress ed incertezza finanziaria: in questa situazione, le famiglie e le imprese percepiranno la *CBDC* come un'attività meno rischiosa sia dei depositi delle banche commerciali (nonostante i depositanti al dettaglio godano delle protezioni *FSCS*), sia di alcuni tipi di obbligazioni statali come i Buoni Ordinari del Tesoro, innescando una più ampia instabilità sistematica. In questo senso, un periodo di rapida sostituzione dai depositi in *CBDC* sarebbe equivalente a una corsa agli sportelli. Questa situazione potrebbe incentivare le banche a prendere provvedimenti prociclici per coprirsi

dal rischio, ad esempio "accumulando" riserve in un periodo di stress. Questo comportamento avrebbe un ulteriore impatto sul regolare funzionamento dei mercati monetari.

Nello scenario più estremo, in cui una *CBDC* abbia sostituito completamente i depositi a vista presso le banche commerciali, quelle banche - se non dovessero ridurre i loro prestiti - farebbero affidamento interamente su altre fonti di finanziamento. Nella misura in cui ciò includesse una maggiore dipendenza dalle strutture esistenti della banca centrale, o se la carenza di finanziamenti del mercato privato inducesse le banche centrali ad adeguare la dimensione dell'offerta dei finanziamenti, ciò avrebbe implicazioni significative per il ruolo svolto della Banca Centrale nell'esercizio delle sue funzioni di indirizzo della politica monetaria, come influenzare il costo del credito. Qualsiasi espansione del bilancio della Banca Centrale a sostegno del finanziamento bancario solleverebbe la questione di quali attività corrisponderebbero alle passività aggiuntive e come sarebbero fornite. Infatti, l'emissione di denaro è normalmente redditizia e genera reddito da signoraggio a causa della differenza tra la remunerazione delle attività della Banca Centrale e il tasso di interesse applicato alle sue passività. In una ipotesi di completa sostituzione dei depositi in *CBDC*, se le banche commerciali dipendessero esclusivamente dalle strutture di finanziamento della Banca Centrale, questa si troverebbe costretta ad offrire prestiti tramite operazioni di rifinanziamento a più lungo termine (*LTRO*, di conseguenza il differenziale tra la remunerazione della *CBDC* ed il tasso di interesse applicato nelle operazioni di *LTRO* sarebbe fondamentale per determinare la redditività della banca centrale.
Oltre ai rischi legati alle dimensioni e alla composizione del suo bilancio, la Banca Centrale potrebbe anche essere esposta a passività finanziarie in quanto operatore di un sistema di pagamento al dettaglio. Ad esempio, il malfunzionamento dell'infrastruttura informatica alla base della *CBDC* potrebbe causare perdite e danni ai singoli utenti, sollevando dubbi sulla responsabilità della Banca Centrale ed abbassando il livello di fiducia verso il sistema di pagamento digitale.

CONCLUSIONI

In questo studio sono stati analizzati gli *hot trends* legati al mondo della finanza decentralizzata e digitale; un mondo che, come si è potuto evincere leggendo, è destinato a rivoluzionare i più antiquati paradigmi della finanza tradizionale, creando nuovi sviluppi che troveranno applicazione nei più disparati settori: dalla speculazione individuale, a nuove forme di raccolta di *equity* per le imprese, dalla sicurezza e la *privacy* nei pagamenti, alla creazione di un sistema centralizzato di emissione di moneta digitale sotto il controllo diretto delle Banche Centrali Nazionali e/o Comunitarie.

L'approccio seguito non è stato solo quello di affrontare lo specifico argomento dal punto di vista macro/microeconomico, considerando quindi gli effetti sull'economia reale e/o i benefici/svantaggi che ne derivano a livello di singolo mercato/impresa/*holder* o *trader*, ma anche dal punto di vista informatico, seppur in maniera piuttosto esemplificativa, al fine di coinvolgere ambiti che, seppur vengano da sempre considerati a compartimenti stagni, da qui ai prossimi dieci anni vedranno una sempre maggiore convergenza, generando situazioni in cui competenze di *governance* e di programmazione informatica diventeranno variabili *driver* del nuovo paradigma struttura-condotta-performance per le imprese digitalizzate.

Lo studio non vuole essere inteso come una mera enciclopedia di termini astrusi e (talvolta) troppo ricchi di tecnicismi, ma come un punto di inizio per una più ampia ricerca in continua evoluzione, che spazia dalla costruzione algoritmica di *smart contracts* alla definizione di nuove metodologie di analisi tecnica sulle cripto-valute, al fine di elaborare strategie anche per coprirsi dall'eccessiva volatilità del mercato, il quale, si è ben evidenziato, è lontano dall'essere efficiente.

Le cripto-valute hanno segnato l'inizio di una nuova epoca, ancora agli albori in termini di efficacia ed efficienza: sono molte, infatti, le problematiche legate al corretto funzionamento di un *network* che abbia adottato una tecnologia *blockchain*; scalabilità, e vulnerabilità strutturali sono soltanto alcuni esempi dei rischi che stanno alla base di un così complesso sistema, formato da un sempre maggior numero di partecipanti tutti con interessi economici differenti; tuttavia, sempre più numerosi sono i nuovi ambiti di applicazione e le opportunità che questi *assets* hanno creato *ex-novo*, sospinti dalla propulsione derivante sia dall'ambito delle tecnologie cibernetiche sia dal fervore degli operatori finanziari, che hanno portato i *network* a migliorarsi per poter sostenere volumi e frequenze di *mining* sempre più costosi in termini di *difficoltà*.

Al momento della relazione di questo studio, Governi come gli Stati Uniti d'America e la Cina stanno disincentivando la speculazione sulle cripto-valute anche imponendo un pesante sistema di tassazione sui profitti raggiunti da siffatte operazioni. Da un lato questo dimostra come la portata di questi strumenti finanziari sia oggigiorno più che mai rilevante e stia impattando anche direttamente (seppur ancora in maniera molto contenuta) le economie reali delle più grandi potenze mondiali.

BIBLIOGRAFIA

Ametrano, Ferdinando M. 2016. «Hayek Money: The Cryptocurrency Price Stability Solution.» *SSRN*. 23 Agosto. Consultato il giorno Maggio 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425270.

Banca d'Italia. 2017. «Le funzioni della moneta e le proposte di "moneta fiscale".» *Banca d'Italia.it.* 11 Novembre. https://www.bancaditalia.it/media/views/2017/moneta-fiscale/Moneta-fiscale-dic2017.pdf.

Bank of England . 2020. «Central Bank Digital Currency: opportunities, challenges and design.» 12 Marzo. Consultato il giorno Marzo 2021. https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593.

Binance Academy. 2021. *Che cos'è lo Yield Farming nella finanza decentralizzata (DeFi)?* . Aprile. Consultato il giorno Maggio 2021. https://academy.binance.com/en/articles/what-is-yield-farming-in-decentralized-finance-defi.

—. 2021. *Che cos'è uno scambio decentralizzato (DEX)?* Aprile. Consultato il giorno Maggio 2021. https://academy.binance.com/en/articles/what-is-a-decentralized-exchange-dex.

—. 2021. *Cosa sono i prestiti flash in DeFi?* Aprile. Consultato il giorno Maggio 2021. https://academy.binance.com/en/articles/what-are-flash-loans-in-defi.

—. 2021. *Cosa sono le pool di liquidità nella DeFi e come funzionano?* Aprile. Consultato il giorno Aprile 2021. https://academy.binance.com/it/articles/what-are-liquidity-pools-in-defi.

—. 2021. *Cosa sono le StableCoin?* Aprile. Consultato il giorno 2021 Maggio. https://academy.binance.com/it/articles/what-are-stablecoins.

—. 2021. *Cos'è un market maker automatizzato (amm).* Aprile. Consultato il giorno Maggio 2021. https://academy.binance.com/it/articles/what-is-an-automated-market-maker-amm.

—. 2021. *La guida completa per principianti alla finanza decentralizzata (DeFi).* Aprile. Consultato il giorno Maggio 2021. https://academy.binance.com/en/articles/the-complete-beginners-guide-to-decentralized-finance-defi.

—. 2021. *Spiegazione dei gettoni di rifornimento elastico.* Aprile. Consultato il giorno Maggio 2021. https://academy.binance.com/en/articles/elastic-supply-tokens-explained.

—. 2021. *Spiegazione della perdita impermanente.* Maggio. Consultato il giorno Maggio 2021. https://academy.binance.com/en/articles/impermanent-loss-explained.

—. 2021. *Spiegazione delle organizzazioni autonome decentralizzate (DAO).* Aprile. Consultato il giorno Maggio 2021. https://academy.binance.com/en/articles/decentralized-autonomous-organizations-daos-explained.

Burniske, C. 2017. *The Crypto J-Curve.* 12 Agosto. Consultato il giorno Maggio 2021. https://medium.com/@cburniske/the-crypto-j-curve-be5fdddafa26.

Buterin, Vitalik. 2013. «DETERMINISTIC WALLETS, THEIR ADVANTAGES AND THEIR UNDERSTATED FLAWS.» *Bitcoin Magazine.* 2013 Novembre. Consultato il giorno Maggio 2021. https://bitcoinmagazine.com/technical/deterministic-wallets-advantages-flaw-1385450276.

C. Burniske, J. Tatar. 2017. *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond.* McGraw-Hill Education.

Candiloro, Davide. 2015. «La sicurezza informatica di Bitcoin.» In *Ciberspazio e diritto, vol. 16, n. 53 (2-2015), pp. 331-356*, di Davide Candiloro, 25. Milano: Torrossa Online Digital Bookstore.

Carstens, Agustín. 2015. "Digital currencies." *Bank for International Settlements.* Novembre. https://www.bis.org/cpmi/publ/d137.pdf.

Castells, Manuel. 2001. *The Rise of the Network Society. The Information Age: Economy, Society, and Culture, Vol. 1.* Blackwell Pub.

Chaum, David. 1983. *Blind Signatures for Untracable Payments.* Santa Barbara, California (USA): CRYPTO 1982.

coblee. 2012. «Proof of Activity Proposal.» *Bitcoin Talk Forum.* 21 Agosto. Consultato il giorno Maggio 2021. https://bitcointalk.org/index.php?topic=102355.0.

CONSOB, Commissione Nazionale per le Società e la Borsa. s.d. *Lo scoppio della bolla delle c.d. Dotcom.* Consultato il giorno Marzo 2021. https://www.consob.it/web/investor-education/la-bolla-delle-c.d.-dotcom.

Dowd, Kevin. 2013. «Contemporary Private Money Systems.» 2 Agosto.
Draghi, Mario, intervista di Twitter. 2021. *#AskDraghi* (3 Febbraio).
Eich, Brendan. 2021. Basic Attention Token (BAT) - A Blockchain Based Digital Advertising. 10 Febbraio.
European Central Bank. 2020. «Report on a Digital Euro.» Ottobre. Consultato il giorno Marzo 2021. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.
European Central Bank. 2012. «Virtual Currency Schemes.» Bruxelles.
Evans, Alex. 2018. *On Value, Velocity and Monetary Theory: A New Approach to Cryptoasset Valuations* . 18 Gennaio. Consultato il giorno Maggio 2021. https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f.
Franco, Pedro. 2015. *Understanding Bitcoin - Cryptography, engineering, and economics.* Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom: John Wiley & Sons Ltd.
G7 Working Group on StableCoin. 2019. «Investigating the impact of Global StableCoin.» *Bis.org.* Ottobre. Consultato il giorno Marzo 2021. https://www.bis.org/cpmi/publ/d187.pdf.
Galia Kondova, Renato Barba. 2019. «Governance of Decentrilized Autonomous Organizations.» (David Publishing) 15 (8).
Goldwasser, S. 2008. « Lecture Notes on Cryptography - UCSD CSE.» *Computer Science & Engineering, UC San Diego.* http://cseweb.ucsd.edu/~mihir/papers/gb.pdf.
Hajric, Vildana. 2021. *Don't Count on Bitcoin to Be a Sure-Thing Inflation Hedge.* 17 Marzo. Consultato il giorno Maggio 2021. https://www.bloomberg.com/news/articles/2021-03-17/is-bitcoin-an-inflation-hedge-the-opposite-effect-could-happen-in-recession.
John Stuart Mill, Anonymous user. 2016. «A Distributed Consensus Algorithm for Cryptocurrency Networks.» *Skycoin - WhitePapers.* 22 Ottobre. Consultato il giorno Maggio 2021. https://downloads.skycoin.com/whitepapers/a-distributed-consensus-algorithm-for-cryptocurrency-networks.pdf.
K. Bheemaiah, A. Collomb. 2018. «CRYPTOASSET VALUATION - Identifying the variables of analysis.» Louis Bachelier. Ottobre. Consultato il giorno Maggio 2021. https://www.louisbachelier.org/wp-content/uploads/2018/10/cryptovaluationreport-v20181016-vf.pdf.
Lannquist, Ashley. 2018. *Today's Crypto Asset Valuation Frameworks.* 7 Marzo. Consultato il giorno Maggio 2021. https://medium.com/blockchain-at-berkeley/todays-crypto-asset-valuation-frameworks-573a38eda27e.
Meek, James Gordon. 2007. "Feds out to bust up 24-karat Web worry." *Daily News.*
Mullan, P. Carl. 2014. *The Digital Currency Challenge: Shaping Online Payment Systems through US Financial Regulations.* New York: Palgrave Pivot.
Murad Mahmudov, David Puell. 2018. «Bitcoin Market-Value-to-Realized-Value (MVRV) Ratio - Introducing Realized Cap to BTC Market Cycle Analysis.» *@kenoshaking.* 2 Ottobre. Consultato il giorno Maggio 2021. https://medium.com/@kenoshaking/bitcoin-market-value-to-realized-value-mvrv-ratio-3ebc914dbaee.
Nakamoto, Satoshi. 2008. «Bitcoin: un sistema di moneta elettronica peer-to-peer.» *Bitcoin.org.* https://bitcoin.org/files/bitcoin-paper/bitcoin_it.pdf.
Pannetta, Fabio. 2020. «Stablecoin: due facce della stessa moneta.» *Intervento di Fabio Panetta, Membro del Comitato esecutivo della BCE, al Salone dei Pagamenti 2020.* Francoforte sul Meno.
Parlamento Europeo. 2018. «Cripto-valute e Blockchain.» *Studio richiesto dal comitato TAX3.* Bruxelles: Ufficio Pubblicazioni dell'UE. 103.
Pitta, Julie. 1999. *Requiem for a Bright Idea.* Novembre 1. https://www.forbes.com/forbes/1999/1101/6411390a.html?sh=f86561e715f6.
portafoglioelettronicomigliore.com. 2019. *DigiCash: funzionamento del sistema online e offline.* 8 11. http://www.portafoglioelettronicomigliore.com/digicash.asp.
PwC Italia. 2020. «Central Bank Digital Currency.» *PwC Italia.* PricewaterhouseCoopers Advisory SpA. Consultato il giorno Maggio 2021. https://www.pwc.com/it/it/publications/assets/docs/central-bank-digital-currency.pdf.
QuantumMechanic. 2011. *Proof of stake instead of proof of work.* 11 Luglio. Consultato il giorno Maggio 2021. https://bitcointalk.org/index.php?topic=27787.0.
Rossen, Jake. 2017. *Before Bitcoin: The Rise and Fall of Flooz E-Currency.* 14 Dicembre. https://www.mentalfloss.com/article/517911/bitcoin-rise-and-fall-flooz-e-currency.

Securities & Exchange Commission. 2018. *Ponzi schemes Using virtual Currencies.* Washington DC: Office of Investor, Admistration and Advocacy.

Shin, Laura. 2021. «Could Digital Currency Make Our Money More Secure?» *Forbes.*

Shirakashi, Renato. 2019. «Introducing SOPR: spent outputs to predict bitcoin lows and tops.» *Unconfiscata.* 25 Aprile. Consultato il giorno Maggio 2021. https://medium.com/unconfiscatable/introducing-sopr-spent-outputs-to-predict-bitcoin-lows-and-tops-ceb4536b3b9.

Spagnolo, Eleonora. 2021. «Mario Draghi e Bitcoin: il pensiero del quasi premier italiano.» *The Cryptonomist,* 3 Febbraio.

Stanford Computer Science. 2010. «Liberty Dollars.» *stanford.edu.com.* Novembre. https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/Bitcoins/liberty-dollars.html.

Stewart, Ian. 2018. *Proof of burn.* 15 Gennaio. Consultato il giorno Maggio 2021. https://en.bitcoin.it/wiki/Proof_of_burn#:~:text=Proof%20of%20burn%20is%20a,to%20a%20verifiably%20unspendable%20address.

Tepper, Taylor. 2021. «Bitcoin Rises Above $50,000. Where Does It Go From Here?» *Forbes Advisor.com.* 22 Marzo. https://www.forbes.com/advisor/investing/bitcoin-price-near-highs/.

Torchiani, Gianluca. 2018. *Altcoin: cosa sono e come funzionano le criptovalute sorelle di Bitcoin.* 2 Febbraio. https://www.techcompany360.it/tech-lab/altcoin-cosa-sono-e-come-funzionano-le-criptovalute-sorelle-di-bitcoin/.

TUB - Testo unico delle leggi in materia bancaria e creditizia. 1993. «Testo Unico Bancario, arti. 1, comma 2, lettera h-ter.» Roma: Banca d'Italia.

United States Distrisct Court for the District of Columbia. 2008. *Transcript of Sentence before The Honorable Rosemary M. Colliver.* Washington DC: United States District Judge.

United States Mint. 2006. *Justice Determines Use of Liberty Dollar Medallions as Money is a Crime.* Washington DC: United States Mint, sezione stampa.

University of California, Bakerley. n.d. *Rise and Fall of Nescape Browsers.* Accessed Marzo 2021. https://inst.eecs.berkeley.edu/~eecsba1/sp98/reports/eecsba1c/pj1/.

Weber, Warren. 2018. *The Quantity Theory of Money for Tokens.* 26 Febbraio. Consultato il giorno Maggio 2021. https://blog.coinfund.io/the-quantity-theory-of-money-for-tokens-dbfbc5472423.

White, Lawrence H. 2014. *The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-Gold.* Contea di Fairfaix, Virginia (USA): George Mason University - Department of Economics.

Wikipedia, l'enciclopedia libera. 2016. *E-Gold.* Maggio 30. https://en.wikipedia.org/wiki/E-gold#:~:text=E%2Dgold%20was%20a%20digital,to%20other%20e%2Dgold%20accounts.

—. 2021. *Netscape - Wikipedia.* 1 Aprile. Consultato il giorno Marzo 2021. https://en.wikipedia.org/wiki/Netscape.

Woo, Willy. 2017. *Is Bitcoin In A Bubble? Check The NVT Ratio.* Forbes. 29 Settembre. Consultato il giorno Aprile 2021. https://www.forbes.com/sites/wwoo/2017/09/29/is-bitcoin-in-a-bubble-check-the-nvt-ratio/?sh=24b9616c6a23.