LUISS

Dipartimento di
Impresa e
Management

Cattedra di Finanza Aziendale

Crypto-Awareness: Rischi e psicologia nel cryptoinvestment

Prof. Roberto Mazzei
RELATORE

Jacopo Di Fiore Matr. 247201
CANDIDATO

Anno Accademico 2021/2022

A chi crede in sé stesso,

e nei propri sogni.

INDICE

INTRODUZIONE

Da qualche anno a questa parte, spesso si sente parlare di criptovalute. Le criptovalute rappresentano una delle più grandi innovazioni degli ultimi anni, non solo nel campo della finanza, ma anche in ambito tecnologico, e possono pertanto essere comprese nel settore FinTech. La scoperta di queste valute virtuali viene attribuita ad un giapponese, conosciuto con lo pseudonimo di Satoshi Nakamoto, che nel 2009 ha presentato al mondo intero quella che oggi è considerata la madre di tutte le criptovalute, la più chiacchierata, discussa, e utilizzata: il Bitcoin.

Oltre al Bitcoin, tutte le altre criptovalute esistenti possono essere scambiate attraverso l'utilizzo di chiavi di crittografia, pubbliche e private, ed essere depositate e custodite all'interno di portafogli virtuali. Lo scambio delle criptomonete avviene tramite la Blockchain, uno strumento che, per il suo elevato grado di innovazione e affidabilità, ha assunto negli ultimi anni un'importanza vitale nell'utilizzo delle criptovalute. Il sistema Blockchain garantisce sicurezza, trasparenza, e immutabilità delle transazioni che, una volta registrate nella "catena di blocchi", non possono essere modificate in alcun modo e possono essere tracciate e visionate da chiunque. L'innovazione della Blockchain risiede in particolar modo nel carattere della decentralizzazione: gli scambi di valute virtuali infatti, a differenza di quanto accade con la moneta fiat nei sistemi centralizzati, avvengono senza che vi sia alcun intervento da parte di intermediari finanziari.

La formazione dei blocchi di informazioni che costituiscono la catena, avviene grazie al lavoro incessante dei miners, individui che impiegano tempo, energia e denaro, nel processo di ricerca di un codice che appunto allunghi la blockchain, in cambio di una remunerazione consistente in Bitcoin o altre criptovalute.

Oltre al Bitcoin, vengono infatti analizzate nella tesi le cosiddette "Altcoin", ovvero criptomonete che rappresentano un'alternativa rispetto alla moneta madre. Tra queste, spicca Ethereum, che ad oggi rappresenta la criptovaluta più propensa all'innovazione e all'evoluzione, tanto che presenta un'estensione che prende il nome di Ethereum 2.0, dotata di caratteristiche nuove e avanzate rispetto alla criptomoneta originaria.

Dopo aver evidenziato le opportunità e le potenzialità delle criptovalute, verrà condotta un'analisi degli aspetti critici di questi strumenti. Saranno pertanto esaminate le varie tipologie di rischi che si celano dietro l'utilizzo delle valute virtuali e le problematiche che potrebbero sorgere non solo in ambito finanziario, ma anche informatico, monetario, e in tema di riciclaggio del "denaro sporco". Lo studio dei rischi sarà di fondamentale importanza per trattare il successivo argomento: la costruzione di un portafoglio di criptovalute. Saranno quindi enunciate le regole fondamentali per la creazione di un cryptowallet completo, diversificato, e adatto alle esigenze del singolo possessore.

Nella parte finale della tesi, saranno analizzati gli aspetti psicologici che influenzano le decisioni e i comportamenti degli individui nello svolgimento di un'attività complessa e articolata come quella del trading di criptovalute. L'attenzione sarà quindi focalizzata sugli elementi psicologici e mentali che determinano le scelte dei trader, e sui principi basilari che questi ultimi dovrebbero adottare nel percorso di gestione delle vincite e delle perdite.

Nelle conslusioni, si tenterà di comprendere come le criptovalute potranno sopravvivere, e svilupparsi in modo tale da rappresentare una risorsa importante per le nuove generazioni, al fianco della tradizionale moneta centralizzata.

CAPITOLO 1: BITCOIN, BLOCKCHAIN E CRIPTOVALUTE

1.1 Bitcoin: principali caratteristiche e funzionamento

Il 31 Ottobre del 2009, un utente del sito di crittografia *metzdowd.com*, sotto lo pseudonimo di Satoshi Nakamoto, presenta il dominio (bitcoin.org) di quella che, nell'arco di pochi anni, sarebbe diventata la moneta virtuale più conosciuta e discussa al mondo, il Bitcoin. Nakamoto sosteneva di aver scoperto una nuova valuta virtuale generata da un software open source, decentrata, basata su un sistema network peer-to-peer, e totalmente convertibile. Per comprendere al meglio il funzionamento del bitcoin è necessario analizzare singolarmente queste quattro caratteristiche appena elencate.

Un software si dice *Open Source* quando è disponibile agli utenti in forma di codice sorgente senza costi aggiuntivi. Si tratta quindi di un codice disponibile pubblicamente, accessibile, modificabile e distribuibile da chiunque, e sviluppato tramite un approccio decentralizzato. Il concetto di decentralizzazione rappresenta una delle colonne portanti del bitcoin, nonché il suo più grande punto di forza. Il bitcoin è infatti totalmente privo di un centro di potere, a differenza di quanto accade invece per le monete fiat che, essendo emesse dalla Banca Centrale, sono soggette alle sue decisioni. Una moneta decentralizzata non può essere controllata o gestita da nessuno, e ciò azzera il rischio che corrono tutte le monete centralizzate, ovvero quello di essere distrutte dalla Banca Centrale. Ad esempio, nell'aprile del 2009, il governo dello Zimbabwe per cercare di stabilizzare l'economia del paese e per far fronte ad un tasso di inflazione eccessivamente elevato, ha deciso di interrompere la stampa della moneta locale (dollaro zimbabwiano), e di adottare come valute il rand africano e il dollaro statunitense. Anche il Bolivar, moneta locale del Venezuela, sta andando incontro alla stessa fine della moneta zimbabwiana. L'indistruttibilità del bitcoin ci fa quindi comprendere quanto questa moneta sia potente rispetto a una moneta centralizzata, che dimostra, al contrario, di essere enormemente vulnerabile.

Il terzo aspetto fondamentale da analizzare al fine di inquadrare correttamente il bitcoin è il sistema network peer-to-peer. Un sistema P2P è un network di nodi in cui le transazioni avvengono direttamente tra i nodi coinvolti, senza intermediari. In questo tipo di sistema non esistono quindi gerarchie, non esistono client o server, ma solo nodi equivalenti e scambi "da pari a pari". Un network peer-to-peer consente quindi che i pagamenti e le transazioni da una parte all'altra avvengano in maniera diretta, e senza l'intervento di istituzioni finanziarie.

La quarta caratteristica fondamentale del bitcoin è quella della piena convertibilità. Un bitcoin può essere acquistato con moneta tradizionale su una piattaforma di scambio da chiunque ne possieda

uno. L'acquirente potrà detenere il (o i) bitcoin in uno specifico portafoglio elettronico (nel gergo tecnico "wallet") attraverso il quale sarà in grado di effettuare acquisti presso qualsiasi attività commerciale che accetti il bitcoin come mezzo di pagamento, oppure convertire la moneta virtuale in moneta legale.

Avendo analizzato le principali caratteristiche che rendono il bitcoin una moneta indistruttibile, potente, e in un certo senso irriverente, può esserci chiaro anche il fine ultimo del creatore della moneta: rimpiazzare il sistema finanziario tradizionale ormai debole e vulnerabile, attraverso la creazione di un sistema di pagamenti decentralizzato, incorruttibile e privo di gerarchie, in grado di agevolare la trasmissione di ricchezza tra individui rendendo nulla l'influenza degli intermediari finanziari. L'ingresso in scena dell'hacker giapponese ha quindi segnato l'inizio del propagarsi di una minaccia sempre crescente per il sistema oligopolistico bancario e per il ruolo delle istituzioni finanziarie.

Dopo aver esaminato gli elementi fondamentali del bitcoin, è necessario comprenderne il funzionamento. Come detto in precedenza, i bitcoin possono essere scambiati con moneta tradizionale su piattaforme di scambio e, una volta acquistati, non vengono depositati in una banca fisica come accade per le monete centralizzate, ma in wallet digitali privati. Il tasso di cambio del bitcoin grava sull'acquirente e varia in base alla domanda e all'offerta del mercato.

Le transazioni possono avvenire tra tutti coloro che accettano il bitcoin come valuta di pagamento e che dispongono del software (portafoglio) necessario sul proprio dispositivo elettronico. Così come riteniamo che il bitcoin sia diverso dalle normali banconote e monete, dovremmo saperlo distinguere anche dalle monete digitali. I bitcoin, più che unità digitali custodite nella memoria di un computer, devono essere considerati come fondi all'interno di un conto.

Ogni transazione tra individui si basa su un sistema di crittografia asimmetrica. Il termine crittografia deriva dal greco κρυπτός [kryptós], "nascosto", e γραφία [graphía], "scrittura", e possiamo quindi tradurlo come "scrittura segreta". L'aggettivo "asimmetrica" si riferisce al fatto che, in ogni scambio, vengono utilizzate due chiavi crittografiche: una pubblica, e una privata. Ipotizziamo che due individui, che per comodità chiameremo X e Y, intendano effettuare una transazione in bitcoin. Il pagamento dal mittente X al destinatario Y, viene effettuato tramite uno scambio di messaggi criptati. Entrambe le parti possiedono due chiavi di cifratura uniche e che nessun altro può avere, una pubblica e una privata. Supponiamo che X voglia inviare un messaggio crittografato a Y: X usa la chiave pubblica di Y per criptare il messaggio, e Y, per decrittografare e leggere il messaggio ricevuto, utilizza la propria chiave privata. Il processo appena descritto è lo stesso che avviene quando X acquista un bitcoin da Y. Condizione necessaria affinchè avvenga lo scambio è, come già specificato precedentemente, che sia X che Y dispongano ciascuno di un wallet dotato di una chiave pubblica e

una privata. L'inizio della transazione coincide con il momento in cui Y invia la propria chiave pubblica ad X, come se la chiave pubblica fosse un indirizzo o un numero di conto. X effettua l'ordine di pagamento di un bitcoin a favore di Y, e lo firma con la propria chiave privata. La transazione viene quindi immessa nella rete, e la rete stessa sottopone la transazione ad un processo di verifica ed eventuale validazione. È importante specificare che tutti i soggetti coinvolti nelle transazioni rimangono anonimi e le transazioni sono irreversibili, perciò una volta effettuate non possono essere annullate.

L'operazione di verifica avviene tramite il lavoro dei cosiddetti *"miners"*, utenti speciali della rete che ciclicamente, ogni dieci minuti, raccolgono tutte le transazioni proposte alla rete negli ultimi dieci minuti, raggruppandole insieme in un unico *"blocco"*.

Ogni blocco, viene infine aggiunto a quello che può essere considerato il registro ufficiale delle transazioni verificate: la blockchain.

1.2 La Blockchain e il mining

Nella nostra quotidiana realtà esplorativa, lavorativa e interattiva, di pari passo con l'avanzamento della tecnologia e dell'innovazione digitale, si sta sviluppando l'impellente bisogno di percepire sicurezza e trasparenza nell'insieme di attività e processi che svolgiamo nel web.

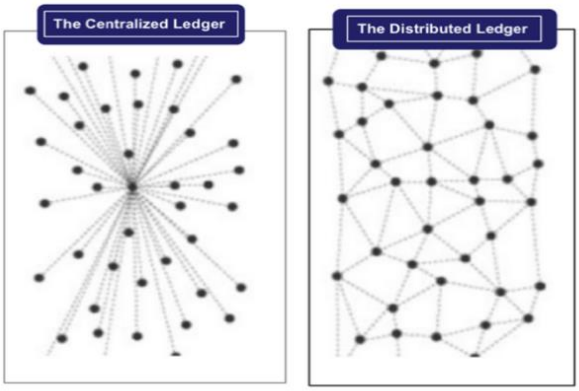
Oggi avvertiamo la necessita di sapere chi si nasconde dietro la piattaforma digitale su cui effettuiamo un pagamento, a chi arrivano i nostri soldi, e tramite chi stanno passando.

Il sistema Blockchain nasce per soddisfare questa urgenza ed ingloba temi e concetti che solitamente fatichiamo ad associare al processo di innnovazione digitale. Esistono svariate definizioni di Blockchain: c'è chi la definisce la *"nuova internet"*; chi ne parla come un'evoluzione dell'*"internet of things"*; chi, ancora, la qualifica come *"internet del valore"* relativamente alla sua capacità di agevolare e velocizzare la trasmissione del valore tra gli utenti del web. Personalmente però, nonostante ad un primo impatto possa risultare una scoperta rivoluzionaria, preferisco rimanere con i piedi ben ancorati a terra. Pertanto, accetto come definizione soddisfacente quella che inquadra la blockchain come un enorme registro, strutturato secondo una catena di blocchi contenenti l'insieme delle transazioni che avvengono tra i vari nodi della rete. Ogni transazione è verificata tramite un meccanismo di consenso e validazione, e presenta attributi di immutabilità ed irreversibilità.

Le principali caratteristiche su cui si fonda il concetto di blockchain sono le seguenti: trasparenza, sicurezza, responsabilità, consenso, immutabilità, e decentralizzazione. Si tratta di un insieme di proprietà che difficilmente riescono a coesistere nei prodotti dell'innovazione digitale odierna. Con

la blockchain, possiamo affermare di essere di fronte al nuovo concetto digitale di fiducia. La convivenza delle caratteristiche appena elencate all'interno del sistema Blockchain, è garantita dal network peer-to-peer, grazie al quale tutti gli utenti della rete agiscono come pari, e hanno la possibilità di consultare, verificare, e convalidare le informazioni immutabilmente registrate nel sistema. Questo sistema, inserisce la blockchain nella categoria dei *Distributed Ledger Technology (Tecnologia degli Archivi Distribuiti)*.

Figura 1.1: The Centralized Ledger vs The Distributed Ledger, fonte: Blockchain4Innovation



La *Distributed Ledger Technology (DLT)* rappresenta un'evoluzione della *Centralized Ledger Technology*. Infatti, mentre quest'ultima si caratterizza per la presenza di una *central authority* - solitamente un'entità che controlla e gestisce tutte le transazioni che vengono registrate - la DLT non prevede un amministratore centrale, ma un'archiviazione basata sul libero accesso e sul consenso di tutti i nodi della rete. Solitamente, la registrazione dei passaggi di proprietà, che si tratti di denaro o di attività finanziarie, immobiliari *et cetera*, viene effettuata su sistemi centralizzati (*centralized database*), e spetta poi alle banche il compito di aggiornare continuamente i propri database locali. Con il *distributed ledger*, all'opposto, il database di operazioni si distribuisce su una rete di più computer, alla quale possono accedere liberamente tutti i membri, con la possibilità di consultare e validare autonomamente le transazioni. Questo sistema basato su una logica distributiva, rende la rete più sicura e trasparente, e rappresenta un importante incentivo non solo per le aziende, ma anche per quegli utenti che esitano ad utilizzare internet come mezzo di acquisto o di vendita.

Addentriamoci adesso nel funzionamento del sistema blockchain, che talvolta può risultare di difficile comprensione.

L'elemento iniziale è un blocco di informazioni trasparenti, irreversibili, immutabili e permanenti, prodotte in uno specifico arco di tempo. Inizialmente, le informazioni vengono sottoposte ad un sistema di validazione tramite un software e, una volta convalidate, vengono salvate all'interno di un registro pubblico al quale tutti gli utenti della rete hanno accesso. In un secondo lasso di tempo, nuove

transazioni e nuove informazioni creano un nuovo blocco, più aggiornato, che si "concatena" al blocco precedente. È importante ricordare che qualsiasi nuova informazione o transazione, una volta accettata, non può essere modificata o eliminata, ma resta registrata nel sistema che funge, in un certo senso, da garanzia di sé stesso.

Ogni blocco, oltre all'insieme di transazioni avvenute in un determinato arco temporale, contiene due hash: uno che identifica il blocco stesso, e un altro che identifica il blocco precedente. Un hash è un codice alfanumerico di dati, che cambia se uno dei dati relativi al blocco viene modificato. Più semplicemente, se le informazioni all'interno di un blocco cambiano, anche l'hash di quel blocco si modifica. Ogni hash quindi, basandosi su un algoritmo matematico, traccia dati di lunghezza arbitraria in codici di dimensione fissa. A questi due hash si aggiunge poi una marca temporale che svolge una funzione cronologica all'interno della catena, specificando il momento esatto in cui ogni blocco è stato creato. L'insieme di questi tre elementi (i due hash e la marca temporale), garantisce l'immutabilità dei blocchi che costituiscono la blockchain. La tentata modifica di un blocco, comporterebbe infatti una variazione dell'hash e della marca temporale, e il blocco successivo non includerebbe più lo stesso hash del blocco che lo precede. Analizziamo un esempio che potrebbe rendere tutto più chiaro. Immaginiamo tre blocchi concatenati: X (primo blocco), Y (secondo blocco) e Z (terzo e ultimo blocco). Prendiamo in considerazione il blocco Y e il blocco Z. Ognuno ha due hash (H), l'hash di sé stesso e l'hash del blocco precedente: Y possiede Hx e Hy; Z possiede Hy e Hz.

Se qualcuno tentasse di modificare il blocco Y, l'hash Hy si modificherebbe, così come subirebbe una variazione anche la marca temporale del blocco Y. Il blocco Z, contenente Hy e Hz, non avrebbe più l'hash del blocco precedente, perché con la modifica del blocco Y anche l'hash di Y (Hy) si è modificato. Ciò renderebbe evidente l'alterazione della catena.

Oltre a questo meccanismo, ciò rende la blockchain un sistema ampiamente sicuro e trasparente, è il lavoro dei cosiddetti "*miners"*. I miners sono degli utenti della rete che hanno il compito di verificare le informazioni e le transazioni che compongono ogni blocco, e di allungare la catena con nuovi blocchi. La missione di questi operatori della rete consiste nel districare un complesso problema matematico, raggiungendo la cosiddetta "*Proof-Of-Work"*, ovvero la soluzione. Una volta arrivati a capo di questo puzzle matematico, un nuovo blocco viene convalidato e "agganciato" alla catena, sbloccando così un nuovo nodo nella rete. Tuttavia, è sbagliato pensare che i miners ricerchino la soluzione seguendo un vero e proprio metodo matematico. L'unico modo per giungere a capo del problema è infatti quello di procedere per tentativi, servendosi di computer veloci, processori programmabili a livello hardware e schede grafiche ad elevatissima potenza di calcolo che consentano di fare un enorme numero di tentativi al secondo, e di calcolare hash il più rapidamente possibile.

Il nome “miners” è legato al fatto che questi utenti della rete operano come dei veri e propri minatori o “cercatori d’oro”. Infatti, il loro sforzo in termini di tempo, fatica e denaro, è finalizzato all’ottenimento di una remunerazione in bitcoin o criptovalute. Il primo minatore che riesce a trovare il cosiddetto *Nonce (Number used once),* si aggiudica la ricompensa. Ovviamente, più la catena si allunga con nuovi blocchi, più sarà complesso e impegnativo riuscire a trovare nuovi Nonce. Nonostante la *mission* dei miners risulti estremamente difficile e dispendiosa, lo sforzo è premiato talmente bene da incentivare sempre più utenti ad investire il proprio denaro nella realizzazione di grossi sistemi di computer iperattrezzati che consentano loro di raggiungere per primi la Proof-of-Work. (Berretti A., 2018)

Grazie alle componenti finora descritte, le potenzialità del sistema blockchain si espandono su più campi di applicazione. Da alcuni studi emerge che, al momento, le ricerche svolte sull’utilizzo della blockchain sono focalizzate per l’80% sul bitcoin, mentre solo il 20% riguarda l’applicazione di questo sistema ad ambiti diversi come quello delle licenze e degli smart contract. Ulteriori analisi stanno puntando al miglioramento dei limiti della blockchain in tutto ciò che concerne privacy e sicurezza, con il fine di promuovere, più di quanto non sia già stato fatto, la libertà individuale degli utenti e il loro senso di fiducia nel web. La “catena di blocchi” funge, tra l’altro, da garanzia di accesso libero e paritario per tutti gli utenti del web alle istituzioni digitali di base tra cui mercati, sistemi giudiziari e sistemi di pagamento. In un mondo orientato alla riduzione delle minacce digitali e al soddisfacimento dei bisogni di trasparenza e limpidezza percepiti dagli utenti del web, la blockchain si presenta quindi come un’innovazione di enorme spessore, ponendosi fini non solo tecnologici, ma anche relativi ad importanti cambiamenti nel campo della pubblica amministrazione.

1.3 Le Criptovalute

Il bitcoin esaminato nella prima parte di questo capitolo, appartiene alla categoria delle criptovalute (o criptomonete). Pertanto, tutti i bitcoin sono criptovalute, ma non tutte le criptovalute sono bitcoin. La parola criptovaluta è la traduzione del termine inglese cryptocurrency, e significa “valuta nascosta”. “Nascosta” (o “criptata”), perché è visibile (o “decrittografabile”) solo conoscendo o possedendo specifiche “chiavi di cifratura” pubbliche e private. La foto di seguito descrive in maniera precisa il processo di scambio di messaggi criptati tra due soggetti, già analizzato nel paragrafo 1.1 dedicato al bitcoin:

Figura 1.2, fonte: CONSOB

A usa la chiave pubblica di B per criptare il testo che intende inviare a B; il testo criptato viene decriptato tramite l'utilizzo della chiave privata di B, e B può finalmente leggere il messaggio.

Le criptovalute vengono definite monete "virtuali" poiché non esistono in forma fisica. Gli scambi di criptomonete non possono pertanto avvenire in forma cartacea, ma solo digitalmente e in via telematica tramite l'utilizzo di e-wallets (o "cryptowallets").

Tutte le criptovalute si basano su un sistema network Peer-to-Peer, in cui le transazioni vengono effettuate tra utenti considerati "pari", e senza l'intervento di intermediari finanziari. Inoltre, le monete virtuali sono decentralizzate, ovvero non sono sottoposte al controllo di un ente centrale governativo, ma vengono emesse e controllate dall'ente emittente. Questi due aspetti (assenza di intermediari nelle transazioni, e decentralizzazione), suscitano il malcontento e la diffidenza del settore bancario nei confronti delle criptovalute. Il timore delle banche, è che una tale libertà individuale degli utenti e l'annullamento totale del ruolo degli intermediari finanziari, possano pian piano determinare una drastica inversione di rotta dell'attuale business aziendale. Ma non è tutto, perché preoccupazioni rilevanti sorgono anche nei settori della pubblica amministrazione e delle istituzioni finanziarie, che stanno vedendo la loro influenza nelle transazioni online ridursi gradualmente fino a scomparire del tutto.

Al momento infatti, le monete virtuali sono ancora illegali nella maggior parte dei paesi, e pertanto, la loro accettazione come metodo di pagamento è del tutto arbitraria e volontaria. Non mancano però le eccezioni: alcuni paesi come l'Uruguay (con l'e-peso) e il Venezuela (con il Petro), hanno infatti deciso di testare l'utilizzo delle criptomonete sotto il proprio controllo. Altri paesi ancora, tra cui Svezia ed Estonia, stanno lavorando ad iniziative in ambito criptomonetario.

Inoltre, per ridurre paure e preoccupazioni, gli operatori del settore delle criptovalute sono impegnati nella ricerca di risposte in materia di regolamentazione dell'utilizzo di queste monete. La difficoltà nel trovare una regolamentazione efficace, nasce dal fatto che il target di questa disciplina risulta essere particolarmente ampio, e riguarda molteplici soggetti operanti su scala globale. L'obiettivo di

fondo è quindi quello di ridurre il più possibile i rischi collegati alle valute virtuali, senza però porre limiti all'innovazione delle stesse. La missione è sicuramente ardua e richiederà del tempo, ma una volta portata a termine potrebbe dare il via libera alla diffusione di standard condivisi a livello internazionale, che condurrebbero ad un'armonizzazione tra il "mondo criptovalute" e le politiche regolatorie a livello nazionale. La regolamentazione quindi, scaccierebbe via paure ed incertezze che ad oggi ancora allontanano i governi dei paesi dall'adozione delle criptovalute.

Prima di analizzare singolarmente le principali criptovalute, è necessario soffermarci su una classificazione che prevede la distinzione tra moneta virtuale *"chiusa"*, *"unidirezionale"* e *"bidirezionale"*. Gli elementi su cui si fonda questa classificazione sono essenzialmente due: il primo è quello della convertibilità, o meglio, lo scambio della criptovaluta con moneta a corso legale (o "moneta Fiat"); il secondo riguarda la tipologia di beni e servizi acquistabili.

La moneta virtuale chiusa è solo ed esclusivamente una valuta virtuale, che non può essere convertita in moneta "ufficiale" (o Fiat), e può essere utilizzata solo per l'acquisto di beni virtuali e servizi.

L'unidirezionalità della moneta virtuale invece, prevede che una moneta "ufficiale" può essere convertita in valuta virtuale, ma la valuta virtuale non può essere riconvertita in valuta "ufficiale". Una volta che la moneta Fiat viene convertita in moneta virtuale, l'operazione è quindi irreversibile e la moneta può essere utilizzata per l'acquisto di beni virtuali, reali e servizi.

Infine, la moneta virtuale bidirezionale, prevede la totale conversione tra valuta "ufficiale" e valuta virtuale. Dunque, una moneta Fiat, una volta convertita in valuta virtuale, può essere: riconvertita in moneta "ufficiale"; oppure utilizzata per l'acquisto di beni virtuali, reali e servizi. Ad esempio, il bitcoin è una moneta virtuale bidirezionale poichè dotato, come si è detto nel primo paragrafo, di piena convertibilità.

Dopo un'analisi generale delle criptovalute e delle loro potenzialità, è giunto il momento di focalizzare l'attenzione su quelle che sono, al momento, le criptocurrencies più innovative e importanti in termini di capitalizzazione di mercato.

1.3.1 Le Altcoin

Il termine altcoin viene utilizzato per indicare la grande categoria delle *"Alternative Coin"*, ovvero tutte le criptovalute nate dopo il bitcoin e che, rispetto ad esso, rappresentano un'alternativa. Le altcoin sono sviluppate dallo stesso codice sorgente di bitcoin, e nascono generalmente come una sua "estensione", ma presentano importanti differenze per quanto riguarda obiettivi e funzionamento. L'obiettivo delle alternative coin è "semplicemente" quello di migliorare alcune specifiche funzionalità del bitcoin, al fine di rendere la tecnologia di base della moneta di Nakamoto, più rapida

ed efficiente. Ad esempio, le alternative coin riducono in maniera esponenziale i tempi di trasferimento della moneta: se il bitcoin impiega dieci minuti per l'autenticazione di un blocco, un'altcoin è in grado di ridurre questo intervallo di tempo anche al di sotto del minuto.
Differenze sostanziali si presentano in ambito di funzionamento delle due tipologie di monete. Il bitcoin, come si è visto nel paragrafo ad esso dedicato, si fonda su un efficace meccanismo di convalida dei blocchi chiamato Proof-of-Work (PoW), che richiede però un enorme dispendio di energia, tempo e denaro. Molte altcoin stanno invece puntando su un sitema Proof-of-Stake (PoS). Mentre nel sistema PoW viene premiato con una ricompensa in bitcoin il minatore più veloce, ovvero colui che per primo riesce a trovare il Nonce, nel Proof-of-Stake, il miner che riesce ad aggiungere un nuovo blocco alla catena, ottiene come ricompensa una commissione della transazione proporzionale al proprio lavoro.
I vantaggi del PoS rispetto al PoW sono quindi diversi: una migliore efficienza energetica con importanti riduzioni del consumo di energia; un sistema di ricompensa al mining più equo; una maggiore scalabilità delle transazioni (la blockchain è in grado di gestire un numero più elevato di transazioni senza incorrere in un peggioramento delle prestazioni); e infine non è necessario spendere una fortuna nella creazione di un hardware iperaccessoriato per riuscire a creare nuovi blocchi.
Nonostante queste differenze, bisogna sempre tenere a mente che le altcoin sono derivate dal bitcoin, e tendono pertanto ad imitarne la traiettoria di prezzo. Al momento è quindi normale che, se il prezzo di mercato del bitcoin aumenta, si noterà un leggero aumento anche del prezzo delle altcoin. Gli analisti affermano però che, una volta che il sistema avrà raggiunto uno stadio di maturità, questo effetto imitativo tenderà a scomparire e le altcoin svilupperanno una totale indipendenza rispetto al bitcoin.

1.3.2 Ethereum

Ethereum nasce nel 2013, quando un programmatore appena diciannovenne, Vitalik Buterin, presenta il progetto di una blockchain flessibile, capace di eseguire e registrare qualsiasi tipo di transazione. Ethereum viene ufficialmente lanciata nel 2015, e ad oggi è la seconda moneta per capitalizzazione di mercato (dopo il bitcoin). Lo scopo del team di fondatori di Ethereum era quello di estendere il campo di utilizzo della blockchain, facendo leva sui suoi classici attributi di sicurezza e trasparenza (Coinbase, 2021).

Oggi infatti, il sistema blockchain di Ethereum viene utilizzato per il funzionamento di strumenti finanziari, funge da custodia e da mezzo di codifica di database complessi, e il suo raggio d'azione è stato esteso anche al mondo del *gaming*.
Uno dei maggiori punti di forza di ethereum è l'utilizzo degli *"smart contracts"*: contratti definiti appunto intelligenti ("smart") perché, a differenza dei contratti tradizionali, vengono eseguiti in maniera automatica. Più semplicemente, l'esecuzione del contratto avviene automaticamente, e senza l'intervento delle parti o di intermediari, quando le condizioni fissate dai contraenti vengono soddisfatte. Tramite l'utilizzo di questi particolari contratti, gli sviluppatori di ethereum sono in grado di creare applicazioni complesse, riducendo al minimo frodi e interferenze di terze parti.
Per l'esecuzione di questi smart contracts vengono utilizzati dei token, o meglio delle frazioni di token, chiamati "ETH" (o anche "Ethereum"). Le commissioni di ETH vengono comunemente denominate "gas", in quanto fungono da carburante per il funzionamento dell'intero sistema. Non a caso, spesso si sente definire Ethereum come il *"new digital oil"* ("nuovo petrolio digitale").
Se a questo punto verrebbe da pensare a Ethereum come ad una delle scoperte più innovative degli ultimi anni, è perché ancora nulla si è detto riguardo a Ethereum 2.0.
Ethereum 2.0 rappresenta un'estensione della rete Ethereum, nata per due motivi: innanzitutto perché, per i prodotti dell'innovazione digitale, l'aggiornamento è indispensabile per garantire l'evoluzione e il miglioramento delle loro principali caratteristiche. Con ethereum 2.0 si punta infatti al potenziamento degli attributi di flessibilità, sicurezza, velocità ed efficienza.
Inoltre, gli sviluppatori di Ethereum si sono accorti della scarsa sostenibilità del metodo di verifica denominato "Proof of Work", su cui ci si è già ampiamente soffermati. L'aggiornamento Ethereum 2.0 è stato quindi necessario per introdurre nella blockchain di Ethereum il meccanismo di validazione "Proof of Stake", che garantisce un più equo sistema di remunerazione dei "validatori" e, soprattutto, una significativa riduzione del consumo energetico.
Secondo alcune stime, il processo di transizione da ETH1 a ETH2 si chiuderà entro l'inizio del 2023.

1.3.3 Ripple

Ripple si presenta come una delle criptovalute più innovative e atipiche del settore. Essa nasce infatti come criptomoneta centralizzata, impiegata tra intermediari finanziari al fine di soddisfare le specifiche esigenze del settore bancario. Ripple rappresenta quindi la prima criptomoneta "filobancaria", avente come fine quello di agevolare gli scambi interbancari riducendo in maniera significativa i costi di commissione (Perugini M. L., 2018). La "pecora nera" delle criptovalute, è

riuscita quindi a conquistarsi la fiducia delle istituzioni bancarie, garantendo una maggiore efficienza in termini di velocità, sicurezza e tracciabilità delle transazioni.

Il meccanismo di consenso e validazione delle transazioni è affidato ad un soggetto validatore denominato *"Ripple Consensus"*, e le informazioni vengono archiviate all'interno di un registro distribuito che prende il nome di *"Ripple Consensus Ledger"*. Il sistema di pagamenti si basa sull'utilizzo di crediti IOU ("I Owe You") che definiscono il saldo attuale di ogni utente. Come afferma Gianluca Comandini, uno dei massimi esponenti italiani del settore delle criptovalute, attraverso questo particolare sistema di pagamenti, le transazioni possono essere effettuate "senza continuità di forma" (Comandini G., 2020). Gli utenti sono quindi liberi di scambiarsi denaro in qualsiasi valuta, sia essa una moneta fiat o una criptovaluta, e sarà poi compito degli intermediari convertire la valuta in Ripple. Questi intermediari, prima di effettuare la conversione, devono occuparsi dell'identificazione degli utenti e dell'accettazione e tracciamento dei depositi da essi effettuati.

Oltre alla centralizzazione, Ripple presenta altre importanti differenze con il bitcoin. Infatti, se il bitcoin è caratterizzato da un network al quale tutti possono accedere, nel sistema Ripple l'ingresso degli utenti è limitato, e la gestione delle modifiche del registro distribuito è affidata ad un gruppo ristretto di soggetti identificati con il nome di "trusted validators".

Un'ulteriore distinzione rispetto al bitcoin riguarda la distribuzione dei token. I crediti IOU che costituiscono il sistema di pagamenti Ripple sono infatti già tutti in circolazione, e il loro numero ammonta a un totale di cento miliardi, di cui: il 55% è destinato alla vendita al pubblico, il 20% ai fondatori del progetto, e il restante 25% ai Ripple Labs (laboratori che sviluppano il protocollo di pagamento e la rete di scambio).

Chissà se, con questo avvicinamento delle banche alla criptovaluta Ripple, anche altre criptomonete non decidano di assumere una natura finanziaria che le renda appetibili per il settore delle istituzioni finanziarie.

CAPITOLO 2: RISCHI CONNESSI ALLE CRIPTOVALUTE E COSTRUZIONE DEL PORTAFOGLIO

2.1 Premessa

Nel primo capitolo ci siamo soffermati sugli aspetti più innovativi, irriverenti e rivoluzionari delle criptovalute, accennando solamente ai pericoli che questi strumenti possono nascondere. Infatti, nonostante il mondo delle criptomonete possa sembrare ad un primo impatto una "pentola d'oro", è necessario studiare in maniera approfondita i rischi ad esso connessi. Pertanto, EBA (*European Banking Authority*), ESMA (*European Securities and Markets Authority*) ed EIOPA (*European Insurance and Occupational Pensions Authority*), sono intervenute per sottolineare i principali aspetti che rendono le valute virtuali prodotti altamente rischiosi e ampiamente soggetti alla speculazione di coloro che ne usufruiscono. Le tre autorità europee evidenziano in particolar modo la mancanza di trasparenza nel settore delle *cryptocurrencies*, e la presenza di numerosi segnali riconducibili ad una bolla speculativa di dimensioni macroscopiche. Il fatto che dietro a queste particolari monete non vi sia una banca centrale o un'autorità pubblica a fare da garante - secondo quanto riporta il comunicato di EBA, ESMA ed EIOPA – priva i consumatori di qualunque tipo di tutela giuridica. Inoltre, l'enorme volatilità di tali strumenti, espone gli *users* al rischio di perdere in breve tempo il capitale investito, in maniera parziale o totale. Pertanto, le tre autorità europee di vigilanza (AEV) sconsigliano fortemente di convertire in valuta virtuale somme ingenti di capitale, poichè le perdite potrebbero non solo riguardare l'intero investimento, ma avvenire anche nell'arco di poche ore. (Banca d'Italia, 2018).

Le preoccupazioni dei cosiddetti *regulators* sono perciò giustificate, in quanto una graduale diffusione e accettazione delle criptovalute come mezzo di pagamento, avrebbe un impatto ampiamente negativo sull'attuale base monetaria. Il timore delle banche centrali è che le valute virtuali possano, in maniera progressiva, destabilizzare e addirittura rimpiazzare il sistema monetario tradizionale, prendendo il posto del contante e della moneta la cui emissione spetta attualmente agli stati sovrani. Nel caso in cui gli stati decidessero di adottare le criptovalute come strumento di pagamento, gli emittenti pubblici non avrebbero più alcun controllo sulla funzione per la quale vengono istituiti, e dalla quale effettivamente prendono il nome: l'emissione di moneta.

Oltre ai rischi concernenti l'ambito finanziario, sorgono allarmismi anche rispetto ai temi di sicurezza e protezione degli asset digitali. Il sistema DLT (Decentralized Ledger Technology) che si pone alla base delle criptovalute, non garantisce infatti alcuna tutela dell'utente in termini di protezione delle

chiavi crittografiche e problematiche di tipo informatico. La mancanza di una figura istituzionale che faccia da garante, e lo stato ancora troppo arretrato del processo di disciplina delle criptovalute, determinano insieme un tasso di rischio particolarmente elevato per quanto riguarda frodi, sottrazioni illecite delle chiavi private di crittografia, e perdite di capitale per malfunzionamenti dei sistemi informatici.

Perdipiù, l'utilizzo delle criptovalute non contrasta, ma anzi favorisce la diffusione di pratiche illegali come il riciclaggio di denaro. Ad esempio, le organizzazioni criminali avrebbero la possibilità di convertire il denaro proveniente da attività illecite in criptovalute, in quanto il processo di conversione non prevede al momento alcun tipo di controllo o intervento da parte di intermediari finanziari.

Data la varietà di rischi appena presentati, sarà necessario nei prossimi paragrafi analizzare più nel dettaglio le singole tipologie: rischi finanziari, rischi informatici, rischi in materia di riciclaggio del denaro illecito, e rischi per la stabilità economica.

2.2 Le varie tipologie di rischi connessi al mondo delle criptovalute: rischi finanziari, rischi informatici, rischi per attività illecite

Come spiegato nella premessa di questo capitolo, l'utilizzo delle criptovalute può comportare per gli utenti una serie di rischi, che possiamo suddividere in tre categorie principali: rischi finanziari, rischi informatici, e rischi per attività illecite. Nel seguente paragrafo analizzeremo nel dettaglio le diverse classi di rischio, cercando di comprendere gli aspetti che necessitano di maggior prudenza da parte degli utenti.

La macroarea dei rischi finanziari può essere suddivisa in tre sottogruppi: rischio di volatilità; rischio di liquidità; e rischi per la stabilità economica. Uno degli aspetti più attraenti delle criptovalute è sicuramente quello del rendimento. Infatti, se da un lato è vero che i rischi di perdita del capitale sono decisamente elevati, è vero anche, d'altra parte, che negli ultimi anni le curve di mercato dei maggiori criptoasset hanno riportato rendimenti da capogiro, rappresentando un elemento di appetibilità per moltissimi investitori. Ogni investitore pertanto, più che essere scoraggiato dall'elevata probabilità di registrare una perdita di capitale, è attratto dai cospicui proventi che potrebbe ottenere nel caso in cui l'investimento andasse a buon fine. Tuttavia, capire quale investimento potrà rivelarsi fruttuoso, risulta essere una pratica estremamente complessa, proprio a causa delle continue e spesso inaspettate fluttuazioni dei prezzi. È questo il motivo per cui le tre AEV (EBA, ESMA, EIOPA) mettono in guardia i consumatori da una possibile bolla speculativa, e sottolineano la scarsa convenienza di convertire in valute virtuali grandi somme di capitale.

Il secondo sottogruppo compreso nella macroarea dei rischi finanziari, è quello del rischio di liquidità. Dal momento che l'offerta non è tuttora più in grado di assorbire la domanda di criptoasset (cresciuta esponenzialmente negli ultimi dieci anni), i vari Exchange stanno prosciugando le loro riserve per cercare di soddisfare la richiesta degli acquirenti, rendendo illiquido il mercato delle criptovalute. Questa illiquidità comporta, per gli investitori, un elevato rischio di vendere gli asset digitali a un prezzo inferiore rispetto a quello desiderato, e in un momento sbagliato. Rischi di liquidità e rischi di volatilità sono quindi accomunati dal fatto che i prezzi vengono fondamentalmente determinati dal mercato, nel punto in cui la domanda incontra l'offerta.

Il terzo ed ultimo sottogruppo di rischi finanziari è quello dei rischi per la stabilità economica. Al centro dell'analisi di questa categoria di rischio, c'è un particolare tipo di criptomoneta: la stablecoin. Le stablecoin, come si può facilmente intuire dal nome, sono criptovalute di valore stabile (Rasera S., 2021). La stabilità di queste monete virtuali è dovuta al fatto che esse sono legate o ad una valuta FIAT, o al valore dell'oro. Per questo motivo, le oscillazioni di prezzo delle stablecoin sono molto meno frequenti e veloci rispetto alle fluttuazioni di prezzo delle normali criptovalute, e possono essere monitorate e tenute sotto controllo dai consumatori. Per intenderci, gli aumenti o le diminuzioni del prezzo delle stablecoin saranno comunque elevate, ma avverranno in un arco di tempo decisamente più lungo rispetto al tempo di oscillazione dei prezzi delle altre criptomonete. Ma allora quali sono i rischi? La risposta va ricercata nelle preoccupazioni delle AEV e delle Banche Centrali, le quali sostengono che l'emissione di stablecoin, contribuisce ad alimentare in maniera significativa il fenomeno del cosiddetto *"shadow banking"*. Lo shadow banking è un sistema che consente agli investitori di finanziarsi tramite canali di finanziamento non ufficiali, e quindi non regolamentati. La mancanza di regolamentazione nelle operazioni di finanziamento, suscita l'allarmismo delle banche centrali, in quanto lo shadow banking ha rappresentato uno degli aspetti più critici della crisi finanziaria del 2008: i mezzi di finanziamento alternativi erano, in quel caso, i celebri mutui *sub-prime*.

La seconda categoria di rischi legati al mondo delle criptovalute è quella dei rischi informatici. È frequente infatti, che nelle transazioni di criptoasset si verifichino criticità di carattere informatico, dovute a malfunzionamenti dell'hardware, interruzioni dei sistemi operativi o più semplicemente ad errori degli operatori stessi. Le problematiche appena citate, oltre a non essere prevedibili, presentano enormi difficoltà di risoluzione e rendono il sistema inutilizzabile, impedendo agli utenti di effettuare qualsiasi tipo di operazione di acquisto o di vendita. Durante queste interruzioni operative, gli exchange e le piattaforme di negoziazione smettono di funzionare e tutte le contrattazioni vengono sospese, o addirittura annullate. Ciò comporta, per i consumatori, il verificarsi di importanti perdite di capitale che non potranno essere rimborsate in alcun modo. Infatti, nonostante si potrebbe pensare

ad un risarcimento degli utenti, non esiste alcuna norma o disciplina che preveda questa possibilità. La mancanza di un'autorità centrale che gestisca le varie piattaforme di scambio, e che si prenda la responsabilità del corretto funionamento di esse, rende gli utenti completamente sprovvisti di tutele giuridiche. In breve: i soldi persi, restano persi.

Tra i rischi informatici, oltre ai malfunzionamenti tecnologici, figurano anche reati come l'hackeraggio e il furto di chiavi crittografiche. Come detto in precedenza, le chiavi private di crittografia degli utenti hanno un'importanza fondamentale, e devono pertanto essere conservate con estrema attenzione. Inoltre, spesso accade che le chiavi vengano gestite e conservate automaticamente dalla piattaforma di scambio su cui si effettuano le transazioni. Gli exchange che custodiscono le chiavi private degli utenti, rappresentano la preda perfetta degli hacker, che mettono in atto operazioni di attacco informatico in grado di rubare anche centinaia di migliaia di chiavi. Ad esempio, nel gennaio del 2018, la piattaforma Coincheck ha subìto un potente attacco hacker, finalizzato al furto di oltre 250 mila chiavi di crittografia private. Gli utenti della piattaforma hanno registrato perdite parziali e totali del capitale investito, per un valore totale di circa 500 milioni di dollari. Nel 2019, sono stati registrati ben dodici attacchi informatici a diverse piattaforme di scambio, per un furto di ammontare complessivo pari a ben 290 milioni di dollari in criptovalute. L'insieme di questi problemi sul fronte informatico, rende l'utilizzo delle criptovalute estremamente rischioso e dovrebbe mettere in allerta – quantomeno per limitare i danni – tutti coloro che si apprestano ad investire in questo settore.

La terza macroarea di rischio che andremo ad analizzare, è quella dei rischi relativi ad attività illecite. Mentre l'attività di hacking appena citata è strettamente limitata all'ambito informatico, in quest'ultima parte del paragrafo saranno trattati nello specifico aspetti legati al riciclaggio del denaro sporco e al finanziamento del terrorismo. Nonostante nel 2018 siano entrate in vigore le disposizioni previste dall'UE per la lotta al riciclaggio e al finanziamento del terrorismo, il settore delle criptovalute risulta ancora una sorta di nascondiglio virtuale per i soldi delle criminalità organizzate. Le associazioni criminali, sfruttando la scarsa regolamentazione e la natura decentralizzata del settore delle criptovalute, possono infatti agire in due modi. Da un lato possono adoperarsi per convertire il denaro illecito in valute virtuali, approfittando del fatto che la conversione della moneta tradizionale avverrebbe senza alcun tipo di controllo. Dall'altro, hanno la possibilità di vendere merci illegali a fronte di un pagamento in criptovalute. In questo secondo caso, l'ammontare di criptovalute ottenuto tramite la vendita di merci illecite verrebbe poi semplicemente convertito in denaro apparentemente legale. Risulta quindi estremamente facile, per coloro che possiedono le necessarie conoscenze, dare una seconda vita "legale" al denaro proveniente dalle attività criminali (spaccio, vendita di armi, prostituzione, ecc…).

Per far fronte a questa problematica, in Italia è stata introdotta una normativa specifica per tutti coloro che svolgono attività e offrono servizi nel settore delle criptovalute. Essa prende il nome di "*Anti Money Laundering"* (Antiriciclaggio) e di *"Counter Terrorist Financing"* (Contrasto al finanziamento del terrorismo). La normativa prevede che, su qualunque fornitore di servizi legati all'utilizzo di criptovalute, vige l'obbligo di registrarsi presso un'apposita sezione del registro dell'OAM (Organismo degli Agenti e dei Mediatori). Tuttavia, identificare il reale soggetto a cui le criptovalute sono effettivamente intestate risulta essere un'operazione decisamente complessa (e spesso non possibile) proprio per la natura decentralizzata del sistema. Il reale possessore del wallet (e quindi delle valute virtuali), può infatti essere identificato solamente se ha effettuato le proprie transazioni su una piattaforma di scambio centralizzata. Se, quindi, non è possibile associare le singole transazioni al vero possessore del portafoglio virtuale, non è possibile neppure determinare il soggetto su cui debbano ricadere gli obblighi previsti dalla suddetta normativa. Essa è, pertanto, facilmente raggirabile, e necessita di ulteriori e significativi sviluppi per potersi presentare come serio ostacolo per le organizzazioni criminali.

Analizzate queste tre principali categorie di rischi connessi alle criptovalute, si può comprendere quanto sia importante, per chiunque decida di investire in questo settore, adottare precauzioni in termini di sicurezza dei dati personali e di affidabilità degli hardware utilizzati. Inoltre, per concludere, è fondamentale riconoscere che tra tutte queste situazioni spesso non controllabili e non prevedibili dall'utilizzatore di criptovalute, c'è una responsabilità dalla quale egli non può essere esonerato: quella di investire in valute virtuali una quantità di denaro che non può permettersi di perdere.

2.3 Costruzione e diversificazione di un cryptowallet

Fino a questo punto abbiamo descritto le diverse tipologie di criptovalute, sottolineandone le caratteristiche e specificando, nella prima parte di questo capitolo, i rischi ad esse connessi. Una parte fondamentale del settore delle valute virtuali che, invece, non è ancora stata approfondita, è quella che comprende i dispositivi virtuali adibiti alla custodia delle criptomonete: i portafogli di criptovalute, anche detti *Cryptowallet*.

Un *cryptowallet* è, in linea di massima, molto simile a un portafoglio di investimento, definito come l'insieme di tutti gli asset di cui siamo proprietari: azioni, obbligazioni, o titoli di altro tipo. La differenza tra i più comuni portafogli di investimento e i cryptowallet, è che i secondi si compongono esclusivamente di criptovalute. Quando si vuole creare un portafoglio di criptovalute, la prima cosa

da fare è quella di studiare nel dettaglio l'andamento, attuale e storico, della valuta virtuale che si intende acquistare. Tuttavia, l'analisi rigorosa dell'asset su cui si vuole puntare non basta, ed anzi, rappresenta solo una minima parte dell'insieme di aspetti di cui bisogna tener conto per creare un cryptowallet ben strutturato. Dopo aver risposto alla domanda "cosa comprare?", bisogna porsi perciò un altro quesito: "come acquistare?". Esistono due tipi di strategie di acquisto delle cryptocurrencies: PIC e PAC. La prima strategia prende il nome di Piano di Investimento di Capitale (PIC) e consiste, molto semplicemente, nell'acquistare tutto in un'unica soluzione. Si tratta quindi di effettuare l'intero investimento di una determinata somma di denaro in una sola volta. La seconda strategia invece, denominata Piano di Accumulo del Capitale (PAC), "prevede ingressi dilazionati nel tempo". Il vantaggio dell'opzione PAC è, rispetto alla prima, che l'investimento può essere effettuato a rate, e non devono essere versati ingenti capitali in una soluzione unica. (The Crypto Gateway, 2022)

Una volta stabilita la strategia di acquisto, è fondamentale determinare la propria propensione al rischio, tenendo conto di una regola perentoria: a maggiori rischi, corrispondono maggiori rendimenti. La differenza tra un portafoglio di criptovalute "da principiante", ed un cryptowallet ben strutturato, sta proprio nella pianificazione di questi tre aspetti: analisi di ciò che si sta acquistando, determinazione della modalità di acuisto, e propensione al rischio. Procediamo con un esempio pratico ipotizzando due situazioni: un portafoglio costruito senza pianificazione, e un portafoglio costruito sulla base di una rigorosa programmazione.

Nel primo caso, supponiamo di acquistare tre criptovalute diverse, Bitcoin, Ethereum e Ripple, senza aver previsto alcun tipo di piano di acquisto e di rischio. Custodiamo quindi le tre tipologie di criptomonete nel nostro cryptowallet, senza conoscere né il loro andamento presente e passato, né la loro quantità in percentuale.

Nella seconda situazione, mettiamo per iscritto una strategia con la quale stabiliamo di investire 1500 euro in Bitcoin utilizzando una strategia PIC, effettuando quindi l'intero investimento in un'unica soluzione, e di proseguire con un investimento di 1000 euro in Ethereum e 500 euro in Ripple adottando il metodo PAC. Stabiliamo inoltre le percentuali di allocazione del capitale totale: 50% bitcoin, 35% Ethereum, e 15% Ripple.

La differenza di rendimento tra i due portafogli si vedrà, più che nel breve, nel lungo periodo. La corretta progettazione di un cryptowallet deve quindi basarsi su tre elementi: lo studio e l'analisi degli asset che si vogliono acquistare; la stipulazione di un insieme di regole da rispettare; e la redazione di un documento contenente informazioni e dettagli rilevanti. Se volessimo essere ancora più puntigliosi, dovremmo considerare altri quattro elementi: la quantità esatta di un certo asset, il prezzo attuale, il "prezzo di carico", e l'equity. Pianificare la quantità di coin detenute nel portafoglio, ci

consentirebbe di conoscere non solo la percentuale di allocazione del nostro capitale, ma anche l'esatta quantità dell'asset presente nel nostro portafoglio.

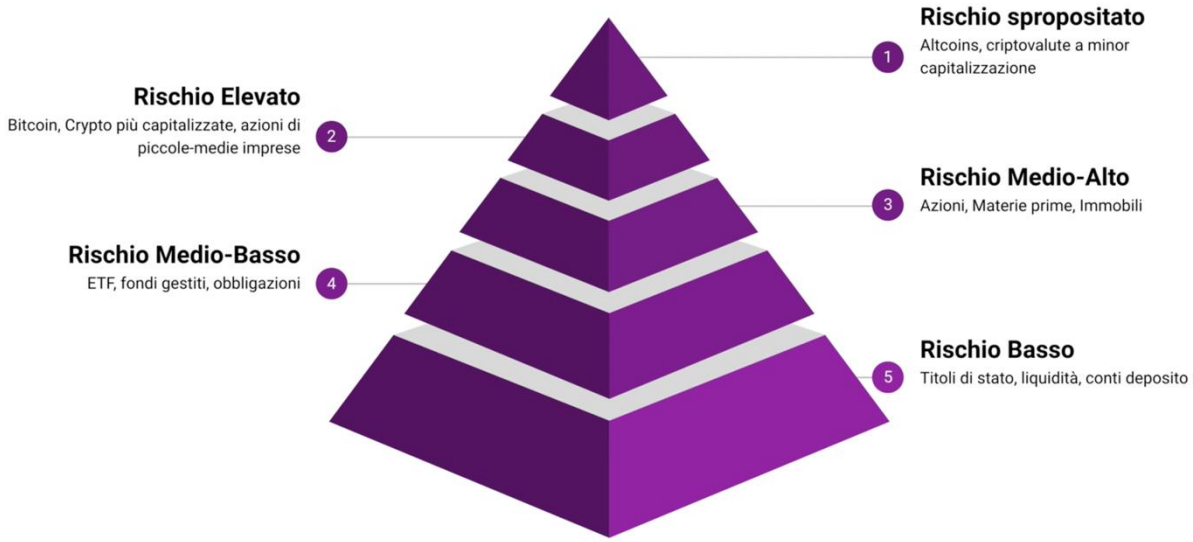
Il prezzo attuale permetterebbe invece di effettuare un confronto diretto tra le performance dei diversi asset detenuti nel nostro portafoglio, effettuando paragoni anche con le performance storiche delle singole criptovalute.

Il terzo elemento che darebbe uno sprint ulteriore al nostro portafoglio è il prezzo di carico, fondamentale per monitorare l'andamento dell'equity complessivo del portafoglio, e dell'equity delle singole criptomonete.

Per equity si intende il dato, o meglio ancora il numero, che riflette chiaramente l'andamento del nostro investimento, consentendoci di capire se stiamo guadagnando o perdendo capitale.

Ogni portafoglio ben organizzato, oltre all'insieme di elementi appena descritti, dovrebbe presentare un determinato grado di diversificazione. Per diversificazione si intende la riduzione del rischio dovuta alla presenza, in uno stesso portafoglio, di asset finanziari diversi tra loro, e caratterizzati da rendimenti indipendenti l'uno dall'altro. L'unico modo per far fronte al rischio di volatilità, e alle fluttuazioni continue dei prezzi delle criptovalute, è quello di diversificare il portafoglio investendo in monete virtuali il più possibile diverse tra loro. Ad esempio, se acquistassimo Bitcoin ed Ethereum, dal momento che tra le due valute esiste una certa correlazione nei rendimenti (al crescere del prezzo di una si verifica un apprezzamento dell'altra), la diversificazione sarebbe sicuramente minore rispetto alla situazione in cui decidessimo di acquistare Bitcoin e Solana. Attenzione però, a non confondere il concetto di diversificazione con il concetto di dispersione: sovraccaricare il portafoglio con asset diversi senza un criterio preciso, significa adottare una strategia caotica e mal progettata. Una diversificazione corretta, non deve quindi avvenire tramite una sovra-frammentazione del capitale, bensì attraverso uno schema ben preciso e secondo criteri logici e ragionati. Supponiamo allora di utilizzare uno schema piramidale. Al vertice della piramide si posizionano i titoli a rischio massimo, mentre alla base della piramide si pongono i titoli a rischio minimo. Nel mezzo della piramide troviamo tre fasce di rischio: rischio elevato, rischio medio-alto, e rischio medio basso. La piramide alla quale facciamo riferimento si compone perciò di cinque livelli: i due estremi massimo e minimo, e i tre livelli intermedi.

Figura 1.3, fonte: The Crypto Gateway



Ogni portafoglio dovrebbe essere strutturato in modo tale da presentare titoli appartenenti a ciascun livello della piramide, in percentuali diverse. Ad esempio, sarebbe corretto comporre il portafoglio nel seguente modo: il 40% del capitale di investimento dovrebbe essere destinato ad attività a basso rischio come titoli di stato o conti deposito; il 30% dovrebbe essere investito in titoli a rischio medio-basso come EFT o fondi gestiti; il 15% in azioni o sul mercato immobiliare, o comunque per titoli di rischio medio-alto; il 10% in attività a rischio elevato come, appunto, le criptovalute ad alta capitalizzazione e facilmente monitorabili (Bitcoin, Ethereum, ecc…); e il restante 5% in attività di rischio massimo come le altcoins o le criptovalute a bassa capitalizzazione. Ovviamente, queste percentuali possono e devono variare da soggetto a soggetto, in base alla propensione al rischio di ognuno. Per concludere, è possibile affermare che oltre alla prudenza e all'adozione delle dovute precauzioni per l'utilizzo delle criptovalute, è fondamentale che nelle operazioni di criptoinvestimento ogni cosa venga pianificata, e che nulla sia lasciato al caso. Strategie confusionarie e mancanza di obiettivi ben definiti sono i due elementi che più facilmente potrebbero condurre a ingenti perdite di capitale. Pianificazione, programmazione e fissazione di regole precise, sono invece le chiavi per intraprendere operazioni di investimento di successo e redditizie.

CAPITOLO 3: COMPONENTE PSICOLOGICA NEL CRYPTOTRADING

3.1 Premessa

La psicologia è la scienza che studia il comportamento umano e che analizza ed interpreta i processi psichici che stanno alla base di ogni nostra azione.

La componente psicologica è presente in tutto ciò che facciamo, diciamo o pensiamo, in maniera conscia o inconscia, e da essa dipende fortemente l'esito di qualunque nostra decisione. Pertanto, avendo descritto le molteplici insidie e opportunità insite nel mondo delle criptovalute, è fondamentale precisare che chiunque intenda operare in questo settore agisca sempre, per quanto possibile, in condizioni mentali e psicologiche ottimali.

In questo capitolo andremo ad esaminare i vari modi in cui la mente umana influisce e determina l'esito delle decisioni di investimento degli individui, focalizzando la nostra analisi su un'attività oggi molto diffusa soprattutto nel settore delle criptovalute: il trading.

Per cominciare, è necessario soffermarsi sulla distinzione tra investimento e trading. La principale differenza tra i due concetti, risiede nel cosiddetto *timeframe*, ovvero il lasso di tempo dell'operazione. Mentre l'investimento prevede timeframe più lunghi, e quindi operazioni a medio-lungo termine, per trading intendiamo un'operazione a breve o brevissimo termine. Molte piattaforme di trading e strumenti di analisi, consentono infatti di effettuare micro-operazioni di durata anche pari a un minuto. Ovviamente, la scelta di effettuare un investimento, o di operare su piattaforme di trading, spetta sempre a colui che decide di esporre al rischio di perdita il proprio capitale. Il trader di criptovalute, è quindi colui che effettua in nome proprio operazioni di compravendita di monete virtuali a breve (o brevissimo) termine.

Come affermato da uno dei più grandi esperti della *"Trading psichology"*, Mark Douglas, nella prefazione del suo libro-manuale *"Trading in the Zone: master the market with confidence, discipline and a winning attitude"*, «l'obiettivo di ogni trader è quello di ottenere profitti su base regolare, eppure sono così poche le persone che fanno davvero soldi con costanza come trader. Per me, il fattore determinante è quello psicologico: i vincitori costanti pensano in modo diverso da tutti gli altri.» (Douglas M., 2001). La vera chiave del successo di un trader, risiede quindi nel modo di pensare, ed è proprio la componente psicologica a fare la differenza nel lungo periodo.

Gli aspetti da considerare nella sfera psicologica di un trader sono molteplici, e riguardano non solo la personalità dell'investitore stesso, ma anche le scelte effettuate dagli altri, e il peso con cui esse possono influenzarlo. L'attività di trading, soprattutto se svolta quotidianamente e con ampia

frequenza, rappresenta una fonte di stress estremamente rilevante per il trader. Se lo stress dovuto ad ansie, preoccupazioni, ed eventuali perdite, non viene metabolizzato e arginato adeguatamente, può portare il trader a compiere errori di valutazione e di gestione del patrimonio che potrebbero rivelarsi deleteri. Gli elementi che costituiscono, nel loro insieme, la componente psicologica che determina l'agire di ogni individuo, sono principalmente quattro: bias cognitivi; euristiche; rischi emozionali; autodisciplina e assunzione delle responsabilità. Ognuno di questi fattori merita di essere analizzato singolarmente per comprendere il ruolo fondamentale che gioca nel processo decisionale di un soggetto operante nel trading delle criptovalute.

3.2 Bias cognitivi

Partiamo quindi dall'analisi di uno degli elementi che maggiormente influenzano le nostre decisioni dal punto di vista psicologico: il bias cognitivo. Per bias cognitivo si intende, semplicemente, una distorsione mentale della realtà. Si tratta di un pregiudizio sviluppato a livello cognitivo e formulato sulla base dell'intreccio di una serie di informazioni in nostro possesso, ma che effettivamente non presentano alcuna correlazione o nesso logico oggettivo tra loro (Cannito L., 2014). Il nostro cervello tende quindi a dare un'interpretazione di queste informazioni e a legarle insieme in maniera spesso irrazionale. L'estrema soggettività delle interpretazioni e l'irrazionalità del legame che creaimo tra le informazioni di cui disponiamo, ci portano a costruire una percezione distorta della realtà che a sua volta influenza e determina le nostre decisioni. Dal punto di vista di un trader, l'unico modo per evitare che queste deformazioni abbiano ripercussioni incorregibili sul proprio operato, è quello di conoscere le diverse tipologie di bias che la propria mente può generare.

Esistono numerosi tipi di bias cognitivi, e da alcune ricerche è emerso che la nostra mente è in grado di sviluppare fino a 100 bias cognitivi differenti. Possiamo però operare una classificazione dei bias distinguendo quattro macrocategorie: i wish biases, cioè distorsioni della realtà causate dai nostri desideri; gli anchoring biases, che riguardano l' "ancoraggio" della nostra mente ad un punto di riferimento che influenza la nostra scelta; i cost biases, che riguardano una percezione errata del valore dei costi; e i framing biases, ovvero percezioni errate della realtà dovute al contesto in cui ci troviamo.

In ognuna di queste quattro macroclassi di bias cognitivi, rientrano bias differenti l'uno dall'altro, e che possono manifestarsi più o meno frequentemente. I bias cognitivi che maggiormente ricorrono nel campo del trading, sono i seguenti: l' *"hindsight bias"*; l' *"hot hand bias"*; l'eccessivo ottimismo; e l' *"overconfidence"*. L'hindsight bias (in italiano "bias del senno di poi"), è una percezione distorta della realtà che ci induce a pensare che il verificarsi di un evento già accaduto potesse essere previsto

con facilità, quando in realtà le probabilità che la nostra previsione fosse esatta erano basse. Ad esempio un trader, una volta osservato il crollo del valore di una determinata criptovaluta, potrebbe erroneamente pensare che quell'evento potesse essere previsto anticipatamente, anche se effettivamente le sue possibilità di pronosticarlo erano scarse.

L' "hot hand bias", ovvero il "bias della mano calda", è la convinzione (sbagliata) che una serie di vincite possa essere seguita da ulteriori vincite continue. Nel trading, questo tipo di certezza rappresenta un pericolo da non sottovalutare, poiché un trader, dopo aver registrato un filone di trade positivi, potrebbe farsi prendere la mano e aumentare in maniera smisurata e irrazionale il livello di rischio delle proprie operazioni. Al contrario invece, dopo una "streak" di trade vincenti, sarebbe bene fermarsi e tornare con i piedi per terra senza lasciarsi condizionare da un eccessivo entusiasmo e da convinzioni irrazionali.

Un altro bias da tenere in considerazione è quello dell'eccessivo ottimismo, che consiste nel pensare, senza alcuna logica di fondo, che i risultati positivi si verifichino con maggior frequenza rispetto a quelli negativi. Un individuo che opera nel campo del trading deve essere sempre consapevole del fatto che, a parità di condizioni, un evento favorevole può verificarsi con le stesse probabilità di un evento sfavorevole.

Il quarto ed ultimo bias ricorrente che merita di essere analizzato più nel dettaglio, è quello dell' "overconfidence". Si dice *"overconfident"* colui che sovrastima le proprie abilità, capacità e conoscenze. In un settore come quello del criptotrading, caratterizzato da elevata volatilità ed incertezza, adottare un simile atteggiamento potrebbe risultare controproducente, in quanto la sopravvalutazione di sé stesso e dei propri mezzi, porterebbe il trader ad innalzare in maniera eccessiva l'asticella del rischio delle proprie operazioni.

Tutti i bias cognitivi che abbiamo analizzato in questo paragrafo, costituiscono una "strada sterrata" per coloro che operano nel campo del trading, e conoscerli nel dettaglio è l'unico modo per limitarne, del tutto o in parte, gli effetti negativi.

3.3 Euristiche

Oltre ai bias cognitivi, un altro driver importante delle decisioni di trading nel settore delle criptovalute, è quello delle euristiche. Esse sono scorciatoie mentali di cui il cervello umano si serve per facilitare e velocizzare un determinato processo decisionale (Kahneman D., Tversky R., 1974). Ipotizziamo il caso in cui un individuo abbia come unico obiettivo quello di prendere una decisione che gli consenta di risolvere un problema nel minor tempo possibile. Non importa come, o con quali mezzi egli riuscirà a raggiungere il suo obiettivo, l'unica cosa che conta è raggiungerlo. L'euristica,

è esattamente l'espediente mentale di cui l'individuo si servirà per perseguire il suo fine. Le informazioni di cui il soggetto dispone, vengono organizzate ed elaborate dal cervello in maniera rapida e spesso irrazionale, in modo tale che il processo decisionale termini nel più breve tempo possibile. Il problema insito nel concetto di euristica, è legato proprio all'ampio spazio lasciato all'irrazionalità. Dal momento che queste "approssimazioni mentali" vengono sviluppate in maniera inconscia dal nostro cervello, evitarle è estremamente difficile, e le probabilità che ci portino a compiere la scelta sbagliata (o non ottimale) ed errori di valutazione, sono elevate.
Mentre un bias cognitivo può essere individuato ed arginato, e i relativi effetti negativi possono essere limitati, un processo euristico è imprevedibile, e le sue conseguenze, positive o negative, si conosceranno solo dopo averlo adottato. Ciò che però è sicuro, è che nel trading il miglior sentiero percorribile è quello dell'analisi numerica dei dati che si hanno a disposizione. Se il nostro cervello può indurci a compiere scelte sbagliate per via di un'elaborazione illogica delle informazioni, l'analisi numerica e finanziaria non lasciano spazio ad irrazionalità ed incertezza, e rappresentano pertanto alcuni dei fondamentali strumenti di cui un trader dovrebbe sempre servirsi nelle sue operazioni.

3.4 Rischi emozionali

Ognuno di noi, durante la giornata, è influenzato da innumerevoli fattori e da altrettanti input derivanti dall'ambiente in cui vive. Tutti questi stimoli provenienti dall'esterno, generano in noi emozioni variabili, che inevitabilmente influenzano in maniera decisiva il nostro modo di pensare e di agire. Pertanto, un elemento che incide fortemente sulle scelte operative dei traders nel settore delle criptovalute è il rischio emozionale. Si utilizza il termine "rischio", proprio perché le emozioni accumulate durante la giornata (o in un arco di tempo più o meno lungo), possono rappresentare un serio pericolo per il trader, se non vengono gestite in maniera corretta. Quante volte accade infatti, che i sentimenti e le emozioni che proviamo in un determinato momento della giornata ci portino ad effettuare scelte e decisioni che in un altro momento non avremmo fatto? Ogni nostra decisione è influenzata dal nostro momentaneo stato d'animo.
Si pensi dunque a un trader, in procinto di decidere se "aprire" o meno una posizione, e quindi se investire o meno il suo capitale. Le emozioni che il trader ha accumulato durante l'arco della giornata, determinano il suo mindset, influenzando aspetti fondamentali come: propensione al rischio; scelta del timeframe di investimento; ammontare di capitale investito; ecc…
L'emozione forse più frequente nelle operazioni di trading è la paura. Soprattutto agli inizi dell'esperienza di un trader, la paura di perdere il proprio capitale è elevatissima. Come detto più volte però, tramite razionalità e pianificazione, è possibile ridurre i timori e le preoccupazioni

scaturite dalle continue oscillazioni dei prezzi delle criptovalute. Uno dei principali modi per contrastare le paure legate alla volatilità dei prezzi nel trading, potrebbe essere quello di impostare un *set-up* (una strategia) più prudente, basato su timeframe più lunghi, e su un livello di propensione al rischio medio-basso. Attenzione però: ogni operazione nel criptotrading dipende da diversi fattori, e soprattutto dalla natura della specifica criptovaluta, e pertanto elementi come timeframe e propensione al rischio, rappresentano solo due dei principali aspetti su cui bisognerebbe fare leva per ridurre il timore legato all'incertezza di questo settore.

Ci sono altri innumerevoli stati d'animo che possono determinare il comportamento e le decisioni di un trader, ma bisogna essere consapevoli del fatto che la bravura di un operatore consiste proprio nel saper tenere alla larga qualsiasi tipo di emozione, positiva o negativa che sia. Nel lungo periodo, freddezza e lucidità nell'atto operativo sono le caratteristiche che rendono un trader vincente.

3.5 Autodisciplina e assunzione delle responsabilità

Un'altra caratteristica che determina il successo di un trader è quella dell'autodisciplina. L'autodisciplina, a differenza di come molte persone sostengono, non è un tratto proprio della personalità di un individuo. Essa non è una caratteristica innata, ma si sviluppa con il tempo, in base ad una serie di eventi passati, o sulla base della specifica educazione che una persona riceve fin dall'infanzia. Per autodisciplina, si intende piuttosto la tecnica mentale che consente ad un individuo di focalizzare la propria mente su un determinato obiettivo, anche quando stimoli e impulsi mentali, inducono il cervello a seguire un'altra direzione. Si tratta quindi di un processo mentale attraverso il quale un soggetto reindirizza la propria attenzione sul ciò che vuole realizzare o raggiungere, senza farsi influenzare da distrazioni o pensieri conflittuali.

Nel trading, questo aspetto è fondamentale. In questo tipo di attività infatti, il mercato scandisce i tempi e i ritmi dell'operatività dei trader, i quali devono adeguarsi senza lasciare nulla al caso. La vita di un trader dotato di autodisciplina è fatta di rinunce e sacrifici, di orari sballati e impegni rimandati, al fine di adeguarsi ai ritmi incalzanti e spesso imprevedibili del mercato. Si pensi ad esempio ad un trader che, per comprendere l'andamento di una determinata criptovaluta, ha bisogno di monitorare i mercati esteri la cui apertura è prevista in orari per lui scomodi come le quattro del mattino. Il trader non potrà rimandare ad un altro orario il monitoraggio di quel mercato, perché spesso le modificazioni dei prezzi si verificano frequentemente anche nell'arco di un'ora. Rapidità e frequenza delle fluttuazioni dei prezzi delle criptovalute, richiedono altrettanta rapidità di risposta da parte dei trader, e chi non è in grado di sviluppare una forte autodisciplina, spesso viene tagliato fuori da un mercato che possiamo definire spietato.

L'autodisciplina è strettamente legata al concetto di assunzione delle proprie responsabilità. La capacità di indirizzare il cervello verso una determinata direzione, significa anche capire quali sono gli aspetti che contano e quelli che invece non meritano di essere considerati.
Il trader che, dopo una perdita, attribuisce le colpe a fattori esterni, o al caso, o alla sfortuna, o a cause a lui non imputabili, non è assolutamente dotato di autodisciplina, proprio perché lascia che il cervello segua una direzione diversa da quella che porta al suo obiettivo principale: comprendere realmente cosa è andato storto.
"Ammetto di aver sbagliato" è una delle frasi più complesse da pronunciare per una persona. Saper riconoscere le proprie colpe e i propri errori è sintomo di maturità e intelligenza, poiché richiede lo sforzo di mettere da parte l'orgoglio personale, e di accantonare elementi di analisi superflui. Il trader che riesce ad assumersi le proprie responsabilità per errori valutativi che hanno portato a risultati economici negativi, è in grado di riformulare la propria strategia in un modo diverso, e di comprendere cosa ha funzionato nel set-up precedente, e cosa invece è andato storto. È possibile pertanto affermare che autodisciplina e capacità di assumersi le proprie responsabilità, rappresentano per il trader elementi di crescita e maturità fondamentali, che possono aiutarlo a risollevare strategie economiche infruttuose, e a raggiungere importanti obiettivi in termini di profitto.

3.6 Gestione delle vincite e gestione delle perdite

Uno degli aspetti indubbiamente più critici nel trading di criptovalute, è quello della gestione delle vincite e della gestione delle perdite. Quali e quante sono le componenti mentali e psicologiche che determinano i metodi di gestione di una serie di operazioni positive o negative? Dare una risposta completa a questa domanda non è possibile, per il "semplice" fatto che la psicologia di ogni individuo è infinitamente complessa, e presenta combinazioni e intrecci di elementi estremamente variabili tra loro. È però possibile procedere con degli esempi, per avere chiare alcune situazioni che si verificano di frequente nel criptotrading.
Ipotizziamo che un soggetto abbia registrato in pochi giorni una serie di sei o sette vincite consecutive. Lo stato d'animo del trader sarebbe ovviamente positivo, e si tratterebbe del momento più rischioso per la formazione di bias cognitivi nella sua mente. Avendo registrato questa *streak* di operazioni positive, il trader potrebbe sviluppare il dannoso e già citato bias dell'overconfidence, che lo porterebbe a sopravvalutare le proprie abilità e capacità, oppure il bias della mano calda, con il quale sovrastimerebbe le probabilità di ulteriori vincite.
Supponiamo adesso che si verifichi la situazione contraria, ovvero quella in cui un individuo operante nel trading delle criptovalute subisca una serie di sei o sette perdite consecutive. In questo caso

potrebbero entrare in gioco fattori mentali come sconforto, paura di ulteriori perdite, smania di recuperare il capitale perduto, e altri elementi che rappresenterebbero per il trader stati d'animo negativi. Potrebbe addirittura accadere che l'individuo rinunci a prodeguire con la sua attività.
E allora come dovrebbe comportarsi un trader in queste situazioni? Quali dovrebbero essere le precauzioni da adottare per proseguire nella stessa direzione o per invertire la rotta? E soprattutto quanto capitale in più o in meno dovrebbe essere investito dopo una serie di vincite o di perdite?
Dal momento che più volte è stata sottolineata l'importanza dell'analisi razionale, basata su principi numerici e finanziari, la base per rispondere a queste domande è costituita dal cosiddetto "criterio di Kelly". Esso rappresenta il principio numerico su cui ogni trader dovrebbe fare affidamento sia prima che dopo ogni sua operazione. Il criterio di Kelly consente di conoscere, stimando le probabilità di vincita e di perdita, la percentuale ottimale del capitale di rischio che si intende utilizzare nell'operazione. La formula è la seguente:

$$F^* = \frac{bp-q}{b} = \frac{p(b+1)-1}{b}$$

*F** è la percentuale di capitale di rischio ottimale da investire nell'operazione di trading; b rappresenta il guadagno in caso di vincita; p è la probabilità di vincita (il cosiddetto *"win rate")*; e q è la probabilità di perdita pari anche a *1-p*.
Questo criterio rappresenta un metodo razionale attraverso il quale il trader è in grado di capire esattamente quanto capitale di rischio investire in una determinata operazione di trading, e dovrebbe essere utilizzato dopo ogni vincita e dopo ogni perdita.
Il criterio di Kelly è però un metodo statico, basato sulla singola operazione.
Un metodo dinamico, che consente invece di gestire una serie di vincite o di perdite, e che non si basa esclusivamente sulla singola operazione, è quello del risk management. Questo sistema prevede che, dopo una *streak* di vincite o di perdite consecutive, il trader effettui un adeguamento del capitale di rischio che da adesso in poi chiameremo R. La regola di base, prevede che dopo una serie di vincite, un trader è legittimato ad aumentare la propria propensione al rischio. Dopo una serie di perdite invece, il trader dovrebbe ridurre il rischio per evitare ulteriori perdite di capitale. L'adeguamento del capitale a rischio può essere di due tipi: lineare o esponenziale. L'adeguamento lineare consiste nell'aumentare o diminuire il capitale esposto al rischio di una determinata quantità a partire da una determinata vincita consecutiva. Per adeguamento esponenziale si intende invece l'aumento o la diminuzione del capitale a rischio di una specifica percentuale dopo una determinata serie di vincite o di perdite. La differenza sta quindi nella velocità con cui il capitale a rischio aumenta o diminuisce:

nell'adeguamento esponenziale la velocità di incremento o riduzione di R sarà maggiore rispetto a quella dell'adeguamento lineare. Per comprendere meglio questo metodo, è necessario ricorrere alla descrizione di due situazioni: un primo caso in cui si verifica una serie di vincite; e un secondo caso in cui si verifica una serie di perdite. Nella prima situazione si parla dunque di "*compounding wins*" ("vittorie combinate"). Ipotizziamo che, dopo la quinta vittoria consecutiva, un trader decida di aumentare R secondo un adeguamento lineare, di una quantità pari a 0,5. Mentre fino alla quinta vittoria il trader ha accumulato 5R (W1=R; W2=R; W3=R; W4=R; W5=R), dalla sesta vittoria consecutiva ottiene da ogni win, anziché R, 1,5R (perciò W1=R; W2=R; W3=R; W4=R; W5=R; W6=1,5R; W7=1,5R; …). In questo modo, il trader è in grado di ammortizzare le eventuali perdite successive con il margine ulteriore guadagnato dalla sesta vittoria in poi. Qualora, invece, il trader decidesse di ricorrere ad un adeguamento esponenziale del capitale, il capitale di rischio R crescerebbe, dalla sesta vittoria consecutiva in poi, di una determinata percentuale fissa, pari ad esempio al 50%: W1=R; W2=R; W3=R; W4=R; W5=R; W6=(1+50%)R; W7=(1,5+50%)R; W8=(2+50%)R. Come possiamo notare, la velocità di incremento di R è maggiore nel caso in cui venga scelto il metodo di adeguamento esponenziale.

Nella seconda situazione ipotizzata invece, deve verificarsi un *"cutting losses"* ("taglio delle perdite"), e la dinamica è la stessa prevista per il caso delle "*compounding wins"*. Il trader può decidere di effettuare un taglio lineare di R, riducendolo di -0,5 a partire dalla sesta perdita consecutiva in poi (L1=-R; L2=-R; L3=-R; L4=-R; L5=-R; L6=-1,5R). In caso di scelta dell'adeguamento esponenziale invece, con una riduzione del 50% a partire dalla sesta perdita consecutiva, si avrebbe: L1=-R; L2=-R; L3=-R; L4=-R; L5=-R; L6= (-1 - 50%)R; L7=(-1,5 - 50%)R;…

La gestione delle serie di vincite o di perdite dal punto di vista numerico è ovviamente fondamentale, ma è necessario tenere a mente che oltre alla razionalità insita nei metodi appena descritti, influisce pesantemente sulla gestione anche la componente psicologica, spesso irrazionale. Il trader, è quindi chiamato a svolgere un lavoro di metabolizzazione mentale, per essere pronto a gestire nel miglior modo possibile gli esiti positivi o negativi delle sue operazioni.

Per una buona gestione delle vincite, è sufficiente che il trader non si faccia "prendere la mano" e che non cada nei suddetti bias cognitivi, controllando il suo entusiasmo e soprattutto evitando di sottovalutare i rischi che il mercato delle criptovalute presenta.

Per quanto riguarda invece la gestione delle perdite, la situazione è più complessa, in quanto il trader dovrebbe tener conto di più aspetti diversi. L'individuo che registra una o più perdite, deve adotttare un metodo di gestione mentale dei risultati negativi basato su quattro regole principali.

La prima regola consiste nel saper gestire il rischio di ulteriori operazioni in modo sano. Dopo una perdita, è il caso di limitare il rischio delle successive operazioni, cercando di ridurlo in maniera consapevole.

La seconda regola consiste nell'introduzione del cosiddetto stop-loss, ovvero uno strumento che consente di limitare le perdite. Prima di aprire una posizione, il trader dovrebbe sempre fissare lo stop-loss ad un determinato livello di prezzo che, una volta toccato, chiude automaticamente la posizione evitando che si verifichino ulteriori perdite.

La terza regola prevede l'accettazione delle perdite. Un trader che accetta un determinato livello di rischio non può non accettare le perdite subite. Essere in grado di riconoscere i propri errori, è uno degli aspetti più importanti per la crescita di un trader.

Quarta ed ultima regola: sapersi fermare per un periodo di tempo limitato o in maniera definitiva. Dopo una perdita, il trader deve cercare di allontanare lo stress accumulato e la delusione, e l'unico modo per farlo è quello di prendersi una pausa. Una volta arginate le emozioni negative dovute alle perdite, il trader sarà in grado di operare in maniera più lucida e profittevole.

È chiaro quindi che la gestione delle perdite e delle vincite è probabilmente l'aspetto più critico e complesso per un trader, e rappresenta sicuramente l'attività in cui la componente psicologica gioca il ruolo prevalente. Tuttavia, nonostante le difficoltà, l'esperienza è portatrice di conoscenza e consapevolezza, e pertanto un trader che più volte ha saputo gestire correttamente situazioni favorevoli e sfavorevoli, vedrà ogni evento futuro con un occhio più saggio e più accorto, ottenendo importanti traguardi in termini di profittabilità delle proprie operazioni.

CONCLUSIONI

La scoperta del Bitcoin di Satoshi Nakamoto, ha segnato l'inizio di una rivoluzione nel settore bancario e dell'intermediazione finanziaria, e non è un caso che questa scoperta sia avvenuta proprio a seguito di una delle crisi economiche maggiori mai registrate, quella del 2008. Nakamoto ha voluto dar vita ad un processo di rimpiazzo del sistema finanziario tradizionale - ormai caratterizzato da un'estrema rigidità dovuta al controllo e alla supervisione di banche e istituti di intermediazione finanziaria - con un sistema nuovo, decentralizzato e basato su un sistema network peer-to-peer capace di garantire agli utenti una maggiore libertà e trasparenza. Eliminare gli elementi di corruttibilità e centralizzazione del sistema finanziario tradizionale è, secondo Nakamoto, il passo da compiere per rendere più libero, rapido e trasparente, il processo di trasmissione di ricchezza tra gli individui.

Tuttavia, un cambiamento di tale portata sembra essere al momento qualcosa di irrealizzabile, non tanto per la mancanza di potenzialità delle criptovalute e dei nuovi strumenti che si pongono alla base di questo settore, quanto per il complesso e ad oggi impossibile superamento del pensiero radicato nella mente delle persone. Infatti, nonostante il carattere di decentralizzazione delle criptovalute e il sistema blockchain possano effettivamente rendere più trasparenti le operazioni di scambio di denaro tra gli individui, il problema insormontabile è che essenzialmente la gente non si fida. Sapere che dietro lo scambio di criptovalute non vi sia alcuna figura che possa fare da garante, è un fattore di destabilizzazione per le persone, che quindi continuano a preferire un sistema sicuramente più obsoleto e vulnerabile, ma che almeno garantisca un controllo e un monitoraggio totale delle operazioni.

Peraltro, la varietà di rischi connessi all'utilizzo delle criptovalute, rende il piano di Nakamoto ancora meno realizzabile. La rischiosità del settore delle criptovalute si sta pian piano radicando nel pensiero comune, e questo è dovuto soprattutto all'estrema lentezza del processo di formulazione di una disciplina che po. Soprattutto in tema di riciclaggio del denaro illecito e finanziamento del terrorismo, la disciplina odierna risulta ancora troppo arretrata, e ciò contribuisce a danneggiare gravemente la reputazione delle criptovalute, che si presentano come una risorsa importante per le organizzazioni criminali.

Anche i rischi informatici contribuiscono ad amplificare ulteriormente il problema reputazionale delle valute virtuali e delle piattaforme su cui esse vengono scambiate. La domanda è: perché una persona dovrebbe fare affidamento su una piattaforma di scambio di criptovalute facilmente hackerabile ed esposta a furti di chiavi crittografiche? I numerosi casi di attacchi hacker subiti dalle piattaforme di exchange, hanno determinato ingenti perdite non solo di criptovalute, ma anche di chiavi

crittografiche private necessarie per effettuare gli scambi. Questo ha contribuito ad aumentare in maniera significativa il grado di insicurezza e scetticismo degli utenti.

Nonostante ciò, le criptovalute restano strumenti che, se utilizzati in maniera consapevole, possono portare ad ottenere importanti guadagni sia nel breve che nel lungo periodo. È importante però, che si dia peso alla parola "consapevolezza". Tutti i concetti che sono stati affrontati in questa tesi, a partire dai diversi tipi di criptovalute, passando per le varie tipologie di rischio, fino ad arrivare agli elementi psicologici che giocano un ruolo fondamentale nell'attività di trading di criptovalute, costituiscono la *"Crypto-Awareness"* che un individuo dovrebbe sviluppare per poter utilizzare le valute virtuali in maniera proficua. Promuovere un'istruzione completa su questi strumenti, e sottoporli ad una valida regolamentazione, potrebbe essere la chiave per costruire un futuro in cui monete centralizzate e decentralizzate coesistano. Già alcuni istituti di credito e diversi negozi e piattaforme e-commerce stanno adottando le criptovalute come metodo di pagamento alternativo alla valuta nazionale; diversi paesi stanno lavorando per avviare iniziative importanti in ambito criptomonetario. Le criptovalute, non sono quindi strumenti da respingere, ma piuttosto da conoscere e approfondire, per comprenderne il potenziale e sfruttarli al meglio nella nostra quotidianità. Il loro processo di sviluppo e diffusione è ancora allo stadio iniziale, e i passi da compiere sono molti e complessi, ma alla fine, come sempre, l'esito del percorso di innovazione dipenderà principalmente da noi e dalla nostra società.

BIBLIOGRAFIA

AMATO M., FANTACCI L., *Per un pugno di bitcoin. Rischi e opportunità delle monete virtuali,* Università Bocconi Editore, 2018.

BAKER M., RUBACK R. S., WURGLER J., *Behavioral Corporate Finance: A Survey*, in NBER Working Paper No. 10863, 2014

BANCA D'ITALIA, *Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità Europee,* 19 Marzo 2018.

BELLEMO G., *Blockchain e criptovalute: rischi e opportunità,* per Università Ca' Foscari Venezia, 11 Settembre 2018.

BELLINI M., *Blockchain: cos'è, come funziona e gli ambiti applicativi in Italia,* in Blockchain4Innovation, 2020.

BELLINI M., *Mining criptovalute e bitcoin: cos'è, come farlo (cloud e non) e guadagni,* in Blockchain4Innovation, 14 Aprile 2020.

BERRETTI A., *Blockchain e mining, ecco come funziona: dietro le quinte della tecnologia*, in agendadigitale, 6 Giugno 2018.

BOHR J., BASHIR M., *Who Uses Bitcoin? An exploration of the Bitcoin community*, Institute of Electrical and Electronics Engineers Inc., Toronto, 2014.

BORSA ITALIANA, *Bitcoin: cos'è e come funziona,* FTA Online News, Milano, 8 Gennaio 2019.

BURLONE P. L., DE CARIA R., *Bitcoin e le altre criptomonete,* Istituto Bruno Leoni, aprile 2014.

CANNITO L., *Cosa sono i bias cognitivi?,* 2017.

CAPOTI D., DE LORENZO A., MAGGIORE M., *Tutto su bitcoin. Guida pratica per investire in criptovalute,* Hoepli, Milano, 2018.

COINBASE.COM, *Cos'è Ethereum?,* 2021.

COINBASE.COM, *Cos'è la crittografia?,* 2022.

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

CONSOB, *Errori e trappole comportamentali.*

CONSOB, *Le criptovalute: che cosa sono e quali rischi si corrono.*

CONSOB, BANCA D'ITALIA, *Consob e Banca d'Italia mettono in guardia contro i rischi insiti nelle crypto-attività,* Roma, 28 Aprile 2021.

CRIPTOINVESTIRE.COM, *Crittografia. La sicurezza delle Blockchain,* 2018.

DELL'OSSO A.M., *Il reato di autoriciclaggio: la politica criminale cede il passo a esigenze mediatiche ed investigative*, in «Riv. Italiana di Dir. e Procedura Penale», 2015.

DOUGLAS M., *Trading in the zone. Domina il mercato con sicurezza, disciplina, e una mentalità vincente,* 1 Gennaio 2001

ESMA (EUROPEAN SECURITIES AND MARKETS AUTHORITY), *Avviso. L'ESMA, l'ABE e l'EIOPA informano I consumatori sui rischi delle valute virtuali,* 2017.

EUROPEAN CENTRAL BANK, *Virtual currency schemes – a further analysis*, ECB, 2018.

EUROPEAN CENTRAL BANK, *Occasional paper series. Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area*, Settembre 2020.

GENNAI A., *Cosa sono e come funzionano le criptovalute?*, in IlSole24ore, 1 Ottobre 2018.

IASSP, *Il ruolo delle criptovalute nel riciclaggio di denaro,* 30 Ottobre 2021.

KAHNEMAN D., TVERSKY R. H., *Judgement under Uncertainty: Heuristics and Bias*, Science, New Series, Vol. 185, No. 4157, p. 1124-1131, 1974

LEMME G., PELUSO S., *Criptomoneta e distacco dalla moneta legale: il caso bitcoin,* in Rivista di Diritto Bancario, 2016.

LINCIANO N., *Errori Cognitivi e Instabilità delle Preferenze nelle Scelte di Investimento dei Risparmiatori Retail*, Quadri di Finanza, CONSOB, N. 66, 2010

MAIMERI F., MANCINI M., *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, in Quaderni di Ricerca Giuridica della Consulenza Legale, Settembre 2019.

PERRONE M., *Come creare un portafoglio cripto diversificato,* in criptovaluta.it, 24 Maggio 2021

PERUGINI M. L., *Monete digitali alternative:ripple,* 6 Febbraio 2018.

QUANTALYS.IT, *Finanza comportamentale: il ruolo dell'approccio euristico nel processo decisionale,* 6 Giugno 2016.

RANDO A., *Crittografia, cos'è, a cosa serve, perché non se ne può fare a meno*, in Blockchain4Innovation, 21 Maggio 2020.

RASERA S., *Stablecoin: percezione, elusione e modellizzazione della volatilità*, per Università Ca' Foscari, 22 Luglio 2021.

ROLLING STONE, *Satoshi* Nakamoto*, l'uomo senza volto che ha inventato i Bitcoin*, 21 Novembre 2021.

SALAMI I., *Decentralised Finance: The Case for a Holistic Approach to Regulating the Crypto Industry,* 19 Novembre 2020.

SEGENDORF B., *What is Bitcoin*, in EconomicReview, Febbraio 2014.

THECRYPTOGATEWAY.IT, *Come costruire un portafoglio di investimento in criptovalute*, 2021

THECRYPTOGATEWAY.IT, *Trading consapevole – Trappole emotive. Come non perdere soldi a causa di errori psicologici ed emotivi*, 2021

VAGO C., VILLANO D., *Storia del bitcoin: come è nato e cosa è diventato oggi,* in Valori: notizie di finanza etica ed economia sostenibile, 8 Febbraio 2021.

VERGINE S., BORTOLOTTI A., *Bitcoin, il futuro in blocchi,* in EconomiaComportamentale, 2021.