CRIPTOVALUTA: DIGITALIZZAZIONE DI VALORE E FINANZA DECENTRALIZZATA

Tra regolamentazione ed elusione

GIAMPAOLO MORINI

SOMMARIO: *Introduzione*; 1. Che cosa sono le criptovalute; 2. DeFi; 3. Origini; 4. La Blockchain; 5. Crittografia e firma digitale; 6. La convalida di un blocco; 7. La Blockchain nel Bitcoin; 8. Le Transazioni nella Blockchain del Bitcoin; 9. Il Mining; 10. Zone di Mining; 11. Initial Coin Offering (ICO); 12. Bitcoin e Gold Standard; 13. Non solo bitcoin: altre principali criptovalute; 13.1 Ethereum; 13.2 Ripple; 13.3 Altre criptovalute; 13.4 Le nuove criptovalute; 14. Smart Contract; 15. Sharing Economy; 16. Crowdfunding e ICO; 17. La funzione della criptovaluta e la sua volatilità intrinseca; 18. La criptovaluta come strumento finanziario?; 19. La criptovaluta come valore mobiliare: il titolo digitale; 19.1 Il test di Howey; 19.2 Initial Coin Offers e Security Tokens Offerings; 20. La regolamentazione; 20.1 Regolamentazione europea ed internazionale: La V Direttiva Antiriciclaggio; 20.2 Il D. Lgs n. 90/2017 e la nozione della "digitalizzazione di valore"; 20.3 Nuove prospettive normative 21. Rischi legali per il consumatore; 22. Usi illeciti: riciclaggio, finanziamento illecito, terrorismo; 22.1 Bitcoin come una bolla speculativa.

Introduzione

La creazione delle criptovalute, ovvero di valore non cristallizzato nella moneta legale, ha dato vita ad una realtà finanziaria nuova estranea ai sistemi tradizionali. Considerando l'inasprirsi negli ultimi due decenni delle leggi sull'antiriciclaggio, sull'evasione fiscale e sulla lotta al terrorismo, che hanno inteso rendere trasparente e tracciabile il movimento di denaro, e più in generale della ricchezza, è plausibile ritenere che, la criptovaluta (le criptovalute si fondano su obbiettivi decisamente opposti alle finalità delle discipline richiamate, ovvero mantenere ***oscura*** - almeno in parte - la provenienza e gli spostamenti di valori - più o meno reali), sia frutto di progetti e finalità di dubbia legalità. Ciò tuttavia non toglie che le criptovalute possano anche avere un uso lecito.

Sicuramente, il fatto che le criptovalute, non siano ben viste dal sistema bancario, porta a credere che esista un sistema "finanziario" *sottotraccia* la cui identità resta celata dal mistero così come le finalità. Considerati i volumi della nuova finanza (sempre che tale si possa definire), il sospetto che un nuovo potere si sia affacciato nella realtà quotidiana, o semplicemente si sia esplicitato con tutte le proprie cautele di segretezza, è più che plausibile.

Certamente il *valore* delle criptovalute e la loro circolazione occultati in algoritmi sempre più complessi rendono lo strumento rischioso in quanto a differenza delle banche, non è prevista una copertura di nessun tipo, né tanto meno una assicurazione.

Come diceva Cervantes, "***l'onestà è la miglior politica***".

1. Che cosa sono le criptovalute.

Le criptovalute sono considerate un nuovo tipo di strumento finanziario. La prima criptovaluta successo è stata il Bitcoin, il cui valore non è basato su alcun bene tangibile oppure sull'economia di un paese, ma viene **stimato sulla base della sicurezza di un algoritmo che traccia tutte le transazioni.**

L'uso potenziale di Bitcoin come mezzo di scambio è oggetto di molta attenzione a causa dei suoi **bassi costi di transazione**, il suo **design *peer-topeer*, globale e senza governo**, tuttavia, permane in capo agli utenti una scarsa fiducia nel sistema dimostrato dal fatto che il Bitcoin viene poco utilizzato per effettuare transazioni.

Il Bitcoin è stato concepito come un nuovo tipo di valuta piuttosto che un bene di investimento, tuttavia il prezzo di Bitcoin e di altre criptovalute è aumentato sostanzialmente dal 2010 denotando come questi nuovi strumenti **sono utilizzati principalmente come investimento speculativo piuttosto che una valuta alternativa o un mezzo di scambio**.

La questione che le criptovalute possano ritenersi un investimento è tuttora aperta. **Gran parte delle critiche rivolte al Bitcoin sono basate sulla sua mancanza di valore intrinseco**, tuttavia, la letteratura accademica che esamina la dinamica dei prezzi di Bitcoin e di altre criptovalute è in aumento, con una serie di articoli che studiano le bolle nei mercati delle criptovalute, l'efficienza dei mercati di Bitcoin, le sue proprietà di copertura e la scoperta del prezzo all'interno degli scambi.

Un'area che ha ricevuto una crescente attenzione nella letteratura sulle criptovalute è quella dei benefici di investire in questi asset. **Kajtazi** e **Moro**[1] evidenziano gli effetti dell'aggiunta di Bitcoin a un portafoglio ottimale affidandosi all'approccio meanCVaR per il portafoglio statunitense, europeo e cinese. Tali analisi dimostrano che il Bitcoin migliora i rendimenti del portafoglio, soprattutto grazie all'aumento degli stessi piuttosto che da una minore volatilità, e che il Bitcoin ha un ruolo nella diversificazione del portafoglio.

[1] A. Kajtazi, A. Moro, "The role of bitcoin in well diversified portfolios: A comparative global study", International Review of Financial, vol. 61, pp. 143-157, USA, 2019

Platanakis e **Urquhart**[2] hanno esaminato il beneficio di includere il Bitcoin in otto popolari strategie di allocazione di asset in portafogli di azioni e obbligazioni ed hanno concluso che, l'inclusione della valuta digitale genera rendimenti corretti per il rischio (***risk-adjusted returns***[3]) sostanzialmente più elevati, dove i risultati nei confronti di diverse stime, dell'incorporazione dei costi di transazione, dell'inclusione di un portafoglio di materie prime, di un indice alternativo per Bitcoin nonché di due ulteriori tecniche di ottimizzazione del portafoglio, sono robusti. È poi stato sviluppato uno studio del trading tecnico nei mercati delle criptovalute al fine di valutare se le regole del trading offrono potere predittivo e redditività in vari mercati di criptovalute. Il trading tecnico è di particolare interesse nei mercati delle criptovalute per una serie di ragioni. L'approccio del trading ha un sostanziale successo documentato nei mercati delle valute convenzionali e, in una certa misura, in molti mercati di asset.

Poiché i mercati delle criptovalute hanno avuto la tendenza a seguire forti *pattern*[4] fin dal loro inizio, si ha qualche precedente che le regole tecniche di trading possano essere utili nei mercati delle criptovalute, invero, la relativa mancanza di informazioni rilevanti per eseguire l'analisi fondamentale sulle criptovalute può elevare l'importanza relativa degli approcci tecnici. Ciò in quanto **le criptovalute non hanno fondamentali da esaminare e probabilmente non hanno valore intrinseco**, ne consegue che gli investitori non possono studiare, per esempio, il bilancio o le previsioni dei dividendi per prevedere i prezzi futuri e, quindi, devono fare affidamento sul comportamento passato dei

[2] E. Platanakis, A. Urquhart, "Should investors include bitcoin in their portfolios? A portfolio theory approach". Available at SSRN: https://ssrn.com/abstract=3215321, USA, 2019

[3] Un rendimento aggiustato per il rischio è un calcolo del profitto o potenziale profitto da un investimento che tiene conto del grado di rischio che deve essere accettato per realizzarlo. Il rischio viene misurato rispetto a quello di un investimento praticamente privo di rischio, solitamente titoli del Tesoro USA. A seconda del metodo utilizzato, il calcolo del rischio è espresso come un numero o un rating. I rendimenti aggiustati per il rischio vengono applicati a singoli titoli, fondi di investimento e interi portafogli.

[4] ***Pattern*** significa 'schema', 'modello', 'configurazione', o anche 'struttura', 'disegno', 'motivo', e quindi può essere tradotto con questi termini.

prezzi come segnale del comportamento futuro, che è il concetto fondamentale del trading tecnico.

L'unico articolo a disposizione che esamina il **trading tecnico nei mercati delle criptovalute è a cura di Detzel e altri autori**[5], che mostrano che la regola della media mobile da 5 a 100 giorni, sia all'interno che all'esterno del campione, offre potere predittivo per gli investitori. Mostrano anche che le strategie di trading basate su queste regole generano alfa, utilità e indici di Sharpe sostanziali, riducendo significativamente la gravità dei ***drawdown*** (perdita) rispetto ad una posizione di ***buy-and-hold***[6] in Bitcoin: **questo documento esamina, tuttavia, solo un tipo di regola di trading tecnico, mentre ci sono molti tipi diversi di regole con molte parametrizzazioni diverse.**

In gergo finanziario per *drawdown* di trading si intende la distanza osservata tra il picco più alto e quello più basso di un conto in un intervallo di tempo considerato. Si inizia a parlare di *drawdown* a partire dal primo movimento contrario, e il suo valore complessivo cambierà solo quando ne saranno registrati nuovi massimi o minimi. Questo spesso crea un po' di confusione nei calcoli, anche se in realtà è davvero molto semplice. Il *drawdown* è la distanza tra il punto più alto e quello più basso di un certo periodo, quindi anche in caso di grafici a zig zag, non si parlerà di un nuovo *drawdown* finché i precedenti record non saranno superati. Per poterlo stimare è necessario definire un intervallo di tempo specifico, quindi il dato può essere espresso in percentuale (*drawdown relativo*) o con la stessa unità di misura del conto. La formula per ottenere il *drawdown* percentuale, considerato più fruibile, è:

Drawdown (DD)% = ((Pmax – Pmin) / Pmax)) * 100

dove

[5] A. L. Detzel, H. Liu, J. Strauss, G. Zhou, Y. Zhu, "Bitcoin: Learning, predictability and profitability via technical analysis". Available at SSRN: https://ssrn.com/abstract=3115846, USA, 2018.

[6] L'investimento Compra e Tieni (Buy and Hold) è una strategia semplice ed efficace per i propri investimenti che risparmia gli investitori dai danni al rendimento generati dal tempismo (market timing) e dalla selezione dei titoli (stock-picking).

Pmin = minimo storico (trough)

Pmax = massimo storico (peak)

Un *drawdown* è quindi diverso da una perdita, si tratta semplicemente del movimento da un picco a un minimo. I trader considerano invece le perdite come variazioni negative in relazione al capitale di partenza.

I vantaggi del trading di criptovalute *buy-and-hold* sono: Elimina il 95% del "rumore del mercato". Esistono diverse strategie di trading buy-and-hold (che ci crediate o no). L'idea principale alla base di queste strategie è cavalcare le tendenze rialziste a lungo termine ed eliminare il "rumore" del mercato associato a periodi di tempo inferiori. I trader a breve termine spesso si sentono frustrati quando il mercato li scuote dalle loro negoziazioni mentre si sposta su intervalli di tempo più brevi (ad esempio, l'intervallo di un'ora). L'azione del prezzo su un grafico settimanale è spesso non volatile per un certo periodo di tempo. Quando lo stesso periodo viene analizzato su intervalli di tempo più piccoli, l'immagine è solitamente molto più irregolare e imprevedibile rispetto all'intervallo di tempo settimanale.

Non è necessario un perfetto tempismo di mercato. Ciò che rende attraente il trading ***buy-and-hold*** per molti trader e investitori è che in molti casi, il tempismo perfetto del mercato non è estremamente importante. Per i trader che pianificano di essere in negoziazione per mesi o addirittura anni, ciò che conta di più è entrare effettivamente nel commercio. Questi trader spesso non aspettano grandi pullback contro la tendenza rialzista prevalente perché sanno che potrebbe far loro perdere l'opportunità di entrare nella posizione che stanno cercando.

Costi di transazione ridotti I trader che si impegnano in operazioni ***buy-and-hold*** a lungo termine di solito non esagerano. Ciò può ridurre significativamente i costi di transazione. Un trader che entra ed esce dalle negoziazioni ogni giorno o ogni settimana deve tenere conto del prelievo dei costi di transazione accumulati. Lo spread su alcune criptovalute è significativamente più alto rispetto alle principali coppie di

valute, ad esempio. Ciò può rendere molto costoso e inefficace eseguire molte operazioni a breve termine anziché poche operazioni a lungo termine.

Efficienza temporale. Le strategie di trading di criptovalute *buy-and-hold* sono perfette per investitori e trader che cercano di ottenere guadagni potenzialmente elevati con un dispendio di tempo minimo. Gli investitori di criptovaluta a lungo termine che si impegnano in operazioni *buy-and-hold* non hanno bisogno di tenere d'occhio il prezzo ogni giorno, né hanno bisogno di fare analisi tecniche e guardare i grafici su base frequente. Sarebbe saggio per questi trader/investitori di criptovalute rimanere aggiornati sulle notizie fondamentali, ovviamente, e controllare le loro posizioni di tanto in tanto, ma è comunque molto meno dispendioso in termini di tempo rispetto al trading a breve termine.

Sebbene il mercato del Bitcoin sia il più grande, altri mercati di criptovalute hanno guadagnato un'attenzione che non può essere ignorata in quanto la crescita dell'interesse per le criptovalute diverse dal Bitcoin, è aumentata esponenzialmente negli ultimi anni.

Per lo studio delle criptovalute si considera una gamma di cinque diverse classi di regole tecniche di trading, in cui si esaminano una serie di parametri diversi: se da un lato utilizzare poche regole può causare distorsioni nell'inferenza statistica dovuta al data mining, d'altra, usarne troppe può ridurre la potenza del test motivo per cui, è necessario individuare un equilibrio selezionando una varietà abbastanza ampia di parametri ragionevoli all'interno delle cinque famiglie di regole più popolari.

Viene impiegata una gamma di metriche di performance per valutare i rendimenti del trading tecnico, compresa una serie di misure corrette per il rischio e i costi di ***breakeven*** (pareggio). Poiché si esaminano un certo numero di regole diverse, ci si trova di fronte alla reale possibilità di un ***bias*** (distorsione) da

data-snooping[7] (manipolazione artificiale dei dati o delle analisi per ottenere risultati significativi), dove il gran numero di ipotesi testate porta ad una probabilità piuttosto alta di rigettare l'ipotesi nulla di ogni regola di trading (commettendo un errore del I tipo).

Per evitare questo problema, si calcolano prima i *p-value*[8] individuali di ogni trading tecnico confrontando quello attuale con altri mille *p-value* stazionari "*bootstrapped*"[9]. Successivamente si utilizzano questi *p-value* individuali *bootstrapped* e si adottano una serie di approcci per testare ipotesi multiple, in particolare il *Family-Wise Error Rate*[10] (FWER) e il *False Discovery Rate*[11] (FDR).

Il ruolo del tasso di errore familiare nella determinazione della significatività statistica. La soglia per la significatività statistica è determinata dalla massima probabilità consentita di errore di tipo I (α). Per gli studi che testano ipotesi multiple o effettuano confronti multipli, la probabilità di almeno 1 errore di tipo I (tasso di errore familiare; FWER) aumenta all'aumentare del numero di ipotesi/confronti. In genere è buona norma impostare la soglia accettabile per FWER su un valore inferiore o uguale a α. La correzione di Bonferroni e il test della differenza onestamente significativa di Tukey sono 2 dei metodi più comuni per controllare FWER. Quando si esegue un'analisi

[7] Lo ***snooping*** dei dati si riferisce all'inferenza statistica che il ricercatore decide di eseguire dopo aver esaminato i dati (in contrasto con l'inferenza pre-pianificata, che il ricercatore pianifica prima di esaminare i dati). Lo snooping dei dati può essere fatto in modo professionale ed etico, o fuorviante e non etico, o fuorviante per ignoranza. Lo spionaggio dei dati in modo fuorviante per ignoranza è un errore comune nell'utilizzo delle statistiche.

[8] Il ***p-value*** (o valore p) viene definito in statistica come il livello di significatività osservato e rappresenta la probabilità che il possibile rifiuto dell'ipotesi nulla sia solo dovuto al caso.

[9] Il ***bootstrap*** è una tecnica statistica di ricampionamento con reimmissione per approssimare la distribuzione campionaria di una statistica. Permette perciò di approssimare media e varianza di uno stimatore, costruire intervalli di confidenza e calcolare p-value di test quando, in particolare, non si conosce la distribuzione della statistica di interesse.

[10] ***Il ruolo del tasso di errore familiare nella determinazione della significatività statistica.*** o

[11] ***Il tasso di false scoperte***.

esplorativa o si valutano gli esiti secondari di uno studio, potrebbe non essere necessario o desiderabile controllare per FWER, il che riduce la potenza dello studio. Tuttavia, la decisione di controllare per FWER dovrebbe essere decisa durante la progettazione dello studio.

Invece, *i**l tasso di false scoperte*** (FDR) è il tasso in cui le caratteristiche chiamate significative sono veramente nulle. Un FDR del 5% significa che, tra tutte le caratteristiche chiamate significative, il 5% di queste sono veramente nulle. Proprio come impostiamo alfa come soglia per il valore p per controllare l'FPR, possiamo anche impostare una soglia per il valore q, che è l'analogo FDR del valore p. Una soglia del valore p (alfa) di 0,05 produce un FPR del 5% tra tutte le caratteristiche veramente nulle. Una soglia del valore q di 0,05 produce un FDR del 5% tra tutte le caratteristiche chiamate significative. Il valore q è la proporzione prevista di falsi positivi tra tutte le caratteristiche pari o più estreme di quella osservata.

I risultati hanno mostrano che le regole tecniche di trading offrono un potere predittivo nei mercati delle criptovalute, dove il rendimento medio annualizzato per ogni famiglia di regole tecniche è statisticamente significativo con un livello del 5% per ogni criptovaluta. Inoltre, i risultati sono robusti alle misure corrette per il rischio e i costi di transazione di breakeven della maggior parte delle regole esaminate sono sostanzialmente più alti di quelli riscontrati nei mercati delle criptovalute.

Tenendo conto del ***data-snooping*** attraverso varie procedure di test di ipotesi multiple, gran parte delle regole di trading tecnico continua a registrare rendimenti significativi, indicando il potere predittivo e la redditività del trading tecnico nei mercati delle criptovalute.

In quanto più rilevante, tuttavia, è stato dimostrato come **l'implementazione di regole di trading tecnico riduca significativamente i potenziali *drawdown* affrontati dalla strategia *buy-and-hold* e quindi protegga gli investitori dalle perdite associate ai mercati delle criptovalute**.

Infine, si evidenzia come il Bitcoin non offra alcun rendimento positivo nel periodo fuori campione, ma come le altre criptovalute offrano rendimenti positivi e indici di Sharpe e Sortino[12] relativamente alti. Il successo delle regole del trading tecnico nel generare profitti consistenti è stato sempre oggetto di dibattito nella letteratura accademica.

È stato riscontrato che i professionisti utilizzano ampiamente l'analisi tecnica, con **Smith et al.**[13] che dimostrano che il 21,6% degli hedge fund utilizza l'analisi tecnica, mentre **Menkhoff**[14] riferisce che l'analisi tecnica è diffusa nel mercato dei cambi.

La letteratura ha esaminato dettagliatamente la performance dell'analisi tecnica poiché fornisce prove contro una delle teorie più rispettate in finanza, ossia l'ipotesi di un mercato efficiente. **L'efficienza del mercato in forma debole afferma che tutte le informazioni di prezzo disponibili devono riflettersi nei prezzi dei titoli e quindi l'uso dell'analisi tecnica risulta superflua.**

Dato che il mercato dei cambi è quello in cui l'analisi tecnica è più utilizzata, gli studi sono stati abbondanti e hanno indicato a lungo opportunità di profitto: questa letteratura mostra che semplici regole tecniche di trading sui tassi di cambio del dollaro hanno fornito 15 anni di rendimenti positivi, corretti per il rischio, durante gli anni '70 e '80 prima che questi rendimenti si estinguessero.

[12] L'Indice di Sortino, anche noto come Sortino ratio, è un indice di rischio finanziario sviluppato da Frank A. Sortino, simile all'Indice di Sharpe (o Sharpe ratio): esso si propone di misurare il rendimento di un'attività finanziaria corretto per il rischio. Per meglio dire, punta a misurare l'extrarendimento di un portafoglio rispetto al minimo accettabile (Minimum Acceptable Return, anche noto come MAR).

[13] D. M. Smith, N. Wang, Y. Wang, E. J. Zychowicz, "Sentiment and the effectiveness of technical analysis: Evidence from the hedge fund industry", Journal of Financial and Quantitative Analysis, vol. 51, pp. 1991–2013, 2016.

[14] L. Menkhoff, "The obstinate passion of foreign exchange professionals: Technical analysis", European Journal of Finance, vol. 145, pp. 936-972, 2007

In un'analisi completa, **Hsu et al.**[15] effettuano uno studio su larga scala delle regole tecniche di trading nel mercato dei cambi per 45 anni in 30 mercati sviluppati e in via di sviluppo e trovano alcune prove di sostanziale prevedibilità ed eccesso di redditività in entrambi.

Zarrabi et al.[16] mostrano che dal 1994 al 2014, le regole tecniche di trading sono state redditizie in sei valute quotate in dollari statunitensi; tuttavia, la redditività non è stata costante. Il mercato dei cambi non è l'unico mercato a riportare risultati significativi dall'impiego di regole tecniche di trading.

Nei mercati azionari, **Brock et al.**[17] mostrano che il trading tecnico fornisce una significativa prevedibilità su 90 anni per il Dow Jones Industrial Average, mentre **Sullivan et al.**[18] e White[19] mostrano che i risultati di **Brock et al.** non sono dovuti al data-snooping. Molti altri articoli hanno anche riportato risultati significativi per trading tecnico nei mercati azionari, come Shynkevich[20], Han et al.[21] e Neely et al.[22]. Ci sono inoltre prove di risultati significativi del trading tecnico nei mercati dei

[15] P. H. Hsu, M. P. Taylor, Z. Wang, "Technical trading: Is it still beating the foreign exchange market?", Journal of International Economics, vol. 102, pp. 188-208, USA, 2016.

[16] N. Zarrabi, S. Snaith, J. Coakley, "FX technical trading rules can be profitable sometimes!", International Review of Financial Analysis, Elsevier, vol. 49, pp. 113-127, 2017.

[17] W. Brock, J. Lakonishok, B. LeBaron, "Simple technical trading rules and the stochastic properties of stock returns", Journal of Finance, vol. 47, pp. 1731- 1764, USA, 1992.

[18] R. Sullivan, A. Timmermann, H. White, "Data-snooping, technical trading rule performance, and the bootstrap", Journal of Finance, vol. 354, pp. 1647– 1691, USA, 1999.

[19] H. White, "A reality check for data snooping", Econometrica, vol. 65, pp. 1097–1126, 2000.

[20] A. Shynkevich, "Performance of technical analysis in growth and small cap segments of the us equity market", Journal of Banking and Finance, vol. 36, pp. 193–208, 2012.

[21] Y. Han, T. Hu, K. Yang, "Are there exploitable trends in commodity futures prices?", Journal of Banking and Finance, vol. 70, pp. 214-234, USA, 2016.

[22] C. J. Neely, P. Weller, R. Dittmar, "Is technical analysis in the foreign exchange market profitable? A genetic programming approach", Journal of Financial and Quantitative Analysis, vol. 32, pp. 405-426, 1997.

future delle materie prime, mercati spot delle materie prime, mercati obbligazionari e gli ETF[23] sulle materie prime. Nonostante questi risultati, non c'è un chiaro consenso sulla prevedibilità delle regole di trading tecnico in letteratura, con molti articoli che indicano che le regole tecniche di trading non offrono alcun potere predittivo, specialmente se i costi di transazione vengono presi in considerazione.

2. DeFi.

Negli ultimi anni si sente sempre più parlare di DeFi, o **finanza decentralizzata, e molto spesso viene associata al mondo delle criptovalute e della blockchain.** La DeFi, è considerato per lo più un segnale rivoluzionario che si appresta a stravolgere la finanza cosi come oggi la conosciamo, **con l'obiettivo di rimuovere gli intermediari finanziari e gli enti centrali che governano l'attuale sistema economico (banche, aziende finanziarie...).** Le criptovalute sono spesso associate a questo ambito decentralizzato; **infatti, la finanza decentralizzata prende spunto proprio dalle Blockchain, ossia dalle tecnologie che stanno alla base delle criptovalute come Bitcoin ed Ethereum.**

DeFi, è in realtà un termine generico utilizzato per una vasta varietà di applicazioni finanziarie, in particolare indica quella tipologia di servizi finanziari ***peer-to-peer***[24] che **si sviluppano e vengono eseguiti su strutture che non sono controllate da gerarchie**, mentre normalmente, la maggior parte dei servizi finanziari sono controllati ed eseguiti da un ente centrale.

[23] Gli ETF (acronimo di Exchange Traded Funds) sono fondi o SICAV a basse commissioni di gestione negoziati in Borsa come le normali azioni. Si caratterizzano per il fatto di avere come unico obiettivo quello di replicare fedelmente l'andamento e quindi il rendimento di indici azionari, obbligazionari o di materie prime. Il mercato regolamentato gestito da Borsa Italiana e dedicato a questi strumenti si chiama ETFplus. Nati negli Stati Uniti nei primi anni '90, gli ETF sono entrati a far parte dei titoli a disposizione degli investitori italiani a partire dal settembre 2002.e Da allora hanno conseguito un successo crescente, testimoniato dall'incremento sia dei volumi degli scambi che delle masse in gestione e dal sempre più elevato numero di ETF portati in negoziazione nel mercato ETFplus.

[24] Il termine Peer-to-Peer inserito nella tecnologia dedicata alla finanza sta per scambio di Criptovalute attraverso un Network distribuito.

Dunque, ogni movimento finanziario è soggetto al controllo di un terzo, che decide o meno se approvarlo: tale tipo di sistema è noto come Finanza Centralizzata o CeFi (rappresenta la finanza classica); **tale caratteristica la differisce dalla DeFi dove è possibile scambiare beni, prestare o prendere in prestito denaro, il tutto legalmente e senza che nessun ente, come ad esempio le banche o il governo, si intrometta nelle attività private.**

L'aspetto della finanza decentralizzata, che attira gli *operatori -speculatori,* **è la possibilità di effettuare investimenti e guadagnare interessi completamente passivi, prospettiva che ha avvicinato tantissimi investitori**. Infatti, per quanto riguarda specialmente le crypto monete basate sul PoS, vi sono delle APY, molto più elevate per certi aspetti, rispetto agli altri mercati. **Esistono perlappunto, delle piattaforme che sfruttano la DeFi (es: pancakeSwap[25]) per permettere a chiunque di guadagnare passivamente degli interessi, semplicemente depositando il proprio denaro o la criptovaluta di riferimento.** Tali piattaforme hanno un successo crescente, tanto che al loro interno, miliardi di dollari sono stati depositati in vari protocolli di finanza decentralizzata.

La DeFi, dunque, mira ad offrire strumenti e servizi grazie alla blockchain e, di conseguenza, alle criptovalute. Si basa principalmente sugli smart contracts, anche detti contratti intelligenti, che prevedono una esecuzione automatica senza alcun intermediario.

Quest'ultimi **sono dei veri e propri programmi** che si avviano quando si verificano delle condizioni prestabilite, così facendo si elimina la possibilità, per una delle parti coinvolte, di decidere arbitrariamente di non rispettare pagamenti e/o

[25] PancakeSwap è un AMM, ovvero un exchange decentralizzato in stile UniSwap, che viene utilizzato da decine di migliaia di utenti per scambiare token contro token dello standard di BNB Chain, ovvero la blockchain che è legata a Binance. Il suo token di riferimento può essere utilizzato sia per partecipare alla governance, sia invece per lo staking e per il fornimento di liquidità. E anche come asset sul quale investire in senso stretto. Nell'approfondimento vedremo cos'è, come funziona e perché potrebbe essere interessante.

condizioni stabilite. Con la DeFi è possibile effettuare un gran numero di operazione come:

- ***Pagamenti***: trasferire denaro attraverso le criptovalute e, di conseguenza, effettuare dei pagamenti.

- Esecuzione degli ***smart contracts*** (V. § 15): sono un'innovativa forma contrattuale che vengono eseguiti nel momento in cui si presentano le condizioni prestabilite. Infatti, un carattere importante da cui nasce la DeFi, è rappresentata proprio da quest'ultimi che hanno il vantaggio di essere più veloci ed economici, rispetto a quelli classici e che inoltre permettono di effettuare le operazioni in maniera irreversibile ed in maniera automatica.

- ***Prestiti e depositi***: la DeFi ha come obiettivo quello di migliorare sempre di più la finanza centralizzata, offrendo strumenti e servizi come prestiti e depositi, pertanto, ricoprono anche una funzione ausiliaria della CeFi[26]. Spesso questi servizi prevedono come moneta di scambio le criptovalute o stablecoin, ossia quelle valute che replicano il valore delle monete FIAT e che quindi non cambiano di valore con il tempo.

- ***Investimenti e guadagni passivi***: si possono mettere a disposizione di varie piattaforme le proprie criptovalute, ottenendo in cambio dei rendimenti molto alti e completamente passivi e la maggior parte delle piattaforme, rilascia i guadagni ogni giorno/settimana.

- ***Trading***: è possibile effettuare le transazioni *peer-to-peer* di criptovalute, così come avviene per i titoli azionari nella CeFi.

Una delle blockchain più utilizzate per la finanza decentralizzata è Ethereum. Grazie alla sua particolare

[26] ***CeFi*** significa **Centralized Finance**, ovvero finanza centralizzata. Quando utilizziamo questo termine parlando di criptovalute, solitamente ci riferiamo a istituti finanziari che operano nel mondo degli asset digitali e permettono il credito e il debito attraverso di essi. Queste piattaforme sono dette di **lending** e **borrowing**; in esse la nostra posizione varierà tra lender e borrower (creditore e debitore) proprio in funzione di quale sarà la motivazione per cui le utilizziamo.La società paga chiunque voglia depositare all'interno della sua piattaforma un interesse annuo in funzione della tipologia di asset. Tale liquidità viene poi destinata a chiunque voglia ottenere un prestito. Chiaramente, il profitto della piattaforma dipenderà dalla differenza tra quello che viene chiesto al debitore e quello che invece viene dato al creditore.

blockchain, infatti, consente di costruire nuove applicazioni decentralizzate, anche chiamate ***Dapps***[27]. Definite le varie operazione possibili in DeFi, è possibile identificare le caratteristiche di quest'ambito:

- ***Flessibilità***: la DeFi consente di trasferire risorse in ogni momento e in completa libertà ovunque, senza commissioni e senza lunghe attese per il completamento delle operazioni.

- ***Assenza di autorità***: la DeFi non prevede alcuna autorità centrale lasciando il governo del sistema agli stessi utenti nella maggior parte dei casi.

- ***Rapidità***: il sistema DeFi è caratterizzato dalla velocità delle operazioni; i guadagni o le transazioni si aggiornano in modo molto rapido, questo perché le operazioni avvengono in maniera immediata.

- ***Trasparenza***: la DeFi può essere aperta e tutti i soggetti coinvolti nelle operazioni che a loro volta, possono avere accesso alle informazioni e alle transazioni effettuate[28].

- Per tutti: non è necessario rispettare dei requisiti minimi, tutti i servizi sono aperti a chiunque cosi come tutte le piattaforme. Purché sia ottenuto l'accesso creando un tuo ***wallet***[29], o in alcune piattaforme, un ***account***.

Uno degli obiettivi della finanza decentralizzata è quello di rendere accessibile il sistema economico a chi è stato tagliato fuori da quello tradizionale, in maniera efficiente e trasparente. Essa è stata sviluppata per dare una soluzione ad una serie di problemi presenti nella finanza centralizzata, la

[27] Le ***dapp*** sono un movimento crescente di applicazioni che usano Ethereum per interrompere modelli di business o inventarne di nuovi.

[28] Tale caratteristica dipende fortemente dal tipo di blockchain nella quale si opera: pubblica o privata.

[29] "***Un wallet per Bitcoin (così come qualsiasi altro wallet per le criptovalute) è un portafoglio digitale che conserva i materiali crittografici che ti permettono di accedere a un indirizzo pubblico di Bitcoin permettendo così l'esecuzione di transazioni***," dice Alexandre Kech, **CEO** di **Onchain Custodian**, un servizio di custodia per asset digitali. I wallet per Bitcoin non solo conservano le tue monete digitali, ma le tengono al sicuro con una chiave privata unica che garantisce che solo tu — e chiunque altro cui darai il tuo codice — possa aprire il wallet. Puoi considerare questa chiave come la password di un conto corrente online.

maggior parte nati proprio dall'esigenza di eliminare la figura centrale che gestisce ed eroga i vari servizi.

Ad oggi non si è in grado di definire se la mancanza di un'autorità centrale e delle caratteristiche indicate possano rappresentare un valore aggiunto ma, la cosa positiva, è che il sistema sia in continua evoluzione tant'è che, la finanza decentralizzata sta muovendo solamente i primi passi, ed è soggetta ad una innovazione costante che sta portando interessanti novità con nuove applicazioni ancor più sofisticate.

3. Origini.

È di comune esperienza associare il termine criptovaluta a quello di Bitcoin. Le criptovalute possono essere definite come "***uno strumento digitale impiegato per effettuare acquisti e vendite attraverso la crittografia, al fine di rendere sicure le transazioni, verificarle e controllare la creazione di nuova valuta.***"[30]. Nella sua definizione più pura, la crittografia non è altro che **una scrittura segreta**, cioè tale da non poter essere letta se non da chi conosce l'artificio usato nel comporla; **può essere realizzata col sistema della scrittura invisibile** (mediante inchiostri simpatici)**, della scrittura convenzionale** (ove però il testo ha un significato apparente diverso da quello effettivo), e della **scrittura cifrata** (ove il testo non ha significato logico se non per chi sa interpretarlo).

Nell'ambito delle **criptocurrencies**, tale definizione di applica al campo informatico e la finalità della crittografia risiede nel fatto che solo i destinatari delle informazioni siano in grado di leggere le stesse, evitando dunque che terzi soggetti riescano ad accedervi. Questo si basa su determinati algoritmi spesso molto complessi e controlla l'ingresso delle varie criptovalute nel sistema attraverso un processo definito "**mining**'', di cui si parlerà successivamente.

[30] Enciclopedia Treccani. Il vocabolo inglese deriva dalla fusione di cryptography (crittografia) e currency (valuta).

La più importante delle criptocurrencies, per la sua capitalizzazione, caratteristiche innovative e rivoluzionarie, oltre ad essere la prima moneta digitale, è il Bitcoin, valuta digitale che è salita alla ribalta ma che ancora stenta fortemente ad affermarsi come un reale mezzo di pagamento data la sua estrema volatilità e premesso che possa essere considerata come moneta.

Bitcoin è una criptovaluta che nacque e fu presentata nel 2008 ad opera di Satoshi Nakamoto[31], pseudonimo utilizzato dall'inventore di cui tutt'ora risulta incognita tale identità, l'idea di una rappresentazione digitale nasce con il movimento denominato cyberpunk, una corrente letteraria e artistica che pone le sue radici negli anni ottanta del XX secolo.

Tale movimento comincia ad essere influente nell'ambito digitale verso agli anni '80 con **l'obiettivo di mettere in risalto il tema della privacy**, che rappresenta una dei primi tasselli più importanti. Lo scopo era quello di tutelare e migliorare la privacy di ciascun individuo attraverso la crittografia: un'arma, studiata dai cyberpunk[32], al fine di fornire ai cittadini un mezzo che potesse essere per loro un nuovo strumento di difesa nei confronti delle autorità, difesa volta ad applicare il concetto di privacy nella sua pienezza, ovvero non di rendere le proprie azioni o i propri movimenti segreti e quindi nascosti dalle conoscenze di tutti gli altri soggetti, ma di renderli accessibili soltanto a coloro di cui si ha interesse a far conoscere le proprie

[31] Satoshi Nakamoto (中本哲史 Nakamoto Satoshi?) è lo pseudonimo della persona che ha inventato la criptovaluta Bitcoin (codice: BTC o XBT). Il termine "Bitcoin" fa riferimento anche al software open source progettato per implementare il protocollo di comunicazione e la rete peer-to-peer che ne risulta. Nel novembre del 2008 Satoshi Nakamoto pubblicò il protocollo Bitcoin su The Cryptography Mailing list sul sito metzdowd.com. Nel 2009 ha distribuito la prima versione del software client e successivamente ha contribuito al progetto in via anonima insieme ad altri sviluppatori, per ritirarsi dalla comunità di Bitcoin nel 2010. L'ultimo contatto da parte di Satoshi Nakamoto è stato nel 2011, quando dichiarò di essere passato ad altri progetti e di aver lasciato il Bitcoin in buone mani con Gavin Andresen.

[32] Il cyberpunk è un genere narrativo che trae spunto dalla critica alla possibilità di un pericoloso sviluppo senza limite della tecnologia e di un controllo capillare dell'individuo da parte di una società oppressiva, reinterpretandoli in chiave fantastica e trasponendoli in un ipotetico mondo futuro.

informazioni. Dunque, il concetto di **privacy inteso dai cyberpunk**, è un ideale di svelarsi al mondo in maniera selettiva e la crittografia rappresenta ciò che più di ogni altra cosa risulta essere l'essenza di questo pensiero. Soltanto coloro che dispongono le chiavi hanno la possibilità di poter decifrare il messaggio.

Tale processo portò i sostenitori del movimento a rendere pratico tale pensiero e dunque, negli anni'90 di cominciarono a scambiarsi informazioni attraverso delle mail crittografate, al fine di mantenere riservate le informazioni relative a questioni economiche e non solo. Di notevole importanza per questo movimento fu **David Chaum**[33] che, attraverso vari articoli, cominciò a dare una forma al mondo delle criptovalute. **Infatti, fu il fautore dell'invenzione *Digicash*[34], che rappresento la prima impresa ad integrare la crittografia con la moneta al fine di rendere anonime le transazioni con un sistema centralizzato e di compensazione**.

Tale moneta fu ideata nel 1995 e fu utilizzata una banca americana per effettuare micropagamenti.

Il guadagno, dell'impresa, deriva da una piccola commissione applicata ad ogni transazione effettuata. La **moneta Ecash**, seppur bene ideata, a livello pratico non riuscì a colpire pienamente l'interesse della clientela. Si pensa che il **fallimento di questa azienda, nel 1998**, sia frutto di una tecnologia che per

[33] David Lee Chaum (nato nel 1955) è un informatico, crittografo e inventore americano. È conosciuto come un pioniere della crittografia e delle tecnologie per la tutela della privacy e ampiamente riconosciuto come l'inventore del contante digitale. La sua dissertazione del 1982 "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups" è la prima proposta nota per un protocollo blockchain. Completo del codice per implementare il protocollo, la dissertazione di Chaum proponeva tutti gli elementi tranne uno della blockchain successivamente dettagliati nel whitepaper di Bitcoin. È stato definito "il padre dell'anonimato online", e "il padrino della criptovaluta".

[34] DigiCash Inc. è stata una società informatica, attiva nell'ambito della moneta elettronica e della gestione dei pagamenti online. Fu fondata nel 1989 da David Chaum, che impiegò una famiglia di protocolli crittografici da lui ideati per rendere anonime le transazioni nel web. La tecnologia fu implementata nell'anno successivo. DigiCash dichiarò bancarotta nel 1998 e successivamente le sue attività furono rilevate da eCash Technologies, a sua volta acquisita da Blucora (conosciuta ai tempi come Infospace, Inc.) il 19 febbraio 2002.

quel periodo, si stava evolvendo ad un passo talmente elevato tanto che molti utenti non riuscivano a raggiungere e capire tali tecnologie.

ECash (XEC) è la versione rinominata di Bitcoin Cash ABC (BCHA), a sua volta un fork di Bitcoin (BTC) e Bitcoin Cash (BCH). Si definisce una "criptovaluta progettata per essere utilizzata come denaro elettronico ". ECash mira esclusivamente ad essere un mezzo di transazione utilizzato per pagare beni e servizi. La moneta è stata rinominata il 1° luglio 2021 e da allora ha cercato di distinguersi dal suo predecessore. Le unità di base di eCash sono chiamate "bit" e sostituiscono le ingombranti posizioni decimali di Bitcoin Cash ABC. Invece di inviare 0,000001000 BTC, invierai 10 bit con ECash. ECash integra un livello di consenso Proof of Stake (PoS) chiamato "Avalanche", che non deve essere confuso con la blockchain Avalanche (AVAX). Dopo il rebranding, eCash ha annunciato che avrebbe convertito tutte le monete BCHA in XEC con un rapporto da uno a un milione. Gli sviluppatori della criptovaluta hanno puntato su tre miglioramenti principali:

- Ridimensionamento del throughput delle transazioni da 100 transazioni al secondo a più di cinque milioni di transazioni al secondo
- Migliorare l'esperienza di pagamento riducendo la finalità della transazione
- Estendere il protocollo e stabilire aggiornamenti senza fork.

David Chaum non era tuttavia l'unico soggetto che stava sperimentando quel qualcosa di innovativo riguardo al denaro digitale; infatti, seppur l'idea riguardo la protezione della privacy attraverso la crittografia, rimase un punto centrale anche per gli altri progetti, erano tanti i punti da poter migliorare

ulteriormente. **Nel 1997, Adam Back[35] perfezionò *Hashcash*[36], un algoritmo *proof-of-work*[37] utilizzato per limitare email spam.**

Dalla prospettiva di **Back**, si sviluppa nel 1998 **B-money**, un programma ideato da **Dai Wei**, con il fine di realizzare l'obiettivo di fuggire dal controllo delle istituzioni. **All'interno del paper che esponeva l'idea di criptovaluta, erano presenti due tipi di protocolli; il primo, consentiva ad ogni aderente di mantenere un database separato, contenente la quantità nominale di denaro appartenente all'utente stesso; nel secondo, delegava il conteggio dell'ammontare di denaro posseduto da ciascun utente a un sottoinsieme di partecipanti, che attraverso un incentivo economico (basato sulla teoria dei giochi), erano motivati a comportarsi in maniera onesta.**

Tale protocollo, ha fornito le idee di base nel **concetto di blockchain**. Il problema derivante da questo progetto, deriva dal non aver risolto la questione relativa alla double spending, tanto che rimase allo stato prettamente teorico. Nessuno di questi tre progetti, riuscì ad arrivare fino in fondo, ma ambe tre sono riuscite a creare le basi per il progetto di Nakamoto, anche se, molti sospetti ricadono infine su Nick Szabo, creatore di bit Gold

[35] Adam Back (nato nel luglio 1970) è un crittografo e cypherpunk britannico. È il CEO di Blockstream, che ha co-fondato nel 2014. Ha inventato Haschisch, che viene utilizzato nel processo di mining di Bitcoin.

[36] Il nome di HashCash si riferisce a una tecnologia di Proof of Work (PoW) utilizzato per ridurre al minimo la posta indesiderata (spam) e attacchi denial of service (conosciuto come DoS o Protezione). Questa tecnologia ha guadagnato ampia popolarità grazie alla sua implementazione in Bitcoin e molti altri criptovalute. La loro funzione in essi era quella di far parte dell'algoritmo di convalida dei blocchi. Tutto questo attraverso il processo di mining di criptovalute.

[37] Con il termine *Proof-of-Work (PoW)* si intende l'algoritmo di consenso alla base della rete Blockchain. In una Blockchain, questo algoritmo viene utilizzato per confermare le transazioni e produrre i nuovi blocchi della catena. La PoW incentiva i miner a competere tra loro nell'elaborazione degli scambi, ricevendo in cambio una ricompensa. All'interno della Blockchain, gli utenti inviano beni digitali l'uno all'altro. Un registro decentralizzato raccoglie ogni singola transazione: tuttavia, per poter essere considerate valide, queste devono essere prima approvate e organizzate in blocchi. Tale responsabilità ricade su speciali nodi chiamati miner; l'intero processo viene invece definito mining. Alla base di questo sistema troviamo complessi problemi matematici e la necessità di dimostrare semplicemente la soluzione.

nel 1998, che risulta essere considerato il diretto precursore del protocollo Bitcoin di Satoshi Nakamoto.

Si rilevano molte somiglianze nel progetto di Bitcoin e bit gold; in particolare per ciò che riguarda i meccanismi utilizzati per validare le transazioni e proteggere la rete decentralizzata: **entrambi i meccanismi, sono basati sul sistema *proof-of-work*. L'unica differenza, che li contraddistingue è relativa alla risoluzione del problema della double spending.** Questa loro vicinanza, in termini di operatività spesso porta ad accostare Szabo a Nakamoto, cosa che tutt'ora viene smentita.

Nel 2008 Szabo, ricevette una mail da parte di Satoshi Nakamoto, il cui allegato conteneva un paper, di circa 9 pagine, in cui si descriveva in maniera dettagliata tutte le informazioni relative al Bitcoin. Tale pdf diventerà noto come il **Bitcoin White paper.**

4. La Blockchain.

Nakamoto descrisse il funzionamento del Bitcoin introducendo per la prima volta il concetto di blockchain. **La blockchain è come ad un registro distribuito a rete paritetica ("*peerto-peer distributed ledger*") crittograficamente sicuro, di tipo append-only, immutabile e modificabile solo tramite consenso o accordo tra le parti ("*peers*")[38].**

Per comprendere appieno che cos'é la **blockchain** è necessario comrprendere i motivi per cui **la blockchain risulta essere la chiave di volta per il successo delle criptovalute**, e al tempo stesso uno strumento tecnologico primario utilizzato anche in molti altri ambiti.

La prima parola chiave della definizione di blockchain è il cosiddetto registro distribuito (*distributed ledger*), il quale sta ad indicare che la blockchain è del tutto assimilabile ad un registro ripartito tra tutti gli utenti del network, del quale ciascuno di essi ne possiede una copia completa.

[38] Imran Bashir, "Mastering Blockchain, Distributed ledger technology, decentralization, and smart contracts explained", 2 nd Edition, Packt Publishing, 2018.

Il registro distribuito si basa su un modello di architettura informatica noto come *Peer-to-Peer* (P2P) il cui funzionamento si fonda sul concetto di decentralizzazione del network.

Non si è infatti in presenza di un server centrale che raggiunge i client (gli utenti), bensì **ogni utente agisce da server e al tempo stesso da client in modo da decentralizzare il sistema**.

Questa proprietà permette agli utenti di effettuare transazioni senza il coinvolgimento di intermediari terzi, come ad esempio una banca.

Ritenere che la blockchain è crittograficamente sicura significa far riferimento al concetto di crittografia asimmetrica (o crittografia a chiave pubblica), la quale si basa sull'utilizzo di una chiave pubblica e una chiave privata per ogni utente nel network.

Le transazioni in una blockchain avvengono grazie alla coesistenza di questi due requisiti, senza i quali non sarebbe possibile trasferire i beni.

La chiave pubblica ("address") funge da "indirizzo" visibile e identifica ogni utente all'interno della blockchain. Ciascuno di essi è anche in possesso di una propria chiave privata che serve sia per autorizzare la transazione (per il mittente) sia per decriptarla (per il destinatario).

Per esempio, si ipotizzi per semplicità che nel network siano presenti solamente due utenti, A e B. Entrambi hanno a disposizione **due chiavi, una pubblica e una privata.**

A vuole inviare un bitcoin a B e per farlo, si serve della chiave pubblica di B. A avvia e autorizza, attraverso la sua chiave privata, la transazione inviando un BTC a B.

Da questo momento in poi, solo B è in grado di decriptare la transazione e ricevere il bitcoin, poiché solo lui è in possesso della sua chiave privata.

Altra caratteristica della blockchain è quella di essere ***append-only*** che può essere così spiegata: i nuovi dati vengono aggiunti nella blockchain in modo sequenziale e, una volta inseriti, non

possono essere più modificati se non in specifici casi molto particolari, come ad esempio rivendicando il Diritto all'Oblio ("***Right to be forgotten***") regolato negli articoli 17, 21 e 22 del Regolamento Generale Della Protezione dei Dati (GDPR). In ogni caso, situazioni simili sono da trattarsi separatamente e richiedono soluzioni tecniche ad hoc.

Per questo motivo, è consuetudine considerare la blockchain come una struttura immutabile. Alla fine, si trova la parte più delicata e critica della definizione, ovvero la caratteristica di essere modificabile solo tramite consenso o accordo tra le parti; da ciò si comprende il potenziale della decentralizzazione.

Secondo questa definizione, non vi è alcuna autorità centrale che ha il potere di modificare il registro, bensì ogni aggiornamento o variazione viene approvata solo dopo aver rispettato i criteri imposti dal protocollo della blockchain ed è aggiunta alla catena solo quando viene raggiunto un accordo tra tutti gli utenti del network.

Esistono diversi algoritmi che facilitano il raggiungimento dell'accordo, assicurando che tutte le parti siano allineate riguardo lo stato finale dei dati contenuti nel network della blockchain.

Il regolamento generale sulla protezione dei dati (GDPR) disciplina il modo in cui i dati personali devono essere raccolti, elaborati e cancellati. Il "diritto all'oblio", che ha ricevuto molta stampa dopo la **sentenza del 2014 della Corte di giustizia dell'UE**, ha stabilito il precedente per la disposizione sul diritto alla cancellazione contenuta nel GDPR. Naturalmente, dati gli interessi contrastanti e la natura iperconnessa di Internet, il diritto all'oblio è molto più complicato di un individuo che chiede semplicemente a un'organizzazione di cancellare i propri dati personali. Questo articolo esamina più da vicino quando le persone possono presentare una richiesta per il diritto all'oblio, il valore aggiunto per i residenti nell'UE e come le organizzazioni possono creare un modulo per il diritto all'oblio per garantire la conformità al GDPR.

Il diritto all'oblio figura nei considerando 65 e 66 e nell'articolo **17 del GDPR**[39] . Si afferma che "l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare i dati personali senza ingiustificato ritardo" se ricorre una delle diverse condizioni si applica. Il "ritardo indebito" è considerato di circa un mese. È inoltre necessario adottare misure ragionevoli per

[38] 1 L'interessato ha il diritto di ottenere dal responsabile del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il responsabile del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali se ricorre uno dei seguenti motivi:

1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
2. l'interessato revoca il consenso su cui si basa il trattamento ai sensi dell'articolo **6,** paragrafo 1, lettera a), o dell'articolo **9**, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
3. l'interessato si oppone al trattamento ai sensi **dell'articolo 21,** paragrafo 1 e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure l'interessato si oppone al trattamento ai sensi **dell'articolo 21,** paragrafo 2;
4. i dati personali sono stati trattati illecitamente;
5. i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
6. i dati personali sono stati raccolti in relazione all'offerta di servizi della società dell'informazione di cui **all'articolo 8**, paragrafo 1.

2. Se il responsabile del trattamento ha reso pubblici i dati personali ed è obbligato ai sensi del paragrafo 1 a cancellarli, il responsabile del trattamento, tenendo conto della tecnologia disponibile e dei costi di attuazione, adotta misure ragionevoli, comprese misure tecniche, per informare i responsabili del trattamento che sono trattamento dei dati personali di cui l'interessato ha richiesto la cancellazione da parte di tali titolari del trattamento di qualsiasi collegamento, copia o replica di tali dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento è necessario:

1. per l'esercizio del diritto alla libertà di espressione e di informazione;
2. per l'adempimento di un obbligo legale che richieda il trattamento ai sensi del diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento;
3. per motivi di interesse pubblico nel settore della sanità pubblica ai sensi **dell'articolo 9,** paragrafo 2, lettere h) e i), nonché **dell'articolo 9,** paragrafo 3;
4. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo **89,** paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale in lavorazione; O
5. per l'accertamento, l'esercizio o la difesa di azioni legali.

verificare che la persona che richiede la cancellazione sia effettivamente l'interessato.

Il diritto all'oblio coincide con il diritto delle persone di accedere alle proprie informazioni personali di cui **all'articolo 15**[40]. Il diritto di controllare i propri dati non ha senso se le persone non possono agire quando non acconsentono più al trattamento, quando ci sono errori significativi all'interno dei dati o se ritengono che le informazioni vengano archiviate inutilmente. In questi casi, un individuo può richiedere che i dati vengano cancellati. Ma questo non è un diritto assoluto. Se così fosse, avrebbero ragione i critici che sostengono che il diritto all'oblio non è altro che una riscrittura della storia. Pertanto, il GDPR segue una linea sottile sulla cancellazione dei dati.

[40] 1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, l'accesso ai dati personali e alle seguenti informazioni:

1. le finalità del trattamento;
2. le categorie di dati personali interessati;
3. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
4. ove possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
5. l'esistenza del diritto di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che riguardano l'interessato o di opporsi a tale trattamento;
6. il diritto di proporre reclamo a un'autorità di controllo;
7. se i dati personali non sono raccolti presso l'interessato, qualsiasi informazione disponibile sulla loro fonte;
8. l'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui **all'articolo 22**, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato delle garanzie adeguate ai sensi **dell'articolo 46** relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. Per eventuali ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta per via elettronica, e salvo diversa richiesta dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenerne copia di cui al comma 3 non lede i diritti e le libertà altrui.

All'articolo 17, il GDPR delinea le circostanze specifiche in cui si applica il diritto all'oblio. Un individuo ha il diritto alla cancellazione dei propri dati personali se:

- I dati personali non sono più necessari per lo scopo originariamente raccolto o elaborato da un'organizzazione.
- Un'organizzazione fa affidamento sul consenso di un individuo come base legale per il trattamento dei dati e tale individuo revoca il proprio consenso.
- Un'organizzazione fa affidamento su interessi legittimi come giustificazione per l'elaborazione dei dati di un individuo, l'individuo si oppone a tale elaborazione e non vi è alcun interesse legittimo prevalente per l'organizzazione a continuare con l'elaborazione.
- Un'organizzazione sta elaborando i dati personali per scopi di marketing diretto e l'individuo si oppone a tale elaborazione.
- Un'organizzazione ha elaborato illegalmente i dati personali di un individuo.
- Un'organizzazione deve cancellare i dati personali per rispettare una sentenza o un obbligo legale.
- Un'organizzazione ha elaborato i dati personali di un minore per offrire i propri servizi **della società dell'informazione.**

Tuttavia, il diritto di un'organizzazione di elaborare i dati di qualcuno potrebbe prevalere sul diritto all'oblio. Ecco i motivi citati nel GDPR che prevalgono sul diritto alla cancellazione:

- I dati vengono utilizzati per esercitare il diritto alla libertà di espressione e di informazione.
- I dati vengono utilizzati per rispettare una decisione o un obbligo legale.
- I dati vengono utilizzati per eseguire un'attività svolta nell'interesse pubblico o nell'esercizio dell'autorità ufficiale di un'organizzazione.
- I dati oggetto di trattamento sono necessari a fini di sanità pubblica e servono nell'interesse pubblico.

- I dati oggetto di trattamento sono necessari per svolgere attività di medicina preventiva o di medicina del lavoro. Ciò si applica solo quando i dati vengono elaborati da un operatore sanitario soggetto all'obbligo legale del segreto professionale.
- I dati rappresentano informazioni importanti che servono l'interesse pubblico, la ricerca scientifica, la ricerca storica o scopi statistici e dove la cancellazione dei dati potrebbe compromettere o interrompere il progresso verso il raggiungimento che era l'obiettivo del trattamento.
- I dati vengono utilizzati per l'istituzione di una difesa legale o nell'esercizio di altri diritti legali.

Inoltre, un'organizzazione può richiedere una "tariffa ragionevole" o rifiutare una richiesta di cancellazione dei dati personali se l'organizzazione può giustificare che la richiesta era infondata o eccessiva.

Come vedi le variabili in gioco sono tante e ogni richiesta dovrà essere valutata singolarmente. Aggiungete a ciò l'onere tecnico di tenere traccia di tutti i luoghi in cui i dati personali di un individuo vengono archiviati o elaborati ed è facile capire perché i nuovi diritti alla privacy del GDPR possono rappresentare un onere di conformità significativo per alcune organizzazioni.

5. Crittografia e firma digitale.

La crittografia si occupa dello studio dei metodi che permettono di rendere incomprensibile un messaggio a persone che non hanno l'autorizzazione alla sua lettura. Ad esempio se si ipotizza di criptare un messaggio, ad esempio: "*pubblica il seguente testo* …" sapendo che anche chi riceve ne ha una copia identica, si potrebbe sostituire ogni lettera del messaggio con un numero di sette cifre con la seguente regola: tre cifre per la pagina, due per la riga e due per la posizione della lettera (o dello spazio) su quella riga. Avrei dunque una successione di 140 cifre (i caratteri del messaggio sono 20, spazi compresi, moltiplicati per 7).

Per il ricevente non sarebbe difficile, utilizzando il testo già in suo possesso, risalire al testo originale, semplicemente consultando pagina, riga e posizione del carattere. **La procedura di criptaggio viene chiamata chiave e nell'esempio proposto consiste in un testo** (l'edizione specifica del codice civile) e in una regola (pagina, riga, posizione). Se chi riceve il messaggio criptato volesse rispondere potrebbe facilmente usare lo stesso procedimento. **La chiave è la stessa e serve sia per leggere che per scrivere il messaggio: in questo caso si parla di sistema a crittografia simmetrica.** Un sistema del genere non è però troppo difficile da violare con i moderni computer.

Negli anni '70 due ricercatori americani, Hellman e Whitfield, hanno ideato un sistema chiamato a crittografia asimmetrica, basato sull'uso di due chiavi: il messaggio criptato con la prima chiave è decriptato soltanto con la seconda chiave e viceversa, per cui la chiave che cripta un messaggio non riesce a decriptarlo.

La prima chiave di solito viene chiamata chiave pubblica, la seconda chiave privata. In sintesi, quindi, i messaggi criptati con la chiave privata sono comprensibili solo utilizzando la chiave pubblica, quelli criptati con la chiave pubblica sono comprensibili solo utilizzando quella privata.

Teoricamente non sarebbe impossibile violare questo sistema, ma viene considerato di fatto sicuro perché ci vorrebbe un intervallo di tempo molto ampio per decriptare un messaggio. **Si stima, ad esempio, che per violare un sistema che utilizza una chiave a 2048 cifre, anche disponendo di grandi potenze di calcolo, servano centinaia di anni.** Un esempio possibile è quello relativo alla posta elettronica. Tutti possono scrivere i messaggi, ma nessuno deve leggerli senza autorizzazione.

La persona A fornisce la sua chiave pubblica alla persona B (e a tutte le altre persone in contatto con la persona A), ma tiene con sé la chiave privata. Quando la persona B scrive un messaggio, lo cripta con la chiave pubblica di A e nessuno può leggerlo perché, essendo criptato, la chiave pubblica non serve.

L'unica persona che può leggere il messaggio è la A, grazie alla chiave privata. Essendo il sistema asimmetrico, non funziona al contrario. Se la persona A dovesse decidere di rispondere alla persona B utilizzando la sua chiave privata, il messaggio sarebbe leggibile da tutti quelli che dispongono della sua chiave pubblica, e questo però non è desiderabile.

La soluzione allora è semplice: è sufficiente che anche la persona B abbia la sua chiave pubblica e la sua chiave privata e il problema è risolto: ognuno dovrà utilizzare la chiave pubblica dell'altro nel momento in cui scrive il messaggio. La chiave pubblica non deve essere custodita con particolare attenzione, serve solo a far leggere il messaggio al proprietario della chiave. Al contrario quella privata deve essere conservata con grande cautela, perché se qualcuno dovesse sottrarla potrebbe accedere, nei casi più gravi, a tutte le proprietà ed eventualmente rubarle.

La tecnologia blockchain utilizza proprio questi principi per gestire la proprietà di un bene. **Le persone vengono identificate attraverso la chiave pubblica, per esempio con un codice di 40 caratteri**.

Nelle transazioni l'utente A deve fare riferimento alla chiave pubblica di B per trasferirgli un bene. Per fornire la prova che il proprietario A sia d'accordo sul passaggio di proprietà, viene utilizzata la sua chiave privata, come la firma nel caso dell'assegno. L'utente A deve scrivere un messaggio in cui si dichiara d'accordo, lo cripta con la sua chiave privata e ognuno potrà verificare l'effettiva volontà attraverso la chiave pubblica. Solo la chiave privata dunque autorizza le transazioni e conferma le intenzioni di farle per cui, come detto in precedenza, deve essere custodita con la massima attenzione.

6. La convalida di un blocco.

Rimane da spiegare, per concludere, la cosa più interessante, il motivo per cui l'operazione sia così costosa e antieconomica. Prima di tutto va sottolineato il fatto che il sistema è stato congegnato in modo tale che la soluzione non deve essere trovata grazie al talento di un gruppo di persone, ma deve al

contrario richiedere solo un numero altissimo di calcoli, proprio per garantirne la sicurezza.

La logica del problema è la seguente. **Si prende un testo, poi si calcola il suo hash**. Si ottiene un codice che dipende strettamente dal testo iniziale. Poi la regola prevede che si aggiunga un numero in coda al testo, in modo tale che il codice risultante, ottenuto con l'hash, inizi con quattro zeri. Si è già visto che basta una piccola variazione al testo per far cambiare totalmente l'hash finale, per cui l'unico modo possibile per arrivare alla soluzione è fare tutta una serie enorme di prove.

È necessario precisare che un hash è un elemento chiave della tecnologia blockchain e ha un'ampia utilità. È il risultato di una funzione hash, che è un'operazione crittografica che genera identificatori univoci e irripetibili da informazioni date. Il termine hash viene utilizzato per identificare una funzione crittografica molto importante nel mondo dei computer. Queste funzioni sono destinate principalmente a codificare i dati per formare una singola stringa di caratteri; tutto questo indipendentemente dalla quantità di dati inizialmente inseriti nella funzione. Queste funzioni servono a garantire l'autenticità dei dati, a memorizzare in modo sicuro le password e a firmare i documenti elettronici. Le funzioni hash sono ampiamente utilizzate nella tecnologia blockchain per aggiungere loro sicurezza. Bitcoin è un chiaro esempio di come gli hash possono essere utilizzati per rendere possibile la tecnologia delle criptovalute.

Quando verrà trovato un codice che inizia con quattro zeri, si avrà la soluzione richiesta. Altri modi non ce ne sono, se non andare per tentativi: si è visto in precedenza come la funzione di hash sia unidirezionale. Mentre trovare la soluzione è molto oneroso, la verifica è invece agevole: è sufficiente aggiungere al testo la soluzione appena trovata, applicare l'hash e controllare se inizia con quattro zeri: **il livello di difficoltà del problema ovviamente dipende dal numero di zeri richiesto**.

Più sarà alto, più il sistema sarà sicuro, ma inevitabilmente sarà più costoso e si avranno tempi più lunghi. I sistemi basati sulla blockchain possono avere esigenze differenti e quindi cambiare continuamente la difficoltà dei problemi.

Nel caso più famoso, Bitcoin, è programmaticamente previsto che la formazione di un blocco nuovo avvenga in media ogni dieci minuti, per cui la difficoltà deve essere adeguata di conseguenza.

Questo è possibile grazie ad un controllo sui tempi della formazione dei blocchi precedenti; in caso di aumento della velocità di inserimento si alza anche il livello di difficoltà. Un'altra caratteristica della blockchain che favorisce la sicurezza è la presenza di una marcatura temporale, il ***timestamp***[41]. Permette di associare una data e un orario ad ogni blocco, identificati in modo univoco da una stringa di caratteri.

Il problema che deve essere risolto dai miner prevede quindi un hash che tiene conto del contenuto del blocco, dell'ora della formazione del blocco, dell'hash del blocco precedente, del livello di difficoltà del blocco (inserito al suo interno per velocizzare il calcolo) ed infine la soluzione: il primo che arriva ad una soluzione ottiene una ricompensa.

7. La Blockchain nel Bitcoin.

La struttura di una blockchain è molto simile a quella di alcune strutture informatiche quali la lista concatenata o l'albero binario, all'interno dei quali le informazioni sono collegate tra loro attraverso i puntatori, il cui ruolo è quello di contenere un riferimento ai vari elementi presenti nella lista.

Il principio di funzionamento della blockchain è analogo a quello appena descritto, con la grande differenza che fa uso di puntatori "hash". Un puntatore hash esegue lo stesso compito di un puntatore normale, ovvero quello di indicare

[41] Con il termine *timestamp*, ci si riferisce, in ambito informatico, alla misurazione del tempo tramite il conteggio del numero di secondi a partire da una particolare data. Tale data, conosciuta come UNIX epoch, è stata fissata essere: **le ore 00:00:00 del 1° gennaio 1970 UTC.**

il luogo dove è immagazzinata l'informazione, ma con una peculiarità in più, ossia crittografare l'informazione a cui fa riferimento.

Questa è la ragione per cui, sebbene sia affine ad altre strutture, la blockchain risulta essere più resistente ai tentativi di manomissione e corruzione dei dati immagazzinati al suo interno. L'applicazione pratica più famosa e di maggior successo della blockchain è senza dubbio il Bitcoin.

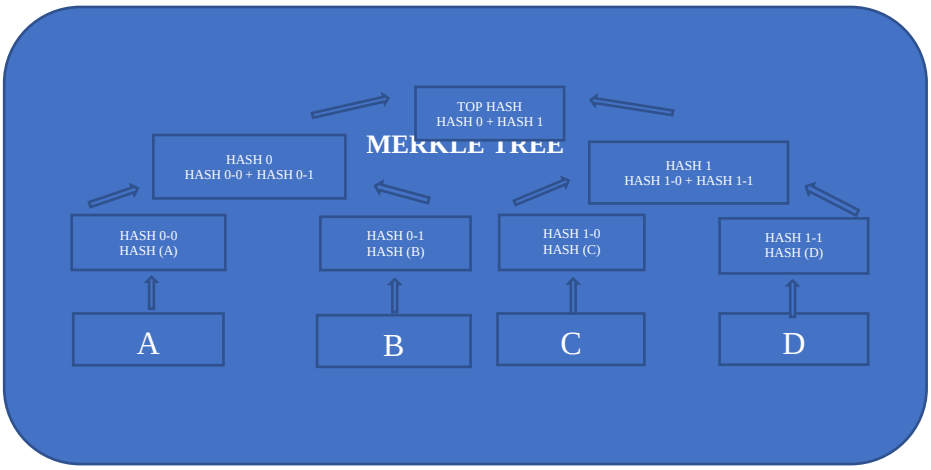
Tra gli elementi del *block header*, di particolare rilevanza è il *Merkle tree*[42] (conosciuto anche come "binary hash tree"); introdotto per la prima volta da *Ralph Merkle* e brevettato nel 1979, si tratta di una struttura utilizzata per verificare l'integrità di grandi ammontare di dati assicurando, in questo modo, che l'informazione contenuta nel blocco sia sicura e non abbia subito manomissione.

Innazitutto un *block header* (letteralmente "intestazione del blocco") è un identificatore univoco per un blocco presente su una blockchain. Questo viene utilizzato per identificare e verificare la validità dei singoli blocchi generati all'interno di una rete blockchain. Una blockchain è costituita da una serie di blocchi che vengono stratificati l'uno sopra l'altro e utilizzati per memorizzare informazioni relative alle transazioni che avvengono su una rete blockchain. Ogni blocco contiene un'intestazione univoca e ciascuno di questi è identificato individualmente dall'hash del *block header*. Il primo blocco della catena è anche noto come "blocco genesi" e non possiede

[42] I merkle tree sono una struttura dati creata con l'obiettivo di facilitare la verifica di grandi quantità di dati organizzati mettendoli in relazione attraverso varie tecniche crittografiche e di gestione delle informazioni. Un albero Merkle è una struttura dati suddivisa in diversi livelli il cui scopo è metterli in relazione nodo con un'unica radice associata ad essi. Per ottenere ciò, ogni nodo deve essere identificato con un identificatore univoco (hash). Questi nodi iniziali, chiamati nodi figlio (foglia), vengono quindi associati a un nodo superiore chiamato nodo padre (ramo). Il nodo padre avrà un identificatore univoco risultante dall'hash dei suoi nodi figli. Questa struttura si ripete fino al nodo radice o radice di Merkle (radice di Merkle), la cui impronta è associata a tutti i nodi dell'albero. Grazie a questa struttura unica, gli alberi Merkle consentono di mettere in relazione una grande quantità di dati in un unico punto (Merkle Root). In questo modo, la verifica e la validazione di questi dati può diventare molto efficiente, dovendo verificare solo la Merkle Root invece dell'intera struttura.

alcuna informazione sul blocco precedente. Il *block header*, inoltre, viene utilizzato per gestire tutti i blocchi di una blockchain (noti anche come nodi) e include tutti i metadati, l'hash crittografica e informazioni sul livello di difficoltà del blocco, il ***timestamp***, il Merkle root delle transazioni e il nonce. *Merkle tree*, noto anche come *hash tree*, è una struttura di dati utilizzata per la verifica e la sincronizzazione dei dati. È una struttura di dati ad albero in cui ogni nodo non foglia è un hash dei suoi nodi figli. Tutti i nodi foglia sono alla stessa profondità e sono il più a sinistra possibile. Mantiene l'integrità dei dati e utilizza le funzioni hash per questo scopo.

Funzioni hash: Quindi, prima di capire come funzionano gli alberi Merkle, dobbiamo capire come funzionano le funzioni hash. Una funzione hash associa un input a un output fisso e questo output è chiamato hash. L'output è unico per ogni input e ciò consente l'impronta digitale dei dati. Quindi, enormi quantità di dati possono essere facilmente identificate attraverso il loro hash.



Questo è un albero ***merkel binario***, l'hash superiore è un hash dell'intero albero.

- Questa struttura dell'albero consente una mappatura efficiente di dati enormi e piccole modifiche apportate ai dati possono essere facilmente identificate.

- Se vogliamo sapere dove si è verificata la modifica dei dati, possiamo verificare se i dati sono coerenti con l'hash di root e non dovremo attraversare l'intera struttura ma solo una piccola parte della struttura.
- L'hash radice viene utilizzato come impronta digitale per tutti i dati.

Come si evince, il Merkle tree è rappresentato come una struttura alla cui sommità troviamo il nodo radice, denominato "***Top Hash***" o "***Merkle root***", da cui si diramano i nodi foglie dell'albero. Alla base troviamo i "data blocks", ossia transazioni che sono state immagazzinate e codificate più volte. Codificando più volte i data blocks, si riescono a creare i nodi intermedi per risalire verso l'alto fino ad arrivare al Merkle root dell'albero.

Con questa struttura, qualora si verificasse un cambiamento o un tentativo di manomissione, si è sempre in grado di capire in quale parte della catena tale evento possa essersi verificato.

Ne consegue che **il Merkle tree è una delle maggiori implementazioni della blockchain ed è la caratteristica che contribuisce in maggior modo alla sicurezza e all'integrità delle informazioni**.

La blockchain, quindi, garantisce che un insieme di nodi appartenenti alla stessa rete, lavorino insieme, gestendo la rete in modo sincrono ed efficace.

La soluzione di Nakamoto è innovativa ma per esserlo richiede un certo consumo di energia e introduce un necessario ritardo tra la generazione di due blocchi, conseguenza quest'ultima di un sistema trustless funzionale e sicuro, a cui si sta rimediando sviluppando nuovi tipi di algoritmi di consenso.

8. Le Transazioni nella Blockchain del Bitcoin.

Nell'ecosistema del Bitcoin, le transazioni non sono tutte uguali e non necessariamente riguardano il trasferimento di moneta tra due utenti del network. **Infatti, la blockchain viene**

impiegata per scambiare molti altri tipi di asset digitali. Tuttavia, indipendentemente dalla loro natura, ogni transazione è composta da almeno un dato di input e uno di output.

In definitiva:

1) Un utente avvia la transazione attraverso l'utilizzo di un software (può essere un'applicazione mobile o per computer).

2) Il software appone la firma sulla transazione utilizzando la chiave privata del mittente.

3) La transazione viene propagata verso il network del Bitcoin attraverso un algoritmo di propagazione.

4) I nodi del network, i cosiddetti "***miners***[43]", approvano e aggiungono la transazione nel nuovo blocco che verrà creato successivamente. Tuttavia, poco prima di essere aggiunta, la transazione staziona in una memoria di buffer speciale chiamata "***transaction pool***[44]".

5) Il mining (processo mediante il quale la blockchain viene resa sicura) inizia e vengono generate nuove unità di moneta per i miners stessi come ricompensa peraver concesso al network risorse computazionali per poter approvare la transazione.

6) Non appena un miner risolve un "PoW" (***Proof of Work***), il processo di mining termina e il nuovo blocco appena creato viene trasmesso all'intero network.

[43] I custodi del registro che lo desiderano, possono non solo scambiarsi valute ma anche diventare minatori (miners). Questi raccolgono le ultime transazioni in un blocco (block) e aggiungono questo blocco alla catena dei blocchi precedenti che costituisce il registro. Questo registro si chiama Blockchain proprio perché, come ci dice la traduzione letterale dall'inglese, non è altro che una catena di blocchi, ciascuna a sua volta costituita da un insieme ordinato di registrazioni di singole transazioni.

[44] Un pool di transazioni o mempool è una struttura dati contenente l'insieme di transazioni che non sono state estratte ma che sono state convalidate da un processore di transazioni (o minatore). Un nodo ha diversi tipi di pool di transazioni e, a seconda di come una transazione è stata classificata, può essere archiviata in uno di essi. Esiste un'aspettativa che se una transazione viene inviata a un servizio di elaborazione delle transazioni o trasmessa sulla rete P2P, risulterà che tale transazione sia nota e conservata in un pool su ciascuno dei nodi di mining in tutta la rete.

7) I nodi verificano il nuovo blocco e lo propagano ulteriormente, in modo tale che il processo di validazione possa iniziare.

8) A questo punto, le notifiche di conferma vengono inviate al software del destinatario e, approssimativamente dopo tre "conferme", la transazione viene considerata ultimata e convalidata. Il numero di conferme può variare da tre a sei, ma è puramente convenzionale, tant'è che la transazione può essere considerata terminata anche solo dopo la prima conferma. La ratio alla base di questa attesa trova argomentazione nel fatto che, dopo tre conferme, la probabilità che si verifichi il fenomeno del double-spending è pressoché nulla.

Al punto 5) si è specificato che i miner vengono remunerati per le risorse offerte alla collettività, e sono loro stessi che determinano il costo (per loro definisce di fatto un guadagno) della transazione. Tale costo dipende dalla dimensione e dal peso della transazione ed è calcolato come differenza tra la somma degli input e la somma degli output. In termini di formula possiamo esprimere il costo come:

$$Costo = \sum(input) - \sum(output)$$

Il costo viene usato come incentivo per incoraggiare i miner a processare le transazioni che si susseguono e ad aggiungerle ai blocchi. **Tutte le transazioni convergono nella *transaction pool*, chiamata anche *memory pool*[45], che ha lo scopo di gestire una lista temporanea di tutte quelle transazioni che non sono ancora state convalidate.**

[45] Un pool di memoria è un blocco di memoria assegnato a uno specifico programma o applicazione sul computer. Le informazioni per un programma in esecuzione, come il sistema operativo o qualsiasi applicazione aperta sul computer, sono archiviate nella memoria ad accesso casuale (RAM) di un computer. L'assegnazione a ciascun programma di un blocco specifico di memoria utilizzando la tecnologia del pool di memoria evita il problema della sovrapposizione della memoria. La sovrapposizione si verifica quando due programmi tentano di utilizzare le stesse sezioni di memoria; come nel tentativo di condividere una fetta di torta, i programmi possono finire per "combattere" sulla **memoria condivisa**, causando errori nel sistema. Con un pool di memoria, a ciascun programma viene assegnata la propria "fetta", con il risultato di un funzionamento armonioso del computer.

Da qui, i miner possono prendere in carico le diverse transazioni secondo il loro ordine di priorità, **ovvero le transazioni che portano un maggior guadagno verranno processate per prime**. Tuttavia, non sempre le transazioni generano ricavi per i miner, poiché il valore delle ricompense non è fissato dal protocollo del Bitcoin ed è possibile che tale valore sia anche nullo. Ciò nonostante, oggigiorno ogni transazione determina un guadagno, seppur minimo, per il miner, in considerazione dell'alto volume di dati processati e dell'elevata competitività della rete del Bitcoin.

Una delle fasi cruciali del ciclo di vita di una transazione è la fase di verifica, la quale viene svolta dai vari nodi del network e prevede più passaggi che si possono articolare come segue:

1) Verifica che la sintassi e la struttura dei dati della transazione siano conformi alle regole previste dal protocollo del Bitcoin;

2) Verifica che nessun input e output siano valori vuoti;

3) Controllo che la dimensione in byte sia minore della massima dimensione consentita del blocco;

4) Verifica che l'output sia compreso nel range previsto (da 0 a 21 milioni di BTC);

5) Tutti gli input devono avere un riferimento specifico ad un output precedente, fatta eccezione per la prima transazione;

6) Verifica che la dimensione della transazione sia almeno pari a 100 byte, pena l'invalidità della stessa;

7) Negare le transazioni non-standard: una transazione viene negata se l'output generato per ogni input esiste in un'altra transazione nella pool;

8) Negare la transazione nel caso in cui il costo sia troppo piccolo per far in modo che la transazione venga processata.

9. Il Mining.

Il mining è il processo al termine del quale i nuovi blocchi generati vengono aggiunti alla blockchain. I blocchi contengono transazioni verificate e validate dai nodi del

network attraverso il processo di mining, e contribuiscono ad accrescere la catena del Bitcoin. La dimensione attuale della blockchain del Bitcoin, **gennaio 2023, è di circa 450 GB**[46]**.**

Nuovi blocchi vengono aggiunti alla catena approssimativamente ogni 10 minuti e la complessità della rete viene ricalibrata dinamicamente ogni 2016 blocchi per mantenere una condizione adeguata in tutta la blockchain. La complessità della blockchain può essere calcolata con la seguente equazione:

$$Target = Previuos\ target * Time\ /\ 2016 * 10$$

dove Target è sinonimo di complessità; Previous target è la complessità precedente e Time è il tempo speso per generare 2016 blocchi. La complessità del network indica sostanzialmente quanto sia complicato e dispendioso per i miner riuscire a generare un nuovo blocco. In altri termini, indica quanto sia complesso risolvere l'"***hashing puzzle***[47]" (o **Proof of Work, PoW**).

Una volta che un nodo si aggiunge alla rete del Bitcoin, questo incorre in alcuni task necessari con cui ogni *miner* deve interfacciarsi:

1) Sincronizzarsi con il network: il *miner* scarica la blockchain richiedendo lo storico dei blocchi che la compongono;

2) Validare le transazioni: le transazioni trasmesse alla rete devono essere validate dai nodi verificando e convalidando firme e output;

3) Validare i blocchi: i *miner* possono validare i blocchi dimostrando che questi rispettino le regole imposte dal protocollo;

[46] https://www.mokabyte.it/2023/01/13/bitcoinmm-3/#:~:text=Tale%20operazione%20pu%C3%B2%20richiedere%20fino,%C3%A8%20di%20circa%20450%20GB.

[47] Il puzzle è trovare il numero casuale che, una volta aggiunto all'intestazione del blocco, genera un hash con un certo numero di zeri iniziali. Provando un nuovo numero trilioni di volte al secondo, l'algoritmo del minatore tenta di trovare quello che genera i risultati desiderati.

4) Generare nuovi blocchi: i *miner* generano nuovi blocchi combinando le diverse transazioni che ricevono dal network;

5) Risolvere i ***Proof of Work***: questo task è il cuore dell'intero processo ed il motivo per cui i miner sono essenziali. Il ***block header***[48] di ogni blocco contiene un *nonce*[49] di 32 bit e ai miners viene richiesto di trovare un nuovo valore finché l'hash risultante sia minore della complessità attuale della rete;

6) Ottenere le ricompense: quando un miner risolve un hash puzzle (PoW), la soluzione viene immediatamente trasmessa al network, permettendo agli altri nodi di verificarla e di accettare il blocco.

Da quanto detto finora emerge che un fattore di fondamentale importanza che fa da comun denominatore a tutto il processo di mining è il Proof of Work.

Il PoW consiste essenzialmente in un problema da risolvere, attraverso l'utilizzo di risorse più o meno ingenti a seconda della prova, al fine di generare un blocco valido da aggiungere alla blockchain. Il PoW si basa sulla scelta casuale di un nodo ogni volta che un nuovo blocco deve essere creato. In questo modello, i nodi "competono" tra di loro per poter essere designati alla risoluzione del problema in proporzione con la loro capacità computazionale.

La seguente equazione riassume i requisiti del PoW nel bitcoin:

[48] Un ***block header*** (letteralmente "intestazione del blocco") è un identificatore univoco per un blocco presente su una blockchain. Questo viene utilizzato per identificare e verificare la validità dei singoli blocchi generati all'interno di una rete blockchain.

[49] In crittografia il termine ***nonce*** indica un numero, generalmente casuale o pseudo-casuale, che ha un utilizzo unico. Nonce deriva infatti dall'espressione inglese for the nonce, che significa appunto "per l'occasione". Un nonce viene utilizzato spesso nei protocolli di autenticazione per assicurare che i dati scambiati nelle vecchie comunicazioni non possano essere riutilizzati in attacchi di tipo replay attack. Ad esempio, i nonce sono usati nelle somme di controllo dei processi di autenticazione HTTP per calcolare gli hash MD5 delle password, come nell'esempio riportato in figura. Sono utilizzati ad esempio anche nella cosiddetta "catena dei blocchi", ossia la tecnologia che permette di effettuare e confermare le transazioni in bitcoin. I nonce sono differenti ogni volta che il codice di risposta del tentativo di autenticazione 401 è presentato, ed ogni richiesta di un client ha una sequenza numerica unica, così da rendere virtualmente impossibili attacchi di tipo replay-attack e attacchi a dizionario.

$$H\,(\,N\,||Phash\,||\,Tx\,||\,Tx\,||\,\ldots Tx) < Target$$

Dove N è un *nonce*, *Phash*[50] è un hash del blocco precedente, Tx rappresenta le transazioni nel blocco e Target è la complessità del network. L'equazione è un vincolo la cui soluzione è trovare un hash, dipendente dalla combinazione dei fattori precedentemente descritti, minore dell'hash target. Seppur non molto raffinato, l'unico modo per soddisfare tale vincolo è il cosiddetto ***trial and error***[51], ossia l'applicare più volte lo stesso metodo finché un determinato pattern non viene trovato dal miner.

La difficoltà del mining aumenta con il tempo e aumenta all'aumentare della complessità del network.

La ragione per cui il processo di mining diviene sempre più complesso risiede nel fatto che nella catena del Bitcoin è necessario generare un blocco ogni 10 minuti circa. **Questo vincolo ha come conseguenza il fatto che la difficoltà verrà aumentata se i blocchi verranno generati in meno di 10 minuti, mentre verrà diminuita se il tempo di creazione dei blocchi supererà i 10 minuti**. La difficoltà viene aggiornata ogni 2016 blocchi (circa due settimane).

Un fattore strettamente correlato alla complessità della rete è il cosiddetto hash rate, ossia il tasso di calcolo degli hash al secondo. In altre parole, è la velocità con cui i miner riescono a calcolare gli hash per riuscire a generare un blocco.

[50] Un hash percettivo è un'impronta digitale di un file multimediale derivata da varie caratteristiche dal suo contenuto. A differenza delle funzioni hash crittografiche che si basano sull'effetto valanga di piccoli cambiamenti nell'input che portano a drastici cambiamenti nell'output, gli hash percettivi sono "vicini" l'uno all'altro se le caratteristiche sono simili.

[51] **Prova ed errore** è un metodo fondamentale di risoluzione dei problemi caratterizzato da tentativi ripetuti e vari che vengono continuati fino al successo, o fino a quando il praticante smette di provare. Secondo WH Thorpe, il termine è stato ideato da C. Lloyd Morgan (1852-1936) dopo aver provato frasi simili "prova e fallimento" e "prova e pratica".

10. Zone di Mining.

Anche ai più alti livelli, sia a quello europeo (European Banking Authority), sia a quello italiano (Banca d'Italia), non sono mancati i pareri sulle criptovalute come strumenti di investimento. Ne hanno sottolineato i rischi e ne hanno sconsigliato il loro acquisto e il loro utilizzo, perlomeno finché non si arrivi ad un quadro normativo meno incerto e più stabile.

I pericoli legati alla bolla speculativa sono ormai sotto gli occhi di tutti, ma vale la pena sottolineare anche il rischio di insolvenze, di frodi o del cosiddetto "attacco del 51%". Come è comprensibile, l'operazione del mining per l'allungamento della catena dei blocchi, sta diventando sempre più costosa.

Nell'ipotesi, seppur poco probabile ma teoricamente possibile, che i quattro consorzi più grossi decidessero di allearsi, supererebbero la fatidica soglia del 51%. Questo potrebbe portare al cosiddetto "*double spending*" (faccio un acquisto e poi mi riprendo i soldi); si potrebbero altresì bloccare le altre transazioni o magari estorcere commissioni più alte. In pratica però questo attacco non avrebbe molto senso in quanto tutti gli utenti, vista l'insicurezza della rete, venderebbero presto tutti i loro bitcoin ed il prezzo crollerebbe quasi a zero, per cui i partecipanti all'attacco perderebbero alla fine tutto il loro patrimonio.

Al di là della fattibilità, rimane comunque il fatto che una tecnologia progettata appositamente per combattere la concentrazione potrebbe teoricamente favorire la nascita di un monopolio. Prendiamo in considerazione, inoltre, il pericolo, da parte degli utenti, di perdere i loro soldi.

Il caso più famoso riguarda sicuramente il fallimento nel 2014 di Mt.Gox[52], uno dei mercati di cambio più importanti di

[52] Mt. Gox, era il mercato di cambio più famoso di bitcoin, uno dei più vecchi e dei più popolari (negli ultimi sei mesi ha gestito circa il 21 per cento di tutte le transazioni bitcoin), chiudeva di colpo. La società con sede a Tokyo spariva di fatto dal web, sul sito solo un messaggio che spiegava come le transazioni fossero bloccate in attesa di fare alcune verifiche sulle ultime vicende. Insomma, un messaggio che non spiegava niente ma che mandava nel panico tutti quegli utenti che avevano depositato su Mt. Gox i propri bitcoin e che quindi non potevano più ritirarli. Mt. Gox era infatti uno dei maggiori

quel periodo. Negli ultimi mesi gestiva oltre il 20% di tutte le transazioni in bitcoin, ma, soprattutto operava come una banca, conservando i soldi dei suoi utenti.

A differenza delle banche, però, non era prevista una copertura di nessun tipo, né tanto meno una assicurazione, per cui i malcapitati utenti hanno seriamente rischiato di perdere tutto. Il mercato di cambio (Exchange) era stato acquistato da Mark Karpeles nel 2011, che lo fece diventare uno dei più popolari. Due settimane prima della chiusura erano stati sospesi i prelievi, con il motivo ufficiale della scoperta di un bug nel sistema delle transazioni che permetteva ad hacker di compiere attacchi informatici.

Secondo la Bitcoin Faundation, simili attacchi possono al più bloccare le transazioni, non manipolarle, in ogni caso 450 milioni di dollari di allora (5 miliardi con la quotazione odierna) svanirono e non si riuscì a capirne la causa con precisione. Karpeles, comunque, è sotto processo per truffa, appropriazione indebita e altre accuse penali, mentre per i creditori, dopo un'infinita battaglia legale, rimane la speranza, usciti dalla procedura fallimentare, di mettere le mani su un tesoretto di 200.000 bitcoin, sfuggiti agli hacker, che valgono oggi più di un miliardo di dollari.

Se il caso di Mt.Gox è il più clamoroso, ce se sono diversi altri che hanno coinvolto varie piattaforme.

cambiavalute (exchange) del settore, e in passato il suo cambio dettava la linea nella definizione di un prezzo standard dei bitcoin. Ma oltre a ciò faceva anche da banca per gli utenti, conservando i loro depositi. I bitcoin si possono custodire, a livello personale, in due forme diverse: su uno di questi exchange online o su un borsellino digitale salvato sul proprio pc. Chi li aveva messi su Mt. Gox al momento attuale, salvo colpi di scena futuri, deve considerarli persi. E diversamente dal fallimento di una banca tradizionale non esiste una copertura statale per i correntisti; inoltre non pare che Mt. Gox fosse assicurata o altro. Sul forum di Reddit c'è una lunga lista di utenti disperati per aver perso i propri soldi. La ragione ufficiale della chiusura era che Karpeles aveva scoperto un baco nel modo in cui le transazioni in bitcoin erano registrate dagli exchange, il che avrebbe potuto permettere delle truffe. Il nome per la presunta vulnerabilità è malleabilità delle transazioni, e anche altri exchange hanno fatto delle verifiche al riguardo. Questo tipo di problema ha permesso in effetti a degli hacker di compiere attacchi informatici (di tipo DDoS) contro i siti di exchange, attacchi che però possono solo rallentare o interrompere le operazioni, e non manipolarle, ha spiegato la Bitcoin Foundation.

Il sito Bitcoin Savings and Trust operava con un sistema Ponzi promettendo interessi del 7% a settimana. Chiuse nel 2012 con perdite per i suoi clienti stimate in 265.000 bitcoin. Nel maggio 2016 Gatecoin denunciò una violazione della sua piattaforma. L'attacco al sistema portò al trasferimento di criptovalute per un valore di due milioni di dollari, ma gli investitori furono ripagati. Sempre nel 2016, in giugno, un altro attacco informatico ha coinvolto The DAO, nato come fondo di investimento che raccoglie capitali in ethereum, la seconda per capitalizzazione delle criptovalute. Sfruttando un grave bug nel codice di programmazione qualcuno riuscì a portar via 3.5 milioni di ethereum (al cambio attuale 55 milioni di dollari).

Sempre sfruttando una falla nel sistema di sicurezza, qualche hacker nell'agosto 2016 ha rubato 120.000 bitcoin dagli account di Bitfinex, una delle maggiori piattaforme di trading, riconosciuta per la sua sicurezza.

Prima di tutto infatti offriva portafogli digitali unici per ogni cliente, a differenza di altre piattaforme che avevano portafogli comuni; aveva inoltre delle limitazioni sulla quantità di valuta digitale da ritirare, eppure tutte queste restrizioni sono state aggirate. Si è deciso di condividere le perdite, per cui ogni cliente dovette rinunciare al 36% del proprio portafoglio. È giusto chiarire, comunque, che tutti questi problemi non sono dovuti ad errori o a delle falle nella tecnologia delle criptovalute, intrinsecamente sicura, ma risalgono spesso alla gestione delle piattaforme di cambio o, sarebbe meglio dire, alla loro malagestione.

Il problema con la Blockchain semmai è legato alla tutela della chiave privata che va dunque costudita con massima attenzione. Se la si perde, i soldi diventano praticamente inaccessibili. È curioso come in un mondo digitale e immateriale possa essere utile un foglio di carta e, magari, una cara vecchia cassaforte.

Oltre ai timori sulla volatilità della moneta, sull'opacità del sistema, sui possibili crimini informatici e sulle connessioni col mercato nero, anche la crescente richiesta di energia ha

alimentato le discussioni nel mondo delle criptovalute. Abbiamo visto che alla base della creazione di bitcoin c'è un complesso processo matematico svolto da potenti computer che permette di generare nuove monete e validare tutte le transazioni.

Più si procede, più cresce il tasso di complessità dei calcoli, più aumenta il consumo di elettricità, per cui gli studi svolti finora concordano sul fatto che il fabbisogno sia destinato a salire in futuro.

I sei consorzi più grandi sono in Cina, dove il prezzo dell'energia elettrica è più basso rispetto a molti altri paesi, come pure il costo per l'affitto di terreni e capannoni. Il problema è che gran parte delle centrali elettriche sono a carbone, con un impatto ambientale preoccupante a causa della loro bassa qualità.

La questione di una produzione più sostenibile, sia sotto l'aspetto economico, sia sotto quello ecologico, ha portato alcuni grandi consorzi a ricercare l'utilizzo di energia pulita proprio in paesi come Canada o Islanda, anche per limitare i danni legati all'inquinamento e al riscaldamento globale.

11. Initial Coin Offering (ICO).

Le ICO (Initial Coin Offering) sono, letteralmente, offerte iniziali di moneta. Si tratta di una modalità non regolamentata, attraverso il quale solitamente una startup o un'azienda che opera nel settore delle criptovalute utilizza, per ottenere dei fondi. Tale modalità spesso viene utilizzata da queste imprese per bypassare i rigorosi e regolamentati processi di raccolta fondi richiesti dai venture capitalists oppure più semplicemente dalle banche. Quando un'azienda decide di voler raccogliere in questo modo del denaro, solitamente crea un piano attraverso un white paper dove viene indicato:

- Di cosa tratta il progetto
- Cosa manca per il suo completamento
- Quanto denaro è necessario per entrare a far parte dell'ICO
- Quanti token i creatori del progetto terranno per sé

- Che tipo di denaro è accettato

- Per quanto la campagna della ICO durerà

Durante la campagna, gli interessati compreranno parte delle criptovalute distribuite con valuta virtuale oppure con valuta classica. Queste monete vengono chiamate Token e sono simili alle azioni che un'azienda vende agli investitori durante una IPO (Offerta Pubblica Iniziale).

Se il denaro ricevuto durante l'ICO non dovesse raggiungere il valore minimo dei fondi richiesti dall'azienda, il denaro viene prontamente restituito agli investitori e l'offerta iniziale di monete viene contrassegnata come fallimentare. Se i fondi richiesti vengono invece raccolti con successo nella finestra di tempo specificata, il denaro viene utilizzato per iniziare il progetto oppure per completarlo.

Ovviamente, gli investitori iniziali sono motivati a comprare le criptovalute con la speranza che il piano possa diventare di successo dopo il lancio, fattore che potrebbe tradursi in un valore maggiore della criptovaluta rispetto al momento in cui venne acquistata. Inoltre, possedere dei token potrebbe dare all'investitore il diritto di prendere delle decisioni sul progetto, se previsto dal piano iniziale di offerta. Una buona parte delle ICO avvengono in Svizzera.

Secondo una recente classificazione dell'autorità finanziaria elvetica, la FINMA, si possono distinguere tre tipi di Token:

- Payment Tokens: ambiscono a costruire un mezzo di scambio a circolazione diffusa

- Utility tokens: assimilabili a voucher elettronici che offrono l'accesso a specifici servizi offerti dall'emittente

- Asset tokens: che vorrebbero rappresentare azioni o obbligazioni dell'emittente

Opportunatamente, l'autorità elvetica ha stabilito il principio per cui le criptovalute che pretendono di incorporare diritti dei detentori e doveri dell'emittente dovrebbero essere regolate di conseguenza. Tuttavia, ad oggi, gran parte delle criptovalute non generano alcuna

obbligazione a carico dell'emittente, ossia non lo impegnano in alcun modo: chi le compra non fa un investimento ma una speculazione. Dietro ad un investimento c'è sempre un'attività produttiva, mentre una speculazione è sorretta unicamente dall'aspettativa di guadagno.

Così, anche per le ICO, come per qualunque investimento, ogni reale successo dipende in ultima istanza dal prevalere dell'impresa produttiva sulla sterile speculazione. Sarà difficile immaginare che ciò avvenga senza una adeguata regolamentazione. I primi investitori avranno verosimilmente maggiori vantaggi inclusi nei loro token, come incentivi.

Primo fra tutti, il fatto di non essere sottoposti a tassazione, cosa che invece avviene con le IPO. Secondo punto a favore è che le vendite di token sono dirette e gli investitori basano le proprie decisioni sul contenuto dei progetti preparati dalla stessa società. Ovviamente, non va dimenticato che il collocamento di nuove azioni in borsa è soggetto a precise regole di supervisione regolamentare che tutelino gli investitori, mentre nel mercato delle criptovalute non esiste una regolamentazione che tuteli i partecipanti alla ICO, che possono quindi ritrovarsi con l'investimento azzerato e senza possibilità di rivalersi su alcuno.

Ci si ritrova quindi, in una situazione potenzialmente pericolosa, in quanto vi sono società con la possibilità di ottenere capitali anche in assenza di un prodotto concreto e, se queste dovessero fallire o non produrre alcun valore, non vi sarà alcuna chance di rivalsa per gli investitori.

Per quanto riguarda le ICO va ricordato il caso più famoso e di successo; è la piattaforma chiamata Ethereum, che ha gli Ether come token. Nel 2014, il progetto fu annunciato e la sua ICO riuscì ad ottenere ben 18 milioni di dollari in Bitcoin. Il progetto diventò realtà nel 2015: nel 2016 l'Ether raggiunse un valore di 14 dollari ed una capitalizzazione di mercato di oltre 1 miliardo di dollari e nel 2017 un valore di mercato pari a 30 miliardi di dollari pari ad un prezzo unitario di 300 dollari USA. Ad oggi, nel 2022, Ethereum è la seconda criptovaluta per capitalizzazione del mercato.

12. Bitcoin e Gold Standard.

Dato che la quantità complessiva di Bitcoin in circolazione è fissata da un algoritmo, alcuni hanno colto un'evidente correlazione tra Bitcoin e Gold Standard, il sistema monetario aureo nel quale la base monetaria è ancorata ad una quantità d'oro prestabilita.

Attraverso il **Gold Standard** i paesi legavano le rispettive monete all'oro, consentendone l'importazione e l'esportazione attraverso i confini. In questo modo il Gold Standard, come un sistema a valute di riserva, comporta lo stabilirsi di tassi di cambio fissi tra le valute; una volta che le Banche Centrali dei vari paesi abbiano fissato il prezzo dell'oro rispetto alla valuta nazionale, sarà possibile effettuare il cambio non solo tra l'oro e le singole valute aderenti al sistema ma tra le valute stesse.

Dopo vari tentativi di applicazione (l'ultimo dei quali nel 1947 attraverso gli accordi di Bretton Woods, rimasti in vigore fino alla crisi petrolifera del 1971), il Gold Standard venne definitivamente abbandonato, facendo spazio all'era tutt'ora in corso del denaro privo di una base aurea, la cosiddetta fiat money, in cui sono le Banche Centrali a regolare la quantità di denaro circolante nel paese e il suo costo attraverso il tasso di conto.

Il vantaggio del sistema fiat money è la flessibilità, che consente ai policy makers una migliore gestione dei periodi critici (come una guerra o un'improvvisa crisi petrolifera), attenuandone le conseguenze per la popolazione.

Attraverso il gold standard invece la gestione sociale risulta difficoltosa ed è impossibile abbattere la disoccupazione attraverso ad esempio politiche fiscali espansive (aumenti della spesa pubblica). Al tempo stesso tuttavia il sistema fiat money favorisce il verificarsi di problemi come quelli che l'economia mondiale sta vivendo in questo momento, ovvero il considerevole aumento della speculazione finanziaria, sostenuta dall'incertezza che si ha nel calcolare gli spostamenti di ricchezza dalle diverse zone del mondo.

Da quando l'oro non costituisce più la base dei sistemi monetari, e soprattutto dopo la crisi del 2008, i sostenitori del Gold Standard vedono nella sua riadozione il metodo migliore per stabilizzare il sistema monetario.

Tra questi Ron Paul, membro del partito repubblicano ed ex leader del movimento per il restauro del Gold Standard, il quale nel 1982 auspica addirittura l'abolizione della FED: Paul infatti riconosce nell'assenza del sistema autoregolatore tipico del sistema aureo, la motivazione del "dirigismo distruttivo" da parte della Banca Centrale Americana (Ron Paul, The Case for Gold: a Minority Report of the U.S. Gold Commission, 1982).

Tuttavia, sia concesso di precisare che, ammesso che ci sia una "soluzione", difficilmente questa può risiedere nei sistemi del passato (che hanno già dimostrato i propri limiti) ma debba piuttosto essere ricercata nelle innovazioni e nei cambiamenti che si profilano attualmente.

A questo punto, è doveroso chiedersi quali siano le analogie tra una moneta totalmente virtuale quale il Bitcoin e un metallo prezioso quale l'oro. Per farlo, consideriamo prima di tutto quali siano le proprietà che nel passato hanno reso l'oro la moneta di scambio per eccellenza. Tra le principali:

- Scarsità: in quanto disponibile in quantità limitata
- Durevolezza: è infatti un metallo nobile ed uno degli elementi più stabili in natura
- Divisibilità: per poter essere impiegato come bene di scambio
- Riserva di valore: dotato di un potere d'acquisto stabile nel tempo, garantito anche dalla impossibilità di contraffazione.

Andando a questo punto a confrontare le suddette qualità con quelle del Bitcoin, le somiglianze (dirette o indirette) sembrano numerose. Infatti riassumendone le principali caratteristiche:

1. Scarsità: abbiamo visto infatti che la possibilità di "trovare" monete decresce con il passare del tempo e con il numero di Bitcoin già immessi nel sistema. Il fatto che prima o poi si arriverà al momento in cui non sarà più possibile creare nuova

moneta, una volta stabilizzato il sistema, protegge gli utenti dal rischio di inflazione.

2. Impossibilità (o estrema difficoltà) di falsificazione: la crittografia offre la possibilità di evitare fenomeni come quello del double-spending.

3. Gestione peer-to-peer (P2P): è un sistema distribuito tra tutti i nodi della rete, senza fare capo ad un organismo centrale.

4. Facilità di implementazione: il codice è di tipo open source e non esistono costi di licenza. Inoltre è doveroso notare come l'attuale limitato volume di scambi renda il valore dei Bitcoin particolarmente volatile.

Tuttavia, se il suo uso continuasse ad aumentare, il valore potrebbe stabilizzarsi notevolmente e, come avviene per l'oro, aumentare con il tempo. Il teorico aumento di valore nel tempo andrebbe così a compensare la perdita di potere d'acquisto delle monete tradizionali dovuta all'inflazione.

"Una valuta digitale anonima e a prova di censura": così l'Electronic Frontier Foundation[53] (Associazione no profit che si occupa di libertà civili all'interno del contesto digitale) **definisce il Bitcoin, relativamente al fatto che qualsiasi transazione avvenga tramite questa valuta, risulti non tracciabile né censurabile. Ne deriva uno degli aspetti più discussi sul tema: se da una parte esiste il dubbio circa l'effettiva esistenza dell'anonimato, dall'altro ci si domanda se questo possa essere considerato un bene o meno.**

Relativamente al primo punto: per quanto a livello puramente teorico sia impossibile ricollegare una transazione all'individuo che l'ha effettuata, **nella realtà, occorre tenere presente che**

[53] La principale organizzazione no profit che difende la privacy digitale, la libertà di parola e l'innovazione. La Electronic Frontier Foundation è la principale organizzazione senza scopo di lucro che difende le libertà civili nel mondo digitale. Fondata nel 1990, EFF sostiene la privacy degli utenti, la libertà di espressione e l'innovazione attraverso contenziosi sull'impatto, analisi delle politiche, attivismo di base e sviluppo tecnologico. La missione di EFF è garantire che la tecnologia supporti la libertà, la giustizia e l'innovazione per tutte le persone del mondo. Anche nei primi giorni di Internet, EFF ha capito che proteggere l'accesso alla tecnologia era fondamentale per promuovere la libertà per tutti.

vengono sempre lasciati degli "indizi": ad ogni transazione; movimento; inserimento di Bitcoin in un wallet corrispondono sempre elementi che possono facilmente essere individuati attraverso sistemi di tracciamento, i quali sono già a disposizione delle agenzie governative.

Basti pensare alla semplice raccolta storica di dati che, se analizzati da esperti, possono facilmente condurre all'individuazione di un profilo univoco. Relativamente al secondo aspetto: naturalmente è intuibile, una volta assunto l'anonimato come condizione verificata nella maggior parte dei casi, quanti aspetti positivi e allo stesso tempo negativi esso possa apportare: **l'anonimato facilita ovviamente tutte quelle operazioni illegali che necessitano di tale condizione per la loro realizzazione; vedremo più approfonditamente nel terzo capitolo quanto fondamentale risulti l'anonimato nel commercio di stupefacenti realizzato attraverso il Dark Web.** Esistono tuttavia aspetti positivi di portata non indifferente: chiunque, nel rispetto delle leggi, può sfruttare la condizione di anonimato nello svolgere le proprie attività sottraendosi al controllo perenne delle autorità.

Occorre inoltre tenere presente come in molti paesi, caratterizzati ad esempio da una tassazione particolarmente alta o dal prelievo (di denaro contante) limitato e ristretto, l'alternativa proposta da una moneta anonima e autonoma potrebbe risultare particolarmente interessante, soprattutto in un'ottica di attrazione per nuove forme di investimento.

13. Non solo bitcoin: altre principali criptovalute.

Quando si parla di monete digitali, viene data sempre maggiore attenzione al Bitcoin, essendo questo il primo per capitalizzazione e per anzianità; come giusto che sia ne parleremo in maniera approfondita ma nel capitolo successivo, prendendolo come esempio in cui rientrano tutte le criptovalute analizzandone gli aspetti positivi e negativi. Ma per il momento, in questo paragrafo, ci focalizzeremo maggiormente a menzionare altre criptovalute, non di valore assimilabile al

Bitcoin (forse per il momento) ma certamente non di meno importanza.

Ad oggi, il mondo delle criptovalute è andando sempre più crescendo, tant'è che se ne possono contare più di 1000 diverse tra di loro, che prendono tutte il nome di ***Altcoins***[54]. Altcoins o anche dette alternative coins, sono tutte le crypto diverse da Bitcoin, esse sono nate per differenti obiettivi, alcuni per progetti più seri, altri per ottenere dei fondi, altre per truffa e altre ancora per Fomo (fear of missing out) cioè paura di perdere una grande occasione di guadagno.

Non tutte le altcoins sfruttano la tecnologia *peer-to-peer* e talvolta possono richiedere un processo di mining ai fini della validazione delle relative transazioni. Volendo fare un'analisi delle altre valute digitali che in questi anni si sono ritagliate uno spazio sempre maggiore, va premesso che sono, comunque, molto distanti dal Bitcoin, che resta in assoluto il leader di mercato in tutta la categoria delle monete digitali, vantando elementi chiave come una maggiore sicurezza, identità del marchio maggiormente riconoscibile ed uno sviluppo più attivo e razionale. Dopo aver fatto tali considerazioni, consideriamo alcune migliori criptovalute degli ultimi anni.

13.1 Ethereum.

Ethereum è la seconda blockchain pubblica in termini di valore e la prima in termini di utilizzo. Come il bitcoin, Ethereum opera su una cosiddetta blockchain pubblica: una rete globale distribuita, non censurata, aperta a tutti e senza alcuna autorità centrale. La differenza fondamentale con il bitcoin è che Ethereum permette di creare applicazioni che vengono eseguite e memorizzate sulla blockchain stessa, che è all'origine, tra

[54] Poiché il Bitcoin è la prima e più vecchia criptovaluta, è considerata una sorta di progenitore di tutte le altre oggi disponibili. Nell'aprile del 2018, Coinmarketcap ha elencato più di 1.500 criptovalute, e tutte, tranne il Bitcoin, rientrano nella categoria degli "altcoin". Gli altcoin sono criptovalute alternative al Bitcoin, la prima e più antica criptovaluta. Le criptovalute che sono state lanciate dopo il Bitcoin sono considerate altcoin che è un termine più ampio per indicare le criptovalute diverse dal Bitcoin.

l'altro, della finanza decentralizzata (DeFi). Tecnicamente parlando, Ethereum non è una criptovaluta.

Ethereum, nasce nel 2013 per opera di Vitalik Buterin, **uno sviluppatore di origini russe, cresciuto in Canada, che univa la competenza di programmatore e quello di ricercatore nell'ambito delle criptovalute**. Buterin si appoggiò ad una operazione di crowfunding durante il 2014 e fu nella condizione di completare Ethereum l'anno successivo quando divenne pubblico: **ha innovato in maniera decisiva e aggiunto nuove modalità di utilizzo all'interno del settore, introducendo la funzionalità smart contract, una soluzione che ha aperto la strada alla finanza decentralizzata (DeFi) e alle app decentralizzate, o Dapp.**

L'Ether è la criptovaluta di Ethereum. È infatti Ether, rappresentato dal simbolo ETH, a fungere da valuta di scambio sulla rete Ethereum. Gli Ether vengono scambiati sui mercati e il prezzo è stabilito dalla domanda e dall'offerta. L'ETH può quindi essere utilizzato per il trading, il mining o la semplice archiviazione in un portafoglio. L'Ether presenta diverse caratteristiche peculiari. La più importante da ricordare è che la sua emissione monetaria annuale è fissa e relativamente bassa. Ciò significa che ogni anno vengono creati pochissimi nuovi Ether. Si tratta quindi di un bene raro, ma a differenza del bitcoin, con i suoi 21 milioni di unità, non esiste un limite massimo assoluto.

Ethereum si basa sull'innovazione di Bitcoin, ma con grandi differenze. Entrambe ti permettono di utilizzare moneta digitale senza ricorrere a intermediari o banche. Ma Ethereum è programmabile, quindi la puoi usare per molti tipi diversi di risorse digitali, anche per Bitcoin stesso.

Questo significa anche che Ethereum non è solo pagamenti. È una piazza di servizi finanziari, giochi e app che non possono rubarti i dati e/o censurarti. Inoltre, Ethereum è una piattaforma blockchain open source che utilizza la sua valuta nativa, chiamata Ether o ETH. Tutte le commissioni sulle transazioni di rete sono pagate in ETH e quest'ultimo infatti, è responsabile

dell'alimentazione di quasi tutto ciò che accade all'interno della rete. La rete Ethereum può essere utilizzata da chiunque per creare ed eseguire smart contract, ovvero programmi software che funzionano autonomamente, senza l'intervento dell'utente.

L'Ether è una moneta virtuale accessibile a tutti e creata attraverso il mining. Per funzionare, Ethereum è una rete che richiede Ether. La blockchain di Ethereum è utilizzata per memorizzare la cronologia delle transazioni effettuate sulla rete. È anche in grado di memorizzare codici informatici. Ethereum è una tecnologia simile a una banca con un sistema di conti. La rete registra tutte le informazioni relative a questi conti. I token Ether vengono inseriti in un wallet. L'Ether finanzia le risorse di calcolo necessarie per l'esecuzione delle applicazioni. Il funzionamento è relativamente semplice. La differenza fondamentale tra Ethereum e bitcoin è che Ethereum può eseguire le cosiddette "transazioni condizionate". Ad esempio, è possibile creare una transazione di pagamento che verrà eseguita solo se è stata effettuata un'altra transazione o se il prezzo di un asset ha superato un determinato livello. Questi meccanismi di transazione sottoposta a condizione vengono solitamente definiti "smart contracts". Chiunque può sviluppare applicazioni su Ethereum. L'unico prerequisito è saper codificare in "Solidity", il linguaggio di programmazione della rete.

Una delle prime funzioni utilizzate è la "tokenizzazione", ovvero la creazione di nuove criptovalute. Sono chiamati "token", traducibile con "gettone digitale", emessi attraverso e ospitati sulla blockchain di Ethereum. I token possono essere detenuti, quantificati e scambiati digitalmente tra due persone. Con Ethereum, la creazione di un nuovo crypto-asset equivale alla generazione di uno smart contract e alla sua pubblicazione, e può richiedere anche pochi minuti. Il nuovo asset è immediatamente scambiabile, è protetto dalla rete ed è interoperabile con l'intero ecosistema Ethereum. I creatori si semplificano la vita e utilizzano l'infrastruttura esistente più o meno gratuitamente. Esistono diversi standard per i token. Mentre molti token rappresentano solo il proprio valore, altri

possono ora rappresentare prodotti finanziari tradizionali o oggetti del mondo reale. I token di cui abbiamo parlato sono legati alla distribuzione di un nuovo servizio o applicazione all'interno della blockchain di Ethereum. Il token in questione può essere utilizzato come valuta di scambio, ma può anche rappresentare una quota di un progetto, simile a un'azione. In quest'ultimo caso, potrebbe anche conferire il diritto di decisione sotto forma di voto. La blockchain di Ethereum consente di emettere diversi standard di token. Uno di questi standard ha visto un'accelerazione della sua adozione nel 2021: lo standard ERC721 per i token detti "non fungibili" (dall'inglese non-fungible tokens, NFT). L'Ether è una criptovaluta, al contrario degli NFT, anche se si tratta di due concetti non dissimili. Proprio come una criptovaluta, gli NFT possono essere trasferiti da un portafoglio a un altro.

La crescita di Ethereum può essere attribuita in parte alla sua capacità smart contract, che ha consentito un ecosistema in crescita di Dapp, token non fungibili (NFT) e altro ancora. Per impostazione predefinita, Ethereum utilizza il meccanismo di consenso ***Proof-of-work***[55] (Pow), ma la rete sta lentamente migrando a un ***Proof-of-stake***[56] (PoS) come parte del suo aggiornamento Ethereum 2.0. L'aggiornamento Ethereum 2.0 è iniziato a dicembre 2020 con il lancio della Beacon Chain. La comunità ETH ha supportato questo aggiornamento mettendo in

[55] V. nota 37.

[56] I sistemi di PoS offrono una maggiore democraticità, decentralizzazione e scalabilità rispetto ai sistemi di PoW e richiedono un minore dispendio energetico, tanto che anche Ethereum potrebbe presto passare a utilizzarli. Come molti sanno, nella tecnologia blockchain – così come in tutte le DLT – sistemi decentralizzati e distribuiti, la validazione delle operazioni contenute in un nuovo blocco avviene per opera del consenso distribuito, vale a dire il consenso della rete e non da parte di un ente centrale. Il meccanismo di consenso utilizzato determina le modalità con cui la rete può aggiornare e modificare le informazioni contenute nel registro. Gli algoritmi di consenso costituiscono, quindi, un elemento cruciale per ogni DLT, compresa la blockchain, in quanto hanno il compito di garantire l'integrità e la sicurezza delle informazioni conservate sui registri, attraverso il rispetto delle regole del protocollo. Esistono diversi tipi di algoritmi di consenso, i più comuni sono senza dubbio il Proof of Work (PoW) e il Proof of Stake (PoS).

staking 1 milione di ETH solo nella prima settimana. Ma perché cambiare e passare al proof-of-stake?

''Quello che stiamo costruendo non è più un giocattolo. Stiamo costruendo le fondamenta per il futuro di Internet'': Cosi Vitalik Buterin, spiega questa scelta mentre ancora teorizzava Ethereum 2.0. Quello che conta per il fondatore di Ethereum, è creare un sistema decentralizzato e democratico.

13.2 Ripple.

Ripple un intero protocollo che è nato per offrire trasferimenti rapidi, scalabili e a basso costo. Il suo focus negli anni si è concentrato sui trasferimenti transnazionali, cercando di proporsi sul mercato come intermediario e infrastruttura che possa competere con i sistemi di pagamento tradizionali, in particolare SWIFT, che sono oggi utilizzati dalle banche. Obiettivo già in parte centrato, dati i molti accordi che il gruppo è già riuscito a stringere con diversi gruppi bancari in diverse parti del mondo.

Ripple (XRP) nacque nel 2013 per mano di Chris Larsen Ryan Fugger e Jeb McCaleb ed attualmente per capitalizzazione rientra nella top 10. Come già accade per tutte le criptovalute, anche il valore dei **Ripple non si basa sulla circolazione di alcuna moneta fisica, bensì viene stabilito direttamente dai rapporti monetari che si possono scambiare solamente online.**

L'obiettivo non è quindi creare una nuova criptovaluta sul mercato ma nasce per:

- Costruire una rete di pagamento da utilizzare tra istituti finanziari come le banche;

- Mettere a disposizione un mezzo di pagamento che possa essere utilizzato dalle singole persone;

Fu creato per rendere le persone indipendenti da istituzioni finanziarie come banche e carte di credito.

Ripple un intero protocollo che è nato per offrire trasferimenti rapidi, scalabili e a basso costo. Il suo focus negli anni si è

concentrato sui trasferimenti transnazionali, cercando di proporsi sul mercato come intermediario e infrastruttura che possa competere con i sistemi di pagamento tradizionali, in particolare SWIFT, che sono oggi utilizzati dalle banche. Obiettivo già in parte centrato, dati i molti accordi che il gruppo è già riuscito a stringere con diversi gruppi bancari in diverse parti del mondo.

Benché Ripple sia una sorta di blockchain generalista, il suo focus è stato sempre quello di offrire servizi di livello corporate e bancario. Vocazione che non può essere considerata come velleitaria, dato che il grosso dell'utilizzo del suo chain e dei suoi servizi deriva proprio da quel comparto. Il sistema dei Cross Border Payments, ovvero dei pagamenti che devono superare un confine, è tra quelli più di successo del gruppo.

Il funzionamento dell'economia globale prevede che il trasferimento di fondi possa avvenire tra più istituti bancari, attraverso gli stati nazionali e in valute diverse. A tal fine, la maggioranza delle istituzioni finanziarie utilizza il sistema SWIFT (Society for Worldwide Interbank Financial Telecommunication), introdotto nel 1973. È un sistema caratterizzato da alcune inefficienze di processo e costi di commissione elevati.

Il codice SWIFT, anche chiamato BIC (Bank Identifier Code) o ISO 9362, fa parte delle informazioni necessarie per effettuare un trasferimento di fondi tra banche. È composto da 11 caratteri che contengono una serie di informazioni così suddivise:

- i primi 4 caratteri rappresentano la banca nel mondo;
- i 2 caratteri successivi identificano la nazione, secondo lo standard ISO 3166;
- 2 caratteri corrispondono alla città in cui si trova la banca;
- 3 caratteri (opzionali) rappresentano la filiale dell'istituto bancario

Nel caso in cui lo SWIFT code sia composto da 8 caratteri è possibile aggiungere in fondo al codice XXX, che rappresenta la sede della banca. Quindi, il codice SWIFT identifica nel mondo una specifica banca, inclusa la succursale, e assieme all'IBAN

fa parte dei riferimenti necessari a effettuare un trasferimento di denaro tra banche nell'area SEPA (l'iban non è ancora ampiamente diffuso in tutto il mondo). Oggi esistono due sistemi alternativi a SWIFT: CIPS e SPFS. CIPS (Cross-Border Interbank Payment System) è sistema di pagamento che offre servizi di compensazione e regolamento per i suoi partecipanti nei pagamenti e negli scambi transfrontalieri in RMB (sigla che indica sia l'unità monetaria base cinese, lo yuan, sia i suoi sottomultipli, jiao e fen). Sostenuto dalla People's Bank of China (PBOC), il CIPS è stato lanciato nel 2015 per internazionalizzare l'uso del RMB. Tra gli azionisti di CIPS ci sono anche banche straniere, tra le quali HSBC, Standard Chartered, la Banca dell'Asia orientale, DBS Bank, Citi, Australia e New Zealand Banking Group e BNP Paribas. Nel 2021 CIPS ha processato circa 80 trilioni di yuan (12,68 trilioni di dollari), facendo registrare un aumento del 75% rispetto all'anno precedente. Alla fine di gennaio del 2022, circa 1.280 istituzioni finanziarie in 103 Paesi e regioni nel mondo erano connesse al CIPS. SPFS è stato sviluppato nel 2015 dalla Banca centrale Russa proprio come alternativa al sistema SWIFT. Il sistema di messaggistica finanziaria che conta 399 utenti e che nell'aprile del 2021 ha visto allargare il suo bacino di banche, sino ad oggi ha gestito prevalentemente transazioni a livello nazionale ma ha da poco aperto anche a partecipanti estere. L'adesione e l'estromissione da questi sistemi di messaggistica, oggi più che mai, ricoprono un ruolo strategico non solo dal punto di vista finanziario ma anche geopolitico e rappresentano strumenti con un impatto enorme sulle economie dei Paesi che ne fanno parte o ne vengono esclusi.

È piuttosto lento per i pagamenti internazionali e dato il numero elevato di intermediari coinvolti. La rete Ripple si propone di sostituire SWIFT con un sistema universalmente compatibile, capace di produrre pagamenti in tempo reale, a costi molto bassi. Al momento non c'è un efficiente alternativa a SWIFT sulla Blockchain di Bitcoin in quanto, a causa dell'onerosità del meccanismo di consenso Proof.of Work, il

tempo medio di conferma di una transazione in Bitcoin può superare i 10 minuti.

Ripple ha introdotto un diverso algoritmo che permette la conferma delle transazioni in circa 4 secondi. Un punto che lo distingue dalle altre principali valute virtuali è sicuramente quello che, a differenza di queste ultime che utilizzano sistemi decentralizzati, Ripple ha un network centrale, servendosi di una piattaforma ‘’open source’’, in quanto ogni sviluppatore approvato può dare il proprio contributo con interventi ed eventuali modifiche.

13.3 Altre criptovalute.

Certamente, si sarebbero da dire tantissime cose in merito a decine e decine di criptovalute perché ognuna porta con sé delle novità importanti che, spesso, sono spunto per le più importanti al fine di rinnovarsi e migliorarsi. **Basti pensare al sistema Cardano (ADA) o anche più semplicemente alla Blockchain Terra, la cui crypto prende il nome LUNA, arrivando infine a SOLANA (SOL) non meno importante della sua sua Blockchain.** Di seguito verranno analizzati alcuni esempi.

CARDANO: Ideatore di Cardano è Charles Hoskinson, secondo il quale, dopo Ethereum era necessario pensare a un modello evolutivo, una sorta di blockchain di seconda generazione, da realizzare con particolare cura e attenzione.Cardano è la piattaforma sulla quale si è sviluppata ADA, criptovaluta che può essere utilizzata per inviare e ricevere fondi. Si tratta di una piattaforma di smart contract, con alcune caratteristiche simili ad Ethereum (non a caso dal momento che il suo ideatore, Charles Hoskinson, è uno dei co-fondatori di Ethereum) che offre nuovi livelli di sicurezza e scalabilità grazie a una architettura multilayer. Viene considerata un “unicum” nell’universo delle criptovalute perché nasce con un approccio scientifico e filosofico estremamente rigoroso. Ecco dunque che di Cardano si occupa non una bensì tre organizzazioni distinte: Cardano Foundation, organizzazione no profit che ha un ruolo di custodia rispetto a Cardano con il

compito di standardizzarne, proteggerne e promuoverne la tecnologia; IOHK, ovvero Input Output Hong Kong, fondata nel 2015 dallo stesso Hoskinson insieme a Jeremy Wood, che di fatto è una società di ricerca e sviluppo che si occupa di applicare le innovazioni in ambito blockchain per creare servizi finanziari accessibili a tutti, cui è stato affidato l'incarico di sviluppare, progettare e manutenere Cardano fino al prossimo anno; infine Emurgo, realtà giapponese che sviluppa e supporta iniziative commerciali innovative basate su tecnologia blockchain.

In cardano la blockchain è passata attraverso tre stadi evolutivi.

1. La blockchain di prima generazione è quella correlata ai bitcoin e ai trasferimenti monetari, che risponde a una esigenza fondamentale: creare nuove forme di trasferimento monetario senza intermediari. Il problema connesso a questa prima generazione di blockchain è che è una tecnologia limitata alle sole transazioni monetarie, senza possibilità di aggiungere condizioni all'esecuzione delle transazioni a meno di non aggiungere codici particolarmente complessi.
2. La seconda generazione di blockchain è quella di Ethereum e degli smart conctract, che consentono di scambiare denaro, proprietà, azioni in modo trasparente e senza intermediari. Una soluzione comunque perfettibile, visti i problemi di governance che nel tempo si sono registrati e che sono, ad esempio, culminati nella separazione tra Ethereum ed Ethereum Classic.
3. La terza generazione è quella di Cardano. Per lo sviluppo di questa soluzione Hoskinson ha preso il meglio dalle due generazioni precedenti, aggiungendo ulteriori elementi con l'obiettivo di risolvere tre grandi questioni fino a quel momento insolute:

- Scalabilità, aumentando il throughput grazie a un meccanismo di consenso basato sull'algoritmo proof-of-stake Ouroboros e aumentando la banda utilizzando nuove topologie di rete.

- Interoperabilità, grazie a un approccio specifico che mira a creare una sorta di "Internet delle blockchain", utilizzando le cosiddette sidechain.
- Sostenibilità, attraverso Patrocini e ICO.

Il tutto, va detto, con una attenzione spasmodica alla qualità del codice (Hoskinson parla di High Assurance Code), anche per prevenire possibili separazioni come accaduto in Ethereum. Cardano si distingue per un approccio particolare, quasi filosofico. Il team di sviluppo non è partito da una roadmap, bensì ha voluto per prima cosa identificare i principi, le best practice e le linee di sviluppo ai quali aderire, identificando una quindicina di punti cardine, che riportiamo come presentati sul sito ufficiale:

– Separazione di contabilità e calcolo su diversi livelli;

– Implementazione dei componenti core in codice modulare;

– Piccoli gruppi di accademici e sviluppatori in competizione con ricerche peer-reviewed;

– Ricorso a team interdisciplinari, inclusi gli esperti InfoSec;

• Rapida iterazione tra white paper, implementazione e nuove ricerche necessarie per correggere i problemi rilevati;

• Possibilità di aggiornare i sistemi in fase di post-deployment senza distruggere la rete;

• Sviluppo di un meccanismo di finanziamento decentralizzato per i lavori futuri
• Visione di lungo termine sul miglioramento del design delle criptovalute, perché possano funzionare su dispositivi mobili con un'esperienza utente ragionevole e sicura;

• Avvicinare gli stakeholder alle attività di gestione e manutenzione delle loro criptovalute;

• Riconoscimento della necessità di contabilizzare più risorse nello stesso libro mastro;

• Inclusione dei metadati opzionali nelle transazioni per meglio conformarsi alle esigenze dei sistemi legacy;

• Prendere in considerazione le caratteristiche migliori di tutte le valute alternative in circolazione;

• Adottare un processo basato sugli standard;

• Esplorare gli elementi sociali del commercio;

• Trovare una via di mezzo per consentire l'interazione con i regolatori senza compromettere i principi fondamentali ereditati da Bitcoin.

Il protocollo di Cardano lavora su due layer distinti: sul primo, il cosiddetto **Cardano Settlement Layer (CSL)** si trovano tutte le informazioni sulle transazioni, un po' come accade con Bitcoin (quanto, emissario, ricevente, momento del trasferimento), ed è sempre su questo livello che vengono trasferiti i token della piattaforma, ADA; il secondo livello, **il Cardano Control Layer (CCL)** gestisce invece i dati degli account, dunque le informazioni degli smart contract, come le identità digitali.

La separazione dei due livelli ha il duplice vantaggio di consentire di apportare gli aggiornamenti in modo separato e mirato e di aumentare la sicurezza, dal momento la compromissione di un layer non incide anche sul secondo. Cardano utilizza un protocollo proof-of-stake, che consente dunque agli sviluppatori di controllare in modo molto preciso a quali condizioni un utente può diventare stakeholder. Gli stakeholder possiedono un certo numero di coin che consente loro di verificare le transazioni che avvengono in rete. Se tuttavia lo stakeholder utilizza questi coin a proprio esclusivo vantaggio, il protocollo riconosce il comportamento, facendo decadere l'utente dallo status di stakeholder e facendogli perdere i coin in suo possesso.
Questo significa che a tutti gli stakeholder viene assegnato un ruolo e una funzione di controllo e verifica delle transazioni: più stakeholder le confermano, più transazioni vanno a buon fine. Il sistema ricompensa gli stakeholder per le loro attività di verifica dei blocchi.

LITECOIN: Altra importante criptovaluta e ***Litecoin***, una criptovaluta ed un progetto open-source ispirato fortemente al Bitcoin e rilasciato nel 2017. Litecoin è stato progettato per essere utillizato per piccole transazioni e per essere più efficiente

nell'uso quotidiano. Al contrario, il bitcoin è stato utilizzato più come riserva di valuta e per scopi a lungo termine. Il limite del trading è più rigoroso sul litecoin che sul bitcoin e il processo di *litecoin mining* è molto più veloce. Ciò significa che le transazioni sono più veloci e meno costose, anche se sono più piccole. Litecoin prevede la creazione e il trasferimento di monete digitali tramite un protocollo crittografico open source. Usa la tecnologia blockchain ovvero il registro pubblico decentralizzato o la lista di transazioni delle criptovalute. Mentre i litecoin richiedono una tecnologia più sofisticata per essere estratti rispetto al bitcoin, i blocchi però vengono generati fino a quattro volte più velocemente. I Litecoin elaborano inoltre le transazioni finanziarie molto più rapidamente e possono anche elaborarne un numero più elevato nello stesso periodo di tempo. Sia il bitcoin che il litecoin hanno un numero finito di monete in circolazione. Bitcoin ha 21 milioni di monete disponibili, mentre litecoin ha 84 milioni disponibili - quattro volte più del bitcoin. Litecoin ha una capitalizzazione molto più piccola del bitcoin, ma risulta ancora una delle criptovalute più scambiate. Quando acquisti un cambio litecoin, il suo prezzo è solitamente quotato rispetto al dollaro statunitense (USD). In altre parole, stai vendendo USD per poter acquistare litecoin. Se il prezzo del litecoin aumenta, potrai venderlo ottenendo un profitto, perché il litecoin ora vale più dollari di quando l'hai acquistato. Se il prezzo scende e decidi di vendere, ne risulterà una perdita.

L'idea chiave del progetto è quella di dare vita ad un'alternativa più veloce ed economica rispetto al Bitcoin. Nonostante ci siano alcune similarità con BTC, non è possibile definire il Litecoin senza sottolineare alcune differenze chiave: costo delle transazioni prossime allo zero, maggiore velocità di creazione di blocchi, nonché moneta più facile da minare.

Oggi il ***Litecoin*** è estremamente popolare ed ha una capitalizzazione di oltre 8 miliardi di dollari. ***Dogecoin***[57]: è un

[57] Dogecoin è una criptovaluta sempre più popolare. In Italia la sua adozione è ancora scarsa, ma a livello mondiale la sua capitalizzazione di mercato supera ormai i 400 milioni di dollari americani; tra coloro che ci credono c'è anche Elon Musk, il celebre fondatore di Tesla e di SpaceX che l'ha definita la sua criptovaluta preferita.

crypto peer-to-peer basata su blockchain. Inizialmente il dogecoin era una criptovaluta creata per scherzo, ispirata al tormentone della rete ‘’doge’’. Tuttavia col tempo attorno al Dogecoin si è radunata una grande e amichevole comunità, raggiungendo una capitalizzazione superiore al miliardo di dollari e divenendo una delle monete più importanti del mercato. Dogecoin nasce nel 2013, nello stato americano dell’Oregon, da un’idea del suo fondatore Billy Markus. Fin dal principio la mascotte del progetto è “Doge “, un simpatico cane di razza Shiba Inus che viene spesso utilizzato nel meme (foto divertenti) sul web. Cominciamo dicendo che si tratta di una criptovaluta “pura “, ovvero utilizzata esclusivamente per fare pagamenti. In questo è simile a Bitcoin, ma diversa da altri progetti come Ethereum o Ripple in cui l’aspetto delle transazioni è secondario. Dogecoin serve per comprare o vendere beni e servizi utilizzando un metodo di pagamento decentralizzato, sicuro, con costi minimi di commissione ed estremamente veloce.

DASH: è una criptovaluta totalmente diversa dalle altre. Non si tratta né di una piatttaforma di sviluppo, né di una grossa moneta con lunghi tempi di transazione. Lo scopo di Dash è totalmente diverso. Gli sviluppatori hanno progettato Dash per essere una criptovaluta simile a contanti digitali. Si tratta di una moneta liquida e veloce come il denaro tradizionale, che molti di noi utilizzano regolarmente in rete: l’amministrazione di questa criptovaluta è decentralizzata e alimentata dal mining, rendendola autonoma e indipendente da qualsiasi autorità esterna.

Dash la possiamo ovviamente considerare come una criptovaluta differente rispetto alle altre e ad altri progetti di criptovalute come ad esempio Ethereum o i Bitcoin. In sostanza potrebbe essere definito come una piattaforma di sviluppo che si avvale non solo di denaro elettronico decentralizzato per scambi di tipo peer-to-peer, il quale intende essere liquido come il denaro reale che utilizziamo giornalmente di Paese in Paese, ma che potrebbe essere anche paragonato alle normali valute come

ad esempio: USD; GBP; EUR; INR; CNY. La prima considerazione da fare è che Dash è costruito sulla base del codice utilizzato già per i Bitcoin ma con l'aggiunta di nuove funzionalità come ad esempio privacy e transazioni molto più veloci.

Come anche i BTC, Dash è una moneta open-source tanto che possiede una propria infrastruttura di blocchi, compreso anche portafogli e comunità. Dash è la locuzione che identifica una specifica criptovaluta che inizialmente era intesa come Darkcoin e XCoin. In sostanza si tratta di una criptovaluta open source che sfrutta uno scambio di tipologia peer-to-peer che si è posta come scopo quello di essere la criptovaluta più "amichevole" per tutti i trader ma anche quella maggiormente tradata da questi ultimi. Essa offre transazioni intense e transazioni private. Opera su di un modello auto-finanziato e auto-governante il quale abilita la rete dash a pagare individui e imprese per eseguire lavori che aggiungono valore alla rete. Una delle sue peculiarità è la governance decentralizzata di Dash che ha un sistema di budget tale da renderla la prima organizzazione autonoma decentralizzata.

Dash Coin definito come denaro contante completamente digitale (e quindi assolutamente non fisico) che permette di operare tramite una rete p2p completamente open source in maniera molto veloce e sicura, permette dunque di inviare e di ricevere denaro a bassissime commissioni. Tutto questo avviene all'interno di una rete completamente decentralizzata, che come abbiamo visto è sinonimo di sicurezza, anonimato e affidabilità. Il Dash, grazie alla sua rete completamente decentralizzata infatti non può essere assolutamente intercettata dalle banche centrali né gestita da queste, le quali non possono avere nessuna voce in capitolo all'interno del mondo delle criptovalute. Un aspetto molto interessante per chi utilizza il Dash è quello di offrire a tutti i trader la possibilità di inviare pagamenti praticamente istantanei in tutto il mondo con il massimo della privacy. In breve, altro non è se non un vantaggio molto

allettante per tutti i trader che desiderano iniziare intervenendo in prima persona nel mercato delle criptovalute.

Il tempo di mining è decisamente più veloce rispetto al Bitcoin. Una volta presentate alcune di queste criptovalute, accennato alla moneta digitale per eccellenza, il Bitcoin, e soprattutto aver spiegato la parte più difficile relativa al mondo tecnologico che vi è dietro che si affianca e si abbraccia all'economia, è il momento di riflettere sui risvolti economici dal lato positivo e negativo che le criptovalute apportano a questo mondo.

TERRA – LUNA: Terra è un network in blockchain per i pagamenti digitali, che si appoggia su diversi stablecoin di proprio conio e, per il funzionamento delle sue funzionalità aggiuntive, anche sul token LUNA. È uno dei progetti che ha guadagnato di più nel corso del 2021 ed uno dei più interessanti, sia per il mondo dei tecnici delle criptovalute sia per chi è a caccia di investimenti e diversificazione del proprio portafoglio. Terra è un network in blockchain che oggi offre i tre primitivi del mondo finanziario: possibilità di pagamento, possibilità di investimento (e scambio di titoli) e accantonamento risparmi. Come diventerà più chiaro nel nostro approndimento, abbiamo davanti uno dei sistemi più complessi che abbiamo mai avuto modo di recensire all'interno di Criptovaluta.it. La genesi di Terra e del suo token si ha nell'ambito degli e-commerce. La società è stata infatti fondata da Daniel Shin e Do Kwon, coreani che erano già stati coinvolti nella creazione di sistemi di pagamenti molto utilizzati nel sud-est asiatico e in Corea e anche nello sviluppo e nella fondazione di diversi sistemi di e-commerce. Tramite il sistema Anchor è possibile bloccare della liquidità all'interno del progetto per ottenere dei rendimenti. Sono rendimenti alti rispetto a quanto possono offrire oggi le banche, ma comunque relativamente bassi nell'ambito del mercato delle criptovalute.

La nota positiva è che è possibile bloccare somme anche in stablecoin, rimanendo dunque al di fuori delle oscillazioni

naturali di token crypto come LUNA. La stessa società che gestisce Terra ha fondato anche il sistema Mirror, che integra nella medesima blockchain un sistema intelligente per la tokenizzazione di asset finanziari e non. È possibile, ad esempio, creare un token che rappresenta esattamente il valore delle Azioni Apple, o di qualunque altro titolo quotato in borsa. Il token sarà scambiabile all'interno del network e potrà essere convertito in qualunque momento in denaro.

Il sistema è integrato lungo i tre primitivi del sistema economico: ovvero pagamenti, investimenti e risparmio, con soluzioni intelligenti e innovative e che hanno reso Terra uno dei progetti più interessanti del 2021. Relativamente al sistema di pagamenti, Terra emette degli stablecoin che sono ancorati alla divisa nazionale coreana, a quella mongola e anche al dollaro USA. Un sistema che mette al riparo dalla volatilità delle criptovalute e che è di assoluta stabilità, pur ricorrendo ad un sistema interno basato proprio sui token LUNA. L'aspetto di base del sistema Terra (LUNA) è network di pagamenti, che è già molto popolare attraverso l'App CHAI in Corea del Sud e MemePay in Mongolia. Il sistema è diffuso ubiquamente, viene accettato da moltissimi shop online e muove già circa 1 miliardo di dollari ogni anno.

Gli utenti attivi sono oltre 2 milioni, per un progetto che è in fortissima espansione. In questo caso il network Terra si comporta da intermediario decentralizzato, che permette di spostare gli stablecoin da un wallet all'altro. Il prezzo viene ancorato a quello ufficiale delle valute con un sistema libero e basato sull'arbitraggio. Per ogni stablecoin token emesso, esiste un controvalore in LUNA. Al crescere della domanda per Luna, si aprono situazioni di arbitraggio che i partecipanti al network hanno interesse a riportare in equilibrio, perché si tratta di operazioni con guadagni molto facili. Nel caso di maggiore richiesta per Luna, questo si riflette in un guadagno relativamente distribuito sul network; in caso contrario, ovvero nel caso in cui dollaro USA, di Singapore, Won Coreani,

le perdite sono assorbite, ugualmente, dal network nel suo complesso.

Il sistema Mirror è una delle prime aggiunte al network ed è stato sviluppato dalla stessa casa madre che si occupa di gestire la blockchain Terra. Il sistema permette di creare degli asset tokenizzati che rappresentano il valore di un asset finanziario esterno alla blockchain. Per farlo, è necessario depositare il 150% del controvalore dell'asset tokenizzato, che sarà per sempre ancorato al token che abbiamo creato.

Qualora la copertura non fosse sufficiente, il token viene distrutto e liquidato il controvalore al detentore in quel momento. Immaginiamo che le Azioni Apple che abbiamo tokenizzato, ottenendo un token mApple, crescano di valore dell'80% durante la vita del token. Al raggiungimento della soglia del 150% del valore iniziale, il token viene liquidato, ovvero distrutto, e il detentore incasserà il 150% di controvalore in UST, ovvero nello stablecoin che Terra ancora al dollaro USA.

All'interno del network di Luna è possibile anche scambiarsi questi token, permettendo almeno in via teorica la creazione di un mercato di derivati molto efficiente e con costi di transazione estremamente più bassi rispetto ai broker OTC (Over The Counter). Questo aspetto è uno dei più interessanti del progetto Terra/Luna, anche se con ogni probabilità dovrà attirare, nel futuro di breve periodo, le attenzioni del regolatore, almeno se dovesse cercare di diffondersi all'interno del continente Europeo o negli Stati Uniti.

Per tenere traccia dei prezzi confermati degli asset finanziari che si trovano al di fuori della sua blockchain, Terra integra nel suo progetto gli Oracoli di un altro progetto crypto, ovvero Band. I prezzi sono aggiornati ogni 30 secondi e permettono di avere un mercato efficiente, a basso costo di transazione e soprattutto utile anche per il Trading di breve periodo. A chiudere il quadro delle funzionalità che sono utilizzate dal sistema Terra troviamo Anchor, che è legato ad altre criptovalute emergenti come Solana e Cosmos, nonché alla

Web3 foundation che gestisce anche Polkadot e Kusama. Questo sistema permette di offrire lending dinamico, con prezzi che si muovono automaticamente per far incontrare domanda e offerta. Un buon modo per far fruttare la liquidità che mettiamo a disposizione del network.

SOLANA (SOL): è una criptovaluta progettata per funzionare in modo simile a Ethereum . Solana[58], nasce da un'idea dello sviluppatore di software Anatoly Yakovenko. Nel 2023, finora, Solana ha registrato una crescita del 150%, e a inizio febbraio valeva intorno ai 25$. Tuttavia questo rappresenta soltanto un decimo di quanto valeva nel 2021. Quell'anno, Solana ha raggiunto un picco di 248$. La criptovaluta ha subito in particolare l'effetto del fallimento del crypto exchange FTX a novembre 2022; Solana, sostenuta dal fondatore di FTX Sam Bankman-Fried, oggi agli arresti domiciliari e sotto inchiesta per truffa, ha perso il 94% lo scorso anno. Solana è stata lanciata a marzo 2020 e in breve tempo è diventata una criptovaluta popolare, posizionandosi tra le prime 10 criptovalute per capitalizzazione di mercato. Oggi tuttavia non fa più parte della top 10[59].

Solana è una blockchain che presenta notevoli somiglianze con Ethereum. Il token SOL può essere acquistato sulla maggior parte delle borse crypto. Il vero valore del token consiste nel condurre transazioni sulla rete Solana, che presenta vantaggi unici. La blockchain di Solana utilizza un meccanismo di consenso ***proof-of-history***. Questo algoritmo utilizza i timestamp per definire il blocco successivo nella catena di Solana. La maggior parte delle prime criptovalute, come Bitcoin e Litecoin, utilizzano il protocollo cosiddetto proof of work per definire i blocchi delle loro catene. Questo

[58] Prende il nome da una cittadina costiera della California meridionale.

[59] Nell'agosto 2022 l'ecosistema di Solana è stato anche vittima di un hackeraggio. Potrebbe esserci stata una compromissione di una chiave privata che ha permesso agli hacker di rubare token Solana, noti come SOL, da Slope, Phantom e TrustWallet, tre siti che offrono portafogli per criptovalute collegati a Internet. L'ammontare dei token rubati potrebbe essere stato equivalente a sei milioni di dollari: la quotazione di Solana dell'epoca.

algoritmo utilizza un meccanismo di consenso che si basa sui minatori per determinare il blocco successivo; questo sistema di proof of work è lento e richiede molte risorse, con conseguente consumo di enormi quantità di energia. **Questo è uno dei motivi del recente merge di Ethereum, in cui la rete si convertirà a un sistema proof of stake.** A differenza del meccanismo proof of work, il proof of stake utilizza lo staking per definire il blocco successivo. Ovvero, i token puntati sono tenuti come garanzia dalla blockchain fino a quando i validatori non raggiungono un consenso sul blocco successivo della catena. Secondo Konstantin Anissimov, direttore operativo della borsa di criptovalute CEX.IO, Solana utilizza "***un mix di strategie crittografiche collaudate nel tempo e di innovazioni per risolvere le carenze della prima ondata delle criptovalute***". Il problema principale che Solana cercava di risolvere era quello della scalabilità di Ethereum, sfruttando la sua combinazione unica di algoritmi di proof of history e delegated proof of stake (DPoS), una variante del più tradizionale protocollo di proof of stake.

Solana offre agli utenti diversi vantaggi grazie al suo sistema delegated proof of stake. L'algoritmo storico aggiunge un livello di sicurezza alla rete, afferma Christian Hazim, analista del provider di ETF Global X. In sostanza, Solana affronta due dei tre problemi identificati dal co-fondatore di Ethereum Vitalik Buterin nel suo trilemma della blockchain: **scalabilità, sicurezza e decentralizzazione**. Buterin aveva sostenuto inizialmente che Ethereum avrebbe affrontato tutti e tre gli aspetti, ma la maggior parte degli esperti ritiene che ne affronti solo due: sicurezza e decentralizzazione. Solana è stata invece progettata per risolvere i problemi di sicurezza e scalabilità. L'algoritmo di prova della storia di SOL fornisce una sicurezza unica alla rete, mentre la velocità con cui la piattaforma Solana esegue i calcoli consente una maggiore scalabilità. **Grazie all'utilizzo di una miscela unica di proof of history e delegated proof of stake, Solana offre una velocità di transazione esponenzialmente superiore a quella dei suoi**

concorrenti più vicini, Ethereum e Cardano (ADA), a una frazione del costo.

A differenza della proof of work, che utilizza i minatori stessi per definire il blocco successivo di una catena, o della proof of stake, che utilizza i token puntati per definire il blocco successivo, la proof of history utilizza i timestamp per definire i blocchi della catena Solana. Questo sistema innovativo consente ai validatori della blockchain di votare i timestamp dei diversi blocchi della catena. In questo modo la catena rimane relativamente decentralizzata e allo stesso tempo consente calcoli più veloci e sicuri. **Solana funziona con una combinazione di protocolli proof of history e proof of stake delegata.** Secondo ***Bryan Routledge***, professore associato di finanza alla Carnegie Mellon University, il motivo di questa combinazione di protocolli è che Solana cerca di "elaborare rapidamente molte transazioni". ***Routledge*** sottolinea che il tentativo di elaborare le transazioni in modo rapido di solito richiede una centralizzazione. Ad esempio, Visa utilizza un'enorme rete di computer per mantenere la velocità di elaborazione. Bitcoin, invece, secondo Routledge, "elabora le transazioni molto lentamente" per rimanere decentralizzato. I token SOL di Solana vengono quindi puntati e utilizzati come garanzia per elaborare le transazioni sulla rete. Queste transazioni vanno dalla convalida di smart contract fino all'utilizzo di Solana come mercato di token non fungibili (NFT).

13.4 Le nuove criptovalute.

Nel 2014 le criptovalute erano poco più di 200, nel 2015 hanno superato le 700 unità nel 2023 solo oltre 1600. Paesi come Russia e Venezuela, hanno annunciato l'intenzione di realizzarne una. Anche se i programmatori hanno dato prova di creatività, l'impostazione imperniata sulla tecnologia blockchain rimane alla base delle nuove monete. Alcune rendono il protocollo più veloce nella validazione delle

transazioni, come Litecoin, oppure sono più sicure nel favorire l'anonimato, come ***Darkcoin***.

Darkcoin è un nome precedente per Dash cryptocoin. Darkcoin (Dash) è stato inizialmente lanciato come XCoin nel 2014 da Evan Duffield. Entro il 2017, era diventata una delle prime dieci criptovalute in base alla capitalizzazione di mercato. Darkcoin ha quasi le stesse caratteristiche di Bitcoin, ma le transazioni Darkcoin sono assolutamente anonime; utilizza non solo uno, ma una combinazione di diversi algoritmi di crittografia; Il mining di Darkcoin richiede meno potenza del computer e oltre al mining, utilizza i ***masternode***[60] per l'implementazione di funzioni uniche che non sono disponibili per i nodi comuni. Per fornire il massimo dell'anonimato e della velocità, la piattaforma utilizza servizi come PrivateSend, creato per combinare i trasferimenti, e InstantSend per le transazioni immediate.

Altre ancora modificano il taglio per avvantaggiare i micropagamenti, come Dogecoin. Essendo poco diverse e molto meno diffuse dei bitcoin, rappresentano rispetto a questi ultimi una scarsa concorrenza, ma conservano gli stessi rischi di forti fluttuazioni nel loro valore, rendendoli ancora una volta più strumenti di speculazione che strumenti di pagamento.

Le dinamiche di cui abbiamo parlato in precedenza, le aspettative che si autorealizzano, non cambiano e amplificano le oscillazioni sia in salita, sia in discesa. Ci si è posti questo problema, con un tentativo di aumentare la stabilità, proponendo ***Nautiluscoin***. **Per aggiustare la quantità di moneta in circolazione, una parte dei ricavi dei miner viene destinata ad un fondo di stabilizzazione, da utilizzare in modo**

[60] Un master node o nodo master, è un tipo di nodo completo responsabile dell'esecuzione di una serie di compiti o servizi sulla rete blockchain a cui è collegato. Questi nodi possono essere eseguiti da chiunque, ma per questo bisogna possedere una certa quantità di criptovaluta e conservarla in una sorta di contratto. In questo modo, queste monete vengono utilizzate come "garanzia" delle operazioni effettuate dal nodo. Allo stesso tempo, l'installazione di un nodo master generalmente consente alla persona di far parte della governance o di altre importanti funzioni della blockchain.

automatico per controbilanciare spinte rialziste o ribassiste, quando la quantità di moneta non è adeguata.

Un altro esempio può essere ***Freicoin***, valuta virtuale ispirata all'idea proposta da Silvio Gesell (The natural economic order, 1916) e apprezzata da Keynes (The General Theory of Employment, Interest and Money, 1936), riguardante una moneta a scadenza predefinita, chiamata Freigeld. Il principio alla base è l'introduzione di una "tassa di stazionamento" sui soldi inutilizzati, in modo da spingere i possessori a incrementare la circolazione. Filecoin (il nome della cui criptovaluta è FIL) è una rete di archiviazione dati P2P che permette agli utenti di scambiare lo spazio su disco in un mercato decentralizzato su blockchain.

Filecoin è basato su IPFS, **un protocollo per l'archiviazione di dati distribuiti**. IPFS è basato sulle esperienze maturate negli anni dai diversi protocolli come http, ftp, BitTorrent etc. Ciò nonostante, benché fantastico da un punto di vista della decentralizzazione dello storage, IPFS manca però di un livello di incentivazione. Qui entra in gioco Filecoin, che in sostanza rappresenta un layer per favorire l'utilizzo di IPFS. La blockchain di Filecoin memorizza in uno smart contract l'indirizzo hash generato da IPFS. Per recuperare il file basta trovare l'indirizzo hash dalla blockchain e interrogare IPFS per il relativo file. Filecoin funge quindi da ledger per le transazioni FIL e i saldi degli indirizzi del portafoglio Filecoin, e memorizza gli accordi stipulati tra i miner che memorizzano i dati dei clienti ei clienti che hanno richiesto la memorizzazione di tali dati. Per proteggere la rete dagli attacchi, oltre che a impegnarsi a fornire la capacità di archiviazione i miners devono detenere una certa quantità di token FIL. In questo modo un attaccante, oltre ad avere le risorse hardware deve avere anche un numero sufficiente di token, rendendo i tentativi di attacco svantaggiosi dal punto di vista economico. Gli utenti che desiderano archiviare alcuni dati sulla rete Filecoin devono pagare un miner per farlo. Il prezzo di archiviazione è determinato in un mercato aperto in cui i miner

competono tra loro per offrire il prezzo più basso. Filecoin utilizza due nuove tipologie di prove per verificare che i minatori stiano effettivamente archiviando i dati che sostengono di conservare. La Proof of Replication (PoRep) mostra che un minatore ha veramente archiviato la copia unica dei dati del cliente, mentre la Proof of Spacetime (PoST) dimostra che un miner ha archiviato i dati per il periodo di tempo concordato. Se i miner forniscono queste prove in modo affidabile e forniscono lo spazio di archiviazione che si sono impegnati a fornire, possono creare nuovi blocchi sulla blockchain di Filecoin e ricevere il premio di rete e le commissioni di transazione. Queste prove consentono agli utenti di fidarsi dei miner. Il mercato dello storage di Filecoin è quindi simile a un mercato finanziario in cui gli utenti possono fare e chiedere offerte, permettendo così di scambiare lo spazio di archiviazione e fornire un incentivo a coloro che lo forniscono.

Quindi Freicoin da una parte rappresenta un argine alla spinta deflativa di una moneta a quantità prefissata, dall'altra permette di finanziare un fondo destinato a sostenere attività sociali. Poiché gli imprenditori rappresentano il motore dell'attività economica, si potrebbe affidare a loro il compito di creare moneta. Per realizzare questa idea si è pensato a Organizzazioni Autonome Decentralizzate (DAO), con l'obiettivo di attrarre finanziamenti da trasformare in valuta digitale.

In definitiva, i finanziatori portano soldi (in valuta ufficiale) e ricevono in cambio token che permettono sia di partecipare alla ripartizione dei dividendi dell'impresa, sia di acquistare i prodotti dell'impresa stessa, a vantaggio di tutti gli attori dell'iniziativa. **La tecnologia blockchain ha portato allo sviluppo di quella che rappresenta la più famosa delle sue creature, Bitcoin.** Le sue applicazioni, teoricamente senza numero, peraltro cominciano a diffondersi in molti altri campi, da quello finanziario a quello giuridico e, con esiti molto discussi, a quello politico. Ogni volta che sia necessario garantire una operazione o uno scambio senza la presenza di

un'autorità terza che le ratifichi, con un registro pienamente disponibile e verificabile dal pubblico, la blockchain può entrare in gioco.

La sua caratteristica principale è la possibilità di produrre la trasmissione e la registrazione di informazioni con assoluta sicurezza, prescindendo da rapporti di fiducia o da intermediari, come potrebbero essere banche o notai.

Non solo è possibile trasmettere e registrare transazioni di moneta digitale, ma anche diritti di proprietà (smart property), contratti (smart contract), raccolta di fondi, oltre a scambi di beni e comunicazioni di ogni tipo (ad esempio informazioni sanitarie o votazioni). Si intravede dunque la possibilità del superamento di intermediari o di organizzazioni centralizzate, non solo in campo monetario, ma anche in quello commerciale e giuridico.

Se un bene qualsiasi può essere identificato in maniera univoca da un codice, la sua proprietà può potenzialmente essere registrata grazie ad una blockchain e quindi trasferita o scambiata. Si parla in questo caso di smart property. Teoricamente si avrebbe una specie di catasto digitale diffuso, in cui viene registrato qualsiasi tipo di proprietà.

Potrebbero essere interessate anche tutte le operazioni finanziarie, comprese azioni, obbligazioni e rendite, oppure registri pubblici (per esempio per case, terreni, automobili). Possono essere registrati certificati anagrafici, passaporti, patenti, ma anche contratti, testamenti e assicurazioni. Uno dei problemi più sentiti nell'ambito digitale è quello del riconoscimento della paternità di un prodotto, ad esempio articoli, documenti, filmati, fotografie.

Non c'è un registro che indichi con certezza contenuti e proprietà, né tantomeno passaggi di proprietà: di questi problemi si occupano ora alcune piattaforme come ***Ascribe*** o ***Artplus***.

Gli utenti possono caricare i loro prodotti, legati in modo inequivocabile al loro nome, trasferire i diritti, produrre edizioni limitate con un registro di copie originali, tracciare la sequenza delle transazioni e verificare quindi la liceità dei passaggi, scoraggiare frodi e contraffazioni. Come visto non ci sarebbe più

la presenza di un terzo a riconoscere il valore legale dell'operazione e l'effetto sarebbe quello di una esecuzione immediata e irrevocabile, modificando in modo sostanziale il concetto stesso di proprietà.

Mentre lo stato infatti, pur riconoscendo e garantendo il diritto alla proprietà privata, stabilisce dei limiti di legge, in vista di una funzione sociale, è il caso per esempio dell'esproprio, nel caso della smart property viene esercitata una sovranità piena ed indiscutibile. I sostenitori di questo nuovo sistema ritengono di poter arrivare non solo ad una diminuzione delle frodi e ad un abbassamento delle commissioni, ma anche alla realizzazione di operazioni in precedenza difficilmente concretizzabili.

Permette, per esempio, di ricevere un credito da qualcuno in cambio di smart property, rendendo il credito più conveniente e più concorrenziale: supponiamo che invece di andare in banca a chiedere un prestito per l'avvio di una piccola impresa, si vada alla ricerca di finanziatori tramite internet.

Naturalmente chi presta i soldi pretende garanzie per il rimborso. Si potrebbe dare in cambio la proprietà, temporanea, della casa. Poiché serve il suo uso, si potrebbe aggiungere alla chiave di proprietà anche la chiave di accesso. I finanziatori sono i proprietari, ma la persona che ha ricevuto il prestito può continuare, sempre temporaneamente, ad abitare nella casa. **Nel momento in cui restituisce tutti i finanziamenti, ritorna ad essere il legittimo proprietario.**

14. Smart Contract.

Gli *smart contract*, contratti intelligenti, sono caratterizzati dall'esecuzione automatica e dalla mancanza, anche in questo caso, di una terza parte. Non sono una novità, la prima attuazione di questo concetto risale agli anni 70. L'attivazione di una licenza per particolari tipi di software veniva gestita da una chiave digitale, che permetteva il loro funzionamento in seguito a un pagamento e lo inibiva alla data di scadenza.

Gli smart contract, termine che in italiano possiamo tradurre con "contratti intelligenti", sono dei software basati sulla blockchain. A differenza dei contratti legali nel mondo reale, gli smart contract sono costituiti da un codice crittografico e vengono utilizzati per automatizzare l'esecuzione di un accordo in modo che tutti i partecipanti possano essere immediatamente certi dell'esito, senza intermediari e senza perdite di tempo. In parole più semplici, se con i contratti tradizionali una parte viola i termini di un accordo, l'altra può portarla in tribunale, gli smart contract rafforzano tali accordi, in modo che le regole vengano applicate automaticamente senza che tribunali o terze parti siano chiamati in causa. Lo smart contract può essere definito come un codice digitale che offre una serie di garanzie a condizioni predefinite concordate tra le parti. In sostanza, le parti possono stabilire una condizione che può avviare un'azione o una serie di azioni quando non soddisfatte.

Il primo a teorizzare gli smart contract fu l'informatico e crittografo Nick Szabo nel 1997. Famoso per il suo lavoro e le sue ricerche su blockchain e crittografia, Szabo è così autorevole ed esperto di questo settore da essere stato associato, negli anni, a Satoshi Nakamoto, l'inventore di Bitcoin. L'esempio più famoso utilizzato per spiegare in modo semplice cosa è e come funzionano gli smart contract è quello del distributore automatico di bevande. Se io metto 50 centesimi nel distributore, ricevo il caffè. Se metto 1 euro, riceverò il caffè e 50 centesimi di resto. Un altro esempio è un ipotetico sistema di sicurezza digitale per automobili. Si potrebbe progettare uno smart contract che prevede di perfezionare i protocolli di sicurezza in modo da dare il controllo delle chiavi crittografiche per il funzionamento dell'auto solo al legittimo proprietario, in base ai termini del contratto. L'auto può essere resa inutilizzabile se non viene risolto l'algoritmo if-then con il legittimo proprietario, impedendo il furto. O ancora, se l'auto viene usata per garantire un credito, uno smart contract può far sì che, in caso di mancato pagamento, venga dato il controllo delle chiavi dell'auto alla banca fino all'estinzione del debito, senza il coinvolgimento di alcun intermediario o perdite di tempo.

Utilizzando la tecnologia blockchain diventa ora possibile stipulare contratti senza che nessuno dei due contraenti debba fidarsi dell'altro, i contratti diventano incorruttibili e irreversibili: è definito da un protocollo e viene applicato meccanicamente.

L'ambizione è di garantire una maggiore sicurezza dei contratti usuali ed avere costi minori. Una caratteristica fondamentale è l'autonomia. I due contraenti, una volta mandato in esecuzione il procedimento, non devono più intervenire, è tutto univocamente determinato.

Questo dovrebbe anche ridurre, se non azzerare, la quantità dei contenziosi e delle dispute legali. Proviamo a fare un esempio, per avere un'idea di una tra infinite applicazioni. *Supponiamo di avere un'auto che sia collegata ad una moneta digitale, magari un millesimo di bitcoin. La vendita si potrebbe ottenere semplicemente trasferendo quella stessa frazione di bitcoin. Se questo fosse applicato ad ogni auto, diventerebbero superflui sia il PRA, il pubblico registro automobilistico, sia l'ACI, l'Automobile Club d'Italia che lo gestisce.*

Tutto sarebbe registrato sulla blockchain, con una notevole serie di minori problemi burocratici, per non parlare dei risparmi sui costi. È da notare che se anche non ci fosse il riconoscimento legale da parte del PRA in caso di vendita, in ogni caso la transazione diventerebbe comunque effettiva, in modo automatico e permanente, con la consegna al compratore della chiave di accesso. Si può ipotizzare inoltre la possibilità di un finanziamento per l'acquisto, magari accordato dallo stesso venditore e garantito dall'auto stessa.

Se una sola rata non dovesse essere pagata alla sua scadenza, la procedura potrebbe prevedere il trasferimento della chiave crittografica al venditore, che ritornerebbe il legittimo proprietario. Ancora una volta non servono né garanti, né giudici.

L'esempio appena fatto prendeva in considerazione la vendita di un'automobile ma, naturalmente, può riguardare un numero altissimo di beni o di servizi. Si potrebbe prevedere in modo

automatico il rimborso del biglietto del treno in caso di un ritardo superiore ai trenta minuti o il rimborso di un prodotto acquistato online che non abbia i requisiti richiesti. E a proposito di acquisti, con un uso sistematico di smart contract si potrebbero organizzare mercati online in cui ognuno potrebbe comprare o vendere a piacimento, senza costi e senza intermediari.

Un modello di questo tipo è rappresentato da Open Bazaar, molto simile ad eBay e ad Amazon, ma che opera senza un controllo centralizzato. L'esempio di finanziamento visto in precedenza potrebbe essere esteso a qualsiasi forma di operazione, come mutui, prestiti o raccolta di fondi. Nel momento in cui il contratto viene ratificato sulla blockchain, rimane al sicuro da ogni tipo possibile di manipolazione, diventa immediatamente operativo, le parti sono vincolate al suo rispetto, non c'è necessità di conciliazione giudiziale.

In caso di inadempienza, per esempio nel caso di un passaggio di proprietà di una casa, il protocollo trasferisce automaticamente la proprietà stessa al creditore. Non servono carabinieri o giudici, né ufficiali giudiziari e nemmeno cambiare la serratura. L'accesso all'abitazione viene assicurato dalla chiave digitale, trasferita all'istante dal debitore al creditore.

Questo tipo di operazione avrebbe anche il vantaggio di favorire molte di quelle persone a cui oggi è negato l'accesso ai prestiti. Non è più fondamentale la fiducia sulla controparte, è il protocollo che si preoccupa di salvaguardare il rispetto del contratto. **Non c'è bisogno di indagare sulle possibilità economiche dei debitori, come fanno le banche, o ricorrere a onerose procedure per il recupero dei crediti.** Tutto questo potrebbe potenzialmente favorire di molto l'espansione dei prestiti peer to peer. Siamo di fronte ad una forma estrema di ratifica dei rapporti sociali.

Due parti si accordano affidandosi non a un intermediario o a un giudice, ma ad un protocollo che deve gestire la correttezza della procedura. Con dei vantaggi, sicuramente. **I tempi, generalmente, diventano più brevi. Inoltre aumenta la**

certezza, non si presta il fianco a diverse interpretazioni e si azzerano le controversie. Generalmente si abbassano i costi delle operazioni.

Una società come PayPal, che gestisce uno dei metodi di pagamento più diffusi nel commercio elettronico, chiede generalmente dall'1,8% al 3,4%+0.35€ per ogni transazione nella zona euro; in confronto i costi per le commissioni con i bitcoin sono molto minori, in media 0.0001 BTC. Già si lavora alla realizzazione di smart contract sempre più complessi, senza la necessità di consulenti o avvocati.

In questo caso non solo conviene, diventa obbligatoria. I pericoli però non mancano. Il fatto che la procedura sia completamente preordinata e certa si può scontrare con la natura stessa dei comportamenti umani, tutt'altro che certi. Mancano la discrezionalità e le valutazioni soggettive, per non parlare della saggezza.

Vengono cancellati i motivi per cui un contratto possa essere considerato nullo sia a garanzia del singolo, sia per la tutela dell'interesse generale. Il contratto potrebbe essere illecito, oppure frutto di violenza o di frode. Inoltre la sua natura automatica esclude la rinegoziazione dei termini del contratto, anche in presenza di avvenimenti imprevisti che lo potrebbero rendere difficile da onorare. Non è sempre detto che la sua rigorosa applicazione sia conveniente per tutti e due i contraenti, come nel caso di un prestito o dell'affitto di una abitazione.

Un computer difficilmente è in grado di valutare aspetti così complessi in tutte le sue sfumature, forse è ancora preferibile un giudice nella valutazione sia degli interessi contrapposti sia, come si diceva prima, dell'interesse collettivo. Si corre il rischio che le nuove tecnologie diventino il principale nemico di un mondo che i loro fautori speravano di costruire.

15. Sharing Economy.

Un altro settore in cui gli smart contract potrebbero rappresentare un elemento di enorme impatto è quello della cosiddetta "sharing economy".

La voce **dell'Oxford Dictionary** dedicata al termine recita: "***È un sistema economico in cui beni o servizi sono condivisi tra individui privati, gratis o a pagamento, attraverso Internet. Grazie alla sharing economy, si può agevolmente noleggiare la propria auto, il proprio appartamento, la propria bicicletta o persino la propria rete wifi quando non li si utilizzano***". Da questa definizione si potrebbe dedurre che è sharing economy è il fulcro dell'attività, per esempio, di BlaBlaCar, la startup che consente agli utenti di scambiarsi passaggi in auto. E Uber rientra in questa definizione? In fondo gli autisti di Uber utilizzano la propria auto per trasportare i viaggiatori, seppure intermediati dall'applicazione fornita dalla società californiana. La voce del dizionario non lo specifica. La sharing economy, o economia della condivisione, è un concetto che si è andato affermando negli ultimi decenni, declinato in vari modi e applicato a diversi settori economici e sociali. S

Specialmente ai suoi albori il termine stesso, sharing economy, è stato fonte di dibattito a livello internazionale, proprio perché il fenomeno è recente e l'area concettuale al quale fa riferimento è vasta e variegata. Così si sono sviluppate una serie di definizioni contigue, analoghe o parallele: da peer-to-peer economy a economia collaborativa, da ***gig economy*** a economia on-demand fino a consumo collaborativo. Termini a volte usati in modo intercambiabile, ma che, secondo gli esperti, indicano attività lievemente (o, a volte, sostanzialmente) diverse. Negli ultimi anni ha preso piede il fenomeno della ***sharing mobility***, che potremmo considerare un sottoinsieme della sharing economy: la possibilità di muoversi da un luogo ad un altro attraverso mezzi e veicoli condivisi come car sharing, bike sharing, scooter sharing, ma anche car pooling e analoghe modalità di condivisione. Secondo **l'*ISO Foresight Trend Report***, per i prossimi anni la sharing economy dovrebbe crescere a un ritmo del 25%.

La nascita e la diffusione di internet potevano rappresentare per i più ottimisti l'opportunità di un'economia meno basata

sulla struttura gerarchica precedente, ovvero da una parte le grandi aziende, spesso multinazionali, e dall'altra i consumatori passivi. In realtà in molti casi, Facebook e Uber sono esempi evidenti, la spinta alla centralizzazione ha portato a piattaforme che dominano il mercato e i cui gestori trattengono la grande maggioranza dei profitti.

Qualcuno sperava potesse essere una rivoluzione, ma alla fine si è trovato davanti l'ennesima multinazionale. L'introduzione della nuova tecnologia potrebbe invertire, almeno in parte, la direzione. Una piattaforma decentralizzata potrebbe favorire il coordinamento di un numero altissimo di singoli individui, senza intermediari e senza controllo. Si può fornire un passaggio in automobile, l'utilizzo di una bicicletta, un soggiorno limitato nel tempo in un'abitazione privata.

Ricorrendo ad uno smart contract si permette l'utilizzo temporaneo di in bene o di in servizio e, in cambio di un importo prestabilito, si ottiene la chiave di accesso tramite la blockchain. Un esempio particolare di applicazione è legato a piattaforme che si rifanno ai social network, simili a Facebook.

Una differenza fondamentale è che al posto del gestore che decide regole e contenuti, sono i singoli utenti che decidono di collaborare tra di loro, ma soprattutto possono dividersi i guadagni in base al loro impegno. **Una di queste piattaforme è Akasha, basata sul sistema Ethereum, che aspira a sostenere la creatività, la libertà di espressione e la condivisione delle idee, favorendo la permanenza delle informazioni a rischio censura da parte dei governi o delle grosse corporation che controllano la rete**.

Akasha è la rete di social media di nuova generazione, in cui è possibile eseguire qualsiasi attività consentita da un social network come la pubblicazione, la condivisione, il voto per i contenuti e altro ancora. A differenza dei ben noti social network di Akasha, il contenuto viene pubblicato tramite una rete decentralizzata anziché tramite server centralizzati. La libertà di espressione, l'accesso alle informazioni e la privacy sono diritti

umani fondamentali che deve essere rispettato sia su Internet che nella vita reale. In quanto civiltà in transizione verso una società basata sull'informazione, l'archiviazione permanente di informazioni per le generazioni future è un problema critico che deve essere risolto.

L'obiettivo del progetto Akasha è creare un archivio permanente incorporato nella rete Internet per tutte le informazioni prodotte online. Le informazioni (siti Web, documenti, file di posta elettronica, video, ecc.) Possono essere rimosse di proposito dai governi e / o dalle società che controllano Internet oggi o, più semplicemente ma altrettanto tragicamente, scompaiono semplicemente per mancanza di manutenzione dei server di hosting centrali. Come applicazione decentralizzata, AKASHA implementa un'architettura dell'informazione di nuova generazione nata dalla fusione di Ethereum. E il file system interplanetario (IPFS) che è un file system peer-to-peer distribuito che collega tutti i nodi partecipanti allo stesso file system e consente la creazione di file system con versione, blockchain, persino un web distribuito in modo permanente. Tra gli aspetti positivi di questo progetto che possono essere evidenziati sono:

- Il progetto ha stabilito sviluppatori e consulenti che ci lavorano, inclusi i fondatori di Ethereum.
- Akasha è un social network decentralizzato in cui i dati e l'identità sono decentralizzati e dove segui gli utenti e hai una fonte di notizie associata a quel contenuto.
- Il progetto è open source. E sarà sicuramente un punto di riferimento per molte altre dapp basate su Ethereum.
- Se il progetto risolve i problemi, questo Akasha può diventare un ottimo prodotto da utilizzare per altri sviluppatori di terze parti.
- Il duro lavoro associato alla combinazione di contratti intelligenti di Ethereum con IPFS e altri strumenti è visibile ed è un enorme vantaggio.

I fondatori hanno deciso di costruire un prodotto funzionale prima di pianificare un ICO. Questa è una strategia migliore

rispetto ad altre società che pianificano ICO prima dello sviluppo del prodotto. Questo ti dà ulteriore credibilità nella visione e nella direzione del prodotto Akasha.

Un'altra è **Synereo**, piattaforma nata per la pubblicazione e la monetizzazione di contenuti originali, ma la più famosa è Steemit: invece di regalare il proprio tempo e il proprio ingegno a Zuckerberg, gli utenti possono monetizzare la loro creatività inserendo articoli, notizie, immagini e video.

Sono pagati in criptovalute, in questo caso gli steem, che possono essere cambiate nelle piattaforme di exchange in bitcoin o in valuta corrente. Gli utenti possono svolgere due funzioni: autori, che creano i contenuti, e i curatori, che commentano e votano gli interventi. Più il lavoro ha successo, maggiore sarà il guadagno, in base ai voti ricevuti, i quali, tra l'altro, misurano anche la reputazione degli autori con un algoritmo specifico. Le ricompense di sicuro non sono particolarmente alte, ma sono rivolte soprattutto ai contributi di qualità.

Un ultimo esempio di applicazione di servizi di condivisione è collegato al cosiddetto cloud storage decentrato. **In cambio di micropagamenti gli utenti che dispongono di memoria inutilizzata possono metterla a disposizione mediante la rete, ad esempio con SafeMaid**. **La sharing economy rappresenta in ultima istanza una nuova visione, un utilizzo dei beni slegato dal concetto di proprietà e indirizzato invece verso un uso temporaneo, regolato da contratti digitali, dove le persone sono ricompensate in modo equo per il loro lavoro.**

16. Crowdfunding e ICO.

La logica sottostante alla tecnologia che stiamo trattando ha diversi punti in comune con quella dei sostenitori del ***crowdfunding***. Abbiamo già visto come sia possibile che la piattaforma blockchain possa favorire la raccolta di fondi per il finanziamento di nuove imprese o di imprese già esistenti. **Gli algoritmi possono predisporre sia la distribuzione degli utili, sia il diritto di voto su ogni questione relativa all'uso delle**

risorse. Da questo punto di vista non c'è molta differenza con le normali azioni di una società.

La differenza sostanziale riguarda l'impossibilità di ottenere il rimborso della quota in moneta corrente; la criptomoneta può casomai essere scambiata o per l'acquisto dei prodotti della società, oppure con altre monete nel caso in cui sia sufficientemente credibile per poter circolare. Un caso particolarmente interessante riguarda la fornitura di servizi online. **La moneta fornita ai finanziatori può essere impiegata nell'ambito di un sistema di applicazioni e di servizi, per cui generalmente gli investitori stessi diventano i principali consumatori.**

Tra i vantaggi principali, non serve la quotazione in borsa, né ottenere l'autorizzazione da parte degli enti preposti; ritornano le consuete caratteristiche di trasparenza e sicurezza: i registri non sono manipolabili. Lo scambio di valuta è l'unico requisito che consente il finanziamento; il collegamento tra l'impresa e i suoi finanziatori è interamente gestito dal protocollo informatico. **Ci sono ormai diverse piattaforme, ad esempio Swarm, che permettono di raccogliere capitali per il finanziamento di startup, senza le barriere tipiche dei canali tradizionali**. Qualunque persona può decidere di partecipare e in caso di successo delle imprese finanziate riceverà remunerazioni in moneta digitale, nel caso citato gli swormcoin.

I finanziatori stessi sono incentivati nella ricerca di progetti innovativi e di qualità, per un verso con l'idea di ottenere rendimenti più alti, ma anche per favorire talento e creatività nell'interesse di tutta la comunità. **Un'altra piattaforma è rappresentata da Waves, progettata con l'obiettivo di favorire la creazione di progetti open source e i cui finanziatori ricevono criptovalute denominate appunto waves.**

Tutte queste iniziative rientrano in un modello denominato I.C.O. (Initial Coin Offering), un'operazione di "offerta iniziale di moneta" che somiglia molto a quella dell'I.P.O. (Initial Public Offering) con cui le società intendono quotarsi in borsa. **Gli**

investitori non ricevono azioni, ma token, in cambio di denaro reale, come dollari o euro, con il vantaggio però di non essere sottoposti a tassazione. All'inizio la società predispone la blockchain con i relativi protocolli, poi comunica i dettagli dell'ICO. **I miner cominciano a creare le criptovalute che saranno messe in vendita, con una parte riservata all'autore del progetto.**

Una ICO è una tipologia di progetto in crowdfunding, emersa recentemente nell'industria delle Blockchain e delle criptovalute. Le Initial Coin Offering, o ICO appunto, sono eventi organizzati da alcune aziende allo scopo di promuovere e sovvenzionare il lancio della propria criptovaluta. Generalmente viene rilasciato sul mercato un certo quantitativo di cripto-token, venduto ad un pubblico ristretto di solito in cambio di Bitcoin o altre criptovalute, ma raramente anche per denaro fiat. Così facendo, da una parte l'azienda ottiene il capitale necessario a finanziare lo sviluppo del prodotto, e dall'altra il pubblico interessato al progetto guadagna una certa quota di cripto-token. Gli utenti possiedono pienamente tali quote, e possono utilizzarle come meglio credono.

Il primo progetto rilasciato seguendo il modello ICO fu Mastercoin, che nel 2013 riuscì ad assicurarsi ben 5 milioni di dollari in Bitcoin grazie alla vendita dei propri token. Da allora molte altre aziende hanno adottato il medesimo schema, come Ethereum nel 2014 o Waves nel 2016, raccogliendo rispettivamente più i 18 e 16 milioni di dollari. Il modello ICO si è dimostrato una maniera efficiente ed efficace di avviare un progetto basato sulle criptovalute, a condizione che esista un'effettiva domanda per il prodotto ed un solido team a supportarlo.

Parte l'opera di pubblicizzazione, di solito sui siti internet associati alle valute digitali, sui social network e su Reddit, un sito molto popolare dove gli utenti inseriscono testi, video e immagini, con l'obiettivo di coinvolgere il maggior numero di persone. Vengono predisposti i wallet (portafogli) per i finanziatori, affinché possano acquistare le monete. **La**

partenza viene annunciata ed inizia la vendita attraverso piattaforme apposite, tipo Bittrex, in due modi differenti: o direttamente o prima accumulando tutto l'importo annunciato e poi dividendolo in proporzione ai soldi versati dai finanziatori.

Finita la vendita, inizia la realizzazione del progetto. Come è facile immaginare non è semplice distinguere tra i vari investimenti possibili, tra quelli seri e quelli invece rischiosi. **Proprio l'incertezza sulle normative di legge espone al pericolo di essere soggetti a truffe**. Le proposte sul mercato potrebbero essere allettanti, all'inizio una moneta vale poco, ma c'è la speranza che il suo prezzo aumenti in modo consistente.

Con **la diffusione di moltissime ICO fasulle è però consigliabile di valutare attentamente le informazioni sulle nuove società**, che devono essere precise e aggiornate, e di fare particolarmente attenzione alle attività scorrette, come ad esempio il trading degli insider.

È stato stimato che siano più di 30.000 gli investitori truffati solo tra quelli che hanno finanziato le raccolte di fondi di Ethereum.

17. La funzione della criptovaluta e la sua volatilità intrinseca.

In merito alla qualificazione giuridica, alla normativa che si occupa delle criptovalute in ambito europeo e nazionale, ciò che è necessario è comprendere per quale ragione un soggetto dovrebbe utilizzare la criptovaluta, un "valore digitalizzato", uno strumento non emesso da una Banca Centrale, non controllato dalle autorità, sui cui rischi si discute quotidianamente, sulla cui "alegalità" si è discusso ampiamente, invece di ricorrere alla più 'sicura' moneta, come mezzo di scambio, di investimento? Per quale motivo?

La riposta è semplice: **per una ragione prettamente speculativa**. Se nella prospettiva di un possibile venditore non vi è alcuna plausibile e oggettiva ragione di esporre a rischio il valore certo di un incasso, investendo in azioni quanto

guadagnato in una settimana (oppure in un mese o in un anno), se non **la volontà di trasformare istantaneamente quell'incasso in uno strumento di speculazione; nella stessa prospettiva di un probabile acquirente, la spendita della criptovaluta sottende egualmente un atto di speculazione, con la sola differenza che la cessione della valuta virtuale materializza, con certezza, il risultato di una speculazione pregressa, costituendone, in tal caso, il completamento[61].**

E dunque non si tratta di un motivo soggettivo sotteso al patto di accettazione della criptovaluta quale strumento solutorio (motivo di per sé giuridicamente irrilevante ex art. 1345 c.c.), bensì di una connotazione strutturale e funzionale, dunque oggettiva, del patto stesso, il quale non assolve altra funzione che non sia prettamente, esclusivamente, inequivocabilmente speculativa.

Come non vi è nulla di lucidamente razionale nell'investire in azioni se non una volontà prettamente speculativa, allo stesso modo non vi è nulla di razionale nel pagare in criptovaluta, al cambio attuale della stessa, il controvalore del bene se non nel caso in cui la valuta virtuale sia stata acquistata ad un cambio inferiore a quello corrente al momento del pagamento, con fine speculativo di attuare un guadagno, il più ampio possibile. In mancanza di un controllo di un'autorità centrale che garantisca la convertibilità certa della criptovaluta, nessun venditore l'accetterebbe e nessun acquirente la proporrebbe se non nella speranza (per il primo) e nella certezza (per il secondo) di guadagnare relativamente all'operazione posta in essere. Siffatta assenza implica, del resto, un'esasperazione della volatilità della criptovaluta.

La volatilità del Bitcoin ne sta minando la credibilità. Questa criptovaluta non è un titolo azionario che ha un prezzo di riferimento a cui si potrebbe fare riferimento nel caso in cui si verifichi una caduta repentina di valore. Per questo motivo, sempre più persone che investono in Bitcoin si trovano ad affrontare perdite a causa di false ipotesi sulla criptovaluta.

[61] Girino, E. Criptovalute: un problema di legalità funzionale, cit., p. 754.

La valutazione corretta è quindi un serio problema che blocca definitivamente il percorso di crescita dei bitcoin. Ciò è dovuto principalmente al fatto che i grandi operatori finanziari investono in azioni o beni con un valore fondamentale acquistandone grossi quantitativi e conservandole per anni per ottenere rendimenti adeguati. Questo concetto è assente nel caso del Bitcoin e la sua idea di investimento è altamente illusoria per gli investitori consolidati. Siccome la maggior parte della ricchezza globale che si trova tra gli investitori consolidati non è presente nella comunità del Bitcoin, la valuta si basa esclusivamente su investimenti individuali su piccola scala. La mancanza di investimenti su larga scala e riconosciuti rende il valore del Bitcoin altamente imprevedibile e volatile.

La volatilità, che normalmente rappresenta più o meno un'accentuata rischiosità di un investimento, diviene invece elemento attributivo di natura e funzionalità finanziaria alla criptovaluta, in quanto tale volatilità è particolarmente pronunciata ed è tale proprio in virtù della natura alegale della moneta virtuale e della struttura alternativa che la governa. La volatilità della criptovaluta scaturisce in primis dalle scelte dei singoli utenti/operatori, ed è condizionata da un rapporto di domanda e offerta estraneo da ogni presidio di regolamentazione centralizzata e dunque interamente imponderabile[62].

Per effetto di siffatto rapporto, a fronte di una massiccia richiesta della criptovaluta e di una disponibilità di offerta estremamente limitata oppure a fronte di un numero improvvisamente crescente o altrettanto improvvisamente decrescente, il valore della moneta virtuale può eccessivamente ed in modo fulmineo fluttuare. Tuttavia, un siffatto risultato di volatilità estrema, consegnato a mercati del tutto deregolamentati a livello di politica monetaria, coincide con quello tipico di uno strumento finanziario, non certo di una

62 http://www.consob.it/documents/10194/0/Articolo+su+rischi+criptovalute/10402b10-bc3b4500-a0d4-81cec9a2db23

moneta in senso tecnico, con l'ulteriore aggravante della mancanza di un'autorità atta a calmierare l'andamento del titolo per eccesso di rialzo o ribasso, cosa che avviene sempre nei mercati sottoposti a controllo.

In altre parole, creare una "moneta" al di fuori di un sistema monetario corrisponde certamente a creare un "valore", ma non monetario bensì finanziario, come tale soggetto ad un livello di fluttuazione che oltrepassa il limite di variabilità del mezzo di pagamento controllato e governato.

Infatti, un sistema monetario autoprodotto dove l'assenza di un'autorità centrale non soltanto non garantisce l'universalità solutoria della criptovaluta ma neppure ne controlla l'emissione, dove non esistono politiche di gestione della quantità di valuta circolante né misure ufficiali e legalmente accettate per aumentare o ridurre la liquidità del sistema (misure che non esistono perché, appunto, non esiste un organo legittimato ad adottarle), un siffatto "sistema" non è un sistema: soprattutto non è un sistema monetario[63].

L'estrema volatilità non può essere considerata semplicemente un elemento "accidentale" della criptovaluta bensì una componente "causale" della pseudomoneta, in verità dell'investimento finanziario cui essa è geneticamente protesa.

La comunità Bitcoin è nota per la blockchain, un registro trasparente delle transazioni e la criptovaluta ha dovuto affrontare diversi inconvenienti a causa di questi dati open-source. Molti portafogli sono diventati vulnerabili alle violazioni della sicurezza. Questo, a sua volta, ha provocato enormi casi di bancarotta e di furti di grandi quantità di Bitcoin da parte degli utenti. Queste perdite e violazioni imprevedibili contribuiscono anche alla volatilità della valuta e a una riduzione della capitalizzazione totale di mercato della criptovaluta. La ragione dietro l'ineguagliabile volatilità della valuta Bitcoin è che non lo si può accomunare ad un asset

[63] Girino, E. Criptovalute: un problema di legalità funzionale, cit., p. 758.

tradizionale poiché non produce alcun reddito. L'idea di considerare il Bitcoin come un'opzione di investimento o di business è semplicemente una speculazione arbitraria e fuorviante. Inoltre, siccome gli investitori subiscono le manipolazioni del prezzo del Bitcoin in vari periodi, il mercato risulta altamente imprevedibile.

La volatilità dovrebbe rappresentare l'elemento trainante della criptovaluta, e non il suo limite, essendo questa un prodotto di natura finanziaria e speculativa, e non soltanto un semplice strumento di pagamento[64]. Per tale ragione, sino al momento in cui la criptovaluta rimane un mezzo alternativo, di vocazione anarchica, non garantito né governato da un'autorità centrale, fino a che rimane un mezzo di pagamento "laterale" e più che secondario, il suo trasferimento a fini solutori non prescinde mai da una oggettiva e predominante funzione di speculazione.

La criptovaluta è e rimane, a questo stadio, nulla più che una forma di investimento, mentre la componente monetaria non è che una sorta di copertura, un pretesto di legittimazione per celare una funzionalità di diversa natura[65].

[64] Si veda nel sito https://www.24option.com/eu/it/cryptocurrencies/: "ll prezzo di Bitcoin è cresciuto fortemente dalla nascita, ma è considerato estremamente volatile. Nel 2011 il valore di un Bitcoin era calato a $0,30, ma a metà 2017 il valore di un Bitcoin era di circa $2400. Il 13 agosto 2017 Bitcoin ha raggiunto un massimo record di $4200. Si stima che il prezzo di Bitcoin sia 7 volte più volatile rispetto al prezzo dell'oro, 8 volte più volatile dell'indice S&P 500 e 18 volte più volatile del dollaro Usa. Nonostante il mercato delle criptovalute abbia solo 8 anni, al giugno 2017 ha già raggiunto volumi di trading superiori ai $100 miliardi. Il volume complessivo è generato da oltre 800 valute digitali, con sempre nuove valute che nascono ogni mese. Inutile dire che le opportunità sono molteplici per coloro che sono disposti ad accettare i rischi legati all'ingresso in nuovi mercati. Alla luce della natura volatile e in rapido sviluppo dei mercati delle criptovalute, i trader auspicati devono effettuare le debite ricerche sui volumi di trading attuali, le valute digitali attive e le opportunità presenti sui mercati. Gli investitori di valute digitali possono beneficiare del fatto che tali valute non sono legate ad alcuna banca centrale o singolo paese. Questo comporta che possono essere negoziate agevolmente 24 ore al giorno, 7 giorni alla settimana e 365 giorni all'anno. I trader che si apprestano ad entrare nel mercato delle criptovalute devono tenere in considerazione che queste valute digitali si muovono sulla base di fattori diversi rispetto a quelli che muovono le valute tradizionali. Al posto di reagire alla politica della banca centrale e alla forza economica di un certo paese, queste valute reagiscono ad eventi informatici, come attacchi hacker o l'uscita di nuove tecnologie.

[65] Girino, E. Criptovalute: un problema di legalità funzionale, cit., p. 758.

18. La criptovaluta come strumento finanziario?

Le criptovalute devono essere analizzate, oltre l'aspetto monetario, anche nell'aspetto propriamente finanziario, settore quanto mai delicato, presidiato sotto ogni punto di vista, anche da quello penale. Infatti, un settore che viene spesso affiancato al fenomeno delle criptovalute è sicuramente quello relativo ai servizi di investimento, valutati in **termini "strumenti finanziari", le cd. Securities anglosassoni.**

A seguito della **Sentenza della Corte di Cassazione n. 26807 del 25 settembre 2020**, sono stati pubblicati online numerosissimi articoli dal titolo "Per la Cassazione i bitcoin sono "un prodotto finanziario", non solo una moneta", o ancora "Sentenza storica sui Bitcoin, la Cassazione: Sono prodotti finanziari". La Cassazione scrive "***Infondato è anche il terzo motivo di ricorso, con il quale viene sostenuto che poiché le valute virtuali non sono prodotti di investimento, ma mezzi di pagamento, le stesse siano sottratte alla normativa in materia di strumenti finanziari: tale censura non si confronta però con la motivazione contenuta a pag.13 dell'ordinanza impugnata, ove si sottolinea che la vendita di bitcoin veniva reclamizzata come una vera e propria proposta di investimento, tanto che sul sito ove veniva pubblicizzata si davano informazioni idonee a mettere i risparmiatori in grado di valutare se aderire o meno all'iniziativa, affermando che "chi ha scommesso in bitcoin in due anni ha guadagnato più del 97%"; trattasi pertanto di attività soggetta agli adempimenti di cui agli artt. 91 e seguenti TUF I la cui omissione integra la sussistenza del reato di cui all'art. 166 comma 1 lett. c) TUF***." Parrebbe dunque che per la Cassazione si sia espressa sulla circolazione della cryptovaluta non sulla sua natura.

La prassi interpretativa della CONSOB ha da tempo enucleato in maniera consolidata quali caratteristiche tipiche dell'"investimento di natura finanziaria" i seguenti elementi: l'impiego di capitale; l'aspettativa di un rendimento e il rischio connesso; la casistica presa in esame dai provvedimenti CONSOB è abbastanza ampia e, come confermato in tempi

recenti, "per configurare un investimento di natura finanziaria, non è sufficiente che vi sia accrescimento delle disponibilità patrimoniali dell'acquirente (cosa che potrebbe realizzarsi attraverso talune modalità di godimento del bene come ad esempio con la rivendita dei diamanti) ma è necessario che l'atteso incremento di valore del capitale impiegato (ed il rischio ad esso correlato) sia elemento intrinseco all'operazione stessa"[66].

In virtù di ciò non rientrano nella nozione di "prodotto finanziario", "***le operazioni di investimento in attività reali o di consumo, cioè le operazioni di acquisto di beni e di prestazioni di servizi che, anche se concluse con l'intento di investire il proprio patrimonio, sono essenzialmente dirette a procurare all'investitore il godimento del bene, a trasformare le proprie disponibilità in beni reali idonei a soddisfare in via diretta i bisogni non finanziari del risparmiatore stesso***".

La problematica verte laddove vi sia il compimento di una serie di attività giuridiche, quali acquisto, vendita, intermediazione, gestione o consulenza, con una motivazione finanziaria ed un intento speculativo, anche in situazioni non esattamente chiare e riconoscibili, che abbiano ad oggetto criptovalute: ci si domanda se tali operazioni possano/debbano essere valutati nell'ambito della disciplina dei c.d. "servizi di investimento"; e se quindi quell'attività debba allora ritenersi sottoposta alla disciplina che li regolamenta.

Nello specifico, la questione più urgente si pone in rapporto all' acquisto, la vendita o l'intermediazione di criptovaluta per mezzo di piattaforme digitali, che operano sul web e a cui accedono direttamente gli utenti[67]. Il riferimento normativo a cui

[66] http://www.consob.it/web/investor-education/i-servizi-di-investimento

[67] In virtù della natura "collettiva" della "raccolta" di "risparmio" convogliato poi come "conferimento in" o "finanziamento di" iniziative di varia natura che, a loro volta, possono apparire "polverizzate" e che – a seconda del modello di business variamente osservabile sulle piattaforme, potrebbe giustificare una assimilazione del fenomeno qui in esame a quello dell'equity-based o investment-based crowfunding e, talora, anche a quello del lending-based crowfunding – non può escludersi altresì l'accostamento di taluni modelli operativi e di business del a quello della "gestione collettiva del risparmio", chiamandosi allora in causa la disciplina applicabile oggi ai FIA, come oggi disciplinati

attingere è quello costituito dal Titolo II della Parte II del TUF, "***Servizi e attività di investimento***" e dalle collegate disposizioni di cui al Regolamento Intermediari.

Il TUF ha introdotto, infatti, nell'ordinamento una definizione chiusa di "***servizi e attività di investimento***" predisposta sulla base della direttiva 93/22/CEE; ai sensi dell'art. 1, comma 5, TUF si indicano le seguenti attività: a) negoziazione per conto proprio; b) esecuzione ordini per conto dei clienti; c) ricezione e trasmissione di ordini[68].

Fatta una prima osservazione, si può osservare una piena rispondenza delle attività che hanno luogo sulle piattaforme di "negoziazione" di criptovalute, con le condotte classicamente considerate nella definizione dei citati tipici "servizi di investimento"; ed in particolare con la negoziazione e la mediazione. Tuttavia queste attività risulteranno sottoposte alla disciplina dei "servizi di investimento" ai sensi dell'art. 1, comma 5, TUF qualora abbiano ad oggetto "*strumenti finanziari*", come previsto dall'art. 1, comma 2, TUF.

Se allora facciamo un'ampia valutazione della tipologia di quello che consideriamo "strumento finanziario" nel nostro ordinamento, emerge che le criptovalute non sembrano essere espressamente considerate rientranti nella categoria giuridica in questione, tanto da osservare un'esclusione esplicita, ex art. 1, comma 2, TUF per gli "*strumenti di pagamento*", che non costituiscono "*strumenti finanziari*".

Eppure, nonostante ciò, si deve ammettere che l'attività di negoziazione o di intermediazione in "criptovalute" – anche dove la risoluzione dell'utente **di procurarsi una data criptovaluta di tipo "monetario" o "utility", risultasse condizionata esclusivamente da motivi di natura finanziaria, di investimento, speculativi – non violi, di per sé, alcuna riserva di attività, potendo esser svolta al di fuori di quelle**

dal TUF, a seguito del recepimento della direttiva AIFM n. 2011/61/EU. In tal senso v. anche ESMA, Advice on Initial Coin Offering and CryptoAssets, cit., p. 166.

[68] Cfr. la Direttiva n. 2004/39/CE (c.d. MIFID) e successivamente la Direttiva 2014/65/UE (MIFID II).

che sono le norme comportamentali MIFID previste per il caso in cui quella attività abbia invece ad oggetto "*strumenti finanziari*"[69].

Possiamo dunque considerare non condivisibile l'impostazione che ritiene, dopo aver ricondotto le criptovalute indistintamente intese nell'ambito dell'ampia nozione di "*prodotto finanziario*", applicabile tout court la disciplina dei "*servizi di investimento*", arrivando quindi ad assimilare il servizio prestato dalle piattaforme di negoziazione di criptovalute al servizio di negoziazione, per conto proprio o per conto dei clienti, in strumenti finanziari.

Deve però osservarsi che sia necessario agire con estrema cautela nella comunicazione e nelle modalità di offerta delle criptovalute con finalità latamente di "i*nvestimento*": sarà fondamentale attenersi a rigidi criteri di correttezza, in maniera tale che la condotta tenuta non possa risultare ingannevole e omissiva e /o non si incorra in pratiche commerciali scorrette o in altre violazioni del Codice del Consumo, come rilevato recentemente dall'Autorità Garante della Concorrenza e del Mercato in relazione al caso della vendita di diamanti con finalità di investimento tramite canali bancari[70], e ribadito nella **sentenza del Tribunale di Verona nel "*primo leading case italiano*" avente ad oggetto criptovalute, con particolare riguardo alla "*commercializzazione a distanza di servizi finanziari ai consumatori*"[71].**

[69] Bocchini, R. Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche, cit.".

[70] Si vedano i due noti provvedimenti PS10677 e PS10678 del settembre 2017.

[71] La sentenza n. 195/2017, infatti, è la prima questione giuridica legata ai bitcoin e al loro acquisto tramite una piattaforma di crowdfunding. Il caso, nello specifico, riguarda un rapporto contrattuale stipulato tra alcuni investitori (persone fisiche) e una società promoter di una piattaforma di investimenti. L'oggetto del contratto è l'acquisto di valuta virtuale in cambio di valuta reale. In seguito gli attori hanno lamentato la nullità del contratto stipulato con la società promotrice a causa della violazione delle norme del Codice del Consumo (d.lgs. 6 settembre 2005, n. 206) in tema di informazione alla quale è tenuto il fornitore di un servizio finanziario. La decisione del Tribunale è quella di ritenere «nulli i contratti» in quanto l'attività messa in discussione è effettivamente prestazione di servizi a titolo oneroso svolta in favore dei consumatori, quindi da disciplinare tramite il Codice del Consumo. Questo perché lo scambio di valuta si può

Il **Tribunale di Verona è arrivato a considerarlo come «strumento finanziario per compiere una serie di particolari forme di transazione online».** La valuta digitale, però, non troverebbe posto nell'elenco presente all'art. 1, comma II, T.U.F in materia di strumenti finanziari; più plausibile è la sua appartenenza alla tipologia dei "prodotti finanziari", dei quali viene data una più ampia definizione nell'art. 1, comma I, lett. u) del T.U.F.: "***si intendono prodotti finanziari gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria***"[72].

Il soggetto che eroga tali servizi è tenuto, da norma, ad un innalzamento degli obblighi informativi nei confronti del consumatore. Quest'ultimo deve conoscere i contenuti dell'operazione economico contrattuale, così da maturare una scelta negoziale meditata (art. 67-quater, Codice del Consumo).

Nel caso in esame, l'aspetto riguardante gli obblighi informativi non sono poca cosa (si pensi solo all'oscillazione di valore a cui sono sottoposti i bitcoin). Essi ricadono sì sulla piattaforma di investimenti online, ma anche sul fornitore (o promoter) del servizio.

Queste considerazioni e valutazioni, in merito alle problematiche connesse, sono oggetto di costanti interventi di regolamentazione, anche a livello europeo: nella realtà la

incasellare come erogazione di servizi finanziari ai consumatori, in quanto il bitcoin è da classificarsi come strumento finanziario vero e proprio. Gli obblighi dei fornitori, in questo caso il promoter, sono quelli: di informativa, specie precontrattuale, previsti dagli artt. 67-quater, quinquies, sexies, septies, decies e undecies del Codice del Consumo; ulteriori previsti per gli investimenti ad alto rischio. Disciplina: artt. 13, 14, 15 dell'allegato 1 della Delibera Consob del 26 giugno 2013, n. 18592. Passaretta, M. Bitcoin: il leading case italiano, in: Banca Borsa Titoli di Credito, fasc. 4, Giuffrè Ed., (2017).

[72] L'art. 1, comma 1, lettera u) TUF definisce infatti la fattispecie dei "prodotti finanziari", come quella in cui sono ricompresi, in un rapporto di species a genus, gli "strumenti finanziari", oltreché "ogni altra forma di investimento di natura finanziaria". Si tratta di una definizione aperta che richiede, per poter essere delineata con precisione, di indagare accuratamente la fattispecie delle "altre forme di investimento di natura finanziaria" che completano la definizione "aperta". Lo stesso approccio è stato da tempo sottolineato dalla dottrina e, come già detto, è stato anche recentissimamente ribadito dalla Consob proprio in relazione a schemi negoziali aventi ad oggetto criptovalute.

situazione è molto complessa e rischiosa, ed è ancora molto lunga la strada per ottenere una regolamentazione congeniale.

L'accesso diretto al protocollo bitcoin tramite la tecnologia blockchain, per effetto dell'attività di "***estrazione***" (mining) risulta oggi per difficoltà, tempo, costi e rischi, attività rimessa ad un pubblico di operatori assai ristretto, dotato delle necessarie conoscenze, infrastrutture e risorse.

La maggior parte delle transazioni che oggi si svolgono sul mercato hanno in realtà ad oggetto bitcoin solo "***indirettamente***" e si attuano attraverso servizi di negoziazione over the counter e "deposito e custodia" prestati da intermediari ("*piattaforme di scambio*" o exchange) più o meno improvvisati.

Gli strumenti finanziari derivati, e principalmente quelli negoziati fuori dai mercati regolamentati (*over the counter* o, in breve, *OTC*) sono caratterizzati da una elevata adattabilità alle esigenze delle parti nel singolo caso.

L'esperienza ha tuttavia dimostrato che è efficiente la creazione di contratti (*transactions*) con termini economici ogni volta diversi e adatti al caso singolo, innestati su uno schema pattizio uniforme e già collaudato. Pertanto, poiché il numero delle controparti con le quali si opera è ridotto, ma il numero delle operazioni è elevato, nella prassi commerciale si è da tempo affermato l'impiego di contratti quadro (*master agreements*), normalmente predisposti da associazioni di categoria[73], destinati a regolare tutte le operazioni successivamente poste in essere tra le parti.

[73] Un esame dei vari modelli in LEVIS-PECETTO, *I contratti* swap, Milano, 1996, p. 75 ss. e in CAPUTO NASSETTI, *Profili civilistici dei contratti «derivati» finanziari*, Milano, 1997, pp. 77 e ss., 144 ss., 169 ss., 237 ss., 273 ss. In particolare, nella prassi si rinvengono i seguenti *master agreements*:

ISDA (International Swaps and Derivatives Association), (Multicurrency Cross Border) Master Agreement 1992, riprodotto in BO-VECCHIO, *Il rischio giuridico dei prodotti derivati*, Milano, 1997, p. 151 e in CAPUTO NASSETTI, *Profili civilistici*, cit. p. 287; tradotto in *Dir. comm. int.*, 1992, p. 101, con una premessa di CAPUTO NASSETTI, *Un documento di lavoro per un contratto tipo italiano di* swap, *ivi*, p. 95; un'approfondita analisi del *Master Agreement* ISDA 1992 in CAPUTO NASSETTI, *Considerazioni in tema di swaps*, in *Dir. comm. int.*, 1993, p. 321. Una precedente versione, del 1987, è pubblicata in *Dir. comm. int.*, 1988, p. 542, accompagnato dal

Tali documenti, di uso *standard*, sono molto articolati e tendono a prevedere ogni possibile situazione discendente dal rapporto, rendendo agevole la conoscenza delle regole del rapporto. Per altro verso, sono basati sull'esperienza di un gran numero di operatori, sicché il sistema risulta di sperimentata validità.

Fra i principali vantaggi che offrono, i *master agreements* consentono di semplificare il procedimento di conclusione del contratto: una volta stipulato il contratto, ogni singola successiva operazione, dichiarata all'interno del quadro tracciato dal *master agreement*, è soggetta alla disciplina prevista da quest'ultimo accordo, senza dover sottostare a tutte le formalità e le verifiche richieste per stipulare il *master agreement* o un contratto

commento di RADICATI DI BROZOLO, *Il contratto modello di* swap *dell'International Swap Dealer Association, ivi*, p. 539;

ABI (Associazione Bancaria Italiana), «Norme relative alle operazioni di domestic currency swap tra aziende di credito e/o società finanziarie» e «Norme relative alle operazioni di interest rate swap tra aziende di credito e/o società finanziarie», circolare n. 35 del 12 novembre 1991, riprodotti in BO-VECCHIO, *Il rischio*, cit., p. 315, in RIOLO (a cura di), *I derivati finanziari. Profili economici, giuridici e finanziari*, Milano, 1993, p. 229, in CAPUTO *I modelli ABI di* interest rate *e* currency swap, *ivi*, p. 261;

ABI, « Norme relative alle operazioni di forward rate agreement tra aziende di credito e/o società finanziarie » e « Norme relative alle operazioni di currency option tra aziende di credito e/o società finanziarie », circolare n. I del 4 gennaio 1993, riprodotti in RIOLO (a cura di), *I derivati*, cit., p. 272, in questa *Rivista*, 1993, I, p. 740, con nota di AGOSTINELLI, *I modelli « ABI » di* Forward Rate Agreement *e* di Currency Option, *ivi*, p. 735, e in CAPUTO NASSETTI, *Profili civilistici*, cit. p. 404;

BBA (British Bankers' Association), London Interbank Forwards Rate Agreements Recommended Terms and Conditions « FRABBA Terms », riprodotto in CAPUTO NASSETTI, *Profili*

civilistici, cit. p. 392;

IFEMA — International Foreign Exchange Master Agreement, preparato dalla *BBA*, riprodotto in *Dir. comm. int.*, 1996, p. 125, con nota di CAPUTO NASSETTI, *Considerazioni sull'introduzione dell*'International Foreign Exchange Master Agreement *nei mercati finanziari, ivi*, 1996, p. 117.

NASSETTI, *Profili civilistici*, cit. p. 313 e in questa *Rivista*, 1992, I, p. 267, con nota di AGOSTINELLI, Oltre a quelli già menzionati, esistono diversi altri *master agreements*, quali, ad esempio quelli relativi ai c.d. *credit derivatives*, alcuni dei quali sono riportati da CAPUTO NASSETTI, *I contratti derivati di credito*, Milano, 1998 e da CAPUTO NASSETTI-FABBRI, *Trattato sui contratti derivati di credito*, Milano, 2000, così come esistono *master agreement* che non riguardano i derivati, come ad esempio lo *ISMA (International Securities Markets Association) Global Master Repurchase Agreement*, di diritto inglese, il *TBMA (The Bond Market Association) Master Repurchase Agreement*, regolato dalla legge dello Stato di New York, lo *Overseas Stock Lending Agreement*, soggetto al diritto inglese.

singolo. In realtà, non è tuttora chiuso il dibattito sul dilemma se, secondo il diritto italiano, il *master agreement* sia un contratto, di cui le singole operazioni siano atti di esecuzione, ovvero un semplice accordo normativo, per conseguenza risultando ogni operazione un contratto in sé, autonomo rispetto agli altri nati durante il rapporto i cui termini sono delineati dal *master agreement*[74]. Come vedremo in seguito, il problema potrebbe però essere superato dall'evoluzione normativa.

Ciò non diversamente accade con riguardo alla stragrande maggioranza di operazioni aventi ad oggetto strumenti finanziari dematerializzati emessi da emittenti che aderiscono a sistemi di gestione e negoziazione accentrata e/o a connessi sistemi di ***clearing*** e ***netting***, dove lo strumento finisce per confondersi fino a coincidere con le relazioni giuridiche, soprattutto negoziali, intercorrenti tra emittente, gestore del sistema centralizzato e aderenti[75].

Il *netting*, termine inglese proprio della tecnica finanziaria che definisce un processo diretto a realizzare gli esiti propri della compensazione[76], è concettualmente divisibile in più fattispecie. La prima è costituita dal *netting of payments*, accordo per il quale le parti si impegnano a effettuare un solo pagamento (netto) in caso di debiti e crediti reciproci, i cui importi siano espressi nella stessa divisa e scadano con pari valuta.

Questo tipo di compensazione opera al momento del pagamento e minimizza i costi dell'operazione, perché riduce il numero dei pagamenti e, diminuendo gli importi da trasferire,

[74] CAPUTO NASSETTI, *Profili civilistici*, cit. p. 96 ss. e PERRONE, *La riduzione del rischio di credito negli strumenti finanziari derivati*, Milano, 1999, p. 116.

[75] Sumerville, M. Crypto Trading: Platforms Target Institutional Market' (TABB Group, 5 aprile 2018) https://research.tabbgroup.com/report/v16-013-crypto-trading-platforms-targetinstitutional-market/.

[76] Correttamente PERRONE, *La riduzione del rischio di credito*, cit., p. 85, osserva che la generica espressione *netting agreements*, di normale impiego nella prassi finanziaria, identifica un'insieme di convenzioni bilaterali, che, pur tendendo tutte a realizzare operazioni di compensazione, sono strutturalmente e funzionalmente differenti, rilevando altresì che l'istituto italiano della compensazione non è esatto l'omologo di ciascuna tra le varietà del netting

limita il *rischio di consegna*, cioè che nel momento in cui le parti debbano l'una consegnare all'altra i titoli in cambio del prezzo, una di esse non adempia contestualmente.

Inalterato rimane invece il rischio connesso all'inadempimento della controparte (*rischio di credito*).

La seconda fattispecie viene identificata con l'espressione *netting by novation*: in questa ipotesi le singole operazioni tra le due parti si considerano estinte e sostituite da una nuova, il cui valore risulta pari alla somma algebrica dei valori originari, sempre che si tratti di importi denominati nella stessa divisa e con la medesima scadenza, alla stregua di un procedimento continuo, automatico e indefinitamente ripetibile.

Il miglioramento rispetto al *netting of payments* si rinviene nel fatto che in tal modo si riduce l'ammontare delle operazioni al risultato dalla novazione, così limitando sia il rischio di credito che il rischio relativo ai possibili riflessi dell'insolvenza di una parte sull'intero sistema (*rischio sistemico*).

Il sistema ha però un'efficacia limitata, in quanto richiede l'omogeneità delle prestazioni e l'identità di scadenza dell'obbligazione[77].

L'ultima ipotesi è infine il *netting by close-out* [78]. In questo caso, qualora una parte sia inadempiente o insolvente[79], tutte le

[77] BO-VECCHIO, *Il rischio giuridico*, cit., p. 87 notano che l'uso della novazione ha per effetto che ogni novazione, per la sua natura, è revocabile se avvenuta nei due anni precedenti la data di fallimento di una parte. Sul punto, v. *infra*, § 3 e nt. 24.

[78] Sul quale diffusamente v. PERRONE, *La riduzione del rischio di credito*, cit., p. 79 e ID., *Gli accordi di* close-out netting, in questa *Rivista*, 1998, I, p. 51.

[79]Resta il dubbio sulla legittimità — nell'ordinamento italiano — di una clausola di risoluzione automatica ove si preveda, quale evento che la attiva, la dichiarazione di fallimento di una parte. In senso contrario, BIANCA, *La vendita e la permuta*2, in *Tratt. dir. civ*. fondato da Vassalli, Torino, 1993, II, p. 1114, nt. 1. Favorevoli GUGLIELMUCCI, *Effetti del fallimento sui rapporti giuridici preesistenti. Artt. 72-83*, in *Commentario Scialoja Branca — Legge fallimentare* a cura di Bricola, Galgano, Santini, Bologna-Roma, 1979, p. 136 e GIANNATTASIO, *La permuta, il contratto estimatorio, la somministrazione*, in *Tratt. dir. civ. e comm.*, diretto da Cicu e Messineo, Milano, 1972, p. 346; favorevole all'ammissibilità della clausola con riferimento agli strumenti derivati (precedentemente alla emanazione del t.u.f.) PERRONE, *Gli accordi di* close-out netting, cit., p. 65, nt. 35, ove si vedano ampi riferimenti sullo stato della dottrina. Il problema, che sussiste in linea generale, nello specifico è risolto dall'art. 203 del t.u.f., che, attraverso il rinvio all'art. 76 l. fall., prevede — appunto — la risoluzione automatica dei contratti.

obbligazioni, indipendentemente dalla divisa in cui sono espresse e dalla loro scadenza, si ritengono scadute e sono sostituite da un'unica obbligazione che rappresenta l'esposizione netta di uno dei due contraenti nei confronti dell'altro.

La clausola diviene efficace solo al verificarsi di eventi determinati e, di conseguenza, non ha alcuna influenza sul rischio di consegna e sul rischio sistemico. In questa prospettiva, risulta pertanto evidente come, in termini assoluti, la migliore protezione sia offerta dalla combinazione del *netting by novation* e del *netting by close-out*[80].

Attualmente il *netting* è essenzialmente multilaterale nei mercati regolamentati,dove il suo impiego è possibile grazie all'intervento della *clearing house*, e bilaterale, tra le parti contraenti di ciascun *master agreement*, nel caso di derivati *OTC*. È tuttavia stata sottolineata l'opportunità di creare circuiti di compensazione multilaterale specifici per contratti *OTC* di tipi determinati, innovazione che da un lato contribuirebbe all'abbattimento dei rischi[81] e, in conseguenza, dei costi

[80] TREMANTE, *La compensazione nelle operazioni internazionali di* swap, in RIOLO(a cura di), *I derivati*, cit., p. 115; METELLI, *Il rischio finanziario*, cit., p. 623; CRANSTON, *Netting and Settlement*, in FERRARINI (ed.), *Prudential Regulation of Banks and Securities Firms*, London, 1995, p. 195; CAPUTO NASSETTI, *Profili civilistici*, cit. p. 101.

[81] Negli USA, ritenuta insoddisfacente la regolamentazione introdotta tra il 1989 e il 1991, sulla quale si rinvia a PERRONE, *La riduzione del rischio di credito*, cit., p. 96, è in corso un dibattito sulla regolamentazione degli scambi *OTC*. Il 9 novembre 1999 The President Group on Financial Markets ha pubblicato un rapporto, *Over-the-Counter Derivatives Markets and the Commodity Exchange Act*, che contiene alcune raccomandazioni, quali:

(a) l'esclusione degli swap bilaterali dalle regole del *Commodities Exchange Act*, purché non riguardino operazioni non finanziarie su materie prime, esenzione che si applicherebbe solo a istituzioni finanziarie e persone che possano qualificarsi come investitori professionali,

(b)un'esclusione dal *Commodities Exchange Act* per i sistemi elettronici di *trading* che limitino la partecipazione a soggetti sofisticati che agiscano in conto proprio;

c) creazione di incentiviallo sviluppo di sistemi per il *clearing* dei derivati *OTC*. Sul punto v. HUNTER, *Regulators*

Set New Framework for OTC Markets, in *DerivativesStrategy*, January 2000 (http://www.derivativesstrategy. com), e NAZARETH, *Testimony Concerning the Report to Congress on Overthe- Counter Derivatives Markets and the Commodity Exchange Act by the President's Working Group on Financial Markets*, February 15, 2000

transattivi, là dove, dall'altro, si consentirebbe alle autorità di vigilanza di estendere l'area del proprio intervento[82].

Si aggiunga che già esiste un servizio di *clearing* per derivati *OTC*, nelle forme del *netting* multilaterale (in particolare, si

(http://www.sec.gov./news/testimony/ ts012000.htm). Inoltre nel 2000 sono state presentate due proposte di legge, che prevedono la possibilità di regolare gli *swap* attraverso sistemi di *clearing* e demandando la supervisione delle attività in derivati *OTC* e dei sistemi di *clearing* alla *Commodity Futures Trading Commission*, sulle quali v. *Congress Gets Busy on OTC Derivatives*, in *DerivativesStrategy*, May 2000: il 25 maggio la H.R. 4541, *The Commodity Futures Modernization Act of 2000*, presentata dal Rappresentante Ewing e l'8 giugno la S. 2697, *The Commodity Exchange Act Modernization Act of 2000*, presentata dai Senatori Lugar, Gramm e Fitzgerald. Un contributo alla comprensione del ruolo che viene svolto dal *clearing* multilaterale è HILLS-RULE-PARKINSON- YOUNG, *Central Counterparty Clearing Houses and Financial Stability*, in *Financial*

Stability Review, June 1999, p. 122: Per alcune osservazioni sugli effetti potenziali dati dall'uso di un sistema di *netting* multilaterale, PERRONE, *La riduzione del rischio di credito*, cit., p. 84. Per un'analisi formalizzata dei sistemi « netti » di regolamento, KAHN-MCANDREWSROBERDS, *Settlement Risk under Gross and Net Settlement*, Federal Reserve Bank of Atlanta, Working Paper 99-10a, Atlanta, November 1999.

[82] SODA, *I derivati finanziari nella vigilanza prudenziale*, in RIOLO (a cura di), *I derivati*, cit., p. 60; nell'estesa bibliografia sui temi della vigilanza, si segnalano, *ex multis*, tra i contributi più recenti: TORCHIA, *Il controllo pubblico della finanza privata*, Padova, 1992; COSTI, *L'ordinamento bancario*, Bologna, 1994 (2), p. 493; CASTALDI, *Il riassetto della disciplina bancaria: principali aspetti innovativi*, in *Quaderni di ricerca giuridica*, n. 32, Banca d'Italia, Roma, 1995; DESARIO, *Il Testo Unico delle leggi bancarie e creditizie e il nuovo ruolo della vigilanza*, in Ferro-Luzzi-Castaldi (a cura di), *La nuova legge bancaria*, Milano, 1996, I, p. 52; LAMANDA, *Le finalità della vigilanza*, *ivi*, I, p. 157; GUALANDRI, *Il quadro normativo e di vigilanza sulle istituzioni creditizie*, in M. Onado (a cura di), *La banca come impresa*, Bologna, 1996, p. 67; TARANTOLA RONCHI-PARENTE-ROSSI, *La vigilanza sulle banche e sui gruppi creditizi*, Bologna, 1996; GAMMALDI, *Il controllo dei rischi nell'ottica della vigilanza*, in *Banche e banchieri*, 2, 1996, p. 129; MERUSI, *Vigilanza e « vigilanze » nel nuovo testo unico delle leggi bancarie*, in *Banca, impresa, società*, 1996, p. 189; MASTRANGELO-CAROFIGLIO, *Vigilanza regolamentare*, in Capriglione (a cura di), *La disciplina degli intermediari e dei mercati finanziari*, Padova, 1997, p. 213 ss.; GABBI, *Obiettivi della vigilanza e regolamentazione consensuale nel mercato bancario*, in Carretta (a cura di), *Banche e intermediari non bancari: concorrenza e regolamentazione*, Roma, 1998, p. 140; PARMEGGIANI-ZUCCHELLI, *La disciplina prudenziale degli intermediari del mercato mobiliare*, in Ferrarini-Marchetti (a cura di), *La riforma dei mercati finanziari. Dal decreto Eurosim al testo unico della finanza*, Roma, 1998, p. 355; SABATINI, *La vigilanza sugli intermediari e sui mercati*, in BANFI (a cura di), *I mercati e gli strumenti finanziari*, Torino, 1998, p. 383; DEWATRIPOINTTIROLE, *La regolamentazione prudenziale delle banche*, Bologna, 1998, trad. it. di *The Prudential Regulation of Bank*, Cambridge, Mass., 1994; DI GIORGIO-DI NOIA, *La regolamentazione delle banche: considerazioni critiche*, in *Banca, impr. soc.*, 1999, p. 285; SALERNO, *La vigilanza regolamentare sulle banche: soggetti ed oggetto*, Un. di Siena, Siena, 2000.

tratta di *close-out netting*) svolto dalla *London Clearing House*, che ha iniziato ad offrirlo, nel 1999, anche sul mercato USA[83].

L'impiego di clausole che consentano il *netting* ha l'effetto di ridurre il rischio insito in una posizione dall'intero ammontare del credito al solo saldo, ove creditorio, verso la controparte, con l'importante conseguenza, per le banche e gli intermediari, di ridurre la quantità di capitale proprio impiegato al fine di rispettare le norme in tema di *solvency ratio* e di patrimonio di vigilanza.

Una prima accettazione del *netting* come strumento di riduzione del rischio venne dalla direttiva 96/10/CE, la quale, modificando la direttiva 89/647/CEE del 18 dicembre 1989[84], ha consentito la riduzione al saldo delle posizioni come base per calcolare il necessario patrimonio di vigilanza, qualora ricorra un contratto che preveda il *netting by close-out*[85] e la validità di tale clausola sia attestata da un apposito parere.

[83] Nell'agosto 1998 è entrata in vigore nel Regno Unito la *Financial Markets and Insolvency Regulation 1998*, che modifica il capitolo sull'insolvenza del *Companies Act 1989*. La modifica, fra l'altro, consente alle *clearing house* di chiudere le posizioni aperte, compensare profitti e perdite dell'aderente, realizzare i margini concessi non per cassa e dedurre i margini dalle perdite nette. Inoltre le corti inglesi non possono dare efficacia ai provvedimenti di giudici stranieri che impediscano l'esercizio di tali diritti. Tutti questi diritti possono essere esercitati non solo nel caso di contratti stipulati dalla *clearing house* nell'ambito dei servizi prestati a favore di mercati regolamentati, bensì anche nel caso di contratti stipulati dall'aderente alla *clearing house* per consentire il regolamento delle proprie operazioni di investimento, ciò che automaticamente estende l'applicabilità della norma alle operazioni in derivati *OTC*. Già prima dell'entrata in vigore della legge, nell'estate del 1998 la *London Clearing House (LCH)* aveva offerto di istituire un sistema di *clearing* dei derivati *OTC* per gli operatori del mercato statunitense, fatto che è avvenuto a seguito dell'approvazione, da parte dei regolatori statunitensi, del progetto, concedendo alla LCH una esenzione da approvazioni regolamentari che consente alla *LCH* di offrire il servizio, denominato *SwapClear*, a banche e istituzioni americane.

[84] Ove si stabilivano i requisiti patrimoniali minimi che i singoli ordinamenti avrebbero dovuto imporre alle banche, incentrando il sistema sul coefficiente di solvibilità. La direttiva fu recepita dal nostro ordinamento con il d.lgs. 10 settembre 1991, n. 301, che attribuiva alla Banca d'Italia il potere di emanare disposizioni generali in materia.

[85]Il recepimento della norma è avvenuto in via amministrativa, come ricorda PERRONE, *La riduzione del rischio di credito*, cit., p. 54, nt. 88, nel senso che le Istruzioni di Vigilanza, attualmente contenute nella circolare n. 229 del 21 aprile 1999, al Titolo IV, capitolo 2, Allegato B, paragrafo 3, riconoscono la riduzione della base di calcolo al saldo, in caso di « accordi bilaterali di compensazione tra una banca e la sua controparte ».

Il *netting* ha poi trovato definitivo riconoscimento sul piano normativo con la direttiva 98/26/CE del 19 maggio 1998, che avrebbe dovuto essere recepita, sul piano legislativo, regolamentare ed amministrativo, entro l'11 dicembre 1999 (art. 11, comma 1o). In questa sede il *netting* è definito come «***la conversione in un'unica posizione a debito e a credito dei crediti o dei debiti risultanti da ordini di trasferimento che uno o più partecipanti hanno nei confronti di uno o più altri partecipanti per effetto della quale può essere richiesto o dovuto soltanto il saldo netto***» (art. 2, lett. *k*)).

Come è evidente dal testo riportato e come ben precisa il testo (art. 1, lett. *a*) e art. 2, lett. *a*)), le disposizioni della direttiva sono riferite al *netting* multilaterale, in quanto le disposizioni si applicano ai partecipanti ai sistemi così come ai sistemi, questi ultimi definiti, per quanto sia in questa sede rilevante, come accordi formali tra tre o più partecipanti, oltre a soggetti eventualmente previsti dal sistema (agente di regolamento, controparte centrale, stanza di compensazione, partecipanti indiretti).

Il ***netting*** in linea generale si applica, ed è opponibile ai terzi, nel caso in cui gli ordini di trasferimento (cioè l'ordine di mettere a disposizione di un terzo una somma di denaro per un pagamento e quello di trasferire la titolarità degli strumenti finanziari o i diritti su di essi) siano immessi in un sistema prima dell'apertura di una procedura d'insolvenza, la quale a sua volta è definita come una procedura concorsuale prevista dalla legge, di uno Stato membro o di un paese terzo, per liquidare un partecipante o riorganizzarlo, tale da comportare la sospensione dei trasferimenti o dei pagamenti o l'imposizione di limiti all'attività. Si noti come il *netting* funzioni, nel sistema della direttiva, solo in caso di rapporti tra intermediari abilitati e non in caso di contratti stipulati tra un intermediario e un diverso soggetto.

Da questo punto di vista allora, l'approccio regolamentare che potrebbe da subito risultare opportuno, superata la fase di "***wait and see***" che ha sin qui prudentemente caratterizzato

l'atteggiamento dei regolatori, potrebbe essere quello di estendere al fenomeno in esame il regime di riserva e le connesse fondamentali prescrizioni comportamentali e organizzative oggi applicabili ai "servizi di investimento" ovvero ai "servizi di pagamento", in capo a chiunque offra oggi sul mercato analoghi attività e servizi che abbiano le "criptovalute" ad oggetto, se non in tutto almeno in parte[86].

Oggi, infatti, le principali e più urgenti richieste di tutela dei risparmiatori devono indirizzarsi verso una regolamentazione degli "*intermediari*" che offrono sul mercato servizi di "*negoziazione*" e "*deposito*" delle "*criptovalute*", quindi bisogna concentrarsi su di un'altra dimensione del fenomeno.

Da questo punto di vista si può bypassare la prima fase, che resta comunque complessa e aperta circa la natura giuridica del fenomeno sottostante e della sua regolamentazione giuridica "primaria", per concentrarsi invece, sulla dimensione "esterna" del fenomeno, sull'imposizione ad essi di consolidate regole comportamentali e presìdi organizzativi ben sperimentati.

Il passo logico successivo è quello di rendere uniformi alcune caratteristiche presenti nei vari *master agreements*[87], con ciò eliminando il rischio che i singoli contratti quadro prevedano diversi *events of default*, ovvero termini differenti per i preavvisi o per azionare le clausole di *closeout* [88]. A tale fine, un'organizzazione statunitense, *The Bond Market Association (TBMA)*, insieme ad alcune tra le principali organizzazioni di categoria — *BBA (British Bankers' Association), EMTA*

[86] Greco, M.P. E Bonardi, P. La "resilienza cibernetica", delle infrastrutture del mercato finanziario, in Diritto Bancario, (2019).

[87] Nel gennaio del 1999 dodici importanti banche annunciarono la costituzione del Counterparty Risk Management Policy Group, con l'avallo del Presidente della FED Alan Greenspan, del Presidente della SEC Arthur Levitt e del Segretario al Tesoro, Jerry Rubin. Nel giugno del 1999 il Counterparty Risk Management Policy Group pubblicò il rapporto *Improving Counterparty Risk Management Practices*, che, fra le molte proposte volte a migliorare la gestione dei rischi di mercato, di controparte e di liquidità, a p. 45 raccomanda che « Parties should make the best possible use of multi-product master agreements, and master- masters, to facilitate obligation netting and collateral netting across product lines ».

[88] E anche « *to help keep the anxiety of August 1998 at bay* », osserva il mensile specializzato on-line *DerivativesStrategy*, May 2000.

(Emerging Markets Traders Association), FXC (Foreign Exchange Committee of the Federal Reserve Bank of New York), IPMA (International Primary Market Association), ISDA (International Swaps and Derivatives Association), IDAC (Investment Dealers Association of Canada), JSDA (Japan Securities Dealers Association) e *LIBA (London Investment Banking Association)* — ha promosso la preparazione di un contratto che rispondesse alle nuove esigenze: il *Cross-Product Master Agreement (CPMA)*, presentato agli operatori nel febbraio del 2000[89] e oggetto delle note che seguono. Attualmente la *TBMA*, che ha ottenuto alcune *opinions* di affermati studi legali in Gran Bretagna e negli Stati Uniti, è impegnata nel raccogliere, attraverso le organizzazioni nazionali degli intermediari (in Italia attraverso ASSOSIM) *opinions* legali sulla validità del contratto nei diversi ordinamenti.

Il *CPMA* è una sovrastruttura di natura contrattuale — dai suoi promotori è definito un *umbrella* — che può ricomprendere sotto di sé, secondo la scelta delle parti, tutti quei *master agreement* (definiti *Principal Agreements*) che esse ritengano opportuno includere, siano essi già stipulati al momento di conclusione del *CPMA* o che decidano di stipulare, contestualmente o in tempi successivi. Similmente alla maggior parte dei *master agreement*, il *CPMA* ha struttura modulare, nel senso che le regole sul *Close- Out* (art. 2), la determinazione del *Settlement Amount* (art. 3) e del suo pagamento (art. 4), nonché le dichiarazioni e garanzie (art. 5), e le regole sulla legge regolatrice (art. 6), sulla cessione del contratto (art. 7) e sulle notifiche (art. 8) sono contenute nel testo d ell'accordo, mentre le specificità sono rimesse alla determinazione delle parti. Ad esempio la Parte I della *Schedule* contiene l'indicazione dei *master agreement* soggetti al *CPMA*, tema sul quale torneremo, e la Parte VI consente di scegliere la *Base Currency*, cioè la valuta nella quale, alla fine, regolare i saldi. La legge applicabile

[89]Il testo del contratto può essere letto nella guida all'uso predisposta da GOOCHKLEIN, *Documentation for derivatives. Cross-Product Risk Management Supplement*, Euromoney, London, 2000, oppure scaricato dal sito della *TBMA* (www.bondmarkets.com/market/ agreements.hmtl).

al *CPMA* è, alternativamente, quella inglese o quella dello stato di New York (art. 6 e Parte IV della *Schedule*).

Ove una delle parti sia italiana e l'altra straniera, il soggetto italiano ha diritto di scegliere una legge diversa da quella italiana e, eventualmente, terza rispetto a quelle delle parti[90] (art. 3 della Convenzione di Roma del 9 giugno 1980, Convenzione sulla legge applicabile alle obbligazioni contrattuali), così come è possibile che due soggetti italiani scelgano di regolare il rapporto secondo una disciplina (una delle due previste dal CPMA) diversa dalla legge italiana[91]. Restano ovviamente salve le norme identificate dalla Convenzione come «disposizioni imperative»[92].

Ciò posto, poiché il *CPMA* è un contratto e il sistema italiano prevede la libertà di contrarre, non si incontrano limiti al regolamento dei propri interessi, se non quelli derivanti da disposizioni imperative e, pertanto, è perfettamente lecito che le parti, soggette alla legge italiana, possano disciplinare più serie di rapporti (una serie per ogni *master agreement*, più quegli altri rapporti che esse decidano, come da Parte VII.2 della *Schedule*, definite come *Uncovered Transactions*) con un comune regolamento. La struttura modulare del *CPMA* si riflette nella possibilità di determinare, anche in tempi successivi, il suo ambito di applicazione.

La Parte I della *Schedule* indica una lista di *master agreements*, i più diffusi, così che le parti, barrando le caselle, possano scegliere a quali rapporti applicare i meccanismi contenuti nel *CPMA*; inoltre l'elenco consente la possibilità (casella 15) di sottomettere al *CPMA* tutti i *master agreements*, già sottoscritti e di futura stipulazione, che esistano tra le parti

[90] Argomento da non confondere con il tema, dibattuto in passato, della « delocalizzazione » del contratto rispetto ad una legge statale, ma nel senso di creare una sorta di nuova *lex mercatoria*. Sul punto, anche in connessione con la Convenzione di Roma, CARBONE, *Il « contratto senza legge » e la convenzione di Roma del 1980*, in *Riv. dir. int. priv. E proc*., 1983, p. 284.

[91] In senso conforme MOSCONI, *Diritto internazionale privato e processuale*, Torino, 1996, p. 173.

[92] Sulle quali TREVES, *Norme imperative e di applicazione necessaria nella Convenzione di Roma del 19 giugno 1980*, in *Riv. dir. int. priv. e proc.*, 1983, p. 24.

contraenti, nonché di includere tutti quei rapporti che, pur non essendo incorporati in un *master agreement*, sono oggetto di una conferma scritta o di un documento che richiama, *per relationem un master agreement* (casella 16).

La possibilità offerta dal contratto, si sottolinea, è di includere in epoche successive alla stipulazione nuovi *master agreements* e, a tale scopo, viene fornita una lettera tipo (*Exhibit* 1) per integrare la lista dei contratti con un *master agreement* successivamente stipulato o che, pur essendo già in vigore, non era stato assoggettato al *CPMA*. Non è invece previsto che le parti possano, naturalmente in epoca successiva alla stipulazione del *CPMA*, escludere dalla lista, per i motivi più vari, un contratto esistente.

Poiché l'intero assetto normativo è ampiamente rimesso alla volontà delleparti, non si vede perché, stante il consenso delle parti, non possa essere lecita l'esclusione[93].

La parte finale della lista che costituisce la Parte I della *Schedule* (casella 17) è forse la più innovativa, poiché si prevede che le parti possano assoggettare alle regole comuni del *CPMA* anche operazioni che non sono contenute in alcun *master agreement*, definite *Uncovered Transactions*, e si prevede che, in caso le parti effettuino questa scelta, il corpo contrattuale debba essere integrato con l'inclusione delle regole contenute nella Parte VII.2 della *Schedule*, integrative dell'art. 2.1 del *CPMA* sulla definizione del diritto di *Close-Out* del contratto.

Nel caso in cui almeno una delle parti sia un soggetto italiano, la sua insolvenza potrebbe porre il problema che, se le operazioni ulteriori assoggettate al *CPMA* quali *Uncovered Transactions* non fossero contratti del tipo previsto dall'art. 203 t.u.f., le previsioni della legge fallimentare italiana, di applicazione necessaria e certamente prevalenti rispetto a

[93]Che il consenso delle parti sia sufficiente a permettere la modifica del contratto sembra sicuro, per quanto riguarda la legge inglese: v. TREIXEL, *Consideration*, in CHITTY, *On Contracts*, London, 1989 (26), I, p. 144 ss, e ciò senza scomodare la dottrina degli *implied terms*.

qualsiasi previsione contrattuale, potrebbero confliggere con il meccanismo contrattuale di *close-out* e di regolamento dei saldi. Questa ipotesi è scongiurata da una specifica norma del *CPMA*. L'art. 2.1 esclude dal computo al fine della determinazione dei saldi, e al fine del regolamento quei *Principal Agreements* (o, se del caso, *Uncovered Transactions*) che per effetto di legge o di azione giudiziaria non possano essere risolti, contrariamente al volere originario delle parti espresso con la firma del *CPMA* e l'inclusione nella lista. Il *CPMA* prevede che nel caso un evento costituisca un *Event of Default* ai fini di uno dei contratti ad esso sottoposti quali *Principal Agreements*, allora esso diviene la base contrattuale per risolvere tutti i *Principal Agreements* elencati nella Schedule. Inoltre, la violazione delle dichiarazioni e garanzie rilasciate da una parte nel *CPMA* costituisce di per sé titolo per risolvere il *CPMA*. La parte che ha diritto di *Close-Out* ha solo la facoltà, non l'obbligo, di notificare l'intenzione di risolvere il contratto e tale facoltà deve essere esercitata per tutti i *Principal Agreements*, non essendo possibile risolverne alcuni e mantenere in vita alcuni altri. Nel caso siano previste *Uncovered Transactions*, anch'esse devono essere risolte.

Il *CPMA* costituisce una espressa modifica degli esistenti *Principal Agreements*, nel senso che da un lato specifica quali eventi costituiscano la base legale per esercitare il diritto di *Close-Out* di tutti i *Principal Agreements* e, dall'altro, modifica i termini di notifica o di preavviso che, in ciascuno dei *Principal Agreements* potrebbe rallentare o posporre la risoluzione o la decadenza dal beneficio del termine della parte che ha violato il contratto o che ha dato luogo all'*Event of Default*.

Alcuni eventi (elencati nella Parte II della *Schedule*) ancorché considerati *Event of Default* da alcuni dei *Principal Agreements*, non riguardanoil merito creditizio della parte e pertanto, salvo patto contrario, sono esclusi dalla tipologia degli *Event of Default* che consentono il *Close-Out* di tutti i *Principal Agreements*. È da ritenere che nonostante la regola generale secondo la quale si devono risolvere tutti e non solo alcuni *Principal Agreements*, sia comunque legittimo risolvere un

determinato contratto in forza di fatti o circostanze che rilevano solo ai fini di quel contratto, senza che ciò abbia impatto sulla validità e sulla continuazione di tutti gli altri *Principal Agreements*.

Prescindendo dal fatto che il *CPMA* non può essere soggetto alla legge italiana, si noti che nell'ordinamento italiano non esiste il concetto secondo il quale un inadempimento nel primo contratto possa essere causa di risoluzione del secondo contratto, pure se stipulato tra le stesse parti (il c.d. *cross default*), non spingendosi così lontano il principio *inadimplenti non est adimplendum*[94].

Diverso problema, nel nostro ordinamento, è quello di un inadempimento, al primo contratto, in ipotesi anche stipulato con terzi, che dimostri la diminuita capacità patrimoniale del debitore e che legittimi il creditore, quanto al secondo contratto, alla dichiarazione di decadenza dal beneficio del termine *ex* art. 1186 c.c., con il prevedibile conseguente inadempimento del debitore al secondo contratto e, quindi, la risoluzione per inadempimento. Il principio che governa il *CPMA* è semplice. Avvenuto il *Close- Out*, le parti seguono le regole di ciascuno dei *Principal Agreements* e determinano il saldo netto per ciascuno di essi (art. 3), se del caso includendo nel calcolo la garanzia prestata (*collateral*) per ciascun contratto e che viene impiegata: la parte può infatti decidere, sempre secondo il contratto «sostanziale», se attivare le garanzie. Il *CPMA* non

[94]Diversa prospettiva è la seguente: secondo ampia giurisprudenza e parte della dottrina, permettendoci di rinviare per i riferimenti a SACCO, *I rimedi sinallagmatici*, in *Tratt. dir. priv.*2, diretto da Rescigno, X, Torino, 1995, p. 608, la dichiarazione o la minaccia di non voler adempiere, rese prima della scadenza, sono equiparate all'inadempimento. Ove si argomentasse

che, in caso di contratti fra loro omogenei (nel nostro caso sono tutti contratti afferenti strumenti finanziari) in assenza di una ragione diversa dalla incapacità di adempiere, l'inadempimento dal primo contratto è in sé una minaccia di futuri inadempimenti, allora si potrebbe costruire l'inadempimento al primo contratto come inadempimento anche al secondo, con la conseguente opponibilità, da parte del contraente offeso, dell'eccezione di inadempimento.

modifica le regole per il calcolo dei saldi, limitandosi ad uniformare i termini, in senso temporale.

Si aggiunge che i *master agreements* governati dalla legge inglese normalmente prevedono che i beni consegnati a una parte quale garanzia siano a questa trasferiti, senza obbligo di restituzione; a carico del garantito resta solo un obbligo monetario di restituzione del controvalore e la somma viene inserita a credito della controparte nel calcolo del saldo, così che un solo ammontare è dovuto. Molto diversa è la situazione dei contratti regolati dalla legge di New York, secondo i quali la garanzia in eccesso rispetto al debito deve essere restituita al momento in cui è avvenuto il pagamento del saldo.

L'ammontare dei vari saldi è convertito in una sola valuta (*Base Currency*), scelta dalle parti, salvo il caso in cui tutti i *Principal Agreements* siano denominati in un'unica valuta ed essa sia diversa da quella che le parti designarono come *Base Currency* nella parte VI della *Schedule*. In questo caso, la parte che ha dichiarato il *Close-Out* del *CPMA* (e di tutto quanto da esso regolato) ha la facoltà di designare la valuta prevista da tutti i singoli contratti come nuova *Base Currency* (art. 3.2), evitando la conversione da quest'unica valuta alla *Base Currency* e il conseguente rischio di cambio.

La somma algebrica dei singoli saldi, siano essi calcolati ad un'unica data ovvero in date successive, indipendentemente dal fatto che le parti siano *multi-branch* ai fini di alcuni dei *Principal Agreements*, darà luogo ad un unico saldo, il *Final Net Settlement Amount*, che deve essere pagato non appena determinato, secondo le istruzioni di pagamento previste dalle parti (art. 4). Nel caso in cui i vari saldi siano liquidati in date diverse, la somma algebrica viene effettuata volta per volta e sul primo ammontare decorrono interessi, che sono parte del calcolo del saldo, sul quale, a partire dalla data in cui viene stabilito, decorrono nuovi interessi, che entreranno nel calcolo del saldo successivo, e così fino alla determinazione del *Final Net Settlement Amount* (art. 4.5).

19. La criptovaluta come valore mobiliare: il titolo digitale.

La legge 216/1974, istitutiva della CONSOB, indicava come valore mobiliare ogni documento (o certificato) direttamente o indirettamente rappresentativo di diritti inerenti società, associazioni, imprese o enti di qualsiasi tipo, ivi compresi i fondi comuni d'investimento. Successivamente, il termine valore mobiliare è stato definitivamente sostituito - con il D.Lgs. 58/1998 (Testo Unico della Finanza) - dalla terminologia più ampia di "strumento finanziario", comprensiva anche degli strumenti finanziari derivati[95].

I valori mobiliari si configurano in definitiva quali strumenti atti a consentire all'emittente di ottenere risorse finanziarie non reperibili altrove, mentre per il sottoscrittore rappresentano forme di impiego del risparmio variamente remunerate e caratterizzate da una buona possibilità di circolazione, quindi di smobilizzo[96].

Una valutazione differente viene ad esserci proprio nel caso particolare di quelle criptovalute riconducibili, in relazione al loro modello di business e alle finalità della "raccolta" svolte, alla **criptovaluta come security tokens**, rientrante negli "strumenti finanziari", in particolare nell'ambito del sottoinsieme "aperto" che fa riferimento alla nozione normativa di "valori mobiliari" ex art. 1 bis del TUF, laddove sia riscontrabile comunque l'elemento della cd. "negoziabilità".

[95] https://www.borsaitaliana.it/borsa/glossario/valore-mobiliare.html.

[96] I titoli possono essere emessi: – dallo Stato o da altri enti pubblici, quali regioni, province, nel qual caso si parla di titoli pubblici; – da società o enti privati, nel qual caso si parla di titoli privati. Mentre i titoli pubblici rappresentano sempre prestiti, i titoli privati possono rappresentare prestiti (obbligazioni) o quote del capitale sociale (azioni). Il possessore di un titolo pubblico o di un'obbligazione si trova nella veste di creditore del soggetto emittente, mentre il portatore di azioni diviene socio della società emittente. Considerando la remunerazione fornita dai titoli è possibile distinguere tra: – Titoli a reddito variabile: attribuiscono il diritto di percepire una remunerazione dipendente dai risultati economici conseguiti dalla società emittente, nonché dalle politiche dei dividendi perseguite. Rientrano in questa categoria, essenzialmente, le azioni. – Titoli a reddito predeterminato: sono titoli che attribuiscono il diritto di percepire, a scadenze prefissate, una remunerazione determinata, secondo modalità ben precise, già al momento dell'emissione.

Un titolo digitale[97] è un tipo di strumento finanziario che ricade sotto la supervisione della SEC. Può essere esso stesso digitale oppure una rappresentazione digitale di asset finanziari tradizionali, come azioni od obbligazioni. Un titolo digitale, noto anche come security token, è un asset digitale (come una criptovaluta) che rappresenta la proprietà o altri diritti in un'azienda o un'altra impresa. Il concetto è praticamente identico alle azioni o alle obbligazioni, tranne per il fatto che i titoli digitali sono rappresentati come token. La definizione di titolo digitale può anche includere criptovalute classificabili come titoli nell'ambito del test di Howey[98], anche se i loro creatori affermano che non si tratti di security token. Tutti gli asset che soddisfano la definizione di titolo — che sia digitale o meno — sono soggetti alla supervisione e alla regolamentazione delle authority di vigilanza finanziaria. Queste agenzie sono state lente ad agire su alcuni dei casi più ovvi di titoli digitali mascherati da semplici criptovalute, ma questa situazione non durerà per sempre.

19.1 Il test di Howey.

l test di Howey ha origine dalla sentenza della Corte Suprema del 1946 nel caso SEC vs. W.J. Howey Co.[99] e serve a determinare se una transazione si qualifica come "contratto di

[97] La prima offerta pubblica di un titolo digitale registrato alla SEC sulla blockchain avviene tramite il security token di INX e attualmente scambia sulla piattaforma di trading di INX Securities. Sempre più piattaforme di titoli digitali stanno rapidamente arrivando sul mercato.

[98] Il test di Howey è la definizione più chiara che può essere utilizzata per capire cosa può essere definito un titolo e cosa no. Se la Securities and Exchange Commission (SEC) decidesse di applicare questo test alle criptovalute, le sue conseguenze potrebbero essere catastrofiche per il mercato. Ecco perché tutti coloro che operano nel mercato degli asset digitali dovrebbero imparare a utilizzare il test di Howey.

[99] La Howey Company vendette tratti di agrumeti ad acquirenti in Florida, che avrebbero poi affittato la terra a Howey. Il personale dell'azienda si prendeva cura dei boschetti e vendeva i frutti per conto dei proprietari. Entrambe le parti hanno condiviso le entrate. La maggior parte degli acquirenti non aveva esperienza in agricoltura e non era tenuta a occuparsi personalmente della terra. Howey non aveva registrato le transazioni ed è intervenuta la Securities and Exchange Commission (SEC) degli Stati Uniti. La sentenza definitiva del tribunale ha determinato gli accordi di retrolocazione qualificati come contratti di investimento.

investimento" e quindi sarebbe considerata una sicurezza e soggetta ai requisiti di divulgazione e registrazione ai sensi del **Securities Act del 1933**[100] e del **Securities Exchange Act del 1934**[101] . Secondo l'Howey Test, esiste un contratto di investimento se c'è un "***investimento di denaro in un'impresa comune con una ragionevole aspettativa di profitti derivanti dagli sforzi di altri***". Il test è divenuto il criterio per determinare se qualcosa è un contratto di investimento. I contratti di investimento sono un sottoinsieme di titoli, oltre ad azioni e obbligazioni, che sono soggetti alla regolamentazione e alla supervisione della SEC. La corte ha deciso che i quattro criteri per definire un contratto di investimento sono i seguenti:

- Deve essere un investimento di denaro.
- L'investimento deve essere in un'impresa comune.
- Deve esserci aspettativa di profitto.
- Il profitto deve derivare dagli sforzi degli altri.

In base a questa definizione, la maggior parte delle offerte iniziali di monete (ICO) sono considerate contratti di investimento e quindi titoli. È raro che le ICO siano disponibili per gli investitori statunitensi, probabilmente perché sono estremamente simili alle offerte pubbliche iniziali (IPO) per le azioni. Purtroppo per i regolatori, è molto più difficile definire lo status di altri tipi di criptovalute in base al test di Howey.

[100] l Securities Act del 1933 è stato creato e convertito in legge per proteggere gli investitori dopo il crollo del mercato azionario del 1929. La legislazione aveva due obiettivi principali: garantire una maggiore trasparenza nei bilanci in modo che gli investitori potessero prendere decisioni informate sugli investimenti; e per stabilire leggi contro false dichiarazioni e attività fraudolente nei mercati mobiliari.

[101] Il Securities Exchange Act del 1934 (SEA) è stato creato per disciplinare le transazioni di titoli sul mercato secondario, dopo l'emissione. Il suo obiettivo era garantire una maggiore trasparenza e accuratezza finanziaria e meno frodi o manipolazioni. La SEA ha autorizzato la costituzione della Securities and Exchange Commission (SEC), il braccio normativo della SEA. La SEC ha il potere di supervisionare i titoli - azioni, obbligazioni e titoli over-the-counter - nonché i mercati e la condotta dei professionisti finanziari, inclusi broker, dealer e consulenti per gli investimenti. Monitora inoltre i rapporti finanziari che le società quotate in borsa sono tenute a divulgare.

I primi due criteri sono generalmente facili da determinare. Il problema sorge spesso quando si cerca di capire se una vendita di criptovaluta ha l'aspettativa di profitto e se tale profitto deriva dagli sforzi degli altri. Quando gli investitori acquistano una criptovaluta, essi hanno un'aspettativa di profitto derivante dal lavoro di altre persone come gli sviluppatori, ma ciò non significa necessariamente che ci sia una ragionevole aspettativa di profitto.

La SEC afferma che gli ultimi due criteri vengono soddisfatti se qualcuno coinvolto nel progetto (o anche un soggetto terzo) "fornisce sforzi gestionali essenziali che influiscono sul successo dell'impresa, e gli investitori si aspettano ragionevolmente di trarre profitto da tali sforzi". Queste attività possono includere il burning dei token, che viene quasi sempre avviato per ridurre l'offerta e tentare di aumentare il valore di un token. Esistono pochi o nessun precedente nel settore delle criptovalute, quindi è difficile sapere come verrà applicato il test.

La regolamentazione incombente è una delle maggiori paure di molti investitori in cripto, e a ragione. Molte delle criptovalute più importanti potrebbero facilmente rientrare nell'ampia definizione di titolo derivante dal test di Howey. Comunque, Bitcoin ed Ethereum probabilmente non subiranno pesanti regolamentazioni in tempi brevi perché la SEC ha affermato esplicitamente che questi non sono titoli. Altri token, in particolare quelli i cui progetti sono composti da persone che cercano attivamente di incrementarne il valore, potrebbero invece avere problemi nel prossimo futuro.

19.2 Initial Coin Offers e Security Tokens Offerings.

Oggi, emerge la rilevanza oggi assunta dalle c.d. ICOs, (Initial Coin Offers), e ancor più dalle c.d. STOs, (Security Tokens Offerings), che nella fattispecie sono assimilabili a vere e proprie IPOs, consistenti nelle peculiari modalità con cui sulle piattaforme informatiche avviene l'offerta di "vendita" delle criptovalute. Ognuna delle criptovalute, infatti, può essere

adoperata dall'emittente come funding token, ossia come veicolo per finanziare il proprio progetto.

Le Initial Coin Offering e le Security Token Offering rappresentano oggi il sistema di finanziamento privilegiato dalle aziende in ambito Fintech (dove il termine Fintech, che nasce dalla contrazione di Finance "Fin" e Technology "Tech", sta ad indicare, nella sua più ampia accezione, un qualunque utilizzo di strumenti digitali applicati in ambito finanziario)[102].

Non si deve escludere che nell'ambito delle ICOs, (Initial Coin Offers) o di quella particolare forma che sono le STOs (Security Tokens Offerings), con riferimento al modello adottato, la stessa piattaforma in cui si opera sia da valutare come "emittente" / "offerente", quindi possa attribuirsi il ruolo di manufacturer come previsto dalla Direttiva n. 2014/65/UE (MIFID II) e dal Regolamento 1286/14 (PRIIPs).

Superata la problematica relativa alla giusta collazione dell'emittente offerente-collocatore, potrebbe però risultare comunque applicabile la disciplina della promozione e collocamento a distanza prevista ex art. 32 TUF ed artt. 125 e ss. del Regolamento Intermediari: in tal caso venendosi ad applicare alla piattaforma sia la disciplina della riserva operativa che quella comportamentale.

Tuttavia, non si esclude che, successivamente, potrebbe essere anche necessario valutare la possibilità di considerare le piattaforme stesse come sedi di negoziazione, con tutte le valutazioni e le conseguenze del caso che ne scaturirebbero; laddove **non bisognerebbe, comunque, escludere la possibilità di essere in presenza di un "self-placement", richiedendosi allora alla piattaforma di essere autorizzata al servizio di "esecuzione ordini" ex art. 4,1 della Direttiva**

[102] Dopo un iniziale boom delle ICO non regolamentate, fra il 2017 e il 2018, il quale ha tuttavia determinato l'insorgenza di numerose truffe ai danni dei risparmiatori, le autorità di ogni parte del mondo sembrano ormai concordi sulla necessità di stabilire dei parametri per le cripto-attività, che contemperino da un lato maggiori garanzie per gli utenti e dall'altro una certa flessibilità in considerazione della natura globale e sempre più decentralizzata di tali operazioni. Rif. https://www.opiniojuris.it/guida-alle-criptovalute-inquadramento-giuridico-e-cryptofunding/

MIFID II con applicazioni delle relative regole comportamentali.

Al di là di questo, sempre considerando che la criptovaluta possa essere effettivamente riferibile al valore mobiliare, potrebbe risultare utilizzabile, in merito all'attività di "intermediazione" svolta dalle "piattaforme", in particolare relativamente alle ICOs, la riserva e la disciplina del servizio di investimento individuabile nel "collocamento senza impegno irrevocabile nei confronti dell'emittente" di cui alla lettera c-bis) dell'art. 1, co. 5, TUF, nonché, al ricorrere dei suoi presupposti, la stessa disciplina della offerta al pubblico.

L'elemento caratteristico del servizio di collocamento consiste nell'"accordo tra l'emittente (o l'offerente) e l'intermediario collocatore, indirizzato all'offerta al pubblico, da parte di quest'ultimo, degli strumenti finanziari emessi, a condizioni di prezzo e di tempo predeterminate"[103]. **L'accordo ha una natura promozionale / propulsiva ed è adeguato ad un'offerta avente caratteristiche uniformate nell'ambito di un'operazione di massa.**

La possibilità che il collocatore accetti (o meno) il rischio che l'operazione distributiva non arrivi a buon fine è irrilevante al fine della qualificazione in termini di servizio di "collocamento", in quanto il servizio di collocamento può manifestarsi nel collocamento con o senza assunzione a fermo o garanzia nei confronti dell'emittente, dove per "assunzione a fermo" si intende la sottoscrizione (underwriting) da parte dell'intermediario di tutti o parte degli strumenti finanziari da collocare; e per "garanzia" ci si riferisce all'impegno del collocatore ad acquistare l'invenduto al termine dell'attività promozionale svolta.

Per cui, considerando la formulazione dell'art. 1, co. 5, lett. c), TUF è da ritenersi incluso tra i servizi e le attività

[103] Visentini, G. I valori mobiliari, in Tratt. Rescigno, XVI, (1985). Carbonetti, Che cos'è un valore mobiliare? in Giurisprudenza Commerciale, I, 280; (1989). Ferrarini, G. I nuovi confini del valore mobiliare, in Giurisprudenza Commerciale, I, p. 741. (1989)

d'investimento, dunque soggetto a riserva di attività, anche il solo underwriting, ovvero l'assunzione a fermo[104].

Nel caso in cui vi sia la promozione e il collocamento di "valori mobiliari" attraverso tecniche di comunicazione a distanza, deve essere fatto nel rispetto delle regole dettate dall'art. 32 del TUF, in base alla quale si specifica "per tecniche di comunicazione a distanza si intendono le tecniche di contatto con la clientela, diverse dalla pubblicità, che non comportano la presenza fisica e simultanea del cliente e del soggetto offerente o di un suo incaricato".

La normativa secondaria di cui al Regolamento Intermediari integra, poi, la disciplina in materia: l'art. 125 indica i soggetti legittimati alla prestazione del servizio, precisandosi al penultimo comma dell'art. 125, che non costituiscono promozione e collocamento mediante tecniche di comunicazione a distanza le attività svolte nei confronti dei clienti professionali di cui all'articolo 35, comma 1, lettera d), Regolamento Intermediari, e cioè clienti che possiedano l'esperienza, le conoscenze e la competenza necessarie per prendere consapevolmente le proprie decisioni in materia di investimenti e per valutare correttamente i rischi che assumono nel caso in cui una "criptovaluta" fosse ricostruibile in termini di "valore mobiliare" (e, in particolare, di "strumenti finanziari di raccolta" quindi, fondamentalmente, ove qualificabili come valori mobiliari rappresentativi di "capitale di debito", e non "di rischio"), ciò implicherebbe di dover tener conto altresì della vigente disciplina "della raccolta del risparmio dei soggetti diversi dalle banche" ex art. 11 TUB che dispone una riserva praticamente assoluta a favore delle banche, fuori dal caso in cui la raccolta avvenga tramite emissione di tali strumenti.

Similmente potrebbe risultare talora applicabile la disciplina di cui alle vigenti "disposizioni in materia di segnalazioni a

[104] 9Visentini, G. I valori mobiliari, op. cit.; Carbonetti, F. Che cos'è un valore mobiliare? cit., p. 280. Ferrarini, G. I nuovi confini del valore mobiliare, cit., p. 741.

carattere consuntivo relative all'emissione e all'offerta di strumenti finanziari" ex art. 129 TUB, applicabili anche ai soggetti non residenti che offrano in Italia – sia al "pubblico" che in modalità "private placement" - strumenti finanziari, anche di diritto estero.

L'ESMA, European Securities and Markets Authority[105], ha elaborato un advice per la Commissione europea riguardante in particolare le problematiche di applicazione della disciplina sui servizi di investimento per i token qualificabili come strumenti finanziari.

Il documento affronta in forma sintetica anche il tema dei token che non si qualificano come strumenti finanziari, raccomandando una regolamentazione ad hoc senza, tuttavia, proporre univoche scelte normative.

In Italia, il 5 giugno 2019 si è conclusa la consultazione pubblica in materia di ICO e cripto-attività avviata il 19 marzo dalla Consob, la quale ha suscitato indubbiamente opinioni contrastanti. Da un lato, infatti, non sono mancate critiche autorevoli poiché "***prospettante soluzioni eccessivamente restrittive che mal si conciliano con la natura globale del mercato e che, dunque, potrebbero determinare un danno per l'economia italiana***"[106].

La regolamentazione delle piattaforme, ovvero l'intenzione della Consob sarebbe quella di:

[105] L'Autorità europea degli strumenti finanziari e dei mercati (ESMA) è un'autorità indipendente dell'UE il cui obiettivo è migliorare la protezione degli investitori e promuovere mercati finanziari stabili e ordinati. Gli obiettivi dell'agenzia sono tre: tutela degli investitori - garantire un migliore soddisfacimento delle esigenze finanziarie dei consumatori e rafforzare i loro diritti in quanto investitori, riconoscendo al tempo stesso le loro responsabilità. corretto funzionamento dei mercati - promuovere l'integrità, la trasparenza, l'efficienza e il corretto funzionamento dei mercati finanziari e una solida infrastruttura di mercato. stabilità finanziaria - rafforzare il sistema finanziario in modo che sia in grado di resistere agli shock e al logorio degli squilibri finanziari, e favorire la crescita economica. L'ESMA ha inoltre il compito di coordinare le misure prese da autorità di vigilanza sui valori mobiliari o di adottare misure di emergenza in caso di crisi. Rif. https://europa.eu/european-union/about-eu/agencies/esma_it

[106] https://www.opiniojuris.it/guida-alle-criptovalute-inquadramento-giuridico-e-cryptofunding/

a) ampliare la gamma delle offerte delle piattaforme di crowdfunding con le cripto-attività;

b) applicare tout court agli operatori di piattaforme di ICO la normativa in materia di crowdfunding;

c) stabilire uno stretto collegamento fra l'offerta di criptoattività di nuova emissione, realizzata per il tramite di piattaforme vigilate, e il loro successivo accesso a un sistema di scambi dedicato, soggetto anch'esso a regolamentazione e vigilanza[107].

Infatti, nonostante le piattaforme di crowdfunding risultino naturalmente preposte a tali attività in ragione della sottoposizione a vigilanza ex Regolamento 18592/2013, tuttavia, si rendono necessari importanti aggiustamenti riguardanti la gestione dei wallet e l'uso della tecnologia blockchain; la stessa normativa sul crowdfunding presenta peculiarità che non la rendono estendibile automaticamente alle criptoattività. **Non sono mancate comunque opinioni a favore dell'impostazione della Consob, in particolare per quanto riguarda il sistema c.d. di doppio optin, per l'offerta e lo scambio: qualora venissero oltrepassate le varie criticità, permetterebbe di tutelare i risparmiatori senza tuttavia imporre notevoli restrizioni al mercato.**

Posto che, come detto, per i token assimilabili a strumenti finanziari o prodotti di investimento assicurativi e pre-assemblati (PRIIP, PRIP e IBIP), la disciplina applicabile è quella prevista nel TUF e nelle direttive e regolamenti emessi dall'Unione Europea, anche qualora le offerte vengano svolte tramite le piattaforme previste nel documento stesso, riguardo i token ibridi e gli utility token la Consob ha previsto di svolgere l'offerta senza collocare i token tramite le piattaforme per le offerte di cripto-attività, assumendo però il rischio che detti token vengano successivamente qualificati come prodotti finanziari con le relative conseguenze (ossia una assai probabile sospensione dell'offerta da parte della Consob per violazione

[107] https://www.opiniojuris.it/guida-alle-criptovalute-inquadramento-giuridico-e-cryptofunding/

delle norme in materia di prospetto informativo e di promozione e collocamento a distanza di prodotti finanziari); oppure di collocare e promuovere l'offerta attraverso una piattaforma per le offerte di criptoattività, con conseguente applicazione della disciplina regolamentare che sarà eventualmente emanata; in tal caso il vantaggio consisterebbe nell'eliminazione di qualsiasi incertezza interpretativa sulla disciplina da applicare.

Il 2018 è stato l'anno della tecnologia blockchain. Il primo semestre è stato all'insegna delle richieste di emissione di token basati sulla blockchain (mercato primario). Nel secondo semestre la FINMA ha trattato in maniera crescente anche domande sul commercio secondario di prodotti basati sulla tecnologia blockchain. Inoltre, si è occupata di altre questioni afferenti all'ambito della tecnofinanza.

La Svizzera è diventata una piazza mondiale privilegiata per l'esecuzione di initial coin offering (ICO). Nel quadro di un'ICO, gli investitori trasferiscono mezzi finanziari (generalmente sotto forma di criptovalute) al relativo organizzatore. In cambio ottengono coin o token basati sulla tecnologia blockchain, creati e salvati a livello decentralizzato su una nuova blockchain oppure, mediante un cosiddetto smart contract, su una blockchain esistente.

Attualmente non esistono requisiti normativi specifici inerenti alle ICO, ma vi sono diversi punti di contatto tra le ICO e il vigente diritto in materia di mercati finanziari. Con la sua interpretazione della vigente legislazione sui mercati finanziari la FINMA consente l'uso di tecnologie innovative. Allo stesso tempo la FINMA mette in guardia gli investitori dai rischi legati alle ICO (cfr. in particolare la Comunicazione FINMA sulla vigilanza 04/2017 del 29 settembre 2017). I token acquistati nell'ambito di un'ICO sono soggetti a una forte volatilità dei prezzi. Trovandosi molte ICO ancora a uno stadio iniziale, persistono numerose incertezze sui progetti da finanziare e da realizzare. La FINMA non può escludere che le attività legate alle ICO celino intenti fraudolenti. Essa non tollera condotte

fraudolente o abusive né l'elusione del quadro normativo, e all'occorrenza adotta le necessarie misure.

Essendo le ICO strutturate in modo assai eterogeneo, occorre valutare caso per caso quali leggi in materia di mercati finanziari siano applicabili. Con la guida pratica pubblicata il 16 febbraio 2018, la FINMA ha definito le informazioni minime necessarie per il trattamento delle richieste di assoggettamento riguardanti progetti ICO e i principi in base ai quali vengono fornite le risposte. Per presentare la guida pratica, la FINMA ha organizzato tavole rotonde a Zugo, Ginevra e Lugano, facendo per quanto possibile chiarezza sull'applicazione del diritto vigente affinché i partecipanti al mercato interessati possano orientarsi rapidamente e con facilità, e chiarire in ampia misura in modo autonomo le questioni inerenti al diritto in materia di vigilanza. La FINMA è disposta a fornire ai partecipanti al mercato che desiderano avviare un'attività un parere preliminare sui progetti di ICO concreti. La FINMA ha trattato la maggior parte delle circa 155 richieste dettagliate di assoggettamento di ICO pervenutele nel 2018. Come specificato nella guida pratica, la FINMA distingue tre tipi di token: token di pagamento, token di utilizzo e token d'investimento.

La categoria «token di pagamento» (come le criptovalute) comprende token che, effettivamente o nelle intenzioni dell'organizzatore, sono accettati come mezzi di pagamento per l'acquisto di beni o servizi oppure sono finalizzati al trasferimento di denaro e valori. L'emissione di token di pagamento è soggetta in linea di principio alle **prescrizioni della LRD**[108].

La FINMA[109] definisce «***token di utilizzo***» **quelli che permettono di accedere a un'utilizzazione o a un servizio**

[108] Legge federale relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. Legge sul riciclaggio di denaro, LRD del 10 ottobre 1997 (Stato 23 gennaio 2023); Nuovo testo giusta il n. I 7 della LF del 12 dic. 2014 concernente l'attuazione delle Raccomandazioni del Gruppo d'azione finanziaria rivedute nel 2012, in vigore dal 1° gen. 2016 (RU 2015 1389; FF 2014 563).

[109] **FINMA** protegge la funzionalità dei mercati finanziari, nonché i creditori, gli investitori e gli assicurati. In tale contesto la protezione dei clienti va intesa in senso collettivo – le rivendicazioni che concernono il singolo individuo devono in linea di

digitale, e che sono basati sull'utilizzo di un'infrastruttura blockchain. L'emissione di token di utilizzo non è soggetta all'obbligo di autorizzazione se, al momento dell'emissione, l'utilizzazione o il servizio digitale è pienamente funzionante.

La categoria «***token d'investimento***» comprende i token che costituiscono valori patrimoniali. **Questi token possono costituire, in particolare, un credito nei confronti dell'emittente ai sensi del diritto delle obbligazioni oppure un diritto societario ai sensi del pertinente diritto. Secondo la funzione economica, il token rappresenta quindi un'azione, un'obbligazione o uno strumento finanziario derivato.** L'emissione propria di token d'investimento qualificabili come valori mobiliari non necessita dell'autorizzazione della FINMA, ma è soggetta agli obblighi di

principio essere fatte valere adendo le vie del diritto civile. In qualità di autorità di vigilanza, la FINMA deve prioritariamente adoperarsi affinché tutti gli operatori attivi sul mercato finanziario agiscano nel rispetto delle prescrizioni e il sistema finanziario nel suo complesso conservi la propria stabilità. Per garantire questo, la FINMA emette autorizzazioni per banche, assicurazioni, borse e altri partecipanti al mercato finanziario, come i gestori patrimoniali di investimenti collettivi di capitale. Inoltre, la FINMA vigila sugli operatori autorizzati e procede contro di essi in caso di violazione delle norme. Un importante obiettivo che la FINMA deve perseguire per legge è la protezione dei clienti. Tale protezione investe la collettività dei clienti di tutte le banche e assicurazioni, nonché gli investitori. Per la comunità dei clienti è fondamentale che gli istituti finanziari assoggettati alla vigilanza restino solvibili (tutela individuale tramite la salvaguardia della solvibilità). Garantirlo rientra nei compiti chiave della FINMA che, a tal fine, si avvale degli strumenti del diritto in materia di vigilanza. La FINMA osserva l'approccio degli assoggettati alla vigilanza nei confronti della propria clientela e interviene nel momento in cui la condotta di uno o più assoggettati non è conforme alle disposizioni legali. Tuttavia la FINMA non può intervenire nei rapporti (contrattuali) diretti tra istituto finanziario e cliente. La FINMA impone l'osservanza delle leggi sui mercati finanziari anche presso gli offerenti che non dispongono di alcuna autorizzazione, ma che dovrebbero averne una in ragione dell'attività che svolgono. Di conseguenza la FINMA provvede non di rado altresì alla liquidazione di aziende che operano in maniera illecita, vestendo per certi versi anche i panni di guardia di confine della piazza finanziaria svizzera. Per il lavoro della FINMA le segnalazioni da parte dei privati sono tanto importanti quanto le informazioni che essa acquisisce mediante la propria attività di vigilanza o il monitoraggio del mercato. I reclami dei clienti possono mettere in luce violazioni delle leggi sui mercati finanziari o abusi perpetrati dagli assoggettati. Grazie ai problemi segnalati, la FINMA può per esempio rivolgere la propria attenzione ai fornitori di servizi finanziari che operano nell'illegalità, approfondire presunte manipolazioni di borsa o perseguire i sistematici comportamenti scorretti degli operatori finanziari. Se le segnalazioni dei clienti sono confermate, la FINMA procede contro le irregolarità applicando il diritto in materia di vigilanza.

pubblicazione di un prospetto sanciti dal CO. Esistono anche token ibridi, ovvero qualificabili allo stesso tempo come token di utilizzo e di pagamento.

Nel 2022 hanno assunto una rilevanza centrale le questioni relative ai cosiddetti non-fungible token (NFT), alla finanza decentralizzata (decentralised finance), ai sistemi di negoziazione con la tecnologia di registro distribuito (distributed ledger technology, DLT) e all'intelligenza artificiale (artificial intelligence, AI). La FINMA persegue un approccio di vigilanza improntato alla neutralità tecnologica e, nel confronto con i diversi interlocutori, elabora soluzioni concrete e orientate alla prassi. La FINMA si è nuovamente occupata in modo approfondito delle questioni relative ai servizi finanziari basati sulla tecnologia blockchain e sui beni crittografici. Sono state avanzate richieste mirate in questo ambito sia nel quadro di classici progetti di start-up, sia da parte degli istituti sottoposti a vigilanza. Tra gli sviluppi più recenti si annoverano soprattutto le richieste di assoggettamento dei non-fungible token, nonché l'interesse degli istituti sottoposti a vigilanza per le offerte di finanza decentralizzata.

Nel 2022 il mercato dei beni crittografici è stato caratterizzato da una spiccata volatilità. Mentre all'inizio dell'anno le quotazioni del mercato erano ancora molto elevate, a metà anno si è registrata una correzione sostanziale, in alcuni casi superiore al 50% delle valutazioni totali, che ha messo in difficoltà anche alcuni operatori di maggiori dimensioni non domiciliati in Svizzera, come la borsa di criptovalute FTX, la stablecoin UST dell'ecosistema Terra o le aziende statunitensi Celsius e Voyager Digital specializzate nell'erogazione di prestiti in beni crittografici. L'andamento dell'anno in esame mostra essenzial mente una considerevole volatilità e i rischi sostanziali assunti dagli investitori sul mercato dei beni crittografici. Nel 2022 le banche svizzere con forte orientamento ai beni crittografici hanno ampliato la propria gamma di servizi, inserendovi, per esempio, lo staking sulla blockchain Ethereum, che offre ai possessori di criptovalute la possibilità di mettere a disposizione,

dietro compenso, i propri coin per consentire l'esercizio della blockchain (proof of stake), o proponendo servizi di supporto all'emissione dei cosiddetti non-fungible token. Sono inoltre stati concessi crediti per il mining di nuove criptovalute, offerti servizi di tokenizzazione di valori patrimoniali reali, lanciati valori patrimoniali digitali quotati in borsa (exchange traded crypto, exchange traded products [ETP]) e creati altri strumenti finanziari. In Svizzera una trentina di banche e società di intermediazione mobiliare ha ampliato il proprio portafoglio di prodotti in questo segmento

In ambito blockchain, token e coin vengono gestiti e trasmessi mediante applicazioni software (wallet). Questi wallet vanno intesi sostanzialmente come un portafoglio digitale con il quale gli utenti possono conservare i loro criptovalori patrimoniali o attivare trasferimenti.

Fra i metodi di verifica adeguati si è aggiunta la ***procedura di timeboxing***[110], che consiste nel trasferimento diretto di un importo da parte del cliente in sostituzione di un'antecedente microtransazione. Il cliente deve preannunciare la transazione e l'importo, dopo di che l'intermediario finanziario fornisce l'indirizzo al cliente e gli mette a disposizione una breve finestra temporale (time box). La transazione convenuta può essere effettuata all'interno di questi parametri; la prova della facoltà di disporre viene fornita verificando il rispetto di tali requisiti. Un'altra novità è costituita dal wallet login dei clienti in presenza di collaboratori dell'intermediario finanziario. Se la procedura è documentata in modo sufficiente, anche questa misura è considerata adeguata in conformità alla Comunicazione FINMA sulla vigilanza 02/2019 «Il traffico dei pagamenti nella blockchain».

Ogni trasferimento deve recare come firma la chiave privata (private key) del titolare del token. Esistono due tipi di fornitori di wallet: custody wallet e non-custody wallet. I

[110] Il ***timeboxing*** è una strategia di gestione del tempo basata su obiettivi che ti aiuta ad aumentare la produttività e ridurre gli indugi. Quando crei un blocco di tempo ("timebox"), ti poni l'obiettivo di completare un'attività entro un determinato lasso di tempo.

fornitori custody wallet custodiscono e gestiscono le private key dei clienti e, custodendole, hanno la facoltà di disporre in modo diretto sui valori patrimoniali di terzi affidatigli, erogando quindi un servizio per il traffico dei pagamenti. Il servizio per il traffico dei pagamenti erogato a titolo professionale sottostà alla Legge sul riciclaggio di denaro. Sorgono inoltre questioni afferenti al diritto bancario. In conformità all'attuale prassi della FINMA, non è necessaria a condizioni rigorose un'autorizzazione a operare come banca se le valute virtuali sono custodite separatamente per ogni cliente sulla blockchain e possono essere attribuite al singolo cliente in qualsiasi momento.

Nel caso dei fornitori non-custody wallet, i clienti hanno un accesso esclusivo ai loro privati keys. Questo tipo di fornitori non ha dunque la facoltà giuridica o fattuale di disporre sui valori patrimoniali di terzi. Secondo il diritto vigente e gli standard internazionali, questi fornitori non sono assoggettati alla Legge sul riciclaggio di denaro.

In merito allo scambio ha previsto di far ammettere il token emesso nel regime di optin in un mercato secondario anch'esso autorizzato dalla Consob (facendo godere il token di una maggiore affidabilità presso gli investitori); oppure presso un exchange non autorizzato.

In definitiva, analogamente al sistema francese, quello indicato dalla Consob permetterebbe a chi intenda svolgere un'offerta iniziale di criptovalute di aderire o meno alle nuove direttive e ai risparmiatori di accettare o meno, con cognizione di causa, se rivolgersi a soggetti e offerte disciplinate nello specifico[111].

20. La regolamentazione.

Si è cominciato ad analizzare la questione, da parte delle autorità competenti, dopo quello che era successo a "The DAO" il 18 giugno 2016, quando alcuni hacker avevano violato la

[111] https://www.opiniojuris.it/guida-alle-criptovalute-inquadramento-giuridico-e-cryptofunding/

piattaforma in cui erano depositati gli ethereum raccolti, per un danno di circa 70 milioni di dollari.

L'art. 1 co. 126 della Legge n. 197/2022 (Legge di bilancio 2023) ha, di fatto, ridefinito la normativa fiscale che riguarda le valute virtuali detenute da soggetti fiscalmente residenti in Italia. La norma fa rientrare tra i redditi diversi di natura finanziaria "*le plusvalenze e gli altri proventi realizzati mediante rimborso o cessione a titolo oneroso, permuta o detenzione di cripto-attività, comunque denominate*". A tali fini, per cripto-attività si intende "una rappresentazione digitale di valore o di diritti che possono essere trasferiti o memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga ". In linea generale, possiamo dire che i profili fiscali da analizzare per le cripto-attività riguardano tre fattispecie:

- La normativa legate alle imposte dirette, per la dichiarazione dei proventi (plusvalenze) derivanti dalla cessione di valuta virtuale;
- La normativa legata al monitoraggio fiscale delle valute virtuali, nel quadro RW;
- La normativa ai fini Iva che riguarda gli operatori economici che scambiano criptovalute.

I criteri da adottare, in sede di dichiarazione dei redditi derivanti dagli investimenti speculativi eseguiti con le c.d. cripto attività sono state disciplinata dalla Legge n. 197/22 (art. 1 co. 126) che ha superato le precedenti disposizioni di prassi (Risoluzione n. 72/E/2016). La novità principale rispetto al passato riguarda il fatto che i proventi realizzati tramite rimborso o cessione a titolo oneroso, permuta o detenzione di cripto-attività, rientrano nella categoria dei redditi diversi ex art. 67, co. 1, lettera c-sexies del TUIR. Secondo il successivo art. 68 co. 10 del TUIR tali plusvalenze, costituite dalla differenza tra il corrispettivo percepito o il valore normale delle cripto-attività permutate e il costo o il valore di acquisto. Le plusvalenze così determinate sono sommate alle minusvalenze. Se le minusvalenze risultano essere superiori alle

plusvalenze, per importo superiore a 2.000 euro, l'eccedenza è riportata in deduzione integrale all'ammontare delle plusvalenze dei periodi successivi, ma non oltre il quarto.

Per questo è necessario che la minusvalenza venga indicata nella dichiarazione dei redditi relativa al periodo di imposta nel quale le minusvalenze sono realizzate. Assume rilevanza fiscale il passaggio tra cripto-attività a valuta fiat. Nella relazione illustrativa alla legge viene precisato che "non assume rilevanza lo scambio tra valute virtuali, mentre assume rilevanza fiscale l'utilizzo di una cripto-attività per l'acquisto di un bene o un servizio o di un'altra tipologia di cripto-attività (ad esempio, l'utilizzo di una criptocurrency per acquistare un non fungible token) o la conversione di una currency in euro o in valuta estera". Questo significa che, di fatto la permuta tra cripto-attività non assume rilevanza fiscale, mentre il passaggio da valuta virtuale a valuta fiat, oppure l'utilizzo della valuta per acquistare beni o servizi assume rilevanza fiscale. Il riferimento alla detenzione di cripto-attività (comprese quindi le cripto-valute) sembra voler includere la fattispecie della remunerazione dell'attività di staking fra i redditi diversi, superando i precedenti chiarimenti disposti dall'Agenzia delle Entrate in via interpretativa con la risposta ad interpello n. 437/2022. Tuttavia, si attendono chiarimenti in merito, anche in relazione alle possibili modifiche che verranno apportate in sede parlamentare.

La SEC, la commissione federale degli Stati Uniti preposta alla vigilanza della borsa, cercò di capire se queste raccolte di fondi potessero essere riconducibili ai consueti collocamenti degli strumenti finanziari, per poter applicare in questo caso la "Securities Law".

Nella valutazione emerse che non è indispensabile che l'investimento sia in denaro (nel caso della DAO erano token), che tutta l'operazione aveva uno scopo di lucro (dividendi o aumento di valore) e che le aspettative di guadagno dipendevano dalle capacità gestionali di terzi.

In sostanza si rientra dunque nei parametri del test Howey che la SEC utilizza per capire se si ha a che fare con un "contratto di

investimento", guardando più la sostanza che non la semplice forma contrattuale. Scatta di conseguenza l'obbligo di registrare offerte e vendite sia da parte degli organizzatori, sia da parte dei gestori delle piattaforme di scambio delle criptovalute. Per scavalcare questi obblighi, qualche ICO ha posto l'accento sull'uso commerciale delle loro monete, dato il loro potenziale di scambio.

La SEC ha però recentemente ribadito la prevalenza della sostanza sulla forma, a meno che i responsabili della ICO non dimostrino che le monete prodotte non rientrino nell'ambito dei prodotti finanziari. In caso contrario devono sottostare alle regole che disciplinano le offerte pubbliche di vendita.

Il rapporto della SEC del 2017 ha costituito il punto di partenza per la regolamentazione della questione. Le autorità di controllo di molti altri stati hanno iniziato a prendere posizione. **Alcune, ad esempio in Australia, Canada e Singapore, hanno emesso disposizioni simili, altre, come in Giappone e in Svizzera, si sono limitate a ricordare l'applicabilità della legislazione nazionale in base al tipo di moneta emesso**.

Anche l'autorità europea, l'ESMA, ha ribadito l'obbligo del rispetto delle normative comunitarie, sottolineando altresì i rischi di queste operazioni e mettendo in guardia investitori e imprese. **L'Estonia ha invece addirittura ventilato la possibilità di una ICO per una valuta nazionale**. **In direzione opposta si muove la Cina, che il 4 settembre 2017 ha disposto non solo il divieto di ICO, ma anche la sospensione delle attività di compravendita di criptovalute con moneta corrente, seguita dopo breve tempo dalla Corea del Sud.**

20.1 Regolamentazione europea ed internazionale: La V Direttiva Antiriciclaggio.

Esaminando gli svariati comunicati, le numerose avvertenze e le linee guida derivati dalle autorità di vigilanza di diversi Stati, è possibile osservare come ad oggi non vi sia uniformità in merito alla qualificazione giuridica delle valute virtuali.

Le problematiche legate anche ad una valida qualificazione giuridica, che sia uniformemente approvata dagli Stati,

conducono anche ad un differente approccio attuato dagli stessi, con conseguente diversa regolamentazione, in ambito nazionale.

Negli **Stati Uniti**, per esempio, sulla base di quanto ha dichiarato la Securities and Exchange Commission (US SEC), ente federale statunitense preposto alla vigilanza della borsa valori, le valute virtuali sono considerate "una rappresentazione digitale di valore che può essere scambiata digitalmente e funziona come mezzo di scambio, unità di conto o riserva di valore.

Le monete virtuali possono rappresentare anche altri diritti, di conseguenza, in determinati casi, le monete o i token saranno strumenti finanziari e non potranno essere venduti legalmente senza registrazione presso la SEC o in base ad un'esenzione"[112].

In **Germania**, con l'intervento della Federal Financial Supervisory Authority (BaFin), si è precisato che, in base alla normativa vigente nell'ordinamento tedesco, "***i bitcoin sono da considerarsi essenzialmente alla stregua di strumenti finanziari***"[113].

Relativamente al quadro normativo russo riguardante le criptovalute, occorre evidenziare che ad oggi in Russia non vengono ancora ufficialmente definite. A riguardo è stato pubblicato il progetto di legge n. 419059-7 sui "Digital Financial Asset" che seppur ancora provvisorio (è stato approvato solo nella prima delle tre letture previste dall'iter legislativo), presenta alcuni spunti interessanti.

[112] US SEC, Investor Bullettin: initial coin offerings, 25 July 2017, disponibile in lingua originale sul sito istituzionale dell'Autorità: https://www.sec.gov/oiea/investor-alerts-andbulletins/ib_coinofferings. Cfr. anche Statement on Cryptocurrencies and initial Coin Offerings, SEC Chairman Jay Clayton, 11 December 2017, secondo cui "while there are cryptocurrencies that do not appear to be securities, simply calling something a "currency" or a currency-based product does not mean that it is not a security. Before launching a cryptocurrency or a product with its value tied to one or more cryptocurrencies, its promoters must either (1) be able to demonstrate that the currency or product is not a security or (2) comply with applicable registration and other requirements under our securities laws".

[113]https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html)

Quest'ultimo infatti definisce "Criptovalute" e "Token" come attività finanziarie digitali, cioè come proprietà (e non come sistema legale di pagamento) create in forma elettronica utilizzando dispositivi crittografici le cui informazioni sono memorizzate in portafogli digitali con l'ausilio di dispositivi hardware e software[114].

In **Svizzera** l'autorità di riferimento (Financial Market Supervisory Authority - FINMA) ha previsto che l'operatività in criptovalute e, in particolare, le attività sottese alle ICO possono presentare caratteristiche tali da essere ricondotte nell'ambito di applicazione della normativa in materia di antiriciclaggio, diritto bancario, intermediazione mobiliare o gestione collettiva a seconda dei casi[115].

Allo stesso modo si è pronunciata la Financial Conduct Authority (FCA) del **Regno Unito**, secondo cui, al fine di stabile se una ICO rientri nell'ambito della regolamentazione, è necessario effettuare una analisi accurata, caso per caso. Secondo tale Autorità "molte ICO cadranno al di fuori dello spazio regolamentato; tuttavia, in base alla struttura, alcune ICO possono comportare investimenti regolamentati e le imprese coinvolte in una ICO possono condurre attività regolamentate.

Alcune ICO presentano parallelismi con le offerte pubbliche iniziali (IPO), il collocamento privato di titoli, il crowdfunding o persino gli schemi di investimento collettivo. Alcuni token possono anche essere valori mobiliari e pertanto possono rientrare nel regime del prospetto"[116].

Il **Giappone** è stato uno dei primi paesi, a livello globale, ad introdurre alcune misure nel tentativo di regolamentare il mercato delle Criptovalute. A riguardo, già nel 2014 furono istituiti presso la "Financial Services Agency" un gruppo di studio ed uno di lavoro per approfondire le tematiche legate ai

[114] https://www.riskcompliance.it/news/criptovalute-normativa-internazionale-a-confronto/

[115] FNMA Guidance 04/2017, Regulatory treatment of initial coin offerings.

[116] Financial Conduct Authority (FCA), Initial Coin Offerings, 12 September 2017: https://www.fca.org.uk/news/statements/initial-coin-offerings

sistemi di pagamento e regolamento introdotti dalle Criptovalute. La relazione finale prodotta da questi gruppi di lavoro raccomandava l'introduzione di un sistema di registrazione per le attività che avevano ad oggetto lo scambio di Criptovalute in modo tale da rendere le transazioni avvenute tramite questi strumenti soggette alle normative sul riciclaggio di denaro e al tempo stesso favorire l'introduzione di un sistema di tutela per gli utenti. Tale legge, ossia il Payment Services Act, venne modificata nel 2016 ed entrò in vigore a partire dal 1° aprile 2017, sancendo così l'accettazione ufficiale delle valute virtuali come sistema di pagamento[117].

La **Cina**, pur avendo portato solo parzialmente a compimento la maggior parte delle raccomandazioni del G.A.F.I., ha fatto recentemente registrare un rapido sviluppo della propria normativa antiriciclaggio, soprattutto grazie alla pubblicazione, avvenuta il 28 dicembre 2016, ad opera della Banca Popolare Cinese del "Decreto N. 3". Relativamente alle criptovalute, nel 2013 la Cina ha definito il Bitcoin e le altre valute virtuali come delle "Virtual Commodity" ossia beni virtuali, ritenendo che le stesse non siano in possesso delle caratteristiche che delineano la moneta e che non ne acquisteranno in futuro lo stesso stato legale. Sebbene il pubblico sia libero di usare le valute virtuali come mezzo di scambio, le istituzioni finanziarie non sono autorizzate a fare altrettanto.

La regolamentazione proibisce infatti a queste ultime di prezzare i propri prodotti e servizi in Bitcoin o simili, di scambiare, fornire assicurazione e servizi correlati, negoziare o gestire valuta virtuale in qualsiasi forma. Il 4 settembre 2017 la Cina ha posto al bando le ICO definendole come "una minaccia seria per l'ordine economico e finanziario"; inoltre è istituita una commissione guidata dalla Banca Centrale Cinese che ha il compito di effettuare ispezioni approfondite presso oltre 60 piattaforme che si occupano di finanziamento tramite ICO, al fine di tutelare gli interessi degli investitori e di gestire le

[117] https://www.riskcompliance.it/news/criptovalute-normativa-internazionale-a-confronto/

ripercussioni di questo tipo di raccolta fondi in termini di rischio finanziario[118].

In altre situazioni si è evidenziato similitudini delle valute virtuali rispetto a beni fisici come i metalli preziosi, i combustibili e i prodotti agricoli, riconducendo le criptovalute alla nozione di commodities, ossia, di prodotti che possono essere utilizzati a scopo di investimento o speculativo[119]. Come si può bene vedere, l'argomento è molto vasto e complesso ed è affrontato in modo multiforme nelle varie realtà.

Il tema delle criptovalute è stato studiato anche dalle autorità europee, che hanno cercato di analizzare le valute virtuali al fine di adottare raccomandazioni nei confronti delle competenti autorità di vigilanza nazionali all'interno del mercato unico, valutando anche la necessità o l'opportunità di predisporre regole ad hoc per regolamentare il fenomeno a livello europeo. In particolare, a seguito di alcune comunicazioni preliminari, nel luglio 2014 la European Banking Authority (EBA) ha pubblicato una opinion indirizzata alle istituzioni dell'UE ed alle autorità di vigilanza degli Stati membri, nella quale ha analizzato le caratteristiche e i rischi connessi alle valute virtuali.

In tale opinion, le criptovalute vengono definite come rappresentazioni digitali di valore non emesse da banche centrali o da altre autorità pubbliche, le quali possono essere accettate da persone fisiche o giuridiche come mezzo di pagamento. Nell'individuare alcuni potenziali benefici delle valute virtuali - come minori costi delle transazioni, velocità e inclusione finanziaria - l'EBA ha sottolineato la sussistenza di numerosi rischi per i consumatori, per l'integrità dei mercati finanziari (come ad esempio in ambito antiriciclaggio e contrasto al finanziamento del terrorismo), per i sistemi di pagamento basati su monete tradizionali e per le autorità di vigilanza.

[118] 60 https://www.riskcompliance.it/news/criptovalute-normativa-internazionale-a-confronto/

[119] Secondo la US Commodity Futures Trading Commission (CFTC) "Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities" (CFTC Docket No. 15-29, Sep. 17, 2015).

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

Oltre all'EBA e alla BCE, anche l'Autorità Europea dei Mercati Finanziari (ESMA) ha rilasciato uno statement nel quale ha affermato che "a seconda di come sono strutturate, le ICO potrebbero non rientrare nell'ambito delle regole esistenti e quindi rimanere al di fuori dello spazio regolamentato. Tuttavia, laddove le monete o i token si qualifichino come strumenti finanziari, è probabile che le imprese coinvolte nelle ICO conducano attività di investimento regolamentate, quali collocamento, negoziazione o consulenza su strumenti finanziari o gestione o commercializzazione di fondi di investimento collettivo.

Le imprese possono, inoltre, essere coinvolte nell'offerta di valori mobiliari al pubblico"[120]. **La Banca Centrale Europea ha recentemente pubblicato un chiarimento relativamente ai bitcoin, cercando di illustrarne i pericoli per gli investitori ed escludendo contemporaneamente che sia suo compito quello di regolare tale materia.**

Parallelamente l'allora Governatore della BCE, Mario Draghi, in una sessione aperta con gli studenti del febbraio 2018, aveva affermato che bitcoin non può considerarsi una valuta per due ragioni: la prima è che «il valore del bitcoin ha forti oscillazioni», mentre «un euro oggi è un euro domani e il suo valore è stabile», oltre al fatto che mentre le valute hanno «dietro le banche centrali dei loro Paesi e dei loro governi», questo non accade per la criptovaluta. Il governatore si era detto però «molto

[120] https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-andfirms.

interessato» alla tecnologia blockchain, definita «promettente», in quanto permette di fare «più velocemente» alcuni processi[121].

La Commissione Europea ha istituito l'Osservatorio e un Forum sulla blockchain, con l'obiettivo di monitorare gli sviluppi ed i progetti di utilizzo della blockchain più interessanti sul territorio europeo, mettendo a disposizione dei finanziamenti allo scopo di incoraggiare i governi, le industrie ed i cittadini europei di avvantaggiarsi delle opportunità fornite da tale nuova tecnologia: i vari paesi del territorio europeo si stanno invece muovendo in maniera piuttosto autonoma.

La Commissione europea ha comunque assicurato che continuerà a monitorare i mercati con gli altri ***stakeholder*** sia a livello europeo che a livello internazionale. **La Quinta Direttiva Antiriciclaggio dell'Unione Europea (5AMLD)[122]** è entrata ufficialmente in vigore il 10 gennaio 2020. Il disegno di legge è stato presentato il 9 luglio 2018 con il duplice intento di rendere più trasparenti le transazioni finanziarie e di contrastare il riciclaggio di denaro e il finanziamento del terrorismo in Europa.

Per la prima volta, la 5AMLD ha esteso il suo perimetro applicativo includendo i prestatori di servizi basati su criptovalute quali exchange di monete digitali e fiat o fornitori di wallet custodial.

Il progetto è quello di identificare più chiaramente i soggetti che prendono parte alle transazioni di criptovalute. In tal modo sarà possibile contrastare più facilmente il riciclaggio di denaro e il finanziamento del terrorismo. Stando alla scheda informativa della 5AMLD[123], la normativa:

[121] 63
https://www.repubblica.it/economia/2018/02/13/news/bce_askdraghi_bitcoin_crisi-188765722/

[122] La direttiva n. 2018/843 del Parlamento europeo e del Consiglio, del 30 maggio 2018 (cosiddetta V direttiva antiriciclaggio).

[123] 5° direttiva antiriciclaggio.

1) garantirà una maggiore trasparenza riguardo agli effettivi titolari delle persone giuridiche al fine di prevenire episodi di riciclaggio di denaro e finanziamento del terrorismo attraverso l'impiego di meccanismi poco limpidi;

2) darà agli organismi europei di regolamentazione finanziaria maggiore accesso alle informazioni tramite i registri contabili delle banche centrali;

3) affronterà i rischi del finanziamento del terrorismo legati all'utilizzo in anonimato di valute digitali e di strumenti prepagati;

4) migliorerà la cooperazione e lo scambio di informazioni tra gli organismi di vigilanza e la BCE;

5) estenderà i criteri di valutazione di Paesi terzi ad alto rischio e assicurerà un alto livello di garanzie per i trasferimenti di denaro verso o da tali Paesi. Qualora non si rispetti tale normativa, saranno chiaramente irrogate delle pene pecuniarie. Le attività basate sulle cryptovalute non avranno vita facile se si ritroveranno a dover pagare le sanzioni di non conformità alla 5AMLD[124].

Questa nuova direttiva è finalizzata ad accrescere ulteriormente la trasparenza generale del contesto economico e finanziario dell'Unione, ben consapevoli del miglioramento già avvenuto nel corso degli ultimi anni, a livello di Stati membri, sul fronte dell'adozione e dell'applicazione delle norme del gruppo di azione finanziaria internazionale (GAFI)[125].

Inoltre, queste misure rispecchiano con esattezza gli impegni assunti e gli sviluppi a livello internazionale: basti pensare alla

[124] https://it.cointelegraph.com/news/what-the-5th-anti-money-laundering-directive-means-forcrypto-businesses

[125] GAFI (Gruppo d'Azione Finanziaria internazionale). Si tratta di un organismo intergovernativo, costituito nel 1989 in occasione del G7 di Parigi, che ha come obiettivo quello di elaborare e sviluppare strategie di lotta al riciclaggio dei capitali di origine illecita, di contrastare il finanziamento al terrorismo e la proliferazione di armi di distruzione di massa. Del GAFI fanno parte trentacinque membri in rappresentanza degli Stati o delle Organizzazioni regionali che corrispondono ai principali centri finanziari internazionali. Rif. https://www.fiscalfocus.it/prime/crypto-valute-e-blockchain/il-gafi-e-l-anonimato-delle-valute-virtuali,3,111056

risoluzione del Consiglio di sicurezza delle Nazioni Unite (UNSCR) 2195 (104) sulle minacce alla pace ed alla sicurezza internazionale causate da atti di terrorismo[126].

20.2 Il D. Lgs n. 90/2017 e la nozione della "digitalizzazione di valore".

Nel 2015 la Banca d'Italia delimitava le valute virtuali come "rappresentazioni digitali di valore, utilizzate come mezzo di scambio o detenute a scopo di investimento, che possono essere trasferite, archiviate e negoziate elettronicamente", osservando che l'impiego del termine "valuta" veniva adoperato unicamente per identificare il fenomeno abitualmente noto sotto tale qualificazione, non volendo manifestare alcuna valutazione sulla natura di tali strumenti, non ancora perfettamente qualificati, quantomeno da un punto di vista giuridico[127]. **La qualificazione giuridica delle valute virtuali rappresenta, infatti, una questione molto articolata, non ancora definitivamente risolta attraverso una soluzione giuridica univoca.**

Numerosi tentativi sono stati fatti tutt'oggi per trovare una definizione precisa di valute virtuali, attualmente mai confluiti in una soluzione in grado di spiegare il fenomeno totalmente, complice anche l'inclinazione fortemente sovranazionale e la rapida variabilità del mercato in cui è inserita.

Il legislatore (sia italiano che europeo) si è limitato ad intercettare il fenomeno, inquadrando, di volta in volta, in base al settore da regolare, gli aspetti maggiormente rilevanti. **In proposito, merita il richiamo alla definizione generica ed onnicomprensiva di cripto-valuta fornita dal legislatore europeo – e poi assunta dal legislatore italiano - in materia di antiriciclaggio, finalizzata a rendere la relativa disciplina più pervasiva ed efficace, attuata al fine di combattere principalmente l'anonimato delle transazioni.**

[126] giurisprudenza Penale Web, 2018, 7-8 – ISSN 2499-846X.

[127] Banca d'Italia, Avvertenza sull'utilizzo delle cosiddette "valute virtuali", 30 gennaio (2015).

Nel nostro paese le criptovalute sono regolamentate unicamente dalla normativa sul contrasto al riciclaggio di denaro.

Si tratta del D. Lgs.90/2017, introdotto in attuazione della IV Direttiva Antiriciclaggio dell'Unione Europea (Direttiva UE 2015/859), prima esaminata, che fa in realtà riferimento ai concetti di "valuta virtuale" e di "prestatore di servizi relativi all'utilizzo di valuta virtuale" ed opera alcune modifiche alle normative pregresse.

Attualmente tali definizioni, riferite unicamente agli obblighi antiriciclaggio, non sono riprese da ulteriori testi normativi, con la conseguenza di incidere unicamente su tali vincoli. **Il D. Lgs.90/2017, intervenendo sul Decreto Legislativo 231/2007 (strumento normativo adottato in attuazione della precedente direttiva 2005/60/CE sempre in tema di antiriciclaggio), inserisce nell'art. 1 del D. Lgs.231/2007** le seguenti definizioni:

a) **valuta virtuale**, ossia "***la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente***".

b) **prestatori di servizi relativi all'utilizzo di valuta virtuale**, come "***ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale***".

Ulteriori interventi sul D. Lgs.231/07 inseriscono i prestatori di servizi relativi all'utilizzo di valuta virtuale nella categoria degli operatori non finanziari, solo limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso; **il D. Lgs.90/2017 attua, inoltre, anche una modifica del D. Lgs.13 agosto 2010, n. 141**.

Al comma 8-bis dell'articolo 17-bis (Attività di cambiavalute), si dispone che le previsioni ed i requisiti per

l'esercizio dell'attività di cambiavalute si applicano anche "ai prestatori di servizi relativi all'utilizzo di valuta virtuale, come definiti nell'articolo 1, comma 2, lettera ff), del decreto legislativo 21 novembre 2007, n. 231" ***i quali sono altresì tenuti all'iscrizione in una sezione speciale del registro tenuto dall'Organismo degli Agenti e dei Mediatori che raccoglie tutti i soggetti autorizzati ad esercitare l'attività di cambiavalute*****".** Per il popolamento di tale sezione speciale del registro bisognerà attendere però apposito decreto del Ministro dell'economia e delle Finanze (come dispone l'art. 17 bis co. 8 ter del D. Lgs.141/10).

La normativa precisa inoltre che la comunicazione ai fini dell'inserimento nel registro, una volta operativa, rappresenterà la condizione essenziale per l'esercizio legale dell'attività da parte dei prestatori di servizi relativi all'utilizzo di valuta virtuale, stabilendo altresì forme di cooperazione fra il MEF e le forze di polizia per interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione. Il D. Lgs.90/2017 interviene infine sul D.L. 167/90, imponendo agli intermediari finanziari e agli operatori non finanziari di trasmettere all'Autorità i dati anche con riguardo alle operazioni transfrontaliere oltre i 15.000 € avvenute in valuta virtuale.

Ebbene, se appare giusto da un punto di vista regolatorio che chi professionalmente si occupa convertire valuta virtuale in valuta corrente (o viceversa) venga a tutti gli effetti considerato un cambiavalute e debba iscriversi in un relativo registro, sembra difficile da capire perché tale obbligo debba essere esteso a chi professionalmente svolga una diversa attività, appunto commerciale, e si limiti unicamente ad accettare dei pagamenti in queste forme.

Tale particolare previsione potrebbe avere come effetto quello di intralciare la diffusione dell'utilizzo di tali strumenti nel nostro Paese, mentre nel resto dell'Europa e del mondo gli interventi regolatori hanno altre finalità, tese a regolare il fenomeno della raccolta di capitali di rischio per una valida

tutela degli investitori. Come effetto riflesso di una tale disciplina, ci potrebbe essere quello di scoraggiare le aziende che vogliono incrementare soluzioni e prodotti relativi a questa tecnologia dall'operare in Italia, preferendo collocarsi in Paesi in cui la legislazione sia più favorevole ed incentivante.

Tralasciando per un istante la specifica funzionalità settoriale della norma, per sua natura tesa a prevenire l'uso della criptovaluta come canale di riciclaggio, nonché il fatto che la misura resta allo stato ancora inattuabile per carenza di completamento del relativo percorso normativo e le eventuali critiche di cui può essere oggetto, è palese la portata legittimante insita in quelle previsioni, diretta conseguenza delle disposizioni unioniste.

Il legislatore prende così atto dell'esistenza del fenomeno criptovalutario così come di una nascente categoria di operatori impegnati professionalmente a consentirne lo sviluppo, fornendo servizi funzionali all'uso, allo scambio, all'utilizzo della criptovaluta e alla sua conversione in valuta avente corso legale. È interessante analizzare, allora, quella definizione in tutte le sue componenti. Secondo il legislatore la criptovaluta è:

a) una "digitalizzazione di valore" in primis;

b) non emessa da una banca centrale o da altra pubblica autorità;

c) non necessariamente collegata ad una valuta con corso legale;

d) utilizzata come "mezzo di scambio" per acquistare beni o servizi;

e) "trasferita, archiviata e negoziata" elettronicamente.

Ovvia la portata dei requisiti b) e c), i connotati di maggiore rilievo risiedono certamente nelle lettere a) e d). Alla criptovaluta viene riconosciuta, ad un tempo, natura di "valore" e di "mezzo di scambio", dunque la natura di mezzo di pagamento.

La definizione non si sospinge sino al punto di creare una perfetta equiparazione istituzionale fra valuta virtuale e

valuta tradizionale, con la quale la prima addirittura potrebbe non essere necessariamente collegata (lett. c), ma proprio la negazione di un cambio assicurato, nell'esatto momento in cui toglie pari dignità alla criptovaluta, non si traduce affatto nel disconoscimento della sua funzione solutoria, precisamente affermata invece dal requisito sub d)[128].

Nella disposizione manca il presupposto che rende utilizzabile la criptovaluta come mezzo di scambio, ovvero quel rapporto di fiducia fra chi la trasferisca e chi l'accetti, indispensabile ad attribuirle, inter partes, un'efficacia solutoria. Tuttavia, si tratta di un requisito implicito, come rammentato dalle stesse Autorità monetarie, che da solo basta a rendere legittimo l'uso volontario di tale mezzo alternativo di pagamento[129]. In realtà si potrebbe saggiamente affermare, con prudente equidistanza istituzionale, che la norma confermi la natura non illegale ma neppure legale bensì, propriamente, alegale della criptovaluta[130].

Si realizza, per dirla secondo alcuni autori, una specie di licenza ordinamentale: **non è una valuta ma è un mezzo di pagamento per coloro che, a loro pieno rischio, decidano di servirsene; lo Stato non la vieta né la protegge, semplicemente la tollera relegandola in definitiva in quel "limbo etico-volontaristico", schematizzato dall'art. 2034 c.c., che va sotto il nome di obbligazione naturale.**

Da ciò ne consegue che il patto solutorio, legato al negozio di scambio, con cui i contraenti liberamente convengono di ritenere soddisfatto il debito pecuniario attraverso il trasferimento di un mezzo alternativo, non può ritenersi illecito né potrà essere

[128] Girino, E. Criptovalute: un problema di legalità funzionale, cit., p. 750

[129] "Modern economies are typically based on "fiat" money, which is similar to commoditybacked money inits appearance, but radically different in concept, as it can no longer be redeemed for a commodity. Fiat money is any legal tender designated and issued by a central authority. People are willing to accept it in exchange for goods and services simply because they trust this central authority. Trust is therefore a crucial element of any fiat money system" (BCE, Virtual currencies schemes. cit., 9 ss).

[130] Girino, E. Criptovalute: un problema di legalità funzionale, cit., p. 751.

invalidato (il venditore, accettata la criptovaluta, non potrà esigere una reiterazione del pagamento restituendola al solvens in cambio di moneta avente corso legale) né potrà estendere il suo raggio di azione al di fuori di quella specifica pattuizione (l'accipiens non avrà titolo alcuno per pretendere da chiunque, senza il consenso di questi, la conversione della criptovaluta in denaro tradizionale)[131].

La criptovaluta sembra essere stata "sdoganata" anche sotto il profilo fiscale.

La Corte di Giustizia europea, con una pronuncia del 201573, ha riconosciuto che un'operazione di cambio di valuta tradizionale contro criptovalute e viceversa, compiute mediante pagamento della differenza tra il prezzo di acquisto delle valute e quello di vendita praticato dall'operatore ai propri clienti, costituisce, ai fini Iva, una prestazione di servizio a titolo oneroso.

A sua volta, la stessa **Agenzia delle Entrate, con una risoluzione del 2016, riprendendo l'insegnamento della Corte unionista ed equiparando la moneta virtuale a quella tradizionale, giunge alla conclusione per cui ai fini Iva, la remunerazione che il cambiavalute ritrae dalla differenza fra l'importo corrisposto dal cliente per la compravendita della criptovaluta e la migliore quotazione reperita dalla società sul mercato, ricada nell'art. 10 comma 1° n. 3) del d.p.r. 633/1972, il quale manda esente dall'applicazione dell'imposta in parola "*le operazioni relative a valute estere aventi corso legale e a crediti in valute estere, eccettuati i biglietti e le monete da collezione e comprese le operazioni di***

[131] 3 Sentenza Hedqvist, causa C-264/14, del 22 ottobre 2015, secondo la quale "l'art. 2, par. 1, lett. c), direttiva 2006/112/Ce del consiglio, 28 novembre 2006, relativa al sistema comune d'imposta sul valore aggiunto, va interpretato nel senso che costituiscono prestazioni di servizi effettuate a titolo oneroso, ai sensi di tale disposizione, operazioni, come quelle oggetto del procedimento principale, che consistono nel cambio di valuta tradizionale contro unità della valuta virtuale «bitcoin» e viceversa, effettuate a fronte del pagamento di una somma corrispondente al margine costituito dalla differenza tra, da una parte, il prezzo al quale l'operatore interessato acquista le valute e, dall'altra, il prezzo al quale le vende ai suoi clienti."

***copertura dei rischi di cambio*": l'equiparazione della valuta virtuale a quella tradizionale risulta perciò confermata[132].**

In realtà la legittimazione della criptovaluta e la sua equiparazione tributaria a quella tradizionale trova naturalmente conforto nell'entrata in vigore, nel frattempo, della nuova disciplina antiriciclaggio dianzi richiamata.

Comunque sia, questo percorso normativo, che si snoda lungo due percorsi specifici e settoriali quali l'antiriciclaggio e il prelievo fiscale, contribuisce comunque a fondare la legittimità della criptovaluta e del suo impiego, quantomeno a fini solutori. Questo atteggiamento di "resa", di cui si parlava inizialmente, è l'esito di un processo valutativo di natura prettamente politico-finanziaria, in cui troviamo due primarie componenti: l'assenza di un preesistente divieto di emissione alternativa e il timore di introdurre una proibizione che rischierebbe di non essere seguito per la sostanziale impossibilità di sradicare il fenomeno, a causa della resistenza e della sfuggevolezza del sistema informatico che lo genera e lo moltiplica ogni giorno.

Affascinante sul piano sociologico, angosciante su quello politico, terrificante su quello della stabilità finanziaria, tutto ciò è semplicemente irrilevante sul piano giuridico: allo stato attuale del diritto e almeno nella più parte degli ordinamenti, l'emissione e lo scambio di criptovaluta non sono atti, in sé, qualificabili come illeciti[133].

20.3 Nuove prospettive normative.

Nel marzo 2022 il Parlamento ha approvato nuove norme per supportare la sperimentazione della tecnologia del registro di contabilità distribuita come le blockchain per il commercio di criptovalute. Tali tecnologie consentono la registrazione delle interazioni e il trasferimento di criptovalute. L'obiettivo di questa legislazione è incoraggiare lo sviluppo di soluzioni per il trading di

[132] Ris. 2 settembre 2016 n. 72.

[133] Girino, E. Criptovalute: un problema di legalità funzionale, cit., p. 753.

criptovalute, preservando un elevato livello di stabilità finanziaria, trasparenza e integrità del mercato.

È in **Senato il Disegno di Legge numero 2572** contenente la normativa positiva italiana sulle valute virtuali.

L'obiettivo del Legislatore è quello di superare la situazione di incertezza in cui si trova la fattispecie, soprattutto in relazione al trattamento fiscale, proprio in conseguenza della mancanza di norme specifiche.

Oggi il trattamento fiscale delle criptovalute assume contorni non sempre chiaramente definiti e non privi di incertezza; chi scrive ha analizzato la questione con l'articolo **Criptovalute: tassazione e obblighi dichiarativi, come orientarsi**.

Semplificando per brevità, **l'inquadramento fiscale attuale,** costruito su interpretazioni di prassi in buona parte ben accolte dalla giurisprudenza, **fondamentalmente assimila le valute virtuali alle valute estere,** con tutte le conseguenze fiscali del fatto.

Il nuovo impianto normativo, che cerca di superare i limiti più marcati dell'inquadramento attuale senza stravolgerlo, è figlio della necessità di definire con chiarezza il trattamento fiscale della fattispecie, in attesa che l'Unione Europea completi il percorso normativo del Regolamento MiCA (acronimo di *Markets in Crypto Asset*), che tratta più generalmente del più complesso mondo delle diverse cripto-attività, con il quale la normativa nazionale si dovrà poi necessariamente relazionale.

Il Disegno di Legge numero 2572 al comma 1 definisce la valuta virtuale e al comma 2 le inquadra fiscalmente.

Una valuta virtuale viene definita "*una forma di unità matematica*"; l'unità matematica è definita **"*l'unità minima matematica crittografica, statica o dinamica, suscettibile di rappresentare diritti, con circolazione autonoma*".**

Tale definizione integra la definizione di valuta virtuale già presente nell'ordinamento italiano, quella dell'articolo 1 comma 2 lettera qq del Decreto Legislativo 231/2007, ed ha

l'obiettivo di superare le ambiguità derivanti dal fatto che della medesima attività si possono dare definizioni diverse.

Dal punto di vista fiscale la novità di maggiore rilievo è costituita dalla definizione del momento impositivo, che non sarà il prelievo, come avviene con le valute estere, il quale diviene una situazione fiscalmente irrilevante, **quanto piuttosto l'utilizzo della criptovaluta come mezzo di pagamento o la sua conversione in una valuta tradizionale** (sia in euro che valuta estera).

Di conseguenza non assume rilevanza fiscale la conversione di una valuta virtuale in altra valuta virtuale.

Fondamentalmente il momento impositivo è costituito dalla "*manifestazione di ricchezza*", per usare le parole del Legislatore, che è il momento in cui la criptovaluta è utilizzata per pagare un bene un servizio o viene convertita in valute tradizionali.

Il nuovo inquadramento fiscale eredita dalla precedente assimilazione alle valute estere la previsione che **l'imponibilità fiscale è subordinata al possesso**, da parte del contribuente, **di valute virtuali per un controvalore superiore a 51.645,69 euro per almeno sette giorni lavorativi continui nello stesso anno fiscale**.

Di non secondaria importanza il fatto che il Disegno di Legge definisca anche gli **obblighi relativi al monitoraggio fiscale e all'IVAFE,** confermando le interpretazioni finora fornite dalla prassi sul tema:

- ai fini del monitoraggio fiscale sarà **obbligatoria la compilazione del quadro RW** in sede di dichiarazione annuale dei redditi, ma **solo per le consistenze di valute virtuali superiori a 15.000 euro** nel periodo di imposta;
- **ai fini dell'IVAFE le criptovalute non sconteranno l'imposta** non essendo qualificati come prodotti finanziari.

In considerazione delle notevoli oscillazioni di valore che possono interessare le valute virtuali nello stesso periodo di imposta, è previsto che **l'obbligo di monitoraggio va**

adempiuto considerando il costo o il valore di acquisto della criptovaluta.

Viene infine prevista una norma transitoria di rideterminazione dei valori di acquisto al 1° gennaio 2022, con annessa imposta sostitutiva per scaglioni, che richiede apposita perizia giurata.

Effetto premiale di tale rideterminazione, e quindi limitata ai soli contribuenti che l'effettuano, **sarà l'esenzione dalle sanzioni per l'omissione degli obblighi relativi al monitoraggio fiscale** avvenuta negli anni fiscali precedenti.

21. Rischi legali per il consumatore.

Sin dal gennaio 2015, la Banca d'Italia e la UIF hanno messo in guardia i consumatori e gli intermediari su tutti i possibili rischi collegati alle valute virtuali. La mancanza di un quadro giuridico pertinente ha determinato l'impossibilità di attuare un'efficace tutela legale e/o contrattuale degli interessi degli utenti, che possono così trovarsi a subire ingenti perdite economiche, ad esempio nel caso di condotte fraudolente, fallimento o cessazione di attività delle piattaforme on-line di scambio presso cui vengono custoditi i portafogli digitali personali (i cosiddetti e-wallets).

In un contesto di assenza di obblighi informativi e di regole di trasparenza, le piattaforme di scambio sono altresì esposte a elevati rischi operativi e di sicurezza: tali piattaforme, infatti, a differenza degli intermediari autorizzati, non sono tenute a fornire alcuna garanzia di qualità del servizio, né devono rispettare requisiti patrimoniali o procedure di controllo interno e gestione dei rischi, con conseguente elevata probabilità di frodi ed esposizione al cybercrime[134].

Tra i vari aspetti sottolineati, vi sono i rischi di perdite permanenti delle somme utilizzate per l'acquisto di valute virtuali a causa di malfunzionamenti, attacchi informatici, smarrimento della password del portafoglio elettronico, da parte

134

http://www.consob.it/documents/10194/0/Articolo+su+rischi+criptovalute/10402b10-bc3b4500-a0d4-81cec9a2db23

degli utenti. Di recente si sono verificati episodi, anche gravi, di attacchi informatici alle piattaforme di scambio che hanno comportato la perdita parziale o totale dei soldi investiti in valute virtuali da parte di numerosi consumatori.

Si sono registrate inoltre situazioni di estrema volatilità dei prezzi di molte valute virtuali, problematica di cui abbiamo parlato e che ampiamente analizzeremo in seguito. Sussistono, inoltre, rischi di controparte, di mercato, di liquidità e di esecuzione.

Priva di ogni garanzia è d'altronde la futura possibilità di un'immediata conversione dei bitcoin e delle altre criptovalute in moneta ufficiale a prezzi di mercato. **Non è un caso, quindi, che la finanza e il settore bancario guardino con diffidenza e riluttanza alle criptovalute, temendo che siffatte evoluzioni, nel determinare, in particolare, la possibilità di trasmettere valore senza l'intervento degli intermediari, possano finire per spiazzare il business normalmente svolto dall'industria.**

L'Autorità Bancaria Europea (EBA), l'Autorità Europea degli Strumenti Finanziari e dei Mercati (ESMA) e l'Autorità Europea delle Assicurazioni e delle Pensioni (EIOPA) sono intervenute insieme, con un'avvertenza per i consumatori sui rischi delle valute virtuali.

Le tre autorità europee in particolare sottolineano che le valute virtuali sono prodotti estremamente rischiosi e speculativi; che la formazione del loro prezzo è spesso non trasparente; che vi sono chiari segnali di una bolla speculativa nei prezzi di queste valute o di strumenti finanziari a esse collegate; che non vi sono né forme di protezione né specifiche garanzie legali.

Inoltre, le tre autorità europee segnalano che le piattaforme di scambio di valute virtuali non sono regolate; che possono avere problemi di natura operativa che in talune circostanze impediscono ai consumatori di comprare o vendere le valute virtuali, nonché di scambiarle con le valute tradizionali. Si

raccomanda ai consumatori, infine, di non convertire in valuta virtuale più denaro di quanto ci si possa permettere di perdere[135].

[135] Le tre AEV avvertono i consumatori del fatto che le valute virtuali possono essere estremamente rischiose e sono di solito altamente speculative. Chi acquista valute virtuali deve essere consapevole che vi è un alto rischio di perdere una parte consistente, o persino la totalità, del denaro investito. L'acquisto di valute virtuali o di prodotti finanziari che forniscono un'esposizione diretta a tali valute comporta una serie di rischi, tra i quali: - rischio di volatilità estrema e di bolla speculativa – la maggior parte delle valute virtuali è soggetta a un'estrema volatilità dei prezzi e ha evidenziato chiari segnali di una bolla dei prezzi. Chi decide di acquistare valute virtuali o prodotti finanziari aventi queste valute come sottostante dev'essere consapevole che può perdere una parte significativa, o persino la totalità, del denaro investito. - Assenza di protezione – nonostante i requisiti dell'UE in materia di lotta contro il riciclaggio, che entreranno in vigore nel 2018 e che saranno applicabili ai fornitori di portafogli e alle piattaforme di negoziazione delle valute virtuali, queste ultime rimangono non regolamentate ai sensi del diritto dell'Unione. Analogamente, neppure le piattaforme su cui le valute virtuali sono negoziate e i portafogli digitali usati per detenere, conservare e trasferire le valute virtuali sono regolamentati ai sensi del diritto dell'UE. Ciò significa che, chi acquista o vende valute virtuali, non beneficia delle garanzie e delle salvaguardie associate ai servizi finanziari regolamentati. Per esempio, se una piattaforma di negoziazione di valute virtuali o un fornitore di portafogli digitali fallisce, cessa l'attività, subisce un attacco informatico, è accusato di appropriazione indebita di fondi o è soggetto a confisca dei beni in seguito ad azioni di contrasto, la legislazione dell'UE non offre alcuna specifica tutela giuridica che protegga il consumatore dalle perdite o alcuna garanzia che possa riavere accesso alle valute virtuali che possiede. Questi rischi si sono già manifestati in numerose occasioni in diverse parti del mondo. - Assenza di opzioni di uscita – chi acquista valute virtuali rischia di non riuscire a venderle o a scambiarle con valute tradizionali, come l'euro, per un lungo periodo di tempo, e potrebbe quindi subire perdite nel processo. - Mancanza di trasparenza sui prezzi – la formazione dei prezzi delle valute virtuali spesso manca di trasparenza. Sussiste pertanto un rischio considerevole che chi acquista o vende valute virtuali non riceva un prezzo equo e accurato. - Interruzioni delle operazioni – alcune piattaforme di negoziazione di valute virtuali hanno sofferto di gravi problemi operativi, come la sospensione delle contrattazioni. Durante queste interruzioni i consumatori non hanno potuto acquistare e vendere valute virtuali nel momento in cui lo desideravano e hanno subito perdite dovute alle fluttuazioni dei prezzi delle valute virtuali detenute nel periodo dell'interruzione. - Informazioni fuorvianti – le informazioni divulgate ai consumatori che desiderano acquistare valute virtuali, laddove vengano fornite, sono il più delle volte incomplete, di difficile comprensione, non comunicano correttamente i rischi delle valute virtuali e potrebbero quindi essere fuorvianti. - Inidoneità delle valute virtuali per la maggior parte degli scopi, tra cui la pianificazione d'investimenti o previdenziale – l'elevata volatilità delle valute virtuali, l'incertezza sul loro futuro e l'inaffidabilità delle piattaforme di negoziazione e dei fornitori di portafogli rende le valute virtuali inadatte per la maggior parte dei consumatori, inclusi quelli con un orizzonte d'investimento di breve periodo, e specialmente per coloro che perseguono obiettivi di lungo periodo come risparmiare per la pensione. Rif.https://www.esma.europa.eu/sites/default/files/library/joint_esas_warning_on_virtual _curren cies_it.pdf

Chi decide di acquistare valute virtuali o prodotti finanziari che forniscono un'esposizione diretta a tali valute dovrebbe comprendere perfettamente le loro caratteristiche e i rischi a cui si espone. Come regola aurea non si dovrebbe investire, in nessun caso, denaro che non ci si può permettere di perdere.

Il consumatore dovrebbe assicurarsi di adottare precauzioni adeguate e aggiornate per la sicurezza dei dati sui dispositivi e sugli hardware usati per accedere alle proprie valute virtuali o per acquistare, conservare o trasferire queste valute. Inoltre, bisognerebbe essere consapevoli che l'acquisto di valute virtuali da un'impresa regolamentata di servizi finanziari non mitiga i rischi sopra descritti[136]: tuttavia, i rischi, come spesso accade, sono affiancati anche dai benefici.

Considerate come fase iniziale di un più ampio processo di sperimentazione tecnologica e finanziaria, le criptovalute e, più in generale, la **distributed ledger technology** potrebbero utilmente porre le basi per dar vita a soluzioni capaci di rendere più efficiente o, secondo i più ottimisti, di trasformare radicalmente l'attuale sistema economico. Lo sviluppo di risposte regolatorie efficaci in merito alle criptovalute è ancora in una fase iniziale: si tratta di un ambito difficile da disciplinare, rientrando nella competenza di differenti soggetti pubblici a livello nazionale e operando, al contempo, su scala globale. Molti sistemi di scambio sono del tutto non trasparenti e operano al di fuori del sistema finanziario convenzionale, ciò che rende difficile monitorarne l'operatività.

I regolatori hanno iniziato ad affrontare tali sfide e le risposte fornite al fenomeno sono state molteplici, con una varietà di approcci tra i differenti Paesi. **Taluni hanno valutato la possibilità di includere le valute virtuali nel novero di fattispecie già appropriatamente regolate, altri hanno diramato apposite avvertenze ai consumatori o hanno assoggettato a un regime autorizzatorio lo svolgimento di talune delle attività proprie del sistema, altri ancora hanno**

[136]Rif.https://www.esma.europa.eu/sites/default/files/library/joint_esas_warning_on_virtual_curre ncies_it.pdf

proibito alle istituzioni finanziarie di negoziare valute virtuali o ne hanno addirittura vietato l'uso, perseguendo penalmente i trasgressori[137].

Si tratta di risposte di policy ancora embrionali rispetto alle sfide poste dalle valute virtuali ed è altamente probabile che, nel prossimo futuro, interverranno ulteriori sviluppi, che quantomeno faranno chiarezza in merito. Sembra, al riguardo, auspicabile che le autorità calibrino i contenuti delle future regolazioni in modo da affrontare adeguatamente i rischi, senza, tuttavia, soffocare oltremodo l'innovazione.

Gli organismi internazionali stanno giocando un ruolo importante nell'identificazione e nella valutazione dei rischi posti dalle valute virtuali e potrebbero senz'altro contribuire a facilitare il processo di sviluppo e di affinamento delle politiche regolatorie a livello nazionale.

A mano a mano che si acquisirà una certa esperienza in ordine al loro funzionamento, la diffusione di standards internazionali e best practices potrà fornire utili indicazioni sulle misure regolatorie più appropriate da implementare nei diversi campi, promuovendo l'armonizzazione e prevenendo il rischio di strategie di arbitraggio.

Tali standards potrebbero comprendere accordi di cooperazione internazionale in settori quali lo scambio di informazioni e lo svolgimento di indagini nel perseguimento dei reati transfrontalieri, onde combattere efficacemente le problematiche legate al fenomeno criptovaluta e far emergere, invece, gli aspetti positivi che il fenomeno porta con sé[138].

22. Usi illeciti: riciclaggio, finanziamento illecito, terrorismo.

[137] Rif. Consob, rischi per i consumatori: valute virtuali e criptovalute. http://www.consob.it/documents/10194/0/Articolo+su+rischi+criptovalute/10402b10-bc3b-4500- a0d4-81cec9a2db23

[138] Rif. Consob, rischi per i consumatori: valute virtuali e criptovalute. http://www.consob.it/documents/10194/0/Articolo+su+rischi+criptovalute/10402b10-bc3b-4500- a0d4-81cec9a2db23

Per il momento abbiamo tenuto conto dell'utilizzo di questa moneta soltanto per scopi speculativi oppure per la tecnologia innovativa che porta dietro con sé; ma è bene ricordare che se il contante fisico è il modo migliore per ovviare alla legge, di certo il Bitcoin non può essere da meno. Seppur digitale, il ruolo di questa moneta può essere utilizzato per scopi illeciti. Numerosi sono i casi in cui vi sono registrate operazioni mediante criptovalute per il sostenimento di fini illeciti, come ad esempio il riciclaggio di denaro. Per rendere evidente il discorso, in materia si è esposta anche Christine Lagarde, presidente della Banca Centrale Europea (BCE) che, ha proposto di regolamentare il Bitcoin durante il forum Reuters Next.

Del resto, Bitcoin, ma anche le altre altcoin presenti sul mercato monetario digitale, sono da tempo nel mirino delle autorità a causa delle attività di riciclaggio. Inoltre, Lagarde per mettere in evidenza questo aspetto negativo, ha messo in risalto un fatto pratico che si sta vivendo in questo periodo storico; si teme infatti che le criptovalute vengano utilizzate per eludere le sanzioni russe: ‘***'Ci sono segnali che alcuni russi stanno tentando di aggirare le sanzioni di guerra in Ucraina convertendo i rubli in criptovalute e stablecoin***''. Tali dichiarazioni sono un chiaro riferimento alle sanzioni decise da molti paesi nel mondo che hanno un chiaro obiettivo di costringere la Russia ad abbandonare l'idea della guerra. Inoltre, tendono a rimarcare che le attività illecite costituiscono una quota significativa dell'economia in Bitcoin ma ad oggi, non è possibile dirlo con certezza; si può soltanto presupporre che tali attività sfruttino il contante digitale e/o gli asset crittografici, il tutto per mancanza di prove.

Una delle principali caratteristiche di questi sistemi di pagamento è quella che ne prevede una "scarsità artificiale" (ricordiamo come l'emissione di Bitcoin si arresterà arrivati alla somma di 21 milioni totali), la quale teoricamente permetterebbe anche di trovare una soluzione al problema della "trappola della liquidità" in cui incorrono normalmente le valute emesse dalle banche centrali. Come noto, anche a seguito delle politiche di

quantitative easing poste in essere dalla Banca Centrale Europea (sotto l'egida di Mario Draghi prima e, nonostante qualche tentennamento, anche sotto la guida di Christine Lagarde) e da altri istituti finanziari, la quantità di moneta emessa è certamente aumentata; tuttavia a fronte dell'immissione di queste grandi quantità di moneta nel sistema, spesso le economie non registrano un aumento proporzionale della spesa sul mercato (viene posta in essere un'opera di accumulo che non serve a far ripartire il ciclo dei consumi), determinando un'ulteriore contrazione dell'economia reale. Tali fenomeni sono influenzati sicuramente da più fattori, come l'assenza di politiche che determinino un surplus di moneta con riferimento ai soggetti che abbiano un'alta propensione al consumo ovvero la presenza di politiche restrittive sulla concessione del credito da parte degli istituti bancari o, ancora, le semplici aspettative negative degli operatori economici che accumulano liquidità anziché spendere. Tali fenomeni non vedrebbero la luce nel sistema di criptovaluta singolarmente inteso (vds. Bitcoin), in quanto la quantità di criptovaluta potenzialmente a disposizione viene limitata a monte ad un quantitativo specifico, oltre a non essere presente alcuna autorità centrale che ne possa determinare la nuova emissione. Come dato positivo per gli utilizzatori si ha anche l'uso delle Criptovalute come modalità di finanziamento in crowdfunding di nuove iniziative imprenditoriali senza passare necessariamente da una quotazione in Borsa. In questo caso il finanziamento si ottiene, a livello tecnico, mediante una ICO14, in occasione della quale le imprese che la lanciano entrano in contatto diretto con i soggetti che hanno intenzione di sostenere la loro iniziativa. In tali casi siamo in presenza di una forma di crowdfunding decentralizzato, che non necessita di una piattaforma terza (ad esempio come "Kickstarter" o altre) che funga da abilitatore della transazione. Questo in quanto il crowdfunding e i Bitcoin (ma in generale tutte le criptovalute) condividono la medesima filosofia di fondo, che consiste nella disintermediazione dei flussi finanziari rendendo i meccanismi di controllo e finanziamento più trasparenti e democratici. già nel corso del 2013 l'Autorità bancaria europea aveva diramato

un'allerta pubblica, per mezzo della quale, in sostanza, riferiva ai consumatori di operare con prudenza nel settore delle criptovalute in quanto le stesse facevano parte di un campo di attività non regolato, determinandosi come conseguenza una mancata "mitigazione" dei rischi alle stesse connessi. L'EBA ha ritenuto necessario precisare come in Europa le criptovalute non possono avere corso legale in quanto, prima di qualsiasi problema tecnico, l'unico soggetto autorizzato all'emissione di moneta è la Banca Centrale Europea, secondo quanto stabilito dal TFUE. I rischi che vengono indicati per l'integrità del sistema finanziario nel suo complesso comprendono al loro interno sia quelli che possono portare all'uso del sistema finanziario con finalità di riciclaggio e finanziamento del terrorismo, che quelli relativi ad eventuali crimini finanziari che possono perpetrarsi per mezzo di questo strumento. In ogni caso va tenuto presente come questi rischi siano principalmente collegati all'anonimato riconnesso all'uso delle criptovalute e alla loro natura di strumenti di pagamento che non tengono conto di confini nazionali. Intanto bisogna considerare come eventuali criminali potrebbero essere in grado di compiere attività di riciclaggio di proventi illeciti a causa del fatto che possono sia depositare che trasferire criptovaluta in maniera completamente anonima; ciò e reso possibile da un lato dallo pseudonimato connesso ai wallet (che non identificano direttamente il possessore dello stesso) e, dall'altro, dal fatto che sono possibili conto del concreto meccanismo di funzionamento della maggior parte delle criptovalute. trasferimenti di criptovaluta senza passare per alcun tipo di intermediario che abbia l'obbligo di segnalare alle autorità eventuali transazioni che siano "a rischio". Il presente fattore di rischio, invero, aumenta ancora di più se si tiene conto del fatto che i depositi in criptovaluta (ipoteticamente proventi di reato) possono essere facilmente e rapidamente trasferiti in tutto il mondo semplicemente mediante l'accesso alla rete internet. Attraverso l'uso delle criptovalute è tecnicamente possibile commerciare prodotti illegali senza essere scoperti, soprattutto per mezzo dell'uso del dark web; a ciò va aggiunto che non è difficile immaginare come possano

esservi soggetti partecipanti, a vario titolo, al mercato delle criptovalute che siano a loro volta controllati da parte sia di organizzazioni criminali che da parte di singoli che vogliono rimanere ignoti. la Direzione Nazionale Antimafia è impegnata in prima linea nel contrasto ai fenomeni di riciclaggio e di finanziamento del terrorismo, funge infatti da soggetto privilegiato nei flussi di lavorazione delle segnalazioni di operazioni sospette che vengono trasmesse dalla UIF da una parte alla Direzione Investigativa Antimafia e dall'altra al Nucleo Speciale di Polizia Valutaria della Guardia di Finanza per i rispettivi campi di interesse. Tralasciando quanto precisato sui rischi per consumatori e investitori, ciò che viene rilevato come "rischio di sistema" deriva essenzialmente dal regime di anoni- 371 Fulvio Fontana Criptovalute e rischi di riciclaggio mato che connota le transazioni della specie, precisando come questo genere di rischi aumentino qualora le transazioni vengano effettuate senza il coinvolgimento di soggetti terzi come exchanger o wallet provider (obbligati a porre in essere gli adempimenti antiriciclaggio secondo la disciplina normativa attualmente in vigore). I punti di arrivo della disciplina in materia sono da ritrovarsi nella c.d. V Direttiva Antiriciclaggio – Direttiva UE nr. 2018/843 del Parlamento Europeo e de Consiglio del 30 maggio 2018, che ha modificato la Direttiva UE nr. 2015/849 – in relazione alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo.

Nella prassi consolidata, che ha portato all'emanazione delle precedenti quattro direttive AML in ambito europeo, la cadenza temporale tra una direttiva e la successiva è stata di solito abbastanza ampia (1991, 2001, 2005 e 2015); peraltro l'emanazione di una direttiva da parte delle competenti autorità europee si vedeva come aggiornamento normativo necessario alla luce di una nuova edizione o revisione delle Raccomandazioni che, in materia, vengono emanate dal GAFI/FATF. Difatti le raccomandazioni del GAFI costituiscono gli standard sovranazionali per il contrasto al fenomeno del riciclaggio, del finanziamento del terrorismo. La citata V

Direttiva, quindi, segue solo di tre anni la precedente, in assenza di una modifica o revisione delle Raccomandazioni del GAFI.

Posto che le necessità emerse furono anche altre, per la tematica in oggetto si pose come necessario stabilire, in maniera omogenea per tutto il territorio dell'Unione, l'assoggettamento agli adempimenti previsti dalla disciplina antiriciclaggio per i soggetti che eroghino servizi di piattaforme di scambio di valute virtuali (exchangers) ed i prestatori di servizi di portafoglio digitale (wallet service providers). All'interno della stessa vengono anche fornite delle definizioni sia del concetto di valuta virtuale, che di exchanger e di wallet service provider31. In tal senso bisogna ammettere che il legislatore italiano aveva precorso i tempi inserendo già nel d.lgs. n. 90 del 2017 – di recepimento della IV Direttiva UE – tra i soggetti obbligati a porre in essere l'adeguata verifica della clientela i prestatori di servizi di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali in valute a corso forzoso (e viceversa); contestualmente venne previsto uno specifico obbligo di iscrizione, per i prestatori di servizi relativi all'utilizzo di valuta virtuale, in una sezione speciale del registro dei cambiavalute tenuto presso l'Organismo degli Agenti e Mediatori (OAM).

Appare evidente che le caratteristiche delle criptovalute in totale anonimato e senza il controllo di un'autorità centralizzata rappresenta una formidabile occasione di riciclaggio e, in genere, di reinvestimento di capitali di provenienza illecita. Anche in Italia, la criminalità organizzata è arrivata a capire le potenzialità delle monete virtuali, soprattutto per pagare le partite di stupefacenti da fornitori sudamericani. Appare emblematico il caso di un broker dei clan della 'ndrangheta che non ha saputo pagare lo stupefacente in Bitcoin perché i narcos brasiliani non sapevano usarli, come accertato nell'ambito dell'operazione "***European 'ndrangheta connection***".

Nel mondo della fintech, ossia della tecnologia applicata alla finanza, un ambito che sta destando ampio interesse ma anche preoccupazione finanche tra i non addetti ai lavori è quello delle

criptovalute, ossia, secondo la definizione fornita da Banca d'Italia di cui abbiamo più volte parlato, "rappresentazioni digitali di valore non emesse da una banca centrale o da un'autorità pubblica.

Esse non sono necessariamente collegate a una valuta avente corso legale, ma sono utilizzate come mezzo di scambio o detenute a scopo di investimento e possono essere trasferite, archiviate e negoziate elettronicamente. Le valute virtuali non sono moneta legale e non devono essere confuse con la moneta elettronica"[139].

Il mercato delle criptovalute vanta una crescita esponenziale, nonostante la mole di critiche che, fin dalle origini, ha accompagnato la diffusione della peer to peer e-money. La crescita del fenomeno, come visto, non riguarda soltanto la più celebre criptomoneta, il Bitcoin, ma vede l'affermazione di molte altre valute virtuali, come abbiamo analizzato. Un recentissimo studio interdisciplinare sull'evoluzione del mercato relativo alla criptomoneta ha evidenziato come quest'ultimo sia molto più maturo e complesso di quello che si pensava.

L'incremento del volume delle transazioni e dei valori "circolanti" ha attirato l'attenzione degli investitori del mercato del capitale di rischio, facendo spuntare nuove figure di operatori professionali, rectius di prestatori di servizi di intermediazione nell'acquisto, vendita e trasferimento di criptovalute. Si tratta di attività dai contorni estremamente non trasparenti, quasi completamente prive di disciplina dal punto di vista giuridico, sebbene vi siano manifeste similitudini tra l'attività svolta da costoro e quella esercitata da operatori ed intermediari autorizzati nel settore bancario e finanziario.

[139] Cfr. Banca d'Italia, Comunicazione del 30 gennaio 2015 – Valute virtuali. Per un approfondimento sugli aspetti tecnico-informatici delle criptovalute. Bocchini, R. Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche, cit., p. 27; Gasparri, G. Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema? in Dir. dell'informazione e dell'informatica, n. 3, p. 415. (2015).

L'assenza di regolazione è il logico corollario delle esigenze di "democratizzazione finanziaria" e "disintermediazione" che hanno ispirato gli ideatori della moneta peer to peer nel dar vita ad un sistema di condivisione non governato da alcuna Autorità centrale[140]. Tuttavia, gli eccessivi spazi di autonomia, come abbiamo visto, possono condurre al rischio di un impiego sistematico delle criptovalute come mezzo elusivo della tracciabilità dei flussi di denaro per il compimento delle più svariate attività illecite.

I dati dell'ultimo rapporto Internet **Organised Crime Threat Assessment** dell'EC3 di Europol evidenziano un rapporto di diretta proporzionalità tra l'aumento di capitalizzazione del mercato delle criptovalute e lo sviluppo del cybercrime, specialmente con riferimento alle condotte di diffusione di ransomwares e al dilagare sulla parte oscura della rete di criminal markets per la compravendita di droga, armi, materiale pedopornografico e ogni genere di traffico illecito[141].

Inoltre, non dobbiamo dimenticare che la diffusione delle criptovalute ha dischiuso nuove frontiere per il riciclaggio digitale c.d. integrale – noto come cyberlaundering – in cui la fase di placement si caratterizza per l'inserimento nel circuito economico di capitali di provenienza illecita già disponibili su conti on-line allo "stato digitale", senza necessità di alcun contatto materiale tra il riciclatore ed il contante.

Così, allo stesso modo, l'acquisto di criptovaluta sulle piattaforme di intermediazione (idest, il cambio di moneta reale per quella virtuale) offre la possibilità di "polverizzare" ingenti quantità di denaro via Internet nel più completo anonimato[142].

---

[140] Passarelli, N. Bitcoin e antiriciclaggio, in Gnosis, (2016), www.sicurezzanazionale.gov.

[141] IOCTA 2017, a cura dell'Internet Cybercrime Centre (EC3) costituito presso Europol. Il documento è disponibile sul portale istituzionale www.europol.europa.eu.

[142] Si tratta di veri e propri "supermercati" virtuali per lo scambio di beni intrinsecamente illeciti. Basti pensare che AlphaBay, un portale nascosto sul deep-browser Tor, contava oltre 200.000 utenti e 40.000 venditori; tra le merci si contavano oltre 250.000 inserzioni di sostanze psicotrope illegali, più di 100.000 aste per l'acquisto di

Vi sono, inoltre, moltissimi operatori che offrono servizi di mixing in grado di dissolvere le tracce di una transazione lungo la blockchain attraverso operazioni intermedie di ramificazione del flusso di criptomoneta. Si potrebbe dire che, metaforicamente, in questi ultimi anni si sia verificata una transizione da un sistema della paper trial alla digital trial, laddove l'unica strada da seguire, complicatissima, tende ad articolarsi lungo i nodi della catena di validazione delle transazioni[143].

Sorge così la necessità per Stati di disciplinare le attività di emissione, cambio e trasferimento di valute virtuali nel quadro di regime autorizzatori ben definiti, con l'obiettivo di contrastare la notevole "spinta criminogena" legata alla diffusione delle criptovalute. La Commissione Europea ha recentemente espresso la propria preoccupazione per la nuova dimensione del fenomeno del cyber laundering.

Nella V Direttiva, attuata per la modifica della IV Direttiva sul riciclaggio relativa "alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo", si legge come operazioni in valute virtuali beneficino di un tal grado di anonimato rispetto ai classici trasferimenti di fondi, che le organizzazioni terroristiche potrebbero facilmente abusarne per nascondere e trasferire denaro, indispensabile per compiere atti terroristici.

A ciò si aggiungono altri rischi potenziali quali l'irreversibilità delle operazioni, la gestione delle operazioni fraudolente, la natura oscura e tecnologicamente complessa di questo settore nonché la mancanza di varie garanzie regolamentari. Quest'ultimo rappresenta il dato più allarmante: oggi i trasferimenti di valute virtuali non sono oggetto di alcun tipo di monitoraggio nell'ambito dell'Unione Europea da parte delle Autorità pubbliche.

documenti falsi o rubati e un pari numero di annunci per l'acquisto di beni contraffatti, armi, o starter-packs per l'accesso abusivo a sistemi informatici.

[143] Simoncini, E. Il cyberlaundering: la "nuova frontiera" del riciclaggio, in Rivista Trimestrale Diritto Penale dell'Economia., 4, p. 901. (2015).

La stessa Commissione, però, riconosce come la distribuzione della moneta digitale offra vantaggi potenziali in termini di efficienza, proprio perché, a differenza delle operazioni in contanti, si fonda su un registro pubblico di annotazione continua dei trasferimenti.

D'altronde, la stessa credibilità delle valute virtuali non potrà che venir meno, se queste sono principalmente utilizzate per scopi criminali. **In questo contesto l'anonimato diventerà più un ostacolo che una risorsa per il successo delle cryptocurrencies e per la diffusione dei loro potenziali vantaggi.** Gli interventi dovrebbero essere sostanzialmente due: da una parte, l'introduzione di misure rafforzate di verifica della clientela da parte degli operatori professionali nel settore delle criptovalute; dall'altra, l'individuazione delle operazioni sospette in valute virtuali. **Con l'emanazione del D. Lgs. 25 maggio 2017 n. 9019 il legislatore italiano ha voluto, per così dire, "giocare d'anticipo" rispetto alla proposta europea.**

La novella ha infatti modificato le definizioni contenute nell'art. 1, comma 2, del D. Lgs. 21 novembre 2007 n. 231 inserendovi una specifica nozione di valuta virtuale e di prestatore di servizi relativi all'utilizzo di valuta virtuale. Tale figura viene inserita nel novero degli altri operatori non finanziari di cui al comma 5 dell'art. 3 D. Lgs. 231/2007 22, inclusi tra i soggetti destinatari degli obblighi della normativa antiriciclaggio, cosa poi attuata successivamente con la V Direttiva.

La V direttiva estende ai prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale (per esempio monete e banconote considerate a corso legale e la moneta elettronica di un paese, accettate quale mezzo di scambio nel paese emittente) e ai prestatori di servizi di portafoglio digitale, che non sono soggetti all'obbligo della UE di individuare le attività sospette, particolari obblighi antiriciclaggio.

L'anonimato delle valute virtuali, come detto, ne consente il potenziale uso improprio per scopi criminali, in maniera molto

ampia e diffusa. Al fine di evitare che i gruppi terroristici possano trasferire denaro verso il sistema finanziario dell'Unione o all'interno delle reti delle valute virtuali dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme, è stato ampliato l'ambito di applicazione della IV direttiva (UE) includendo i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale. In tal modo, le autorità competenti avranno la possibilità di monitorare, attraverso i soggetti obbligati, anche l'uso delle valute virtuali.

Ora, a livello europeo, è stato compiuto un ulteriore progresso: tra i soggetti obbligati vi sono anche le persone che commerciano opere d'arte o che agiscono in qualità di intermediari nel commercio delle stesse, anche quando tale attività è effettuata da gallerie d'arte e case d'aste, nel caso in cui il valore dell'operazione o di una serie di operazioni legate tra loro sia pari o superiore a 10mila euro.

Tali obblighi sono previsti anche per le "Criptovalute". Infine, la V direttiva antiriciclaggio prevede anche l'accesso pubblico alle informazioni sulla titolarità effettiva dei trust e degli istituti giuridici affini sul presupposto che tale accesso possa contribuire a combattere l'uso improprio di società o altri soggetti giuridici per riciclare denaro o finanziare il terrorismo, anche quando si parli in termini di valute virtuali.

Un maggiore controllo pubblico contribuirà a prevenire l'uso improprio di soggetti giuridici ed istituti giuridici, anche a fini di evasione fiscale. Di recente il GAFI (Gruppo per l'Azione Finanziaria Internazionale)[144] ha pubblicato delle Linee guida per contrastare l'utilizzo delle valute in parola per il riciclaggio

[144] GAFI (Gruppo d'Azione Finanziaria internazionale). Si tratta di un organismo intergovernativo, costituito nel 1989 in occasione del G7 di Parigi, che ha come obiettivo quello di elaborare e sviluppare strategie di lotta al riciclaggio dei capitali di origine illecita, di contrastare il finanziamento al terrorismo e la proliferazione di armi di distruzione di massa. Del GAFI fanno parte trentacinque membri in rappresentanza degli Stati o delle Organizzazioni regionali che corrispondono ai principali centri finanziari internazionali. Rif. https://www.fiscalfocus.it/prime/crypto-valute-e-blockchain/il-gafi-e-l-anonimato-delle-valute-virtuali,3,11105

di denaro sporco e il finanziamento al terrorismo. Le criptovalute, infatti, sono utilizzate anche per gli scopi indicati.

La GDF (Global Digital Finance), un'organizzazione che rappresenta i criptooperatori, pur accogliendo con favore il documento del GAFI, che 'impone' la fine dell'anonimato nelle transazioni di valute virtuali, ha ribadito che sarà molto difficile esaudire la richiesta.

Il 14 settembre 2020, il GAFI ha pubblicato il Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing[145] con cui, per certi versi, integra **le Linee Guida del 2019 ribadendo che l'utilizzo di nuove tecnologie per trasferire rapidamente valori in tutto il mondo, oltre ad avere potenziali vantaggi dati dalla rapidità ed economicità dei pagamenti, può essere utile strumento a disposizione della criminalità.** Infatti l'anonimato che caratterizza i virtual assets può consentire il riciclaggio di proventi di reati come il traffico di droga, il contrabbando illegale di armi, la frode, l'evasione fiscale, gli attacchi informatici, l'aggiramento delle sanzioni internazionali, oltre che il finanziamento del terrorismo.

In tale ottica, il Rapporto evidenzia una serie di indicatori di anomalia (red flag indicators) che potrebbero suggerire l'uso illecito di virtual assets, utili a supportare, da un lato, i VASPs, le istituzioni finanziarie, i professionisti e i soggetti obbligati a rilevare e segnalare le transazioni sospette e ad applicare una corretta customer due diligence, dall' altro, le Autorità di Controllo nell'analisi delle segnalazioni di operazioni sospette e nell'attività di vigilanza AML/CFT in generale.

Le informazioni ed i casi che il FATF analizza scaturiscono da uno studio effettuato sulla base di oltre cento casi di utilizzo anomalo di VA, segnalati tra il 2017 e il 2020, e sono un ottimo strumento pratico a disposizione dei soggetti obbligati e delle Autorità di Controllo per l'attività di monitoraggio AML/CFT.

[145] Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing– 14 settembre 2020 - https://www.fatf gafi.org/media/fatf/documents/recommendations/Virtual-A....

Il Rapporto precisa, naturalmente, che la rassegna delle condotte descritte nel resoconto non è di per sé sufficiente per l'inoltro delle SOS ma l'attività di CDD dovrà sempre considerare tali condotte in un contesto più ampio ed in combinazione con i convenzionali indicatori di rischio connessi ai clienti, alle operazioni ed ai prodotti[146]. Comunque sia, si

[146] Nel dettaglio, il GAFI identifica i seguenti sei red flag indicators associati ad alcune macroaree di utilizzo sospetto di virtual assets, indicando per ognuno una dettagliata descrizione di schemi e condotte anomale, accompagnate da alcuni casi pratici maggiormente significativi rilevati nel corso degli ultimi anni: anomalie connesse alle transazioni, quando la loro dimensione e frequenza denoti una serie di criticità, date ad esempio dall'elevato volume di scambi di piccolo importo di VAs o cambio in denaro contante. Oppure trasferimenti di VAs con polverizzazione su differenti VASPs, magari aventi sede in giurisdizioni con assetti AML/CFT a rischio; indicatori riguardanti modelli impropri di transazioni, in particolare relative a nuovi clienti che attivano relazioni non coerenti con il proprio profilo, soprattutto in termini di volumi di virtual assets scambiati o trasferiti, ovvero quando un cliente effettui operazioni utilizzando diversi tipi di VAs e conti senza spiegazioni logiche, se non addirittura conversioni, in perdita, con valuta corrente; indicatori associati a tecnologie che garantiscano l'anonimato, rendendo i VAs appetibili veicoli di ML e TF, in un'ottica di utilizzo strumentalmente patologico. è il caso di clienti che operino mediante sistemi di criptovalute anonime "potenziate"o utilizzino indirizzi IP o email anonime ovvero accedano alle piattaforme dei VASPs con strumenti che non consentono l'identificazione del titolare del dominio. In generale sono anomale tutte quelle operazioni il cui anonimato non permette una adeguata customer due diligence fin dal momento dell'onbording del cliente; indici di anomalia relativi ai mittenti o ai destinatari delle transazioni, in particolare, nel momento dell'attivazione dell'account (indirizzi IP anonimi, molteplici account creati da uno stesso soggetto) oppure quando non sia possibile procedere alla CDD (informazioni insufficienti, incomplete o false sul cliente, origine dei fondi e destinazione).Inoltre potrebbero rilevarsi anomalie connesse a discrepanze tra gli indirizzi IP associati al profilo del cliente e quelli utilizzati per "ordinare" le transazioni. Sempre in relazione al cliente si possono verificare casi in cui venga reclutato come "money mule" per riciclare proventi illeciti; è il caso in cui una persona con un profilo che denota poca familiarità con le tecnologie VA, che attivi uno o più account operando numerose transazioni, magari per importi incompatibili con il suo profilo economico; red flag indicators sulla provenienza dei fondi che, dall'analisi dai casi emersi nel Documento, si sono dimostrati derivare da traffico di droga, frodi, truffe informatiche e attività criminali in genere. Nello specifico il FATF evidenzia come elementi di sospetto l'uso di VAs originati o destinati a servizi di gioco d'azzardo online, l'uso di carte di credito/debito collegate a VA wallet per prelievi di ingenti quantità di valuta corrente (crypto-to-plastic), ovvero elevati depositi di valuta virtuale seguiti da conversioni in valuta fiat che potrebbero indicare un furto di VAs. Altro fattore di rischio potrebbe derivare dalla mancanza di informazioni sull'origine e sui proprietari dei fondi, mediante l'utilizzo di società di comodo, utilizzati per una "offerta" di un nuovo VA (Initial Coin Offering – ICO); indicatori di anomalia collegati al contesto geografico, soprattutto relativo allo "sfruttamento" da parte dei riciclatori di debolezze sistemiche in termini di carenze nell'applicazione degli standards GAFI nello specifico settore dei VAs e dei VASPs. Infatti, è emerso che molti paesi ancora non richiedono il rispetto dei requisiti AML/CFT per i soggetti operanti nell'ecosistema dei virtual assets e, proprio in

tratta di un segnale delle autorità che si pone, apparentemente, non in contrasto con le indicazioni del Parlamento europeo e che vuole superare la frammentarietà delle discipline statali in proposito. L'Italia risulta, come visto ampiamente, uno dei Paesi più all'avanguardia in materia e questo non può che rallegrarci, in attesa di una regolamentazione più esaustiva che possa aiutarci a comprendere e a regolare meglio un fenomeno di sempre più ampia diffusione[147].

22.1 Bitcoin come una bolla speculativa.

Con il termine bolla speculativa si tende a definire quel fenomeno legato alla formazione del prezzo di un bene che, si allontana progressivamente sempre più dai valori compatibili con le fondamentali economiche dello stesso, dove con fondamentali economiche ci si riferisce a quelle particolari ragioni economiche che sottostanno al movimento di un prezzo. Quando l'aumento del prezzo (quindi anche della domanda del bene) capitalizza aspettative impossibili da raggiungere si possono formare bolle speculative, destinate a scoppiare, dato che non tutte le iniziative prese dagli investitori avranno successo. Generalmente, lo scoppio riporta la situazione ai valori originali.

I sostenitori di Bitcoin sono spesso molto critici nei confronti dell'attuale sistema monetario, che si basa su "carta moneta" o fiat money. Con fiat money s'intende un mezzo di scambio (una valuta) che non ha un valore intrinseco e non è legato al prezzo di una merce, come ad esempio un metallo prezioso. La critica a questo sistema riguarda anche le politiche perseguite

queste giurisdizioni "a rischio", si assiste alla domiciliazione di VASPs nonché alla provenienza, destinazione o transito delle operazioni. Il Rapporto infine precisa che i red flag indicators, focalizzati sulle intrinseche caratteristiche e vulnerabilità associate ai VAs, vanno comunque contestualizzati e integrati nell'ambito di una più ampia attività di compliance AML/CFT basata su un risk-based approach dinamico e bidirezionale tra le Autorità di Controllo e i soggetti obbligati. https://www.dirittobancario.it/news/antiriciclaggio/nuovi-indicatori-antiriciclaggio-del-gafi-suivirtual-assets.

[147] 96 https://www.fiscal-focus.it/prime/crypto-valute-e-blockchain/il-gafi-e-l-anonimato-delle-valutevirtuali,3,111056

dalle banche centrali in tutto il mondo, che sono diventate sempre più sconsiderate, soprattutto dopo la crisi finanziaria. L'offerta di denaro è stata massicciamente espansa dal 2009, dal momento che sono state stampate quantità sempre maggiori di denaro. Molti titoli di Stato – per esempio quelli emessi dal governo tedesco – hanno tassi d'interesse negativi, il che significa che gli investitori, invece di guadagnare quando prestano soldi allo Stato, stanno spendendo per il privilegio di comprare obbligazioni. I sostenitori vedono Bitcoin e altre criptovalute come l'attuazione pratica delle idee di Hayek. Ma Bitcoin è davvero una "valuta"? Il denaro e le valute hanno una varietà di funzioni, principalmente sono usate come riserva di valore e come mezzo di pagamento. Bitcoin non è adatto a nessuna delle due funzioni. Date le costanti fluttuazioni del valore di Bitcoin, è completamente inadatto come riserva di valore. E solo in circostanze molto rare è accettato come mezzo di pagamento. Recentemente, Elon Musk ha annunciato che avrebbe accettato pagamenti in Bitcoin per le auto Tesla, ma resta da vedere se questo accadrà veramente. Il termine "criptovaluta" è quindi tecnicamente sbagliato e dovrebbe apparire tra virgolette perché in realtà Bitcoin non è una valuta. Per la maggior parte degli investitori in criptovalute, queste non sono altro che un oggetto di speculazione. Essi comprano una criptovaluta perché sperano che i prezzi salgano e che possano ottenere un buon profitto, cosa che è stata possibile in passato.

Gli investitori che sono entrati al momento giusto in tale mercato hanno fatto importanti guadagni. Tuttavia, la possibilità di realizzare un profitto massiccio non qualifica di per sé una criptovaluta come un investimento. È possibile rastrellare denaro in un casinò, e tuttavia nessuno descriverebbe mai una scommessa in un casinò come un "investimento". I critici di Bitcoin sottolineano il fatto che gli ultimi secoli sono stati pieni di bolle speculative – e alla fine sono tutte scoppiate. Ricordano la bolla del tulipano olandese del 1630, durante la quale i bulbi di certi tipi di tulipani divennero oggetto di speculazione. In alcuni casi, i prezzi dei singoli bulbi rivaleggiavano con quelli delle abitazioni più care di Amsterdam. Come tutte le bolle, la

bolla dei tulipani alla fine scoppiò – e questo è precisamente ciò di cui i critici del Bitcoin sono ora preoccupati.

Il fenomeno delle bolle speculative è più spesso visto come un'anomalia di mercato legata più alla componente psicologica che prevale sull'aspetto razionale. Infatti viene messo in risalto il grado di elevata diffusione del bene oggetto di speculazione, tanto che spesso si arriva a parlare di vere e proprie ''mode'' o addirittura di investimenti 'gregge' quasi a voler calcare la mano sulla componente irrazionale del fenomeno. Si parla in questi casi infatti di stati di euforia collettiva guidata dalla volontà da parte degli investitori di voler fare profitti facili.

Eppure, la definizione stessa di questo fenomeno fa comprendere quanto sia difficile provare in generale che un titolo, un'attività o altro sia una bolla. Non vi sono parametri oggettivi o prestabiliti che regolino le 'ragioni economiche'. Purtroppo prevenire una. Bolla speculativa non è semplice, solo a postumi è possibile rendersene conto. Queste difficoltà diventano ancora più evidenti in un mercato nuovo e privo di storia quale quello delle criptovalute. Basti pensare alla più recente bolla dei Bitcoin a cavallo tra il 2017 ed il 2018.

Si può provare comunque a fare luce su ciò che è avvenuto negli anni. Un'analisi interessante è stata quella del giovane Justas Pikelis, fondatore del token Monetha, eletto dalla rivista Forbes nel 2018 fra gli under 30 più influenti e autorevole voce nel panorama internazionale sulla cripto-economia. Durante un intervento per lo show TEDxSquareMile, Justas Pikelis vuole sottolineare che la sua non è stata solo fortuna. Il giovane economista aveva ben chiare le idee e all'inizio del 2017 sapeva già che si stava trovando dinanzi ad una bolla, la Tech Bubble, e comprese che era il momento giusto per agire e speculare il più possibile su questo asset. La sua analisi prende come esempio l'andamento di Bitcoin.

Pikelis riconosce nell'andamento di Bitcoin le cinque fasi tipiche di una bolla speculativa:

1. **Displacement**, quando il prezzo e l'interesse generale iniziano a salire quasi improvvisamente, come la reazione istantanea tra la Coca cola e le caramelle Mentos insieme;

2. **Boom**, tantissima gente comune vuole partecipare e ciò che crede possa essere l'investimento della vita, facendo in modo che il prezzo continui a salire (fase del gregge). Pikelis paragona questa fase all'entusiasmo americano verso i servizi di car sharing;

3. **Euphoris**, il momento di massimo entusiasmo dei mercati in cui tantissimi individui cercano di partecipare, accecati da questo continuo rialzo del valore, investendo troppo spesso più del dovuto. Si innesca la certezza di stare puntando tutto in un guadagno facile e ci si sente trader al pari dei più grandi investitori di tutte le epoche;

4. **Profit taking**, alcuni investitori iniziano a comprendere il pericolo e iniziano a vendere, realizzando altissimi guadagni che, come ironicamente dice Pikelis, permettono di chiamare questa fase ''ho bisogno di una lamborghini''. Il prezzo inizia inevitabilmente a scendere;

5. **Panic**: L'opinione pubblica cambia radicalmente, il prezzo continua a scendere e chi è arrivato per ultimo, acquistando ad un prezzo elevato, perde tantissimo. Pikelis ribatezza tale periodo come "***Maybe This Isn't The Greatest Thing Since Sliced Bread***", un'espressione per dire che non si è di fronte ad un'innovazione cosi grande e positiva.

Oggi, discutere del Bitcoin come una bolla speculativa appare prematuro. Ci sono pareri discordanti di molti esperti investitori. La motivazione va ricercata, come indicato nei capitoli precedenti, nella volatilità e nelle funzionalità inverse che il Bitcoin presenta nell'incontro domanda e offerta che rende difficile stabilire se quest'ultimo possa colmare questa lacuna di asset volatile, che lo rende ad oggi di carattere speculativo e niente più.