UNIVERSITÀ POLITECNICA DELLE MARCHE
FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea Magistrale in Scienze Economiche e Finanziarie:
Analista Finanziario

"ANALISI TEMATICA DELLE VALUTE VIRTUALI: PROCESSO DI SVILUPPO DI UNA CRIPTOVALUTA"

"THEMATIC REVIEW OF VIRTUAL CURRENCY: DEVELOPMENT PROCESS OF A CRYPTOCURRENCY"

Relatore: Chiar.mo
Prof. Marco Cucculelli

Tesi di Laurea di:
Yuri Kuci

Anno Accademico 2022 – 2023

SOMMARIO

INTRODUZIONE

Negli ultimi anni, protagonisti del macrocosmo economico, e non solo, sono stati travolti dall'interesse per le criptovalute: ad oggi si stima che circa 300 milioni di persone possiedano una qualsiasi criptovaluta, portando il settore ad una capitalizzazione massima di quasi 3 trilioni di dollari. Nonostante il mondo cripto-centrico sia da sempre "macchiato" da mitologia, hype e illiceità che ne offuscano il giudizio, le nuove valute virtuali hanno acquisito una notevole rilevanza nell'ambito finanziario e tecnologico grazie alle nuove opportunità e significative sfide da loro generate.

Decentralizzazione, blockchain, crittografia, anonimato e trasparenza: queste sono le principali caratteristiche che contraddistinguono le criptovalute dai tradizionali strumenti finanziari. L'analisi del processo di creazione e sviluppo delle valute virtuali è fondamentale per delinearne la natura e funzionalità, evidenziando le loro uniche dinamiche, sia come veicolo di investimento sia come catalizzatore di innovazione nel settore finanziario.

Verrà dunque svolta un'approfondita analisi tematica del dinamico mondo delle criptovalute: partendo dalle numerose definizioni delineate negli anni, verrà intrapreso un percorso in grado di illustrare i pilastri che sorreggono la struttura crittografica e i meccanismi che ne permettono il funzionamento. Successivamente verrà evidenziato l'impatto delle criptovalute sulla psicologia degli investitori e come tale fattore abbia influenzato il mercato. Infine, sarà illustrato il processo di creazione, sviluppo e aggiornamento di una valuta virtuale.

Questa "thematic review" potrebbe fornire preziose intuizioni non solo sull'architettura del settore ma anche sulla potenziale portata di nuove classi di attività finanziarie, che potrebbero emergere in futuro e rivoluzionare totalmente il panorama finanziario.

CAPITOLO 1: PANORAMICA SUL MONDO DELLE CRIPTOVALUTE

1.1 CONCETTUALIZZAZIONE DI MONETA E PARALLELISMI

Con il termine "moneta" si intende "qualsiasi oggetto o mezzo di scambio accettato da persone e/o intermediari finanziari per il pagamento di beni o servizi, e per il rimborso di debiti")[1]. Seguendo sempre Mishkin, sono necessari tre requisiti affinché qualcosa possa essere riconosciuto come moneta:

- **Unità di conto**: La moneta si usa per confrontare in maniera omogenea il valore di prodotti e servizi diversi tra loro, agevolando così le decisioni economiche e gli accordi contrattuali;
- **Riserva di valore**: La moneta permette di spostare nel tempo la quota di reddito che non viene utilizzata immediatamente per consumare beni e servizi. In altri termini, consente di conservare (risparmiare) una quota del reddito corrente per spenderlo in futuro;
- **Mezzo di pagamento**: La moneta può essere scambiata istantaneamente con beni e servizi: l'acquirente consegna moneta al venditore e in questo modo si libera da ogni obbligo nei confronti di quest'ultimo che, accettandola, ne riconosce il valore.[2]

[1] Mishkin, Frederic S. (2006). "*The Economics of Money, Banking, and Financial Markets"*, New York: Pearson Addison-Wesley.

[2] Banca D'Italia. *Le funzioni della moneta e le proposte di "moneta fiscale".*

La natura della moneta è mutata nel tempo. In origine era rappresentata dal baratto di merce, successivamente superata dall'inserimento di monete metalliche e banconote che potevano essere cambiate con una certa quantità di oro e argento. Le economie moderne si basano sulla moneta fiduciaria, ossia dichiarata a corso legale ed emessa da una Banca Centrale ma, diversamente dalla moneta rappresentativa, non convertibile in una quantità fissa di oro. Tuttavia, nel corso della storia sono emerse occasioni "emergenziali" nelle quali monete e altre tipologie di transazioni venivano a mancare ed erano sostituite da oggetti specifici, come per esempio, le sigarette tra i prigionieri nei campi di guerra durante la Seconda guerra mondiale.

Dunque, preziosi metalli quali monete d'oro e argento, oppure banconote rappresentanti tali metalli, possono soddisfare i requisiti per essere riconosciuti come moneta. L'assenza di questi elementi induce l'uomo a creare un nuovo sistema basato su elementi non tradizionali, come nel caso dell'isola di Yap 500/600 anni fa.

Il sistema monetario dell'isola Yap[3] viene citato allo scopo di poter fare un parallelismo con il mondo delle criptovalute e analizzare, sotto una lente meno tecnica, questo nuovo strumento finanziario.

Il sistema monetario precedentemente citato getta le proprie fondamenta sulla moneta Rai: dischi di pietra, solitamente calcite, a forma di ciambella, che variano dai 3.5 centimetri fino a 4 metri di diametro. Le pietre non sono estratte sull'isola Yap ma vengono lavorate e spedite da un'isola distante circa 450km: infatti per secoli le pietre hanno viaggiato in oceano aperto per poi esser scaricate sull'isola e collocate in posti

[3] Paul F. Gentle (2021) *"Stone Money of Yap as an Early form of Money in the Economic Sense"* Financial Markets, Institutions and Risks, Volume 5, Issue 2.

dove sarebbero potute restare per sempre. Dunque, come vengono utilizzate queste pietre per le transazioni? Come si identifica il possessore della pietra? Come vengono valutate? Tutte queste domande creano il parallelismo tra la moneta Rai e il funzionamento delle blockchain nel mondo delle criptovalute.

Una moneta Rai deve essere "minata" e rifinita (estratta dal terreno e lavorata); sarà successivamente caricata sull'imbarcazione, dovrà affrontare la traversata dell'Oceano Pacifico e infine posizionata nel luogo richiesto. Maggiore sarà la grandezza della pietra, maggiori saranno il lavoro e gli uomini incaricati per tutte le mansioni e maggiore sarà il valore della moneta Rai.

È lampante il paragone con le criptovalute anch'esse "minate" (metodo con cui vengono create nuove criptovalute) e messe in circolazione mediante ASIC (*application specific integrated circuit*), circuito ad altre prestazioni in grado di risolvere gli algoritmi di mining di una specifica criptovaluta. Anche in questo caso ci saranno dei costi relativi sia all'acquisto degli strumenti di mining, sia all'alimentazione e mantenimento degli strumenti. Parallelamente alle monete Rai, il processo di creazione e distribuzione delle criptovalute risulta complesso, dispendioso e "limitato", fattori che conferiscono il valore alla moneta virtuale.

Ritornando alla moneta Rai, possiamo notare come la maggior parte delle monete siano troppo grosse per essere scambiate o persino semplicemente spostate dopo esser state scaricate dalla nave. In tal caso, le monete vengono posizionate in luoghi particolarmente conosciuti affinché sia noto a chiunque che quella moneta appartiene ad un determinato membro dell'isola. Nel caso in cui la moneta venisse usata come mezzo di scambio o pagamento allora sarebbe trasferita direttamente la proprietà e tutta la popolazione

verrebbe a conoscenza di questo evento: è, paradossalmente, l'assenza di un sistema centralizzato incaricato alla gestione delle proprietà, a ridurre le possibilità di frode, in quanto la consapevolezza collettiva del villaggio relativa alla proprietà di una moneta governa il sistema di scambio dell'isola.

La semplicità di questo sistema è, incredibilmente, anche alla base del mondo delle criptovalute. Con l'esecuzione di una transazione, chiunque stia utilizzando la specifica criptovaluta riceverà una notifica dell'operazione: non è necessaria la tangibilità o fisicità della moneta affinché questa sia scambiabile.

La fiducia che gli operatori del sistema ripongono sull'esistenza e rilevanza di una moneta digitale è il pilastro che sostiene e conferisce valore a questo nuovo mondo.

1.2 OVERVIEW SULLA DEFINIZIONE DI CRIPTOVALUTE

A tal proposito è opportuna una descrizione dettagliata di cosa sia una criptovaluta, o ancor meglio, di come viene vista dai protagonisti del sistema economico e non solo.

Le criptovalute rappresentano un'area di elevato interesse pecuniario, numismatico, tecnologico e di investimento: l'indole lucrativa e l'esponenziale integrazione e crescita del settore, hanno permesso il raggiungimento di una capitalizzazione vicina ai 2,5 trilioni di dollari.

Una valuta emessa da uno stato o da un ente internazionale è caratterizzata da delineazione e regolamentazione dettagliata. Le criptovalute sono strumenti finanziari "indipendenti": non esiste un'unica definizione che possa racchiudere totalmente la sua essenza e che possa conciliare i diversi punti di vista dei soggetti interessati.

Secondo la Banca d'Italia[4], una criptovaluta costituisce uno strumento virtuale quale rappresentazione digitale di valore, utilizzata come mezzo di scambio o detenuta a scopo di investimento: non sono sottoposte ad emissione, garanzia e controllo da parte di Banche cùCentrali o autorità pubbliche.

Per esempio, La Bank of International Settlements (BIS) equipara i concetti di "valuta virtuale"[5], "valuta digitale[6]" e "criptovaluta", introducendo le caratteristiche che le contraddistinguono dalle valute tradizionali:

- Sono unicamente emesse in formato elettronico;
- Non sono emesse in una valuta nazionale e non sono legate a queste;
- Non rappresentano delle obbligazioni;
- Non sono definite da un valore intrinseco e dunque non genera un flusso di pagamenti;
- Vengono utilizzate per scambi peer-to-peer[7], ovvero in un sistema decentralizzato di scambi diretti tra gli utenti del sistema, scambi che avvengono mediante la tecnologia a registro distribuito[8];
- Possono essere considerate come un asset con proprietà simili alla moneta (come, per esempio, la possibilità di effettuare pagamenti). Il BIS individua le criptovalute come asset con caratteristiche uniche, sostenendo come le valute digitali siano in grado di sostituire la moneta elettronica;

[4] https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali/index.html.
[5] "Una valuta virtuale è una tipologia di moneta digitale non regolamentata, emessa e generalmente controllata dal suo sviluppatore con la finalità di essere accettata e usata all'interno di una comunità virtuale" European Central Bank (October 2012) *"Virtual currency schemes"*. ECB Report. 1–55.
[6] Bank of International Settlement 2015, *CPMI. Digital Currencies* /2018, *CPMI. Digital Currencies*.
[7] Rete informatica nella quale i computer degli utenti connessi fungono contemporaneamente da client e da server.
[8] Distributed Ledger Technology: sistema basato su un registro ("libro mastro") elettronico, distribuito ad un'ampia rete di nodi, i cui dati sono verificati, validati e protetti mediante l'adozione di algoritmi di consenso.

La BCE fa riferimento alle criptovalute come "sistema di valute virtuali decentralizzato e bi-direzionale[9]".

Il termine "sistema di valuta virtuale" è utilizzato come rappresentazione di un meccanismo intrinseco garante del trasferimento di valore agli strumenti digitali, indipendente da banche centrali e istituti di credito.

Anche l'International Monetary Fund non fornisce una rigorosa definizione di criptovaluta: secondo l'IMF, le criptovalute non sono generalmente interpretate come valute, bensì come asset e investimenti ad alto rischio[10].

Dal punto di vista del ministero delle finanze della Federazione Russa[11], "le criptovalute rappresentano una tipologia di asset digitale programmate e consolidate in un registro distribuito di transazioni digitali eseguite dagli utenti partecipanti, nel rispetto della regolamentazione per il mantenimento dei tale registro".

Come sostenuto in precedenza, il BIS prende in considerazione le criptovalute come un asset: secondo l'OECD[12] (Organization for Economic Cooperation and Development), gli asset sono entità con la funzione di riserva di valore e dai quali i proprietari possono trarre benefici economici detenendoli o utilizzandoli per un periodo di tempo.

Al contrario, le criptovalute non possono essere associate ad un risparmio sicuro in quanto non forniscono un costante flusso di pagamenti essendo privi di valore intrinseco.

[9] European Central Bank (February 2015) *"Virtual currency schemes: a further analysis"*. ECB Report:1–37.
[10] International Monetary Fund (2018). *"Money, transformed. The future of currency in a digital world. Finance and development"*;55(2).
[11] Ministry of Finance of Russia (January 2018). *"On Digital and Financial Assets".* Draft Federal Law of 05.22.2018
[12] OECD. Glossary of Statistical Terms (Assets).

Gli asset finanziari, invece, vengono qualificati dall'OECD come asset (viene confermata la definizione precedente) rappresentanti obbligazioni di qualcun altro, condizione che non viene riscontrata nell'inquadramento delle criptovaluta.

I dati di Howmuch.net[13] ci permettono di confrontare adeguatamente tutti gli elementi citati precedentemente:

Figura 1: Analisi comparativa tra criptovalute, valute tradizionali e asset

Features	Money	Assets	Financial assets	Cryptocurrencies
Store of value	Yes	Yes	Yes	No
Means of payment	Yes	No	No	Partially
Unit of account	Yes	No	No	No
Granting ownership	No	Yes	Yes	Yes
Providing the owner with economic benefits through storage or use	Possible*	Yes	Yes	Possible
Is the obligation of the other party	Yes	No	Yes	No
Information transfer and storage function	No **	No	No	Yes

Fonte: The Essence of cryptocurrencies: descriptive and comparative analysis. Finance: Theory and Practice

*supponendo sia aggregato monetario M0, il beneficio si riscontra in situazione di deflazione.
**fatta eccezione per la considerazione di "denaro forma primitiva di memoria" secondo la quale il possesso di denaro da parte di un agente economico sia la rappresentazione che questi abbia adempiuto coscienziosamente ai propri obblighi nei confronti della controparte.

Attualmente, le criptovalute svolgono parzialmente la funzione di mezzo di pagamento, essendo accettate da ristretti gruppi di agenti economici per l'acquisto di beni e servizi. Tuttavia, allo scopo di utilizzare un determinato strumento finanziario come mezzo di pagamento, è necessaria l'esistenza di una "convenzione sociale" tra gli agenti economici, relativa alla validità di tale strumento: alta volatilità, elevata componente speculativa della domanda e limitata offerta[14] di token rappresentano i maggiori ostacoli per il raggiungimento di questo obiettivo.

[13] https://howmuch.net/articles/worlds-money-in-perspective-2018.
[14] Relativa alla complessità dell'espansione elastica della sua offerta in risposta alla domanda del mercato.

A differenza della moneta tradizionale, le criptovalute svolgono una singolare funzione di trasferimento e archiviazione di informazioni: la blockchain memorizza tutte le informazioni relative a transazioni sicure e immutabili, permettendo dunque la risoluzione di eventuali discrasie. Difatti, diversi progetti cripto hanno specificatamente la finalità di semplificare i contratti intelligenti[15], riducendo tempi e costi (non è necessaria la presenza di un intermediario).

1.3 CENNI STORICI SULLE VALUTE VIRTUALI

Lo sviluppo tecnologico delle criptovalute è fondato nella costante innovazione sul piano della crittografia, dell'anonimato, della sicurezza e della regolamentazione con autorità centralizzate. L'eredità di ogni progetto ha permesso la realizzazione della nuova frontiera finanziaria delle criptovalute.

Originariamente la tecnologia crittografica veniva adoperata in ambiti militari e da varie agenzie di intelligence, le quali utilizzavano codici differenti per proteggere le informazioni dai leaks.

L'idea di creare una moneta digitale nasce ben più di 25 anni prima della pubblicazione del whitepaper[16] relativo alla blockchain Bitcoin. Nell'aprile del 1982, David Chaum, pioniere della crittografia, pubblicò un articolo intitolato *"Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups"*[17], all'interno del quale delinea le fondamenta del sistema Blockchain, sostenendo la possibilità di costruire un sistema

[15] Protocolli informatici che facilitano, verificano, e regolano la negoziazione e/o esecuzione di un contratto.

[16] Documento informativo pubblicato da una società o ente no-profit, per l'illustrazione o promozione delle caratteristiche di un prodotto o servizio offerto.

[17] Chaum, D. L. (1979). "*Computer Systems established, maintained and trusted by mutually suspicious groups*" (p. 1). Electronics Research Laboratory, University of California.

monetario basato sull'intracciabilità degli spostamenti di denaro e sulla decentralizzazione del sistema stesso rispetto ai classici istituti finanziari.

Tale tesi veniva sostenuta anche in un altro articolo sempre redatto da Chaum *"Blind signature for untarcele payments"*[18], nel quale sostiene la possibilità che il sistema dei pagamenti elettronici possa impattare pesantemente sulla privacy personale, rimarcando la necessità di un sistema di pagamento anonimo crittografato. Il soprannominato "Blinded cash" poteva essere trasferito in modo sicuro tra i soggetti interessati con una firma di autenticità e senza essere tracciato. Ciò sta a significare che le banche e le autorità governative non sono autorizzate a tracciare chi effettua il pagamento nella "two party transaction"[19]; tuttavia è necessario un istituto bancario che agisca come tramite fiduciario per le transazioni elettroniche.

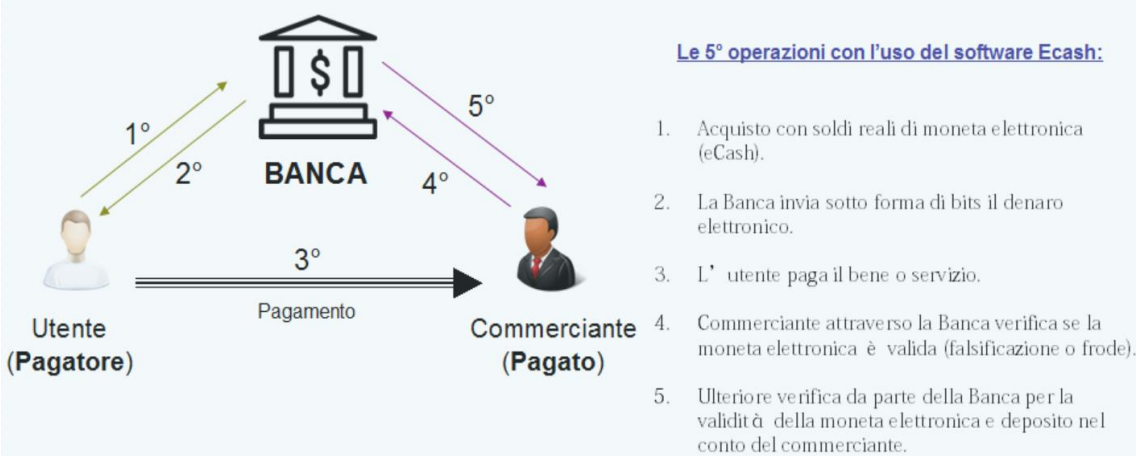
Pochi anni dopo Chaum decise di concretizzare le proprie teorie emettendo una valuta digitale chiamata "ECash" (chiamata anche DigiCash) tramite la sua compagnia DIGICASH INC. ECash può essere descritta come una forma di pagamento elettronico anticipato, che richiede all'utente di prelevare banconote da una banca e designare specifiche chiavi crittografate. Queste consentono l'autenticazione della transazione e permettono di inviare in modo sicuro l'importo ad un destinatario (sotto forma di bits del denaro elettronico). Questo progresso della crittografia a chiave pubblica e privata consentiva alle banche emittenti di confermare l'autenticità del denaro, ma non la provenienza, rendendo il sistema completamente anonimo. Tuttavia, erano necessarie specifiche chiavi crittografate e la collaborazione di enti bancari, ma solo la Mark Twain

[18] Chaum D. (1983), *"Blind Signatures for Untraceable Payments"* In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds) Advances in Cryptology. Springer, Boston.

[19] Transazione tra due parti: generalmente si riferisce a una transazione commerciale o finanziaria coinvolgente solo due parti o entità. Può essere usata per descrivere un accordo, uno scambio o una negoziazione in cui solo due soggetti sono coinvolti.

Bank fu l'unica banca americana a supportare i sistemi ECash; Deutsche Bank fu il secondo istituto di credito al mondo a adottare tale sistema[20].

Figura 2: Iter funzionamento ECash



Fonte: www.portafoglioelettronicomigliore.com/digicash

Ecash ha rappresentato la soluzione ad un problema che le persone comuni non vedevano: nonostante l'evidente crescita dell'eCommerce, gli acquirenti online non erano interessati all' utilizzo di ECash, ritenendo irrealistico che la moneta digitale fosse maggiormente sicura rispetto alle loro carte di credito. Un'idea troppo rivoluzionaria per l'epoca e una importante disorganizzazione in ambito di investimenti hanno portato al fallimento della valuta digitale. L'influenza e l'eredità tecnologica di Chaum hanno permesso a molti sviluppatori di immergersi nel mondo delle monete digitali, creando nuovi token, tra i quali spiccano eGold e BitGold, valute ancorate all'andamento dell'oro. Nonostante il successo riscosso nei primi anni 2000, l'inefficienza dei sistemi di sicurezza nei confronti di hacker, il congelamento delle riserve d'oro del 2001 (Patriot Act) e le problematiche legale al Double Spendig[21], hanno portato al fallimento dei due progetti virtuali.

[20] https://chaum.com/ecash/
[21] Double Spending Problem: le informazioni di una transazione in una blockchain possono essere alterate mediante la modifica dei blocchi; In tal caso il realizzatore dell'alterazione ha la possibilità di reclamare token già spesi (spende il token, attua alterazione, riottiene il token);

Nell'ottobre del 2008, il giapponese Satoshi Nakamoto decise di inoltrare ad un gruppo di cultori della crittografia, una mail contenente una completa descrizione del concetto di Bitcoin, allegando il white paper "*Bitcoin: A Peer-to-Peer Electronic Cash System*"[22].

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one person to another without the burdens of going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted party is still required to prevent double spending. We propose a solution to the double-spending problem using a peer-to-peer network…

Nel gennaio del 2009 è stata lanciata la blockchain Bitcoin e il primo blocco originario è stato minato. Per i primi mesi l'accesso alla blockchain era riservato unicamente ai primi minatori del blocco originario e le transazioni di prova erano effettuate esclusivamente tra di loro. La prima concreta transazione economica globalmente riconosciuta è avvenuta l'anno successivo quando Laszlo Hanyecz acquistò 2 pizze da Papa John al costo di 10000 bitcoin (all'epoca all'incirca 41 dollari, ad oggi "solamente" 270.968.000 dollari). Negli anni successivi diverse monete digitali sono state sviluppate dai primi cultori della blockchain e sostenitori delle potenzialità della tecnologia. In riferimento a ciò ricordiamo principalmente Litecoin, definita come l'argento del mondo cripto (l'oro è rappresentato dal Bitcoin) ed Ethereum, ad oggi la seconda criptovaluta più importante, nota per l'utilizzo e la divulgazione dei contratti intelligenti, e per la vastità della sua rete blockchain.

[22] Nakamoto, S. (2008) *"Bitcoin: A peer-to-peer electronic cash system."* Decentralized business review.

Nonostante il percorso evolutivo del mondo virtuale abbia incontrato diversi ostacoli, ad oggi possiamo annoverare l'esistenza di molti progetti innovativi meritevoli di attenzioni e investimenti, con il potenziale necessario a migliorare il mondo delle monete digitali, della blockchain e della finanza decentralizzata. Allo stesso modo, anche gli Exchange[23] di criptovalute hanno dovuto affrontare diversi ostacoli parallelamente alle valute virtuali stesse. Le difficoltà principalmente riscontrate dal settore Exchange sono da ricondurre alla mancanza di credibilità che gli investitori associavano al mercato; il primo esempio che possiamo citare è il market Bitcoin dell'utente "dwdollar" nel quale potevano essere effettuate transazioni (supportate dal sistema PayPal) per l'acquisto di bitcoin tra gli utenti. Tuttavia, molti di questi sostennero di non aver mai ricevuto i bitcoin acquistati, portando PayPal ad allontanarsi definitivamente dai market bitcoin allo scopo di evitare la gestione di questi reclami. L'Exchange Mt. Gox rappresenta uno dei primi Exchange di criptovalute: fondato nel 2007 come piattaforma di trading online, nel 2010 divenne l'Exchange più rilevante, gestendo ¾ delle transazioni bitcoin. Il declino dell'Exchange è dovuto ad un cambio di gestione che ha comportato una totale mancanza di innovazione ma soprattutto di rispetto della regolamentazione. Infatti l'Exchange venne associato alla Silk Road, ovvero un marketplace del dark web nel quale era possibile acquistare prodotti illegali scambiando bitcoin. Da lì a breve avvennero molteplici hackeraggi dell'Exchange, che portarono addirittura al furto di 850 mila bitcoin, di cui 750 posseduti dai clienti dell'Exchange. La notorietà di Mt. Gox è dunque legata principalmente alle vicissitudini legali intraprese, e non alla sua essenza di pioniere del mondo cripto: ora si contano centinaia di Exchange che non esisterebbero senza lo sviluppo e la crescita delle transazioni virtuali grazie a Mt. Gox.

[23] Piattaforme che permettono la conversione valuta tradizionale-moneta virtuale e che permettono lo scambio tra utenti.

1.4 BLOCKCHAIN

Per illustrare chiaramente tutti gli aspetti tecnici, i pregi e i difetti, il funzionamento e l'impatto socio-economico di questi strumenti virtuali, è necessaria un' introduzione al motore centrale del sistema cripto-centrico: la blockchain.

La grande maggioranza delle criptovalute prende vita sulla base della tecnologia blockchain, la quale può essere associata ad una sorta di registro pubblico (un database) distribuito a tutti i possessori di una criptovaluta. Come suggerisce il nome, la blockchain è costituita da blocchi che contengono le informazioni relative ad un set di transazioni avvenute in un determinato arco temporale. È opportuno e interessante trattare le metodologie di formazione di una blockchain, basate su algoritmi di consenso, ovvero meccanismi che permettono di stabilire il grado di sicurezza, le informazioni condivise e le modalità di creazione dei blocchi.

I 3 principali algoritmi vengono riconosciuti come: *"proof-of-work" (Pow), "proof-of-stake" (PoS) e "proof-of-authority" (FBTA, byzantine fault tolerance algorithms*, basato sulla risoluzione del problema dei generali bizantini[24]).

Prima di procedere con la trattazione degli algoritmi, è fondamentale introdurre il concetto di "nodi". Con questo termine si fa riferimento a qualsiasi dispositivo elettronico munito di connessione ad Internet e collegato alla rete blockchain. I nodi gestiscono la rete (network) salvando una copia della blockchain e in alcuni casi, processando le transazioni: i proprietari dei nodi forniscono le risorse informatiche ("potenza di calcolo") dei propri dispositivi per archiviare e verificare le transazioni allo scopo di poter ottenere

[24] Condizione caratteristica dei sistemi informatici distribuiti che evidenzia le difficoltà nel coordinare le azioni delle componenti indipendenti per il mantenimento dell'integrità del sistema.

una commissione. Questo processo viene comunemente chiamato *mining* (per algoritmi PoW) o *forging* (per algoritmi Pos). Vengono classificate 2 tipologie di nodi:

- Un nodo completo scarica la totalità di dati di una specifica blockchain e convalida ogni nuova transazione, inserendo le informazioni nei blocchi;
- Un nodo parziale (o leggero) non memorizza il registro completo, pertanto, la grandezza della blockchain non rappresenta un problema per il nodo: avviene unicamente il download della sezione di blockchain richiesta per la SPV (Simplified Payment Verification)[25]

Descriviamo ora le tre tipologie principali di algoritmo che diversificano il mondo crittografico[26].

PoW proof of work, rappresenta l'algoritmo di consenso utilizzato dalla principale criptovaluta conosciuta: Bitcoin. L'idea alla base dell'algoritmo consiste nel mining, ovvero una continua operatività di calcolo effettuata da parte dei nodi della blockchain per la generazione di nuovi blocchi. I nodi sfruttano le loro risorse computazionali allo scopo di risolvere problemi crittografici di una certa complessità (hash function)[27].

Questo algoritmo viene considerato altamente competitivo in quanto la natura stessa del mining richiede ai partecipanti una costante e crescente potenza di calcolo per la creazione di nuovi blocchi. Solo il miner in grado di risolvere i puzzle crittografici viene

[25] Permette al destinatario della transazione di dimostrare che il mittente ha il controllo della fonte di finanziamento del pagamento offerto, senza dover scaricare tutta la blockchain.
[26] Sinelnikova-Muryleva, E. V., Shilov, K. D., & Zubarev, A. V. (2019). *"The Essence of cryptocurrencies: descriptive and comparative analysis". Finance*: Theory and Practice, 23(6), 36-49.
[27] Una funzione hash crittografica è usata per scopi di sicurezza e costituisce la colonna portante della sicurezza crittografica: trasforma un input (per esempio un testo) in una stringa di byte con una lunghezza e una struttura fisse

ricompensato: ciò comporta un incremento sia della media di calcoli, sia del costo per la creazione di nuovi blocchi, migliorando indirettamente l'efficienza del sistema.

Come ricompensa per l'operato svolto, il miner vincente ottiene un determinato valore di criptovalute su cui sta lavorando.

L'algoritmo PoW consente a qualsiasi utente della blockchain PoW di effettuare transazioni sicure senza l'intervento di enti terzi. Tuttavia, la decentralizzazione non sopperisce alle principali debolezze che caratterizzano la vera essenza delle monete digitali come il Bitcoin: tempi elevati per le transazioni, commissioni instabili e costose. La principale problematica che può riscontrare una criptovaluta basata sull' algoritmo PoW è il "51% attack", ovvero un attacco organizzato da uno o più miner allo scopo di prendere il controllo della maggioranza di una blockchain e sfruttare la duplicazione dei token[28].

PoS "proof-of-stake", è un algoritmo di consenso che determina la probabilità per un utente di creare un nuovo blocco in base al numero di criptovalute e/o token nel suo bilancio. Il principale vantaggio dell'algoritmo consiste nella importante riduzione di risorse richieste per la risoluzione dei puzzle crittografici, ma allo stesso tempo, nel momento in cui viene creato un nuovo blocco, non viene prodotto un nuovo token: ciò sta a significare che le ricompense per l'utente sono rappresentate dalle commissioni per ogni transazione avvenuta nel blocco. Inoltre, le criptovalute basate su algoritmo PoS sono potenzialmente vulnerabili ad "attacchi profondi"[29]. Ad oggi è pratica comune

[28] Double Spending Problem: le informazioni di una transazione in una blockchain possono essere alterate mediante la modifica dei blocchi; In tal caso il realizzatore dell'alterazione ha la possibilità di reclamare token già spesi (spende il token, attua alterazione, riottiene il token).

[29] Consiste nell'ottenere il controllo di portafogli contenenti token già spesi con l'intento di attuare un ulteriore 51%attack e riottenere le monete.

adoperare entrambi gli algoritmi PoW e PoS per l'emissione di criptovalute allo scopo di ridurre il rischio complessivo di attacchi informatici.

FBTA (byzantine fault tolerance algorithms), conosciuto come *"proof of authority"* è l'algoritmo di consenso incentrato sulla risoluzione del "problema dei Generali bizantini"[30] che viene esplicata con un continuo scambio di informazioni del registro tra gli utenti della rete allo scopo di creare un sistema di consenso.
Questi sistemi sono caratterizzati da una elevata velocità di transazione e mancanza di mining: a tal proposito i nodi partecipanti al sistema di consenso possono ottenere delle commissioni tramite l'approvazione delle transazioni nei blocchi.

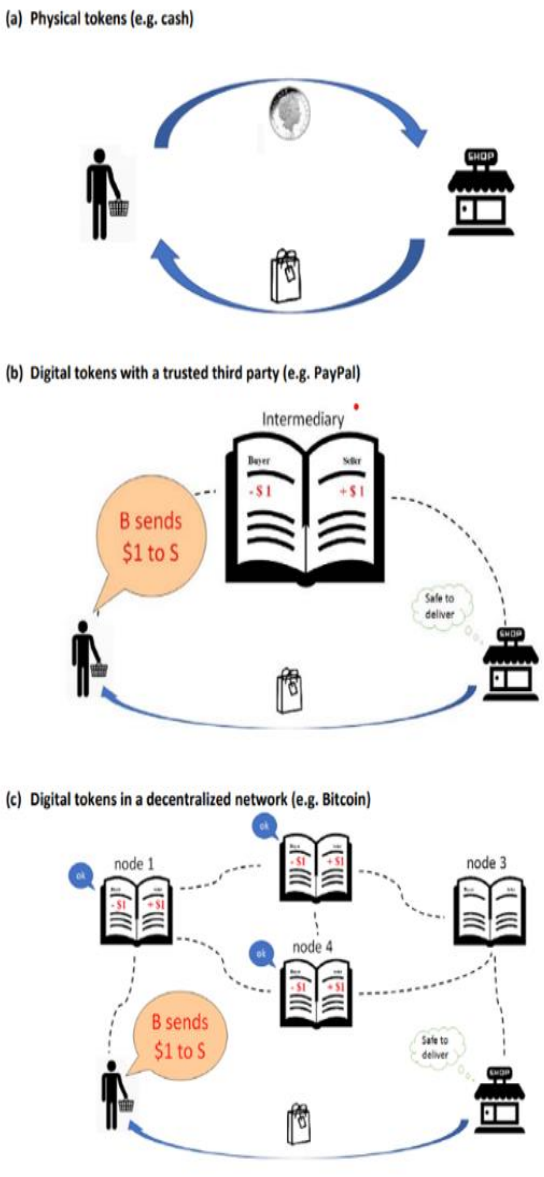
La trattazione relativa ai processi operativi verrà svolta nel capitolo successivo, evidenziando il ruolo che la blockchain assume nel ciclo di funzionamento di una criptovaluta.

[30] Teoria dei giochi basata sull'analogia di un gruppo di generali che assediano Bisanzio, con ogni generale responsabile di una divisione dell'esercito: se il coordinamento nell'attacco è realizzato, il risultato è la vittoria; in mancanza di coordinamento, avviene la disfatta. Dunque, è necessario un protocollo che permetta ai generali (per la blockchain sono i nodi) di raggiungere un solido consenso operativo;

CAPITOLO 2: FUNZIONAMENTO DEL SISTEMA CRIPTOCENTRICO E DOUBLE SPENDING PROBLEM

2.1 PILASTRI DELL'ARCHITETTURA VIRTUALE

Figura 3: Tipologie di valuta



Fonte: The economics of cryptocurrency: Bitcoin and beyond. Canadian Journal of Economics

Per migliaia di anni, la moneta fisica (moneta e banconota) ha costituito l'unico sistema di pagamento tramite il quale è possibile realizzare un'immediata risoluzione della trattazione, con il diretto scambio tra il bene del venditore e il denaro del compratore (a): tuttavia, questa situazione richiede che entrambi gli agenti si trovino nella stessa locazione. Per rimediare a questa problematica, è stata introdotta la moneta digitale (b), esplicando il pagamento tramite una stringa di bit. Le problematiche di tale sistema sono ricondotte unicamente a malfunzionamenti del complessivo sistema di pagamento e ai tentativi di truffa, tra i quali risalta la double spending, ovvero il tentativo di riutilizzare un token digitale già utilizzato per un precedente pagamento (raddoppiare il token). Il problema è risolto con l'inserimento di un ente terzo (intermediario bancario, società finanziaria come PayPal) il quale gestisce un registro

centralizzato, trasferendo i saldi degli utenti tramite accrediti e addebiti. In assenza di una autorità centrale, le criptovalute (c) si affidano ad un registro distribuito che permette la verifica e convalida delle transazioni, delle quali viene conservata e aggiornata la cronologia: ciò richiede che sia stabilito e mantenuto il consenso tra gli utenti del registro distribuito.

Una delle tante finalità delle criptovalute consiste nello svolgere la funzione di mezzo di scambio basato sulla tecnologia crittografica: questa definizione viene citata in molti articoli e si riferisce alla quintessenza della valuta virtuale quale combinazione "economico + tecnologico + crittografico[31]".

Essendo costruite su strutture atipiche, le criptovalute sono spesso descritte come "trustless[32]", decentralizzate e immutabili.

- L' "assenza di fiducia" deriva dal fatto che il processo di consenso avviene mediate algoritmi di rete:non richiede conoscenza tra gli utenti.
- La caratteristica decentralizzazione del sistema è ottenuta mediante la distribuzione del registro tra tutti i nodi partecipanti alla rete: il collasso computeristico di un qualsiasi nodo è dunque irrilevante per l'esistenza della blockchain, in quanto tutte le informazioni sono distribuite tra tutti i nodi. L'assenza di un'autorità centrale costituisce una delle fonti principali di attrazione per i sostenitori delle criptovalute.

[31] Chiu J. & Koeppl, T. V. (2022). *"The economics of cryptocurrency: Bitcoin and beyond".* Canadian Journal of Economics/Revue canadienne d'économique, *55*(4), 1762-1798.
[32] Assenza di fiducia intesa come non necessaria fiducia nei confronti di un soggetto terzo.

Nonostante la decentralizzazione sia un pilastro fondante, nuovi asset virtuali sono indirizzati verso un contesto di centralizzazione, in quanto emessi, legittimati e garantiti da autorità monetarie (es. CBDC, Central Bank Digital Currency).

- L'immutabilità delle criptovalute deriva dal fatto che le transazioni sono convalidate invariabilmente su tutta la rete, rendendo (quasi)[33] impossibile per qualsiasi hacker l'alterazione delle informazioni della blockchain.

Il nucleo del sistema cripto-centrico risiede in due funzioni: produzione (mining) e transazioni (scambio di criptovalute).

2.2 PROCESSO DI MINING

La produzione della maggior parte delle criptovalute avviene tramite un processo definito mining (letteralmente "scavare e produrre" blocchi), il quale prevede lo sfruttamento di elevata e crescente potenza di calcolo allo scopo di raccogliere e raggruppare in blocchi le singole transazioni avvenute in un determinato lasso temporale. Ogni blocco contiene delle informazioni relative al precedente con la finalità di costruire una catena, definita blockchain[34]. I miner, ovvero i proprietari dei nodi operativi, tramite dei software, collegano i propri nodi allo scopo di creare una rete peer to peer per la gestione del registro distribuito (ledger), verificando che siano approvate solo le transazioni legittime. Con la finalità di preservare l'integrità e sicurezza dei blocchi, i miner devono risolvere enigmi crittografici (simbolicamente dei puzzle matematici), scongiurando principalmente il

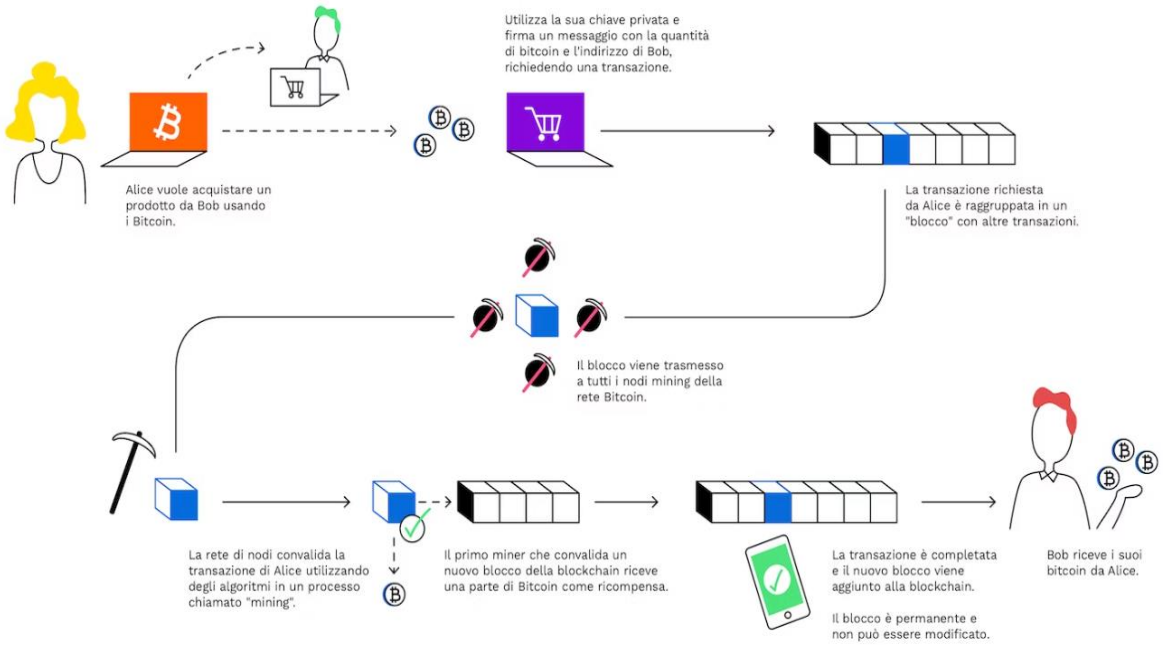
[33] Un hacker avrebbe bisogno del 51% delle blockchain per modificare le informazioni dei blocchi: operazione che richiede uno sforzo monetario e computeristico quasi insostenibile.
[34] Possiamo definire ogni blocco come una pagina di un libro, la quale collegandosi con le altre, compone il libro mastro, ovvero la blockchain.

problema double spending. Dal momento in cui le prestazioni computazionali progrediscono con il tempo, esiste una funzione economica in base alla quale il mining diventa più o meno redditizio in relazione al prezzo della criptovaluta: è evidente come il processo di mining diventerà sempre più proibitivo sia dal punto di vista economico che ambientale[35].

Prendendo per esempio lo schema Bitcoin, la ricompensa consiste in due fattori:

- Creazione di nuovi token per i miner vincitori della competizione, incrementando il bilancio della criptovaluta;
- Una frazione del bilancio che viene distribuita ai miner come commissione;

Figura 4: Processo di funzionamento di una criptovaluta



Fonte: Bitpanda

La seconda funzione è rappresentata dalla transazione, il momento nel quale scambi digitali fungono da "mercato" per i partecipanti intenti a comprare o vendere la

[35] La potenza computeristica richiesta prevede un elevato consumo energetico: verrà trattato nei capitoli successivi

criptovaluta: la transazione può avvenire sia in cambio di valute tradizionali (fiat)[36] che per altre criptovalute. Gli Exchange possono gestire anche volumi considerevoli, creando un ambiente favorevole allo scambio, come per esempio Binance, il quale gestisce le transazioni tra più di 170 milioni di utenti. Tuttavia, fungendo da fornitore di terze parti e mercato fuori dalla regolamentazione finanziaria tradizionale, l'Exchange è intrinsecamente vulnerabile ad attacchi informatici, truffe e accuse.

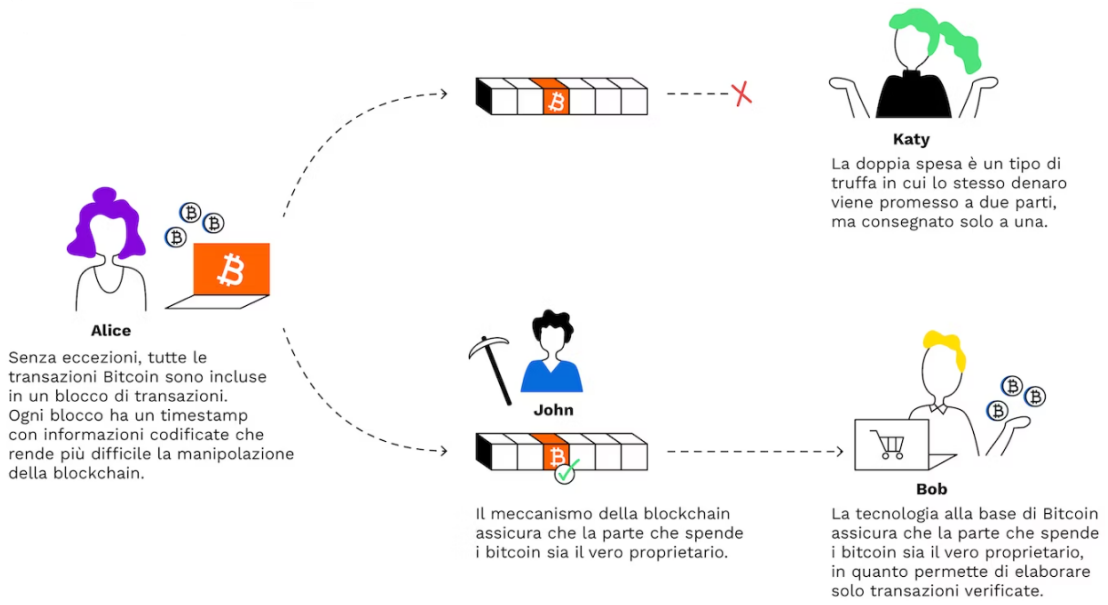
2.3 TRANSAZIONI E DOUBLE SPENDING PROBLEM

L'architettura digitale alla base del sistema decentralizzato cripto è relativamente nuova. Possiamo porre come origine il whitepaper di Satoshi Nakamoto (2008), con il quale è stata proposta la risoluzione del problema dei Generali Bizantini[37] e del double spending problem, che hanno inficiato le prime iterazioni con la moneta virtuale (primi anni 90). Come suggerisce il nome "doppia spesa", il problema informatico consiste nell'utilizzare due volte una stessa moneta: a seguito di una transazione, l'acquirente tenta di eludere l'intera rete definendo una cronologia alternativa in cui il pagamento non è stato effettuato. Ciò sta a significare che l'hacker è stato in grado di costruire un blocco alternativo che rispecchia la coerenza della blockchain sotto attacco, allo scopo di essere verificata e accettata dai miner. All'interno di questo blocco vengono inserite informazioni tali per cui le transazioni precedentemente svolte dall'hacker non vengono registrate, nonostante queste siano concretamente realizzate. Quando l'attacco ha successo, l'acquirente (hacker) conserva sia il prodotto, in quanto lo scambio è avvenuto,

[36] Moneta a corso legale, inteso come strumento di pagamento non coperto da riserve di altri materiali (es. riserve auree) e quindi privo di valore intrinseco: la valenza economica è definita dall'ente emittente la moneta.
[37] Lamport, L., Shostak, R., & Pease, M. (2019). *"The Byzantine general's problem. In Concurrenc".* The Works of Leslie Lamport (pp. 203-226).

sia i token utilizzati per l'acquisto (riottiene il token in quanto l'operazione non è registrata), mentre il venditore non possiede nessuno dei due.

Figura 5: Meccanismo double spending



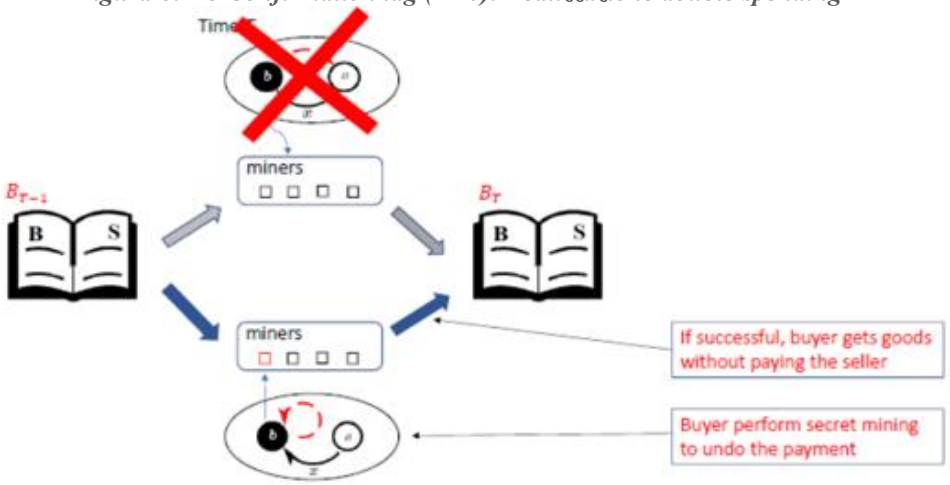
Fonte: Bitpanda

L'architettura stessa della blockchain minimizza le possibilità di realizzazione dell'hackeraggio in quanto la tecnologia di condivisione peer to peer, in sinergia con la crittografia a chiave pubblica disincentiva i tentativi di double spending.

Un hacker dovrebbe minare un blocco alternativo, sostenendo dunque tutti i costi ad esso relativi e dovrebbe agire in maniera tale da bypassare il protocollo di consenso prima che il blocco alternativo sia scavalcato da un ulteriore blocco. A tal punto, l'unica alternativa a disposizione dell'hacker consiste nel 51% attack, attuato con l'assunzione del controllo della maggioranza della blockchain e dunque delle transazioni effettuate. Tuttavia, ciò comporterebbe una richiesta di potenza computazionale, risorse energetiche e soprattutto economiche concretamente impossibili da possedere.

È inoltre possibile scoraggiare gli attacchi introducendo un ritardo di conferma per le transazioni[38], in quanto la consegna ritardata del bene da parte dei venditori rende più difficile la modifica della sequenza (Figura 6).

Figura 6: No Confirmation lag (N=0): Realizzazione double spending



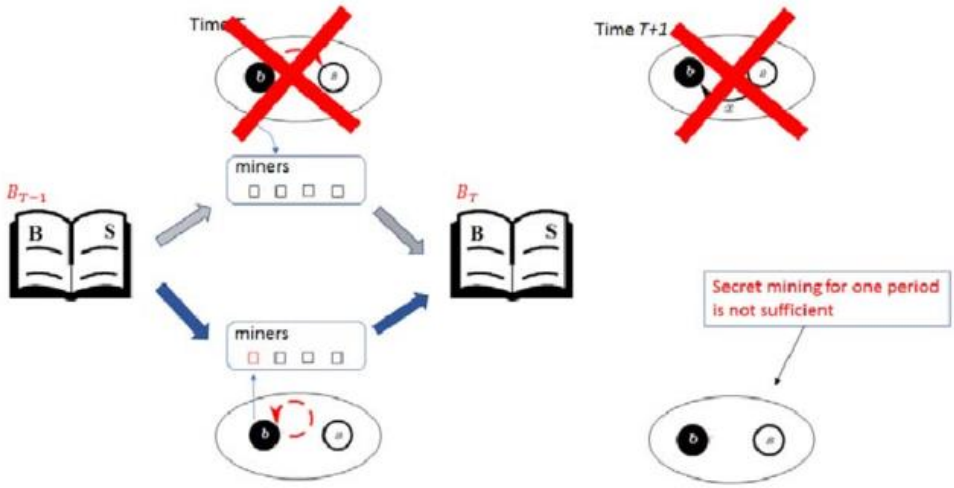
Fonte: The economics of cryptocurrency: Bitcoin and beyond. Canadian Journal of Economics

Se il venditore consegnasse il bene solo dopo l'osservazione di N[39] conferme del pagamento, allora il compratore dovrebbe risolvere N+1 volte l'algoritmo allo scopo di attuare la double spending.

[38] Chiu, J., & Koeppl, T. V. (2022). "*The economics of cryptocurrency: Bitcoin and beyond*". Canadian Journal of Economics/Revue canadienne d'économique, 55(4), 1762-1798.

[39] N costituisce il numero di "ritardi" (lag), che permettono al venditore di ricevere ulteriori conferme del pagamento e posticipare l'invio del bene venduto.
N=0 no confirmation lag N>0 presenza di conferme/ritardi

Figura 7: Tentativo fallito di double spending



Fonte: The economics of cryptocurrency: Bitcoin and beyond. Canadian Journal of Economics

2.4 MODELLO ECONOMICO PER L'EQUILIBRIO DEL MERCATO DECENTRALIZZATO

Prendiamo in considerazione il modello del mercato alternato[40] di Lagos e Wright[41] : questa formulazione ci permette di analizzare i meccanismi che spingono all'uso di una moneta, mantenendo la distribuzione dei bilanci analiticamente trattabili. Il tempo è discreto e descritto con t = 0,1,2… Prendiamo in considerazione i compratori con B (buyers) i venditori con S (sellers) e indichiamo con M i miner.

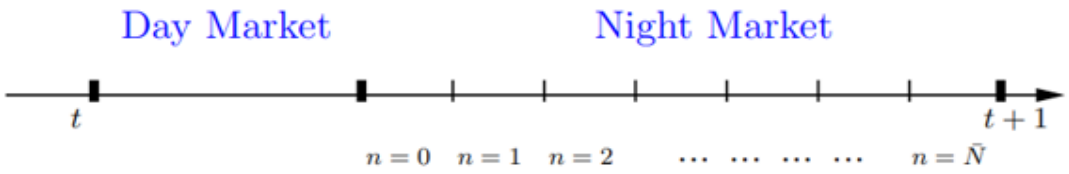
Per ogni periodo *t* preso in considerazione, definiamo un day market e un night market: il primo rappresenta il mercato competitivo per lo scambio di beni generici *h* (mercato tradizionale) per riequilibrare i saldi; il secondo costituisce un mercato decentralizzato per lo scambio di un bene *x*, prodotto dal venditore e acquistato dall'acquirente. Come

[40] Modello economico che permette di delineare elementi esplicitamente microeconomici, consentendo una parallela analisi macroeconomica: il modello è trattabile analiticamente e suscettibile di analisi quantitativa: verrà utilizzato come analisi sull'efficacia delle criptovalute come metodo di pagamento e strumento di politica monetaria.

[41] Lagos, L., and R. Wright, (2005). *"A unified framework for monetary theory and policy analysis"* Journal of political Economy, 113.3: 463-484.

analizzato dalla figura 8, il night market è diviso in N + 1 sessioni di trading consecutive, dove N≥ 1[42].

Figura 8: Orizzonte temporale dei mercati



Il day market è centralizzato e regolarizzato per gli scambi dei beni; nel night market invece gli scambi sono bilaterali e non monitorati. Caratterizzato dall'anonimato, il night market necessita di un mezzo di pagamento che assumiamo essere una criptovaluta[43].

Per comprendere a fondo il modello, introduciamo ulteriori impostazioni. Vengono presi in considerazione sia i bilanci aggregati del mercato day $A_t^D = \{m_t^D(\mathrm{i})\}$[44]. sia i bilanci aggregati del mercato night $A_t^N\{m_t^N(i)\}$.

L'esistenza del monitoraggio pubblico suppone che nel day market i pagamenti eseguiti in questo periodo vadano ad aggiornare automaticamente il bilancio aggregato. Il nuovo stato all'inizio del mercato notturno è dunque definito come $A_{t,0}^N = \Psi_0^N(A_t^D, BL_t^D)$ dove BL costituisce l'intero insieme dei trasferimenti giornalieri ed è definito come blocco.

I pagamenti nel night market entrano nel sistema tramite il processo di mining. Quando un soggetto *i* fa un pagamento al soggetto *j* nel night market, deve comunicare le istruzioni della transazione $\Delta_t^N(\mathrm{i}, \mathrm{j})$ ad un gruppo di miner, i quali competono per l'aggiornamento del sistema con l'inserimento di un nuovo blocco di informazioni di transazione avvenute durante la sessione *n* del mercato night. Il set creato, che ricordiamo essere $BL_{t,n}^N$ è

[42] Molteplici sessioni di mercato ci permettono di valutare anche il confirmation lag.
[43] Il contante non è utilizzabile per gli scambi online e i mezzi digitali non sono disponibili per chi non possiede un conto bancario: la soluzione ricade nelle criptovalute.
[44] La somma di tutti i bilanci (m) degli agenti *i*, al tempo *t,* nel mercato day *D*, costituiscono il bilancio aggregato del mercato day; situazione similare per il mercato night con A_t^N.

l'ennesimo blocco del periodo *t* contenente i pagamenti effettuati nel night market. Una sequenza di blocchi genera una blockchain che a sua volta rappresenta una sequenza di bilanci aggregati costantemente aggiornati.

Come sostenuto precedentemente, l'operato dei miner richiede un importante impiego tecnologico q_n: se la potenza computazionale del miner *i* nella sessione *n* viene definita come probabilità $q_n(i)$, allora la probabilità che un miner *j* possa essere il primo a risolvere l'algoritmo di consenso è definita dalla seguente formula $p_n(j) = \frac{q_n(j)}{\sum_{i=1}^{M} q_n(i)}$

La probabilità di vincere la fase mining p_n è proporzionale alla frazione della potenza computazionale posseduta. Vincendo la competizione, il miner può aggiornare la blockchain e ricevere un premio R, solitamente costituito dai token della criptovaluta su cui si sta operando.

Il day market è caratterizzato da un perfetto monitoraggio in quanto all'acquirente viene riconosciuta l'autenticità dell'operazione e se durante la transazione dovesse avvenire un malfunzionamento, si procederebbe con i rimborsi allo scopo di ristabilizzare il sistema[45].

Nel night market, un compratore incontra un venditore con una probabilità *σ*. Nel caso in cui accordassero lo scambio, il compratore deve fare un pagamento al venditore. In tal caso, dovrebbe mandare una istruzione $\Delta_{t,0}$ ad un gruppo di minatori ma ciò non sarebbe sufficiente poiché un compratore potrebbe intraprendere il mining di un blocco segreto all'interno del quale sono inserite informazioni per cui tale pagamento non avviene.

Come suggerito in precedenza, un venditore potrebbe proteggersi da questa truffa ritardando la consegna del bene finché il pagamento non sia incorporato nel sistema

[45] Ciò riflette la premessa iniziale secondo cui i seller che accettano e utilizzano le criptovalute come mezzo di pagamento, potrebbero essere legalmente responsabili per le perdite subite dalle altre parti (buyer, fornitori…). Il sistema virtuale non è perfettamente anonimo (enti speciali hanno la possibilità in casi estremi di tracciare le transazioni), dunque i double spender possono essere rintracciati: il sistema tende (quasi) sempre all'equilibrio.

distribuito: l'azione prevede il posponimento della consegna con l'attesa di N periodi che possiamo definire come ritardi (lag) della conferma.

Nel momento in cui tale operazione avesse successo, il compratore manterrebbe invariato il suo bilancio e otterrebbe il prodotto, situazione opposta per il venditore.

Questo evento viene definito come double spending problem.

Nel caso in cui il compratore non avesse intenzione di attuare un double spending, farebbe un'offerta al venditore che definiamo DS proof (double spending proof) con l'obiettivo di stabilire un equilibrio tra i partecipanti del night market.

Il buyer acquista il bene *x* nella sessione di trading *t* e otterrà il bene nella sessione *N*, a seguito di *N* ritardi di conferma. Prima della consegna, i miner costruiranno il blocco all'interno del quale saranno inserite le informazioni relative alla transazione e uniranno il blocco alla blockchain esistente così da aggiornare i bilanci.

CAPITOLO 3: CRIPTOVALUTE COME MEZZO DI PAGAMENTO

La diffusione di emergenti strumenti finanziari, tra i quali svettano le criptovalute, ha destato dubbi sull'efficienza dei pilastri finanziari tradizionali:

- Una valuta utilizzata come sistema di pagamento può essere fornita da un privato erogatore di moneta (es. criptovalute)?
- È più efficiente un sistema competitivo di offerta di moneta rispetto al monopolio?

La problematica teoretica e, attualmente, anche pratica è stata analizzata da Waknis[46], il quale ha costruito un modello di analisi monetaria basato su due valute, ispirandosi al modello di Lagos e Wright[47]. Gli attori del modello sono soggetti "miopi", ottimizzatori del consumo nel periodo corrente e focalizzati alla realizzazione dell'equilibrio di Nash[48]. Gli enti che forniscono la moneta (Banche Centrali) sono soggetti caratterizzati da una prospettiva a lungo termine che prevede la massimizzazione dell'utilità optando per il tasso di crescita dell'offerta monetaria più efficiente.

Il mercato centralizzato è un modello dinamico, con due fornitori di moneta e molteplici attori economici. Nella situazione illustrata dall'autore, la competizione tra i fornitori di moneta e il fatto che gli agenti scelgano solo Nash, trasforma il mercato centralizzato in un dilemma tra i due fornitori: se entrambi sono sufficientemente pazienti, allora verrà raggiunto un equilibrio cooperativo caratterizzato da un basso tasso di inflazione. Questo risultato permette di sostenere che ci sono le condizioni per cui un sistema competitivo tra valute permette di portare benefici al sistema macroeconomico.

---

[46] Waknis P. (2017). *"Competitive supply of money in a new monetarist model".* Munich Personal RePEc Archive. MPRA Paper (75401).

[47] Modello introdotto per la descrizione del funzionamento delle criptovalute: CAP 2.4.

[48] Teoria dei giochi per la quale l'equilibrio di Nash si realizza quando la strategia adottata da ogni giocatore consente la massimizzazione della vincita di ogni partecipante.

Nonostante i risultati ottenuti, la natura stessa delle criptovalute contraddice l'idea di una responsabilità centralizzata del sistema finanziario, pertanto, non possono essere considerate sostitutive del sistema monetario esistente, almeno per ora.

3.1 PRINCIPALI DIFETTI

Come sostenuto precedentemente, l'architettura delle criptovalute permette agli agenti economici di adoperarla come strumento di pagamento, nonostante non possa fungere da unità di conto affidabile o da mezzo di risparmio.

La problematica principale risiede nell'ideologia intrinseca delle valute virtuali: trustless, decentralizzate e immutabili. Nonostante la decentralizzazione sia un elemento particolarmente rilevante per la crescita e diffusione delle criptovalute, rappresenta un importante ostacolo per il consolidamento delle criptovalute come mezzo di pagamento. Nasce anche qui un dilemma tra decentralizzazione e ridimensionamento[49].

La struttura rudimentale della blockchain si basa su nodi decentralizzati operanti mediante algoritmi di consenso. Nonostante la decentralizzazione rappresenti il punto di forza della blockchain, nel lungo termine, un decentramento così vasto e la necessità di elaborare un massiccio volume di transazione, saranno di ostacolo per la gestione efficace della totalità delle transazioni. Per esempio, Bitcoin è in grado di gestire 7 transazioni al secondo, contro le 24 mila del sistema Visa e le 193 di PayPal[50]. Un' ulteriore limitazione è legata alla voragine volumetrica di transazioni registrate dai sistemi di pagamento tradizionali in tutto il mondo rispetto all' "insignificante" apporto delle transazioni cripto: questo

[49] Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (July 2018). *"Blockchain and scalability".* In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 122-128). IEEE.
[50] Bank of international settlements. *"BIS Annual Economic Report".* 2018 (dati Howmuch.net).

fattore è principalmente dovuto alla volatilità delle commissioni del sistema cripto-centrico (condizionate dalla "capacità" dei blocchi di archiviare informazioni).

3.1.1 Volatilità

Una delle caratteristiche distintive della valuta virtuale è l'elevata volatilità, ovvero la tendenza dei prezzi a fluttuare in modo significativo in un breve arco di temporale. La principale motivazione per cui le principali criptovalute siano altamente volatili è dovuta al basilare principio economico della domanda e dell'offerta. Così come la produzione delle materie prime influenza il loro valore economico, così il valore di mercato delle criptovalute è ancorato alla possibilità di mining e dunque, dal quantitativo di token minati e in circolazione. Strutturalmente è prevista una produzione limitata di token, il che comporterà un ipotetico graduale incremento di prezzo in funzione dell'avvicinamento al limite strutturale.

Un' altra motivazione è legata alla mancanza di una lineare normativa: il settore relativamente giovane non è ancora adeguatamente regolato il che può contribuire ad incertezza e speculazione. Proprio quest'ultima è alimentata dalla particolare sensibilità alle notizie. Anche una singola dichiarazione di un personaggio pubblico rilevante, una whale, un "esperto" (non sempre attendibile) può generare hype oppure "distruggere" una criptovaluta, pur essendo dichiarazioni non sempre verificate da elementi affidabili.

L'ideale ormai diffuso di poter sfruttare le fluttuazioni per arricchirsi velocemente ha incrementato anche il seguito di speculatori.

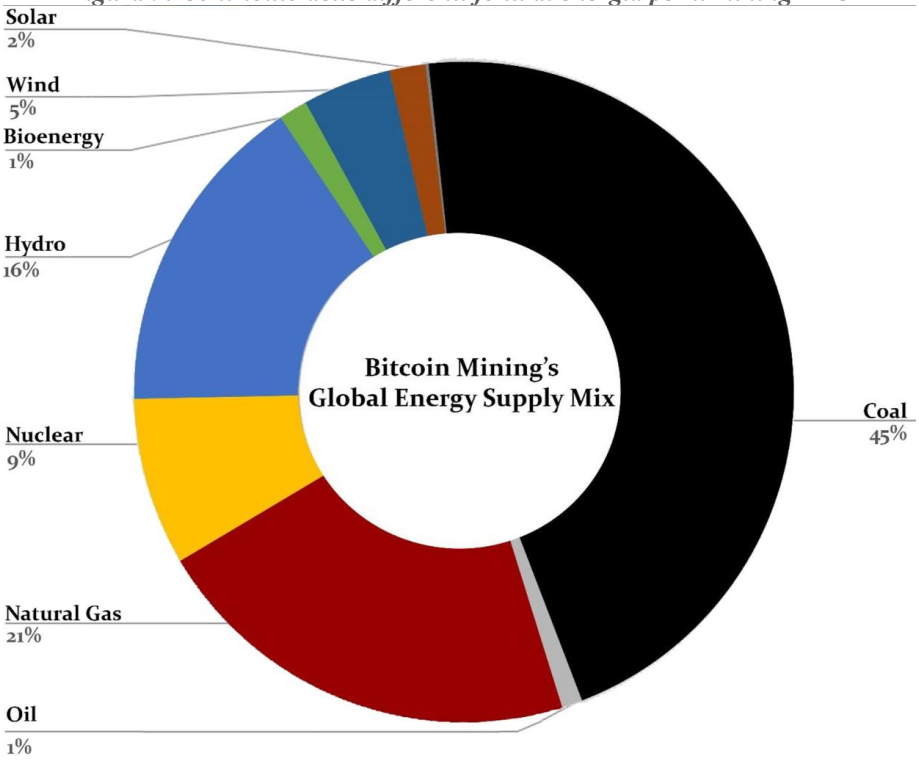
Infine, è importante considerare l'apertura 24/7 degli Exchange, il quale permette di operare costantemente. La disponibilità continua potrebbe innalzare la volatilità in quanto i prezzi reagiscono istantaneamente a qualsiasi avvenimento/dichiarazione.

3.1.2 Questione ambientale

A tal proposito è necessario menzionare la relazione diretta tra la necessaria crescente potenza di calcolo (legata alla creazione dei blocchi) e il consumo di elettricità. Le criptovalute sono note per essere enormi divoratori di energia pura. Bitcoin è estremamente assetato di energia[51], in quanto il suo sistema richiede enormi quantità di calcoli per processare le transazioni nella blockchain. Nel loro articolo, Chamanara e al. (2023)[52] illustrano le risorse energetiche globali sfruttate nel periodo 2020-2021 dal processo di mining di Bitcoin, richiedendo un urgente intervento da parte delle autorità allo scopo di assumere consapevolezza della crisi ambientale silenziosamente in atto. È stato stimato che nel periodo preso in considerazione, il consumo mondiale di energia elettrica per il mining BTC ammonta a 173.42TWh, l'ammontare che sarebbe sufficiente ad alimentare 10, 31 e 52 milioni di abitazioni rispettivamente negli USA, Germania e Giappone, corrispondente a circa il 15% del consumo energetico totale del continente africano. È evidente come il sistema cripto, in particolare BTC, sia fortemente dipendente dalle fonti di energia fossile, costituente circa il 67% del rifornimento energetico: solo il mining bitcoin ha un impatto di circa 85,89 Mt di CO_2 eq[53] nel periodo 2020-2021, circa l'equivalente di emissioni di 190 impianti di gas naturale (sarebbe necessario piantare 3,9 miliardi di alberi per compensare questi volumi).

[51] De Vries, A. (2018). *"Bitcoin's growing energy problem".* Joule, 2(5), 801-805.
[52] Chamanara, S., Ghaffarizadeh, S. A., & Madani, K. (2023). *"The environmental footprint of bitcoin mining across the globe: Call for urgent action"*. Earth's Future, 11.
[53] CO_2eq sono una unità di misura necessaria per esprimere in modo uniforme l'impatto sul clima dei diversi gas serra.

Figura 9: Contributo delle differenti fonti di energia per il mining BTC



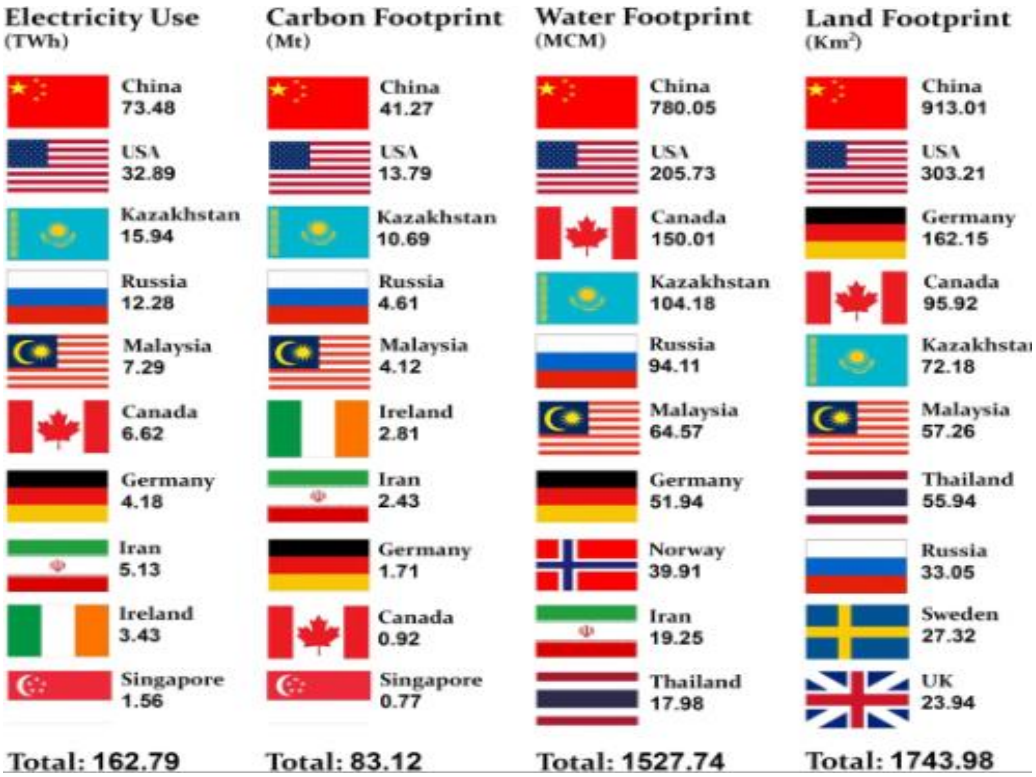
Fonte: Chamanara, S., Ghaffarizadeh, S. A., & Madani, K. (2023). The environmental footprint of bitcoin mining across the globe: Call for urgent action. Earth's Future

Prendendo in considerazione il CBECI (2-year Cambridge Bitcoin Electricity Consumption Index)[54] è possibile avere una visione complessiva dell'impronta ambientale del mining BTC.

USA e Cina sono le nazioni con il maggior impatto ambientale e sfruttamento di risorse; le altre nazioni si classificano in base alle possibilità fornite dalla loro posizione geografica. Per esempio, il Kazakistan rappresenta uno dei principali "produttori" di Bitcoin grazie alle risorse energetiche a disposizione che riducono drasticamente i costi del mining.

[54] Cambridge Centre for Alternative Finance (2023). Cambridge bitcoin electricity consumption index (CBECI): www.cbeci.org.

Figura 10: Principali 10 miner in base a consumi ambientali



Fonte: Chamanara, S., Ghaffarizadeh, S. A., & Madani, K. (2023). The environmental footprint of bitcoin mining across the globe: Call for urgent action. Earth's Future

Tutti questi valori influenzano pesantemente sia il prezzo delle criptovalute stesse sia icosti di transazione per il trading e ciò viene rimarcato dal divario di consumo elettrico per ogni transazione tra i tradizionali sistemi di pagamento e i sistemi basati su blockchain. Il costo energetico monetario di ogni transazione Bitcoin equivale a circa 600 mila transazioni Visa[55], aggirandosi all'incirca sui 100$, 1173kWh per transazione[56].

Esiste quindi una dissonanza tra il concetto generale di economia futuristica e sostenibile, sposata dagli appassionati di criptovalute, e la fame divoratrice di energia della fase mining. A tal proposito, diversi esperti stanno ipotizzando modelli di criptovaluta più

[55] https://www.statista.com/statistics/881541/bitcoinenergy-consumption-transaction-comparison-visa (2019).
[56] https://www.moneysupermarket.com/gas-and-electricity/features/crypto-energy-consumption.

sostenibili. Ad esempio, un nuovo algoritmo "proof of research"[57] potrebbe incanalare la potenza di calcolo verso finalità produttive, guidando la potenza computazionale verso la risoluzione di calcoli per ricerche sulla sostenibilità, piuttosto che essere utilizzata per un'arbitraria elaborazione crittografica.

Nei prossimi anni, la sostenibilità del mining di criptovalute rimarrà un tema saliente e variabili esogene più emblematiche (come inflazione, sussidi energetici, prezzi dei servizi…) giocheranno un ruolo importante per determinare il concreto impatto delle criptovalute nel panorama finanziario. Dunque, si può dedurre come ci sia il massimo interesse da parte dei sostenitori verso la sensibilizzazione all'efficienza energetica e al cambiamento climatico.)

3.1.3 Hackeraggi e vulnerabilità

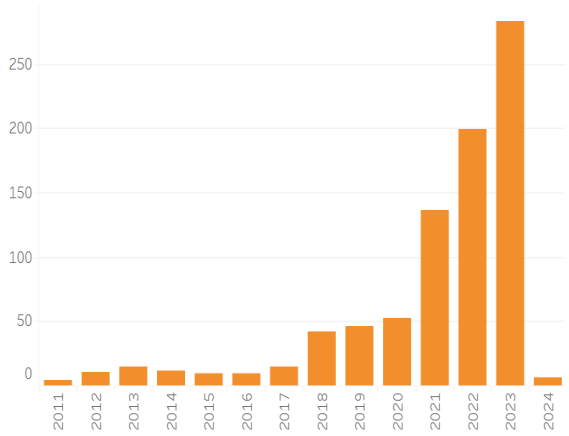
Nonostante l'esistenza di una resiliente architettura peer to peer in grado di verificare e convalidare la transazione, il mercato delle criptovalute è particolarmente soggetto alle esposizioni di società terze, aventi come funzione la custodia e gestione dei portafogli (gli Exchange). La maggior parte dei traders conserva il proprio portafoglio in custodia di terzi, il che li rende vulnerabili a violazioni della sicurezza, attacchi hacker e furti[58]. Esiste dunque una dimensione esterna all'architettura cripto-centrica estremamente vulnerabile, le cui falle si ripercuotono direttamente sulle criptovalute stesse.

[57] Leible, S., Schlager, S., Schubotz, M., & Gipp, B. (2019*). "A review on blockchain technology and blockchain projects fostering open science"*. Frontiers in Blockchain, 2, 16.
[58] Castonguay, J. J., & Stein Smith, S. (2020). *"Digital Assets and Blockchain: Hackable, Fraudulent, or Just Misunderstood?"*. Accounting Perspectives, 19(4), 363-387.

Nonostante le maggiori cripto, BTC e ETH, siano le più colpite singolarmente, la fragilità del sistema è dovuta alla numerosità degli attacchi subiti dalle criptovalute più piccole, le quali costituiscono i 2/3 degli attacchi registrati[59].

Questi sono risultati prevedibili a partire dalla fase di Initial Coin Offering (ICO)[60], tramite la quale i progetti cripto hanno raccolto numerosi fondi promettendo un'offerta di token rivelatasi per la maggior parte instabile o addirittura inesistente, dando vita a vere e proprie truffe.

Figura11: Numero di attacchi hacker per ogni anno



Fonte: Comparitech/crypto/biggest-cryptocurrency-heists

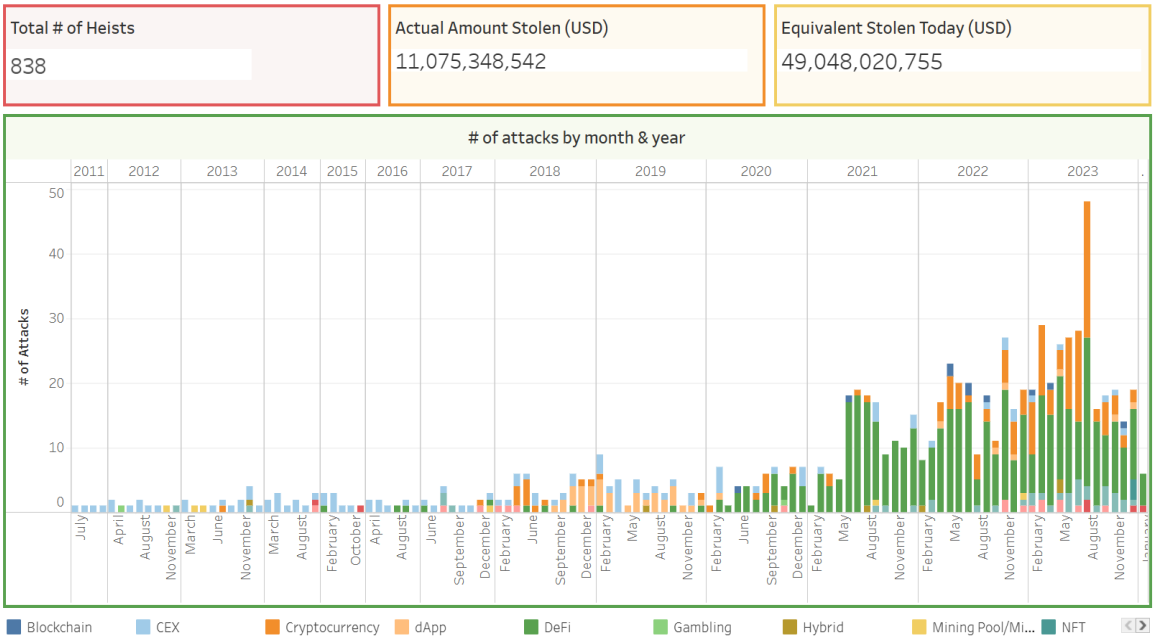
La crescente potenza computeristica ha comportato sia una esponenziale diffusione delle valute virtuali, sia un incremento di potenzialità e disponibilità operative tra gli hacker, comportando un significativo incremento degli attacchi negli ultimi anni ed ingenti perdite per il settore.

L'hackeraggio più importante conosciuto è avvenuto il 29 marzo 2022 quando Ronin Network ha annunciato di esser stata hackerata ammontare di 620 milioni di dollari.

Prendendo in considerazione i dati di Comparitech, è stato stimato un totale di 11 miliardi di dollari in criptovalute rubate, le quali ammonterebbero, con i prezzi di oggi, a circa 49 miliardi.

[59] https://www.comparitech.com/crypto/biggest-cryptocurrency-heists/
[60] Sono associabili alle IPO. Rappresentano i processi attraverso le quali una criptovaluta ottiene i finanziamenti, permettendo agli utenti regolati di investire in opportunità precedentemente aperte solo ad investitori su larga scala (IPO).

Figura 12: Totale Hackeraggi rilevati



Fonte: Comparitech/crypto/biggest-cryptocurrency-heists/

Nonostante anche i tradizionali sistemi di pagamento siano potenzialmente vulnerabili ad attacchi informatici e simili vulnerabilità, la decentralizzazione e la mancanza di una regolamentazione rigida e uniformemente delineata rappresentano elementi che disincentivano gli agenti economici ad adoperare le criptovalute come mezzi di pagamento.

3.1.4 Regolamentazione e Responsabilità

La letteratura pone un'enfasi significativa sul ruolo della governance, relativo alla regolamentazione e responsabilizzazione del settore, proponendo l'applicazione della tecnologia blockchain per questioni amministrative quali contenimento delle pratiche illecite, tutela degli investitori, corporate governance, gestione "territori intelligenti e altri contenuti gestionali/amministrativi. Il particolare interesse per la regolamentazione nasce dall'accusa rivolta alle monete virtuali inquadrate come veicoli di criminalità, quali

strumenti di riciclaggio di denaro e "carburante" della macchina del crimine informatico globale.

L'idea di una maggiore supervisione delle criptovalute riflette un conflitto di interesse tra libertà e sicurezza. Da un lato viene risaltata la libertà offerta dal sistema della valuta virtuale intrinsecamente decentrato; dall'altro, principalmente in situazioni di necessità come attacchi informatici, manipolazioni del mercato e truffe, gli investitori pretendono un maggiore intervento e supervisione del sistema[61]. Questa situazione può essere paragonata al dilemma normativo sul conflitto tra responsabilità e azione dell'ente governativo: in fasi prosperose, la popolazione non desidera l'intrusione del governo nelle proprie attività mentre, durante fasi di crisi, cresce la protesta sul fatto che il governo non abbia fatto abbastanza.

È necessaria una conciliazione tra gli interessi per identificare una regolamentazione efficace che non vada a soffocare le possibilità innovative delle risorse virtuali[62].

Tale questione è stata affrontata in vari modi, riscontrando risposte differenti da ogni Paese. Le categorie normative possono essere identificate come:

- Lasciare "carta bianca" e intervenire in situazioni emergenziali;
- Consolidare un'ambiguità normativa per la delibera sulle questioni, creando una sorta di limbo regolamentativo;
- Delineare una precisa struttura normativa capace di bilanciare gli interessi pubblici;
- Divieti Assoluti;

[61] Chohan, U. (2021). *"Public Value and the Digital Economy"*(1st ed.): Chapter "co-creating value with citizen".
[62] Chohan, U. W. (2022). *"Cryptocurrencies: A brief thematic review".* Available at SSRN 3024330.

Ci sono governi che vedono le criptovalute come una minaccia troppo grande, altri come un'opportunità economica, altri ancora come un equilibrio tra questi fattori.

Gli Stati Uniti rappresentano un esempio normativo di equilibrio tra regolamentazione e innovazione. Paesi come Cina e India considerano le valute virtuali come elementi ingestibili nel lungo termine, pericolose per la sostenibilità economica del Paese proponendo valute digitali delle banche centrali (CBDC) che permettono di esercitare l'autorità monetaria sovrana ed espandere una capillare sorveglianza sull'offerta di moneta (iniziativa allettante per regimi autoritari).

Il Paese più favorevole alla diffusione e adozione delle criptovalute è El Salvador, il quale ha dichiarato Bitcoin una moneta a corso legale, al pari della propria moneta sovrana.

La problematica principale risiede nella diversità giuridica dei Paesi nei confronti del settore cripto. Fino a quando non verrà stabilita una coalizzazione normativa, vi sarà una "cortina di ferro" tra Governi "presuntuosi", restii all'adozione di criptovalute e Governi flessibili, aperti all'impiego degli strumenti virtuali alla stregua di qualsiasi bene sul mercato. La fiducia è il fondamento della vita economica, eppure è qualcosa di molto fugace nel regno virtuale: è necessaria una coesione globale tra gli sviluppatori e sostenitori del sistema cripto-centrico.

Matrici criminali quali terroristi, mafie, apparati statali corrotti e hacker hanno macchiato lo scenario delle criptovalute per i propri fini, soffocandone lo sviluppo e la diffusione.[63]

[63] Stroukal, D. (November 2016). *"Bitcoin and other cryptocurrency as an instrument of crime in cyberspace".* In Proceedings of Business and Management Conferences (No. 4407036). International Institute of Social and Economic Sciences.

3.1.5 Inclusione finanziaria

La promessa e la retorica delle criptovalute risiedono nella loro potenziale capacità di favorire l'inclusione finanziaria e mitigare le diseguaglianze economiche, rendendosi accessibili a chiunque, comprese le popolazioni in via di sviluppo senza servizi bancari[64]. Tale promessa rappresenterebbe un notevole incentivo per l'implementazione delle tecnologie blockchain e criptovaluta in tali paesi.

La duplice finalità consiste dunque, sia nell'aumentare la partecipazione della popolazione nel campo finanziario globale, sia nell'ampliare il seguito di sostenitori delle criptovalute.

Tuttavia, attualmente, l'inegualità del mercato di criptovalute non differisce molto dalle tradizionali forme di capitale. Per esempio, il possesso di token Bitcoin è concentrato in un numero decisamente ristretto di portafogli e questa potrebbe sembrare un'arma a doppio taglio in quanto la ristretta concentrazione della valuta virtuale potrebbe inficiare l'inclusione finanziaria. Tali demeriti sono da ricondurre alla presenza di soggetti nel panorama virtuale che definiamo come "whales"[65], i quali sono in grado di influenzare pesantemente il mercato con i loro comportamenti.

[64] Vincent, O., & Evans, O. (2019). *"Can cryptocurrency, mobile phones, and internet herald sustainable financial sector development in emerging markets?"* Journal of Transnational Management, 24(3), 259-279.

[65] Tradotto con balene, intesi come portafogli importanti costiituiti da un considerevole ammontare della criptovaluta: alludono ai cretacei in grado di sconvolgere il mare (mercato) anche con semplici movimenti (acquisti e vendite).

Figura 13: Distribuzione dei token bitcoin e corrispettivi valori monetari

Bitcoin distribution

Balance, BTC	Addresses	% Addresses (Total)	Coins	USD	% Coins (Total)
(0 - 0.00001)	4165858	7.9% (100%)	22.34 BTC	$954,056	0% (100%)
[0.00001 - 0.0001)	10155787	19.26% (92.1%)	437.15 BTC	$18,669,162	0% (100%)
[0.0001 - 0.001)	13453070	25.51% (72.85%)	5,232 BTC	$223,426,588	0.03% (100%)
[0.001 - 0.01)	12235392	23.2% (47.34%)	44,818 BTC	$1,913,991,779	0.23% (99.97%)
[0.01 - 0.1)	8159039	15.47% (24.14%)	274,847 BTC	$11,737,693,370	1.4% (99.74%)
[0.1 - 1)	3551860	6.73% (8.67%)	1,096,670 BTC	$46,834,729,913	5.6% (98.34%)
[1 - 10)	864827	1.64% (1.93%)	2,148,893 BTC	$91,771,252,011	10.96% (92.74%)
[10 - 100)	138893	0.26% (0.29%)	4,411,434 BTC	$188,395,974,083	22.51% (81.78%)
[100 - 1,000)	13917	0.03% (0.03%)	3,886,301 BTC	$165,969,520,391	19.83% (59.27%)
[1,000 - 10,000)	1904	0% (0%)	4,723,514 BTC	$201,723,784,521	24.1% (39.44%)
[10,000 - 100,000)	103	0% (0%)	2,311,004 BTC	$98,694,431,885	11.79% (15.34%)
[100,000 - 1,000,000)	4	0% (0%)	694,921 BTC	$29,677,504,604	3.55% (3.55%)

History

Addresses richer than

$1	$100	$1,000	$10,000	$100,000	$1,000,000	$10,000,000
45,436,320	19,835,706	8,898,689	2,712,703	449,595	89,101	7,343

Fonte: bitinfocharts.com/top-100-richest-bitcoin-addresses

3.2 BENEFICI NELL'UTILIZZO DELLE CRIPTOVALUTE

Nel panorama accademico-finanziario ci sono differenti opinioni riguardo al futuro delle criptovalute. Il punto di vista ottimistico è fondato su molteplici benefici che hanno permesso fino ad oggi, la diffusione e crescita del mercato cripto[66].

Il primo beneficio è ampiamente descritto dall'architettura stessa delle criptovalute: la decentralizzazione. Tale pilastro permette al sistema di auto-gestirsi senza la presenza di un'autorità centrale in grado di imporre regolamenti e controllare tutte le azioni dei partecipanti. Per esempio, gli istituti bancari possiedono tutte le informazioni relative a dati personali e alle operazioni dei clienti. Tuttavia, gli enti governativi hanno la

[66] Bunjaku, F., Gjorgieva-Trajkovska, O., & Miteva-Kacarski, E. (2017*). "Cryptocurrencies–advantages and disadvantages*". *Journal of Economics*, *2*(1), 31-39.

possibilità e gli strumenti tecnologici adeguati a identificare gli utenti di una blockchain nel caso in cui vi siano sospetti o prove nel coinvolgimento di questi in attività illegali.

Il secondo beneficio è rappresentato dalla semplicità, economicità ma allo stesso tempo robustezza della sicurezza. I sistemi tradizionali, banche e operatori dei sistemi di pagamento (Visa, Mastercard…), investono ingenti somme per garantire la protezione dei dati ai loro clienti. Prendendo sempre come esempio un ente bancario, una problematica della infrastruttura interna potrebbe portare al blocco totale del sistema e dunque di tutte le transazioni. La rete peer to peer permette invece di operare anche nel caso in cui non tutti i nodi siano operativi, in quanto ogni nodo possiede le informazioni necessarie all'operatività della blockchain, a differenza dei sistemi basati su server centrali, il cui disfunzionamento porterebbe a un arresto totale del sistema.
Il sistema crittografico può essere colpito da "51%attacks" e "deep attacks", i quali, come descritti in precedenza, richiedono un elevatissimo costo e rischio per l'hacker, senza offrire una sicura realizzazione dell'attacco. Inoltre, quanti più utenti partecipano allo sviluppo della blockchain, tanto maggiore è il grado di sicurezza della stessa in quanto sarà più complesso minare blocchi segreti che possano alterarla.

Considerando nuovamente l'architettura essenziale delle criptovalute, altri benefici sono associati all'anonimato dei partecipanti e alla trasparenza del sistema. Chiunque può operare nel sistema senza essere identificato, essendo riconosciuto semplicemente come un agente economico, senza dover riferire informazioni personali e senza il timore che queste siano diffuse a soggetti ed enti terzi.

Ulteriori benefici sono legati alle transazioni e commissioni del sistema. L'utilizzo di una blockchain permette di effettuare transazioni rapide a seguito della convalida dell'operazione. Sono particolarmente efficienti le transazioni transfrontaliere, le quali vengono processate in tempi decisamente minori rispetto ai sistemi tradizionali di pagamento. Dunque, un possessore di criptovalute possiede gli strumenti finanziari più efficaci per effettuare le transazioni.

Il tema delle commissioni può essere analizzato sotto punti di vista differenti in quanto rappresenta un punto controverso. In precedenza, abbiamo sottolineato come le commissioni in un sistema di pagamento basato su blockchain siano instabili e volatili, essendo determinate in funzione della partecipazione degli utenti e, dunque, dalla domanda e offerta del mercato.

Dunque, da un lato l'alta volatilità del mrcato cripto-centrico potrebbe portare ad anormali incrementi delle commissioni, dall'altro lato si suppone che la diffusione e graduale stabilizzazione del mercato possa indurre ad una riduzione del valore delle commissioni rispetto ai sistemi di pagamento tradizionali[67]. Nonostante le commissioni siano fortemente influenzate dai costi energetici necessari al sostenimento delle operazioni, permettono di semplificare la loro comprensione rispetto alla loro corrispondente parte tradizionale. Infatti, le commissioni bancarie rappresentano il compenso operativo di tutti i soggetti che lavorano quotidianamente per mantenere l'operatività del sistema bancario, mentre le commissioni legate al mondo cripto sono direttamente applicate ai costi energetici e di servizio degli Exchange.

[67] le commissioni delle transazioni sono legate a tutti gli operatori bancari che operano per la transazione, come venditore, banca del cliente, operatore diretto del sistema…

CAPITOLO 4: INFLUENZA PSICOLOGICA E TECNOLOGICA

Con tali dimensioni in gioco, tutti gli operatori coinvolti sono mossi dall'incentivo di estrarre ogni minimo vantaggio dall' architettura crittografica, fondata su limiti e desideri umani, e idealizzata sottoforma di fiducia, progresso, emancipazione e libertà.

Sotto quest'ottica, il mondo delle criptovalute ha un' influenza virtuale e reale, aspirando a guadagni materiali, pur essendo relegato ad un' architettura digitale decentralizzata, totalmente incentrata su codici, programmazione, potenza computazionale ma in grado di evocare una profonda risonanza emotiva ai sostenitori. Le criptovalute rappresentano un fenomeno intersoggettivo, come il denaro stesso, costituito da elementi interconnessi da fattori sociali, economici, legali e tecnologici.

4.1 "VALORE" DELLE CRIPTOVALUTE

Il quesito apparentemente semplice che ha incuriosito la mente di tutti ruota attorno al "valore" delle criptovalute e la diffusione di esse nel panorama finanziario ha suscitato dubbi e perplessità anche sul significato del denaro stesso nella società. Il guru della tecnologia Palihapitiya ha sagacemente definito bimodale il valore a lungo termine della criptovaluta: o varrà milioni o zero.[68]

L'incessante volatilità dei prezzi ha distolto il pubblico dal valore a lungo termine del mercato cripto: tale "rumore" disorientante è dovuto a mercati imperfetti, asimmetrie informative e normativa inadeguata.

[68] https://zycrypto.com/tech-investor-palihapitiya-says-bitcoin-price-will-either-reach-millions-or-go-to-zero.

Nonostante queste imperfezioni spaventino molti investitori, i veri sostenitori delle criptovalute liquidano il "rumore" sostenendo come non siano altro che "spigoli che verranno smussati" da una sempre più vasta adozione del progetto cripto-centrico.
Il lavoro di Aswanth Damodaran[69] permette di analizzare la logica dietro la valutazione delle criptovalute, osservate come asset, merce, valuta o oggetto da collezione.
In base alla loro concettualizzazione, le criptovalute possono avere utilizzi diversi, come per esempio, l'identità di "oro millenario" (riserva aciclica o anticiclica di valore), la funzione di valuta digitale a tutti gli effetti (in attesa di adozione ufficiale) oppure come semplice curiosità.

Il nuovo e ricco contesto offerto dalle criptovalute crea uno scenario di studio particolarmente complesso relativo alle tendenze degli investitori[70] . Come menzionato precedentemente, i social hanno un emblematico impatto psicologico in grado di generare hype positivo o negativo, sostenendo l'ipotesi che le bolle di mercato siano introdotte gradualmente dalla psicologia stessa. Anche l'indole del soggetto investitore rappresenta una caratteristica chiave per l'inserimento nel mercato delle criptovalute. È stato evidenziato come un soggetto con eccessivo autocontrollo e sicurezza di sé sia il prototipo del principale investitore nel mercato di valute virtuali[71].
In relazione alla psicologia del collettivo, gli studiosi si sono soffermati sul fenomeno di herd behavior (comportamento del gregge)[72], il quale segnala un' imperfezione del mercato basata sull'influenza del pensiero di gruppo. Questo fenomeno condiziona in

[69] Damodaran A. (2017).*" The Bitcoin Boom: Asset, Currency, Commodity or Collectible?"* .
[70] Delfabbro, P., King, D. L., & Williams, J. (2021). *"The psychology of cryptocurrency trading: Risk and protective factors".* Journal of Behavioral Addictions.
[71] Sudzina, F., Dobes, M., & Pavlicek, A. (2021). *"Towards the psychological profile of cryptocurrency early adopters: Overconfidence and self-control as predictors of cryptocurrency use".* Current Psychology, 1-5.
[72] Williams, J. (2021). *"The psychology of cryptocurrency trading: Risk and protective factors.".*

particolar modo la fascia d'età più giovane, creando un giocoforza tra l'avidità del mercato e la paura di commettere errori in esso, tanto da esserne divorato.

La trattazione psicologica richiederebbe una sperimentazione ed uno sforzo maggiore allo scopo di non essere ridotta come un mero repertorio di casi studio: sarebbe opportuno dedicare uno studio sulla psicologia della finanza, intraprendendo un'adeguata analisi sulla psicologia della partecipazione virtuale e dell'approccio alle valute virtuali.

4.2 APPROCCIO TECNOLOGICO

L'uso delle criptovalute offre interessanti opportunità di business nel contesto dei servizi finanziari, dei contratti intelligenti, delle attività basate sui token.

Qualsiasi tipologia di tecnologia viene valutata in funzione di una valutazione "custumer-centric", incentrata sulla figura del cliente, la quale alimenta l'interesse per la creazione di modelli di business innovativi che vadano oltre la performance economica.

Esempi di come le grandi società stiano sfruttando le criptovalute possono essere individuati nell'accettazione delle valute per i pagamenti (Dell, Microsoft, Aliexpress), nello scambio o conservazione di beni e servizi nei mercati virtuali, acquisto di archiviazioni cloud (Golem e Stor), contratti intelligenti e tracciabilità dei clienti, gestione della catena di fornitura e della finanza, sistemi di ricompense e incentivi basati sulla co-creazione di valore (come piattaforme di blog, esempio Steemit), piattaforme di streaming decentralizzate (Dtube), piattaforme social (reddit, discord) o piattaforme di apprendimento (Tutellus).

Al fine di esplorare i fattori che guidano la decisione di utilizzare le criptovalute, l'analisi si focalizza sul valore percepito della tecnologia, dal punto di vista economico ed

emozionale[73]. García-Monleón e al (2023) propongono un modello strutturale basato sul "valore" (VAM, value-based approch model). Nella loro analisi, viene svolto uno studio sul ruolo che assume la "conoscenza delle criptovalute" nel rapporto tra l'opinione che gli agenti economici hanno delle valute virtuali e la loro intenzione di utilizzarle.
I risultati suggeriscono una positiva correlazione tra l'adozione delle criptovalute e i fattori sia economici che emotivi. In particolare, viene evidenziato come la conoscenza della tecnologia abbia un effetto mediatore sul lato emotivo del valore percepito delle criptovalute. Inoltre, è stato notato come le considerazioni per la sostenibilità ambientale sono principalmente guidate dalla percezione finanziaria delle criptovalute, mentre quelle relative alla sostenibilità sociale sono completamente mediate da aspetti finanziari ed emotivi. I benefici vanno oltre gli incentivi economici e finanziari: gli utenti valorizzano fattori come la velocità delle transazioni, la trasparenza, la libertà di investimento senza il controllo governativo, l'anonimato, la privacy, il potenziale contributo all'inclusione finanziaria e aspetti di sostenibilità ambientale[74].

I principali fattori che portano l'individuo a adottare le criptovalute si sono evoluti seguendo una parallela evoluzione delle problematiche, necessità e aspirazioni degli utenti stessi. Il valore percepito è un criterio implicito utilizzato dai consumatori nel processo decisionale che tiene conto dei benefici e sacrifici monetari, così come di valori non monetari (impegno, rischio, tempo). Boksberg e Melsen (2011)[75], hanno suggerito come il concetto di valore potrebbe richiedere delle differenziazioni: dal punto di vista

[73] García-Monleón, F., Erdmann, A., & Arilla, R. (2023). *"A value-based approach to the adoption of cryptocurrencies".* Journal of Innovation & Knowledge, 8(2), 100342.
[74] Lee, B. C. (2021). "*The promise of Bitcoin: The future of money and how it can work for you*". McGraw Hill Professional.
[75] Boksberger, P. E., & Melsen, L. (2011). *"Perceived value: a critical examination of definitions, concepts and measures for the service industry".* Journal of Service Marketing, 25, (3) 229240.

economico, il valore è tradizionalmente inteso come un' utilità mentre la sua natura percepita è un concetto più ampio e complesso che spazia oltre la razionalità.

Prendiamo in considerazione la multidimensionale visione del valore percepito di Hartman[76], distinto tra valore estrinseco (strumentale/utilitaristico), valore intrinseco (soddisfazione emotiva) e valore sistemico (aspetti razionali o logici come l'analisi costi/benefici). Questo framework ci permette di analizzare l'influenza dei valori citati in relazione all' adozione delle criptovalute.

Ipotesi 1, *valore percepito:*

- H1.1: L'intenzione di utilizzare le criptovalute è guidata dalla percezione utilitaristica del soggetto;
- H1.2: Fattori sistemici influenzano positivamente le intenzioni del soggetto;
- H1.3: Le intenzioni sono guidate principalmente da fattori emotivi.

Il modello TAM[77],Technology adoption model, ha confermato come la facilità di uso e l'utilità siano i principali motori trainanti dell'adozione delle tecnologie (nel nostro caso le criptovalute). Hanno un ruolo fondamentale in questi risultati le transazioni veloci e decentralizzate.

Venkatesh (2003) propone un modello sintetizzato basato su otto teorie dell'adozione tecnologica, conosciuto come UTAUT[78] (Unified Theory of Adoption and Use of

[76] Hartman, R. S. (1967). *"The Structure of Value: Foundations of a Scientific Axiology".* Wipf and Stock. OR: Eugene

[77] Davis, F. D. (1989*). "Perceived usefulness, perceived ease of use, and user acceptance of information technology"*. MIS Quarterly, 13(3), 319–340.

[78] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). *"User acceptance of information technology: Toward a unified view*". MIS Quarterly, 27, (3) 425478.

Technology), esteso poi con UTAUT2 model[79], il quale ha permesso di risaltare particolari fattori innovativi come driver trainanti.

Tra i risultati ottenuti da questo modello emerge che le aspettative relative alla stabilità delle transazioni e alla performance del sistema sono elementi importanti per l'adozione delle criptovalute. È stata considerata anche l'influenza sociale, rivelando risultati ambigui: Abbasi e al. (2021)[80] non hanno riscontrato alcun effetto relativo all'influenza sociale mentre JiXi (2021)[81] ha osservato come il driver sociale sia in grado di influenzare la propensione all'investimento nelle criptovalute in soggetti di età intermedia. Questo risultato è dovuto al fatto che condizioni facilitanti come risorse e opportunità siano potenziali determinanti per l'approccio alle criptovalute.

Zhao e Zhang (2021)[82] hanno individuato una correlazione positiva tra la conoscenza finanziaria e la propensione all'investimento in criptovalute, mediato dall'esperienza in campo finanziario. Inoltre, anche la capacità di adattamento personale alle tecnologie influenza positivamente l'adozione. È possibile evidenziare un risultato opposto nel caso in cui un soggetto sia stato influenzato da un eventuale disagio psicologico dovuto al personale approccio al macrocosmo tech, portandolo a scegliere vie alternative.

Ipotesi 2, *knowledge:*

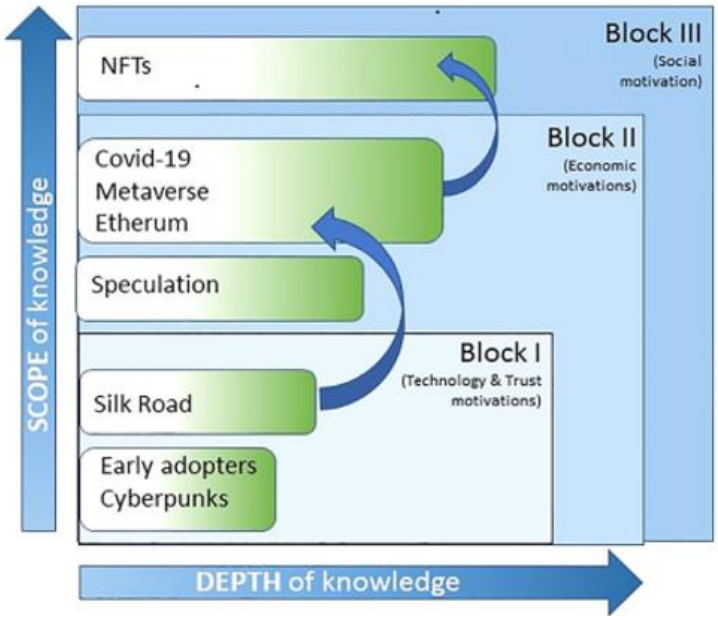
- H2.1: La profondità della conoscenza influenza la relazione tra valore percepito e intenzione di utilizzo delle criptovalute;

[79] Venkatesh, V., Thong, J. Y., & Xu, X. (2012). *"Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology".* MIS Quarterly, 36, (1)
[80] Abbasi, G. A., Tiew, L. Y., Tang, J. Q., Goh, Y. N., Thurasami, R., & Dragan, D. (2021). *"The adoption of cryptocurrency as a disruptive force: Deep learning-based dual stage structural equation modelling and artificial neural network analysis".* PLOS One, (3), 16.
[81] Ji-Xi, J. T., Salamzadeh, Y., & Teoh, A. (2021). *"Behavioral intention to use cryptocurrency in Malaysia: an empirical study"*. Bottom Line, (2), 34.
[82] Zhao, H. D., & Zhang, L. N. (2021)." *Financial literacy or investment experience: Which is more influential in cryptocurrency investment?".* International Journal of Bank Marketing, 39(7), 1208–1226.

- H2.2: Il valore emotivo e le intenzioni di utilizzo sono positivamente correlati in funzione della conoscenza;
- H2.3: Il valore finanziario è totalmente correlato alle intenzioni di uso delle criptovalute mediante la conoscenza finanziaria

Dunque, con l'evoluzione della conoscenza delle criptovalute, l'adattamento del soggetto al mondo cripto-centrico può influenzare le motivazioni per cui queste vengono utilizzate e potenzialmente rafforzare il ruolo dei fattori psicologici, come viene illustrato nella figura 14. Maggiore sarà la conoscenza e comprensione del settore e più profondo sarà il coinvolgimento, permettendo al soggetto di sfruttare tutti gli elementi del macrocosmo virtuale.

Figura 14: Concettualizzazione dell'influenza della conoscenza



Fonte: García-Monleón, F., Erdmann, A., & Arilla, R. (2023). A value-based approach to the adoption of cryptocurrencies.

Oltre agli aspetti determinanti identificati in precedenza, la sostenibilità ha conquistato un ruolo fondamentale come fattore di investimento, con il pubblico sempre più propenso

a scelte ESG[83]. Il tema sostenibilità in relazione alla tecnologia blockchain viene associato ai processi di elaborazione "verde", accessibilità ai mercati finanziari e pari opportunità, lavoro dignitoso e crescita economica.

È risaputo come il mining per le criptovalute costituisca una minaccia per l'efficienza energetica, essendo un importante "divoratore" di energia. Un potenziale contributo alla blockchain potrebbe consistere nell'incremento di efficienza per l'elaborazione dei dati o coinvolgere i propri progetti verso tematiche sostenibili come ecosistemi verdi ed energia pulita.

Le criptovalute possono contribuire alla riduzione della povertà riducendo l'esclusione finanziaria nelle comunità che non hanno accesso ai mercati non disponendo di adeguati istituti finanziari. Le valute permetterebbero l'eliminazione delle barriere all'entrata facilitando le operazioni transfrontaliere, e la gestione della ricchezza al di fuori dei tradizionali istituti finanziari, creando un nuovo sistema decentralizzato.

Differenziando fattori enviroment e fattori social, consideriamo il grado di influenza di questi elementi tramite il valore percepito dell'adozione di cripto.

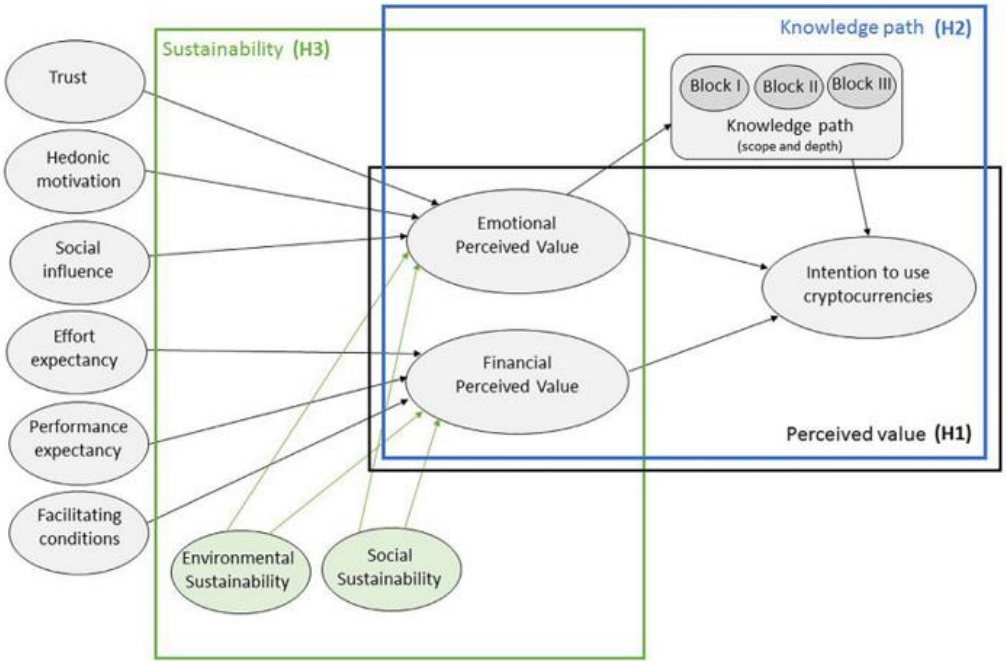
Ipotesi 3, *sustainability:*

- H3.1: le considerazioni sulla sostenibilità influenzano l'intenzione di utilizzare le criptovalute attraverso il valore percepito dagli utenti;
- H3.2: Le considerazioni sulla sostenibilità ambientale influenzano le decisioni degli utenti tramite il valore percepito, sia emotivo che finanziario;
- H3.3: considerazioni sulla sostenibilità sociale influenzano le decisioni degli utenti tramite il valore percepito, emotivo e finanziario.

[83] Environmental, Social and Governance, criteri che permettono di valutare le società (e di conseguenza gli investimenti) sotto un'ottica prevalentemente basata sulla sostenibilità.

La figura 14 riassume tutte le ipotesi (H1, H2, H3), delineando i ruoli della percezione del valore, della conoscenza finanziaria e della rilevanza del tema sostenibilità.

Figura 15: Modello strutturale dei fattori driver per la scelta delle criptovalute



Fonte: García-Monleón, F., Erdmann, A., & Arilla, R. (2023). A value-based approach to the adoption of cryptocurrencies.

CAPITOLO 5: IL MERCATO

Secondo Vora (2015)[84] le criptovalute rappresentano un'evoluzione tanto attesa per l'economia in quanto competeranno con gli approcci finanziari e normativi prevalenti, rappresentando uno strumento operativo alternativo per gli agenti economici, destinati ad essere coinvolti nella futura rivoluzione finanziaria.

L'asset virtuale si è ritagliato una posizione distinta nei mercati finanziari globali, in particolare dopo la sua rapida crescita ed espansione post pandemia. La capitalizzazione del mercato ha toccato quasi i 3 trilioni di dollari a fine 2021, assestandosi oggi a circa 1,7 trilioni (inizio 2020 erano meno di 250 miliardi)[85].

Figura 16: Capitalizzazione di mercato

Fonte: CoinmarketCap

[84] Vora, G. (2015). *"Cryptocurrencies: are disruptive financial innovations here?"* Mod. Econ. 6 (7), 816
[85] www.CoinMarketCap.com

Parallelamente alla crescita di notorietà, anche l'empiricità finanziaria delle criptovalute ha riscosso successo in ambito accademico-filosofico.

Le criptovalute hanno consolidato le proprie radici nel mercato finanziario a tal punto da essere in grado di influenzarne l'andamento. Tutto ciò è legato sia alla tipologia degli strumenti finanziari presi in considerazione, sia agli orizzonti temporali e prospettive di investimento analizzate.

Così come internet è stata una pietra miliare della crescita delle comunicazioni, le criptovalute potrebbero essere un importante aggiornamento del settore finanziario nella crescente era digitale. Secondo Allen e Bryant (2019) [86], le criptovalute sono uno step nell'evoluzione della corrente cultura che sta lentamente modificando il mondo in una versione digitale e virtuale. Nonostante le cripto e la loro innata tecnologia saranno più accessibili e utili in futuro, attualmente è una questione decisamente divisiva.

5.1 CRIPTO E MERCATO TRADIZIONALE

La relazione tra cripto e mercato azionario ha attirato l'attenzione di tutti i partecipanti al mercato, dai capitalisti ai banchieri, agli investitori e politici.

I ricercatori hanno scoperto una relazione multilaterale delle criptovalute con i mercati azionari influenzata dall'inflazione del paese, fluttuazioni dei tassi di cambio, sistema bancario complesso/costoso, incertezza normativa, vincoli finanziari e soprattutto esistenza o minaccia di controllo del capitale.

Possiamo suddividere l'analisi in relazione alla rilevanza economica dei mercati analizzati: emergenti, avanzati, islamici e periodo Covid.

[86] Allen, B., Bryant, S.K., (2019). *"The market for cryptocurrency: how will it evolve?"*. Global Econ. J. 19 (3), 1950019.

5.1.1 Mercati emergenti

Secondo l'indice di mercato MSCI[87], i mercati emergenti sono rappresentati da Paesi in via di sviluppo che stanno rapidamente crescendo e industrializzandosi. Ad oggi è costituito da 25 paesi che possono essere raggruppati in blocchi economici[88] (BRICS, CIVETS, BEM, and MENA). Un riassunto complessivo è proposto dalla tabella 1, nella quale è possibile osservare le principali chiavi che collegano i due mercati finanziari.

BRICS è un blocco costituito dai principali 5 paesi del mercato emergente, ovvero Brasile, Russia, India, Cina e Sud Africa.

L'analisi di Wang e al (2019)[89] osserva come i mercati azionari di Basile e Cina siano prevalentemente più instabili e impredicibili rispetto ai mercati sviluppati.

Lahiani and Jlassi (2021)[90] and Jeribi and Ghorbel (2021)[91] hanno analizzato la correlazione delle 5 principali criptovalute (Bitcoin, Dash, Ethereum, Monero, Ripple) con il mercato del BRICS ma non sono emerse profonde e significative correlazioni tra valute virtuali e BRICS: nessuna criptovaluta possiede la forza necessaria per predire il mercato. Bitcoin non svolge un ruolo di "copertura" nei paesi del BRICS rispetto alle nazioni sviluppate, tuttavia, può essere adoperato come strumento per la diversificazione di asset, pensato come "il nuovo oro". Per riassumere, la maggior parte dei ricercatori ha illustrato come gli effetti della correlazione siano più deboli nel BRICS.

[87] https://www.msci.com/our-solutions/indexes/emerging-markets.
[88] https://ggu.libguides.com/c.php?g¼106866&p¼693916.
[89] Wang, P., Zhang, W., Li, X., Shen, D., (2019)*." Is cryptocurrency a hedge or a safe haven for international indices? A comprehensive and dynamic perspective".* Finance Res. Lett. 31, 1–18.
[90] Lahiani, A., Jlassi, N.B., (2021). *"Nonlinear tail dependence in cryptocurrency-stock market returns: the role of Bitcoin futures".* Res. Int. Bus. Finance 56, 101351.
[91] Jeribi, A., Ghorbel, A., (2021). *"Forecasting developed and BRICS stock markets with cryptocurrencies and gold: generalized orthogonal generalized autoregressive conditional heteroskedasticity and generalized autoregressive score analysis*". Int. J. Emerg. Mark.

Dopo il BRICS, il mercato emergente più animato è costituito dai paesi CIVET (Colombia, Indonesia, Vietnam, Egitto, Turchia).

Riprendendo il lavoro di Kumah e Odei-Mensah (2021)[92], Bitcoin ha un' integrazione positiva nel medio termine con il mercato egiziano. Nel lungo termine, Ethereum presenta un forte effetto negativo mentre Litecoin dimostra un effetto positivo sul mercato azionario egiziano. Per il mercato turco, fatta eccezione per il tasso di cambio con il dollaro, ci sono molte prove dell'influenza di shock bilaterali tra i mercati ed eccessiva volatilità tra Bitcoin e altri asset finanziari.

Hung (2021)[93] ha individuato come Bitcoin abbia una positiva correlazione con il mercato azionario di CEE (Croazia, Ungheria, Polonia, Romania e Repubblica Ceca) utilizzando il Dynamic Equi-Correlation GARCH model. Omane-Adjepong et al. (2021)[94] hanno trovato un asimmetrico comportamento "gregge" tra il mercato cripto e azionario di 10 paesi emergenti all'interno del G20. Le Filippine e la Tailandia presentano una correlazione positiva mentre il mercato della Malesia ha una relazione avversa con le cripto (Thampanya et al., 2020)[95].

Tabella 1: Risultati relativi alla correlazione tra Criptovalute e mercato azionario nei paesi emergenti

Autore	Criptovalute considerate	Paesi coinvolti	Risultati principali
Wang e al. (2019)	*973 criptovalute*	30 indici internazionali (utilizza gli indici al posto delle nazioni)	-I mercati azionari di Brasile, China e Giappone sono più instabili e imprevedibili comparati ai mercati sviluppati;
Lahiani e Jlassi (2021)	Bitcoin, Dash, Ethereum, Monero e Ripple	BRICS	-Non sono state rilevate sostanziali correlazioni tra il mercato cripto e azionario dei paesi BRICS; -Il legame cripto-stocks è migliorato dall'introduzione dei "Bitcoin Future" nel 2017;

[92] Kumah, S.P., Odei-Mensah, J., (2021). *"Are Cryptocurrencies and African stock markets integrated*?" Q. Rev. Econ. Finance 81, 330–341.
[93] Hung, N.T., (2021). *"Bitcoin and CEE stock markets: fresh evidence from using the DECOGARCH model and quantile on quantile regression"*. Eur. J. Manag. Bus. Econ.
[94] Omane-Adjepong, M., Paul Alagidede, I., Lyimo, A.G., Tweneboah, G., (2021). *"Herding behaviour in cryptocurrency and emerging financial markets"*. Cogent Econ. Fin. 9 (1), 1933681.
[95] Thampanya, N., Nasir, M.A., Huynh, T.L.D., (2020). *"Asymmetric correlation and hedging effectiveness of gold & cryptocurrencies: from pre-industrial to the fourth industrial revolution"*. Technol. Forecast. Soc. Change 159, 120195.

			-Tra i Paesi Brics, solo il Brasile evidenzia cenni di relazione con le criptovalute ;
Jeribi e Ghorbel (2021)	Bitcoin, Dash, Ethereum, Monero e Ripple	BRICS	-Comparato ai mercati sviluppati, Bitcoin non gioca un ruolo importante di copertura nei paesi BRICS; -Solo Bitcoin costruisce una positiva correlazione con il mercato brasiliano e sud africano
Kumah e Odei-Mensah (2021)	Bitcoin, Ethereum e Litecoin	Egitto, Sud Africa, Nigeria, Mauritius, Kenya, Ghana, Tunisia e Marocco	-Bitcoin ha un' integrazione a medio termine con il mercato azionario egiziano; -Nel lungo termine, Ethereum mostra un forte effetto negativo su mercato; al contrario LItecoin dimostra un positivo effetto sul mercato;
Vardar e Aydogan (2019)	Bitcoin	Turchia	-Riscontrato shock bilaterale tra i mercati e l'impatto della propagazione della volatilità tra Bitcoin e il mercato azionario turco;
Omane-Adjepong e al. (2021)	Bitcoin, Ethereum, Ripple, Litecoin, Dash, Ethereum Classic, NEO e Zcash	G20	-Rilevato un asimmetrico comportamento di gregge tra le criptovalute e i mercati azionari di 10 emergenti economie;

Fonte: Elaborazione propria

5.1.2 Mercati avanzati

I principali studi hanno individuato una plausibile relazione tra criptovalute e mercato azionario nei paesi sviluppati.

Isah and Raheem (2019)[96] hanno esplorato la teorica abilità predittiva delle criptovalute in relazione ai prezzi delle azioni statunitensi osservando come i modelli predittivi basati su BTC siano in grado di prevedere i ritorni delle azioni[97].

[96] Isah, K.O., Raheem, I.D., (2019). *"The hidden predictive power of cryptocurrencies and QE: evidence from US stock market"*. Phys. Stat. Mech. Appl. 536, 121032.
[97] Precisando come tale previsione può essere ritenuta più affidabile e precisa in situazioni di quantitative easing le quali sostengono anche la crescita delle criptovalute.

Erdas e Caglar (2018)[98] hanno analizzato l'impatto di Bitcoin nell'indice azionario US utilizzando il test delle causalità asimmetriche[99] e i loro risultati indicano che il legame tra Bitcoin e lo S&P 500 è unidirezionale: ciò implica che uno shock negativo di Bitcoin comporta anche una variazione negativa o positiva nel S&P, mentre uno shock positivo comporta solo uno shock negativo nell'indice azionario.

Riproponendo l'analisi di Lahiani e Jlassi (2021), incentrata sul GARCH (Generalized Auto Regressive Conditional Heteroskedasticity)[100] è stato dimostrato come sia le medie che le code tra cripto e ritorni degli stock, siano state influenzate dalla introduzione dei futures[101] sui Bitcoin. Ad esempio, prima dell'inserimento sul mercato dei Bitcoin futures, le criptovalute non avevano una particolare capacità nel proiettare i ritorni dell'equity. Viceversa, con la diffusione dei futures Bitcoin, le criptovalute hanno dimostrato una capacità predittiva estremamente forte nella proiezione dei rendimenti del mercato azionario, descrivendo la profondità della coda delle dipendenze tra i due mercati. Inoltre, lo studio ha rivelato come Ethereum, seguito da Bitcoin, svolge la funzione fondamentale di prevedere i ritorni delle criptovalute e delle azioni nelle economie avanzate. Fatta eccezione per il Giappone, il modello di stima basato su BTC è in grado di leggere i ritorni delle azioni dei paesi del G7 in maniera più adeguata rispetto ad un insieme di fattori macroeconomici.

---

[98] Erdas, M.L., Caglar, A.E., (2018). *"Analysis of the relationships between Bitcoin and exchange rate, commodities and global indexes by asymmetric causality test".* E. J. Eur. Stud. 9 (2), 27.

[99] Test che definisci la struttura asimmetrica delle potenziali connessioni causali tra più variabili, ovvero l'impatto asimmetrico dei valori passati di una variabile sul valore attuale di un'altra quando tutte le altre informazioni pertinenti sono considerate.

[100] Modello auto-regressivo econometrico utilizzato per l'analisi delle serie storiche: rappresenta una generalizzazione del modello ARCH che permette di analizzare la persistenza dei movimenti della volatilità senza dover stimare l'alto numero di parametri presenti nell'equazione della varianza condizionata di un modello ARCH.

[101] Contratti di derivati simmetrici che obbligano acquirente e venditore a scambiarsi una determinata quantità di uno strumento finanziario o sottostante ad un prezzo prefissato e con liquidazione differita a data futura prestabilita.

Il costante evolversi delle relazioni di dipendenza tra i due mercati sono in gran parte positive, stando a significare che i mercati azionari stanno acquisendo le fluttuazioni di prezzo dei mercati cripto: si ipotizza che il legame interattivo tra i due mercati finanziari possa permettere di utilizzare i cambiamenti di prezzi di uno come "segnavento"[102] per le fluttuazioni di prezzo dell'altro.

Altri studi hanno interagito con l'influenza del mercato azionario sulla volatilità delle criptovalute. Applicando il GARCH e l'EGARCH (Exponential Generalized Auto Regressive Conditional Heteroskedasticity) è stato evidenziato come le fluttuazioni di Bitcoin sono particolarmente intense durante cicli speculativi[103].

Tabella 2: Risultati relativi alla correlazione tra Criptovalute e mercato azionario nelle economie avanzate

Autore	Criptovalute considerate	Paesi coinvolti	Risultati principali
Erdas e Caglar (2018)	Bitcoin	USA	-Rilevate relazioni causali;
Salisu e al. (2019)	Bitcoin	G7	-I ritorni dei mercati dei membri G7 riscontrano una forte correlazione positiva:
Wang e al. (2019)	Bitcoin	USA e Unione Europea	-Esiste una significativa relazione temporale di causalità bilaterale tra le variabili monetarie di Bitcoin e del mercato equilty globale;
Zhang e al. (2018)	Bitcoin, Etehreum e Ripple	USA	-L'associazione che viene creata tra Bitcoin e gli strumenti tradizionali è minima, inoltre è molto variabile;
Isah e Raheem (2019)	Bitcoin	USA	-I sistemi di previsione basati sui BTC sono più efficienti nel prevedere i ritorni dell'equity;
Lopez-Cabarcos e al. (2021)	Bitcoin	USA	-Secondo i risultati, l'instabilità di Bitcoin è maggiormente imprevedibile nei periodi di incertezza;
Wang e al. (2020)	Bitcoin	USA	-S&P 500 ha un moderato impatto sui Bitcoin, mentre l'effetto su S&P 500 è diluitivo
Tiwari e al. (2019)	Litecoin	USA	-Litecoin rappresenta lo strumento più adeguato alla copertura dalla volatilità del mercato equity statunitense
Wang e al. (2021)	Bitcoin ed Ethereum	USA	-Rilevati effetti asimmetrici di contagio tra le due tipologie di mercati finanziari;

[102] Wang, H., Wang, X., Yin, S., Ji, H., (2021). *"The asymmetric contagion effect between stock market and cryptocurrency market"*. Finance Res. Lett., 102345.
[103] Lopez-Cabarcos, M.A., Perez-Pico, A.M., Pineiro-Chousa, J., ~ Sevic, A., (2021). *"Bitcoin volatility, stock market and investor sentiment. Are they connected?"* Finance Res. Lett. 38, 101399.

Charfeddine e al. (2020)	Bitcoin ed Ethereum	USA	-La connessione tra criptovalute e asset tradizionali è altamente vulnerabile a sconvolgimenti finanziari ed economici del mondo esterno;
Corbet e al. (2018)	Bitcoin, Ripple e Litecoin	USA	-Le criptovalute possono diventare un ottimo strumento per espandere le opportunità di investimento per i soggetti speculatori;

Fonte: Elaborazione propria

5.1.3 Mercato islamico

Nel corso degli anni sono stati intrapresi numerosissimi studi riguardanti la relazione tra mercato cripto e azionario. A beneficio di futuri investitori desiderosi di allargare i propri orizzonti, è necessario ampliare la letteratura incentrata sul mercato islamico, in quanto caratterizzato da profonde lacune.

Lo studio di Rehman e al. (2020) [104] ha evidenziato come Bitcoin presenti una particolare dipendenza solo con i principali indici islamici. Inoltre, i risultati hanno rivelato l'esistenza degli effetti di ricaduta tra Bitcoin e il mercato islamico. È importante aggiungere come azioni del mercato islamico si comportano come copertura utile in un portafoglio nel quale sono presenti Bitcoin.

Mensi e al. (2020)[105] hanno ottenuto informazioni relativamente simili ma decisamente più specifiche al lavoro di Rehman: gli investimenti a lungo termine nei mercati azionari islamici possono generare minori benefici di diversificazione rispetto a quelli di breve termine. A tal proposito, i vantaggi di diversificare il portafoglio con Bitcoin e materie prime islamiche differiscono in base alle prospettive temporali e alla frequenza di azione

[104] Rehman, M.U., Asghar, N., Kang, S.H., (2020). *"Do Islamic indices provide diversification to bitcoin? A time-varying copulas and value at risk application".* Pac. Basin Finance J. 61, 101326.
[105] Mensi, W., Rehman, M.U., Maitra, D., Al-Yahyaee, K.H., Sensoy, A., (2020). *"Does bitcoin comove and share risk with Sukuk and world and regional Islamic stock markets? Evidence using a time-frequency approach".* Res. Int. Bus. Finance 53, 101230.

sul mercato. Secondo Ahmed (2021)[106] nelle economie sviluppate la volatilità al rialzo di Bitcoin ha impatti negativi simultanei e ritardati negli indici islamici, principalmente nelle fasi bear (ribassiste) del mercato. Nel frattempo, la volatilità a ribasso sembra avere un impatto significativo nei ritorni sia se il mercato islamico tende al rialzo sia se tende al ribasso. Un recente studio di Yaroavaya e al. (2021)[107] ha rivelato come l'oro e il petrolio siano degli importanti predittori del mercato tradizionale mentre Bitcoin non è totalmente attendibile: ciò è legato al fatto che le fluttuazioni finanziarie degli asset islamici sono determinati da fattori ampiamente ancorati all'oro e petrolio.

Tabella 3: Risultati relativi alla correlazione tra Criptovalute e mercato azionario nel mercato islamico

Autore	Criptovalute considerate	Paesi coinvolti Indici fin.	Risultati principali
Rehman e al. (2020)	*Bitcoin*	DJIJP, DJICA, and DJIUK	-Bitcoin ha una correlazione temporale con gli indici indicati
Mensi e al. (2020)	*Bitcoin*	DJIM, IMUS, DJIEU, DJIAP, DJIUK, DJIJP, DJICA, IMXL, DJSUKUK	-Investimenti a lungo termine potrebbero generare un minor effetto diversificazione rispetto ad investimenti a breve termine
Ahmed (2020)	*Bitcoin*	Economie sviluppate	-La volatilità a rialzo di Bitcoin ha effetti negativi istantanei e ritardati sugli indici islamici principalmente in fasi ribassiste; Invece, una volatilità a ribasso sembra avere un significativo effetto sui ritorni del mercato islamico sia a rialzo che a ribasso;
Yorovaya e al (2021)	*Bitcoin*	DJIM, DJIA, ICE BofA Global, DJSUKUK	-Covid 19, oro e petrolio rappresentano i principali predittori del mercato tradizionale islamico, mentree Bitcoin non rappresenta un predittore cruciale;

Fonte: Elaborazione propria

5.1.4 Relazione tra criptovalute, mercati tradizionali e Covid

La crisi pandemica ha modificato drasticamente lo scenario finanziario di questi anni, rendendo vulnerabili molti fattori importanti che caratterizzano i due mercati.

[106] Ahmed, W.M., (2021). *"How do Islamic equity markets respond to good and bad volatility of cryptocurrencies? The case of Bitcoin*". Pac. Basin Finance J. 70, 101667.
[107] Yarovaya, L., Elsayed, A.H., Hammoudeh, S., (2021). *"Determinants of spillovers between Islamic and conventional financial markets: exploring the safe haven assets during the COVID-19 pandemic".* Finance Res. Lett. 43, 101979.

Jeribi e al. (2021)[108] utilizzando il NARDL (Nonlinear Autoregressive Distributed Lag) hanno sostenuto come la dinamica relazione tra ritorni delle criptovalute e ritorni del mercato azionario ha subito delle variazioni durante il periodo di crisi. Inoltre, è stato osservato come le cripto principali hanno costituito una sorta di "porto" per i mercati emergenti, ma non nei mercati avanzati, come dimostrato da Conlon e al. (2020)[109]. Essi hanno notato come i principali token non rappresentino un'ancora nei mercati globali (FTSE 100; S&P 500; IBEX; FTSE MIB e CSI 300), in grado di aiutare gli investitori nel tumulto scaturito con la crisi pandemica. Grobys (2021)[110] ha studiato la correlazione tra azionario americano e Bitcoin, definendo come il crollo del prezzo di Bitcoin non è dovuto unicamente agli effetti del covid ma ad un problema microstrutturale degli Exchange. A tal proposito è stato notato come Bitcoin sia stato uno scarso rifugio durante il Covid al pari della maggior parte degli strumenti finanziari, dimostrati inaffidabili in tale periodo: in fasi di incertezza i due mercati si dimostrano interconnessi.

Infine, Caferra e Vidal Tomas (2021)[111] hanno evidenziato come, a seguito del crollo dei due mercati, le criptovalute abbiano dimostrato una più rapida ripresa rispetto all'azionario, il quale è rimasto a lungo nella fase ribassista.

Tabella 4: Risultati relativi alla correlazione tra Criptovalute, mercato tradizionale e Covid

Autore	Criptovalute considerate	Paesi coinvolti	Risultati principali
Jeribi e al. (2021)	Bitcoin, Dash, Ethereum, Monero, and Ripple	BRICS	-Durante la crisi finanziaria dovuta al covid, le criptovalute considerate si sono rivelate un porto sicuro per 3 economie emergenti: Brasile, Cina e Russia;
Lahmiri e Bekiros (2021)	45 criptovalute	16 mercati Equity internazionali	-La pandemia ha comportato un sostanziale impatto sui ritorni a lungo termine e sulla volatilità di criptovalute e mercati azionari internazionali;

[108] Jeribi, A., Jena, S.K., Lahiani, A., (2021). *"Are cryptocurrencies a backstop for the stock market in a COVID-19-led financial crisis? Evidence from the NARDL approach".* Int. J. Financ. Stud. 9 (3), 33.
[109] Conlon, T., Corbet, S., McGee, R.J., (2020). "Are cryptocurrencies a safe haven for equity markets? An international perspective from the COVID-19 pandemic". Res. Int. Bus. Finance 54, 101248.
[110] Grobys, K., (2021). *"When Bitcoin has the flu: on Bitcoin's performance to hedge equity risk in the early wake of the COVID-19 outbreak".* Appl. Econ. Lett. 28 (10), 860–865.
[111] Caferra, R., Vidal-Tomas, D., (2021). *"Who raised from the abyss? A comparison between cryptocurrency and stock market dynamics during the COVID-19 pandemic".* Finance Res. Lett. 101954.

Conlon e al. (2020)	Bitcoin, Ethereum e Tether	USA (S&P500), UK (FTSE 100), Italia (FTSE MIB), Spagna (IBEX) e Cina (CSI 300)	-Bitcoin ed Ethereum non rappresentano un asset rifugio per la maggior parte dei mercati azionari esteri valutati nel corso del periodo Covid; -È stato evidenziato come invece tether abbia costituito un asset rifugio nel periodo recente, compresa l'era della crisi covid;
Mariana e al (2021)	Bitcoin ed Ethereum	USA (S&P500)	-Bitcoin ed Ethereum sono riconosciuti come rifugio sicuro per il breve termine: Ethereum è preferito come rifugio quando il mercato crolla rapidamente; Etehreum ha un tasso di volatilità dei ritorni maggiore rispetto a bitcoin;
CÒrbet e al. (2020)	Bitcoin	Cina (CSI 300)	-Oro e altre criptovalute non hanno un grande impatto sul mercato azionario cinese, il quale è fortemente connesso a Bitcoin;
Grobys (2021)	Bitcoin	USA (S&P500)	-il crollo del prezzo di Bitcoin non è stato causato solo alla pandemia ma principalmente dai problemi con la microstruttura del mercato exchange delle criptovalute;
Yousaf e Ali (2021)	Litecoin, Bitcoin ed Ethereum	USA	-Nel periodo antecedente l'era Covid, l'instabilità tra il mercato azionario americano e il mercato delle cripto erano basse;
Caferra e Vidal-Tomas (2021)	Bitcoin ed Ethereum	USA ed Eurozona (Francia e Germania	-Entrambi i mercati sono crollati precipitosamente durante la crisi pandemica: tuttavia, nonostante questa correlazione, il mercato cripto ha dimostrato una repentina ripresa mentre il mercato azionario;

Fonte: Elaborazione propria

5.2 PREDITTORI DEL MERCATO

Yukun liu e al. (2022)[112] hanno preso in considerazione un approccio basato su una serie di predittori dei rendimenti azionari, con la finalità di ricostruire strumenti paralleli per l'analisi del mercato cripto. Sono infatti necessarie regole empiriche che facilitino la comprensione dei meccanismi di determinazione dei prezzi degli asset, sia tradizionali che virtuali.

Il mercato azionario è il più studiato e la letteratura ha individuato una serie di fattori in grado di descrivere l'effetto cross section[113] dei ritorni del mercato. Prendendo in

[112] Liu, Y., Tsyvinski, A., & Wu, X. (2022). *"Common risk factors in cryptocurrency".* The Journal of Finance, 77(2), 1133-1177.

[113] Come i ritorni medi cambiano tra azioni o portafogli differenti: non è necessaria una serie storica per attuare il confronto, ma permette di confrontare gli strumenti finanziari in un determinato momento temporale (al massimo un intervallo per ampliare il caso studio).

considerazione i predittori azionari, sono state selezionate informazioni relative ai prezzi e al mercato allo scopo di delineare le controparti del mercato cripto.

In particolare, è stato osservato come 2 fattori siano principalmente in grado di catturare la maggior parte dei rendimenti attesi: dimensioni e momentum[114], ovvero gli elementi principalmente studiati dalla letteratura finanziaria.

Per quanto riguarda le dimensioni, sono state individuate tre osservazioni legate all'illiquidità del mercato:

- Monete "piccole" hanno prezzi minori ma possiedono un valore di illiquidità di Amihud[115] maggiore rispetto alle monete più grandi;
- Nell'analisi cross section, l'effetto legato alle dimensioni della moneta è maggiore nelle monete con alto costo di arbitraggio;
- Nell'analisi delle serie temporali, il premio legato alla grandezza è incrementato in fasi di alta volatilità del mercato;

Inoltre, è possibile discutere sul plausibile meccanismo di competizione tra le criptovalute come veicolo per gli effetti legati alle dimensioni. Sosteniamo infatti come le criptovalute più piccole competano tra di loro e la vincitrice ottenge la notorietà tale da renderla stabile e duratura. Per quanto riguarda le criptovalute "perdenti", costituiscono la miriade di token di breve durata che, affrontando fluttuazioni di prezzo significativamente più importanti, portano a rendimenti medi più alti rispetto alle criptovalute più grandi.

[114] Osservazione finanziaria relativa all'inerzia di un trend: l'asset finanziario che tende ad una direzione continuerà a muoversi verso quella direzione fin quando non sarà interrotto da una forza esterna (teoria simile alla fisica). È principalmente osservato tramite un oscillatore che permette di valutare l'accelerazione (in salita e discesa) dello strumento finanziario.

[115] Misura di illiquidità proposta da Amihud che permette di descrivere la risposta dei prezzi al flusso degli ordini. Si basa sulla teoria che, col tempo, l'illiquidità attesa di mercato ha un effetto positivo sui ritorni in eccesso (rappresenterebbero un premio di illiquidità). Rappresenta la variazione giornaliera del prezzo di un indice in rapporto a ogni dollaro scambiato.

Dunque, il meccanismo di competizione tra le criptovalute è in linea con l'effetto dimensione che stiamo documentando.

Prendendo in considerazione il fattore momentum, i risultati sono in linea con il meccanismo di reazione eccessiva degli investitori, il quale sostiene che, dopo il seguito iniziale, i prezzi sono inclini ad invertire la tendenza nel lungo periodo. Inoltre, l'effetto momentum è marcatamente più forte tra le monete di dimensioni sviluppate, in quanto attirano maggiormente l'attenzione degli investitori[116].

I risultati dimostrano che una strategia a lungo termine basata sul momentum produce importanti ritorni settimanali esclusivamente su token con dimensioni sopra la media: questo risultato è in contrapposizione con il mercato azionario, nel quale l'effetto momentum ha portata maggiore tra azioni "minori" [117].

Prendendo in considerazione il mercato valutario è stato rilevato un forte effetto momentum nei risultati di Menckhoff (2012)[118] , i quali dimostrano come ci sia un effetto di inversione nel lungo periodo e che questo sia più pronunciato tra valute con alta volatilità idiosincratica[119]. Un fenomeno simile è stato riscontrato anche nel mercato delle criptovalute. In altri mercati l'effetto momentum è a livello mensile mentre in quello delle criptovalute è settimanale.

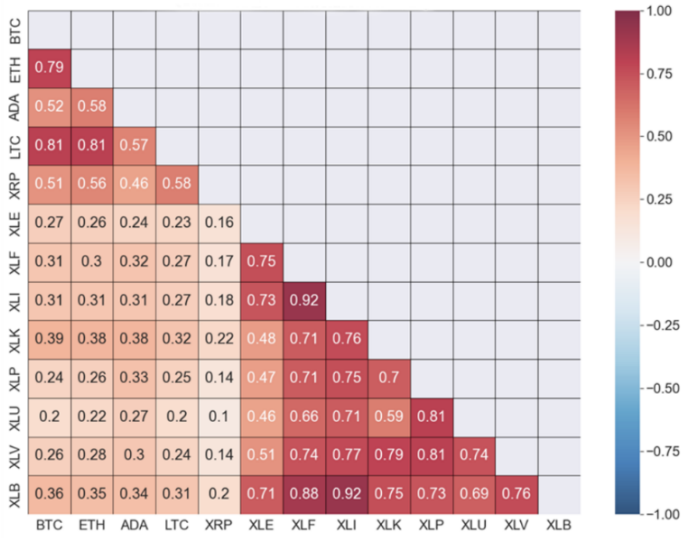
[116] Andrei, Daniel, and Michael Hasler, (2015), *"Investor attention and stock market volatility*". Of Financial Studies, 28, 33–72.
[117] Hong, Harrison, Terence Lim, and Jeremy C. Stein, (2000). *"Bad news travels slowly: Size, analyst coverage, and the profitability of momentum strategies"*. Journal of Finance 55, 265–295.
[118] Menkhoff, Lukas, Lucio Sarno, Maik Schmeling, and Andreas Schrimpf, (2012), *"Currency momentum strategies",* Journal of Financial Economics 106, 660–684.
[119] Volatilità specifica di un asset: componente che non può essere spiegata o correlata con il movimento generale del mercato.

5.3 CORRELAZIONE CRIPTOVALUTE E ASSET TRADIZIONALI

Il ruolo della correlazione è fondamentale per la diversificazione del portafoglio: minore correlazione riduce i rischi e la complessiva volatilità del portafoglio.

Nel report "How Do Cryptocurrencies Correlate with Traditional Asset Classes?"[120] del CFA Institute, è stata condotta un'analisi con la finalità di comparare i prezzi di chiusura delle 5 principali criptovalute, Bitcoin (BTC), Ethereum (ETH), Litecoin (LTC), XRP, e Cardano (ADA), con ETF e materie prime. Lo studio relativo alla correlazione con indici azionari e obbligazionari verrà svolta successivamente.

Figura 17: Mappa correlazione criptovalute ed ETF



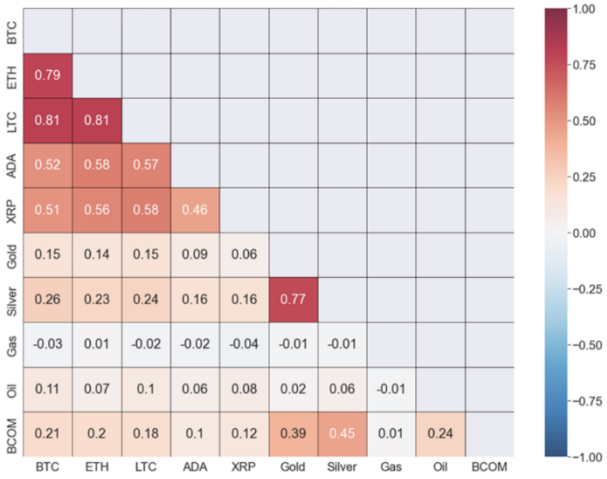
Fonte: CFA Institute: How Do Cryptocurrencies Correlate with Traditional Asset Classes?"

ETF presi in considerazione: XLB (US materials), XLE (US energy), XLF (US financials), XLI (US industrials), XLK (US technology), XLP (US consumer staples), XLU (US utilities), e XLV (US health care).

Le criptovalute dimostrano una debole o quasi inesistente correlazione positiva con il settore ETF, con valori che vanno dal 0.1 (XRP-US utilities) ad un massimo di 0.39 con US technologies e US materials.

[120] https://blogs.cfainstitute.org/investor/2022/11/16/how-do-cryptocurrencies-correlate-with-traditional-asset-classes/

Figura 18: Mappa correlazione criptovalute e materi prime



Fonte: CFA Institute: How Do Cryptocurrencies Correlate with Traditional Asset Classes?"

Per quanto riguarda le materie prime, la mappa termica sottostante dimostra che tutte le criptovalute hanno correlazioni positive o negative trascurabili con esse. Solo il gas naturale mostra basse relazioni negative con le criptovalute.

L'argento ha la correlazione più alta, raggiungendo il picco di 0,26 tra argento e BTC. Bitcoin, il cosiddetto "oro digitale", mostra solo una debole correlazione con il famoso metallo. La bassa correlazione positiva delle criptovalute con gli ETF potrebbe indicare un aumento del trading tra mercati e segnalare la crescente popolarità delle criptovalute. Inoltre, la debole correlazione delle criptovalute con gli asset tradizionali potrebbe offrire potenziali benefici di diversificazione per gli investitori a lungo termine che possono sopportare una maggiore volatilità. Tuttavia, non tutte le criptovalute mostrano la stessa mancanza di correlazione con gli asset tradizionali, quindi gli investitori devono essere selettivi su quali scegliere.

5.4 RUOLO DI BITCOIN NEL PANORAMA FINANZIARIO

Interessante è la considerazione attuale di Bitcoin e altre principali criptovalute, come una rilevante classe di asset di investimento. Il fenomeno, i cui inizi sono da ricondurre all'importante crescita avvenuta a partire dal 2017, ha comportato un cambiamento in

ambito finanziario, rimarcato dallo scoppio della crisi pandemica. Il crollo finanziario ha creato una significativa preoccupazione tra gli investitori, i quali hanno ritenuto opportuno differenziare i propri investimenti anche su asset virtuali.

Il crollo dello S&P 500, indice di riferimento del mercato americano, ha spinto gli investitori ad investire in altri asset, tra i quali le criptovalute. Con il recupero del mercato azionario, gli investitori hanno ribadito la convinzione che le criptovalute fossero degli asset in grado di realizzare ritorni anche in situazioni di mercato particolari. Tra il 2019 e il 2023 i prezzi delle criptovalute sono stati caratterizzati da fluttuazioni simili ai prezzi dell'azionario. In merito a ciò prendendo in considerazione l'indice finanziario SPCBDM (S&P Cryptocurrency broad digital market index)[121], si è osservato come nel periodo di riferimento, sia avvenuta una particolare crescita di correlazione con lo S&P 500, mostrando come le fluttuazioni del mercato cripto stiano seguendo le tracce del mercato azionario.

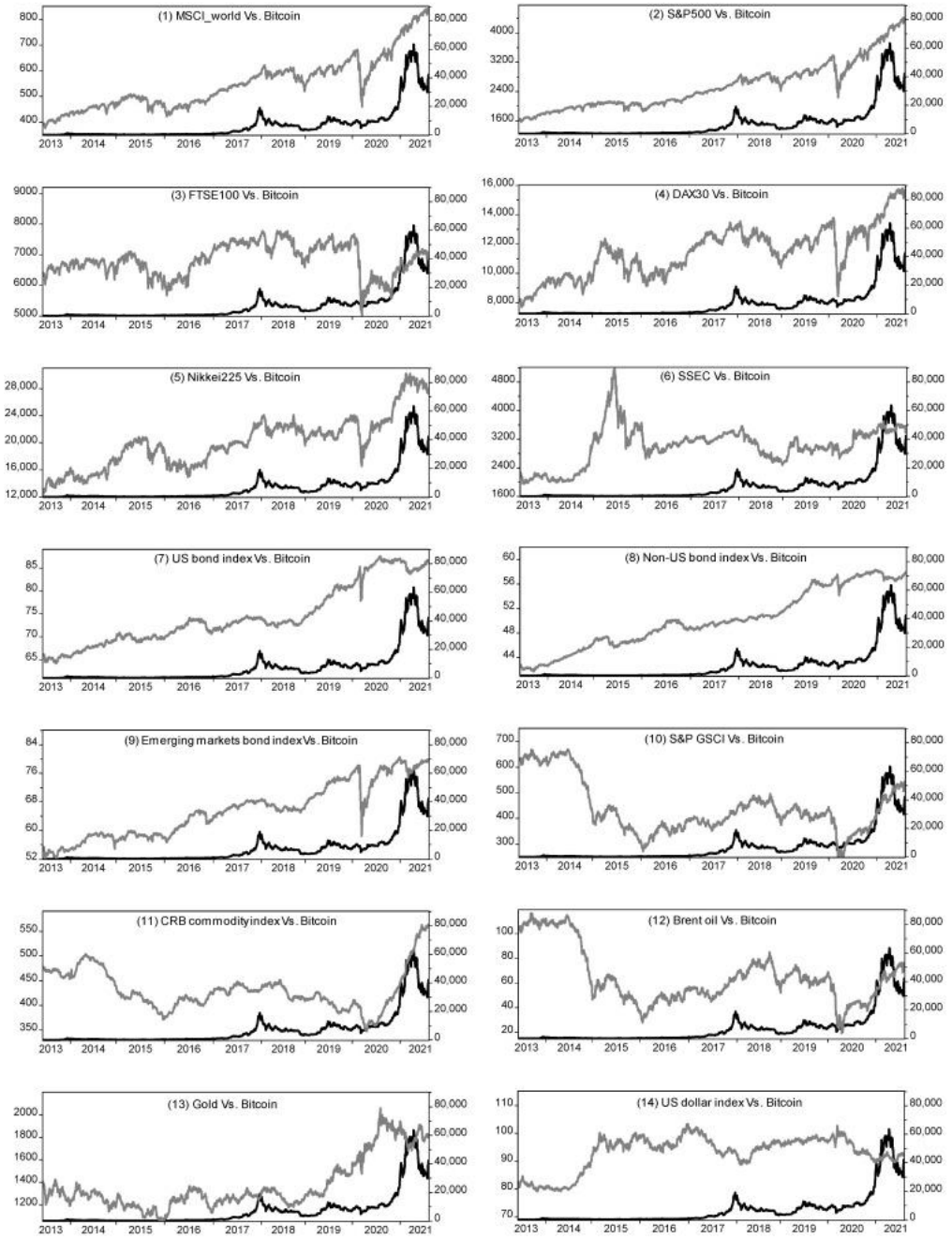
Pnapan Wang (2022)[122] ha svolto uno studio con la finalità di investigare le correlazioni dinamiche tra Bitcoin e altri 14 principali asset finanziari (indici globali, obbligazioni, materie prime e dollaro) in un arco temporale che va dal 2013 al 2021. I risultati ottenuti non solo contribuiscono a chiarire i meccanismi di formazione dei prezzi delle criptovalute e il loro ruolo nella gestione del portafoglio, ma permettono anche il controllo

[121] Indice progettato per tracciare le performance di asset digitali che soddisfano criteri minimi di liquidità e capitalizzazione, e che vengono scambiati in exchange riconosciuti.
https://www.spglobal.com/spdji/en/indices/digital-assets/sp-cryptocurrency-broad-digital-market-index/#overview.
[122] Wang P, Liu X, Wu S. (Oct. 2022). *"Dynamic Linkage between Bitcoin and Traditional Financial Assets: A Comparative Analysis of Different Time Frequencies"*. Entropy (Basel).

dei rischi e il miglioramento delle politiche di monitoraggio dinamico del mercato cripto-centrico. I risultati ottenuti sono i seguenti:

- Bitcoin è correlato positivamente ad azioni, obbligazioni e materie prime, mentre dimostra una correlazione negativa al dollaro statunitense, il quale viene identificato come asset rifugio: ciò sottolinea come la natura finanziaria di Bitcoin sia associata ad asset rischioso;
- L'alta volatilità a breve termine e la natura speculativa del mercato scandiscono una maggiore correlazione a lungo termine con gli asset rispetto a quella di breve termine;
- In caso di shock estremi (come lo scoppio della crisi pandemica) è osservabile un netto incremento della correlazione positiva tra gli asset;
- Bitcoin può fungere da copertura contro il dollaro statunitense e, a lungo termine, anche per il mercato azionario cinese e diverse materie prime. Tuttavia, per la maggior parte degli asset tradizionali, Bitcoin è solo un efficace strumento di diversificazione del portafoglio.

Figura 19: Confronto serie storiche dei prezzi tra Bitcoin e strumenti finanziari tradizionali



Fonte: Wang, P., Liu, X., & Wu, S. (2022), Dynamic Linkage Between Bitcoin and Traditional Financial Asset: A comparative Analysis of Different Time Frequencies

Dunque, le criptovalute devono essere identificate come strumenti per la diversificazione del rischio allocate in portafogli "tradizionali", piuttosto che come strumenti di copertura o rifugio. Inoltre, l'alta volatilità a breve termine influenza gli effetti di diversificazioni

in questi archi temporali, esponendo gli investitori ad importanti rischi di investimento: l'opzione più efficace è la conservazione a lungo termine degli asset virtuali.

5.5 ETF SPOT BITCOIN

Continuando l'analisi sulla principale criptovaluta del mercato è fondamentale menzionare la recentissima notizia relativa all'approvazione di un innovativo strumento finanziario: l'ETF spot Bitcoin.

A seguito di numerosi rinvii e discussioni, la SEC[123], Securities and Exchange Commission, ha approvato 11 nuovi ETF su Bitcoin: il 10 gennaio 2024 l'ente federale ha deliberato positivamente in relazione alle richieste provenienti dalle principali case di investimento sul lancio degli ETF spot su Bitcoin, di cui la prima richiesta risale al 2013.

5.5.1 Analisi degli Exchange Traded Funds

Prima di procedere con la trattazione di questa tematica è necessaria un'introduttiva spiegazione dell'essenza degli ETF.

Gli ETF (acronimo di Exchange Traded Funds) sono fondi o SICAV[124] a basse commissioni di gestione, negoziati in Borsa con l'obiettivo di replicare fedelmente l'andamento e quindi il rendimento di indici azionari, obbligazionari, materie prime e valute virtuali[125]. Gli elementi che hanno contribuito alla diffusione di questi strumenti finanziari sia verso gli investitori istituzionali sia verso i retail sono:

[123] Securities and Exchange Commission, ente federale statunitense incaricato della supervisione ed ispezione della borsa valori, nonché delle attività e agenti che vi partecipano.
[124] Società di Investimento a Capitale Variabile: società di intermediazione finanziaria che svolgono, sotto forma di S.p.a., attività continua di offerta pubblica di titoli azionari allo scopo di investire in valori mobiliari il patrimonio collettivo in tal modo raccolto. (Treccani)
[125] https://www.borsaitaliana.it/etf/formazione/cosaeunetf/coseunetf.htm.

- *Semplicità e trasparenza:* sono strumenti passivi con la finalità di replicare le performance del prodotto finanziario di riferimento, delineando apertamente il profilo rischio/rendimento dell'investimento. Essendo negoziati in tempo reale in Borsa, possono essere acquistati e venduti tramite la propria banca o il proprio broker (investitore costantemente a conoscenza della valorizzazione dell'investimento);
- *flessibilità***:** gli ETF non hanno scadenze permettendo all'investitore di operare seguendo i propri orizzonti temporali d'investimento, dall'intraday a lungo termine;
- *economicità e garanzia***:** la politica di gestione passiva permette sia l'abbattimento dei costi sia l'accesso a mercati e a strategie di investimento difficilmente raggiungibili con commissioni di gestione così ridotte. Inoltre, la regolamentazione permette di salvaguardare il patrimonio dell'ETF anche nel caso di insolvenza della società amministratrice;

5.5.2 Dibattito sull'approvazione degli ETF spot

Nonostante la loro approvazione, l'ente federale conserva una posizione scettica nei confronti delle valute virtuali: l'esitazione degli ultimi 10 anni ha dimostrato come il dibattito tra i sostenitori dell'innovazione cripto-centrica e i "tradizionalisti" finanziari non si sia mai arrestato. Opinioni radicalmente discordanti sulla tematica hanno animato in particolar modo la composizione della SEC stessa: l'approvazione non è avvenuta all'unanimità e il voto decisivo è stato affidato al Governatore Gary Gensler.

Un importante intervento è rappresentato dalla decisa presa di posizione di Hester Peirce, commissario della SEC, la quale nella sua dichiarazione "Out, Damned Spot! Out, I Say!"[126] accusa espressamente il precedente operato della Sec.

Le parole della Peirce[127] hanno rimarcato i pregiudizi nei confronti dell'asset sottostante in quanto il ripetuto rinvio ha comportato un decennio di "opportunità" economiche sprecate, avendo ritenuto il settore ancora immaturo e ingestibile. L'approvazione, che, come sostiene il commissario, è arrivata a "malincuore", è frutto di una solida analisi della Commissione, ritenutasi munita degli strumenti per "prevenire frodi e manipolazioni".

Per supportare l'analisi della SEC, i fondi incaricati alla realizzazione degli ETF spot hanno dichiarato di attenersi rigorosamente alla specifica regolamentazione e colmare le lacune evidenziate dai progetti precedenti, quali la mancanza di meccanismi di garanzia, regolamentazioni antiriciclaggio, violazioni delle leggi sui titoli e numerose frodi e associazioni a delinquere: il dirompente fallimento dell'Exchange FTX alla fine del 2022 e le violazioni commesse da Binance e Coinbase rappresentano gli esempi più importanti.

5.5.3 Confronto tra ETF spot e futures

È importante evidenziare come fino ad ora la SEC avesse regolamentato l'interazione con il mercato delle valute virtuali mediante fondi che registrassero l'andamento dei futures sulle criptovalute o tramite fondi che possedessero azioni societarie con indiretta esposizione al mondo cripto-centrico. I gestori di fondi hanno permesso l'esposizione alle criptovalute proponendo fondi costituiti da contratti Futures[128], ovvero scambi che

[126] Espressione tratta da una celebre frase di Macbeth, proponendo un gioco di parole tra spot (macchia) e l'ETF approvato, rimarcando il tenore della tragedia shakespeariana.
[127] https://www.sec.gov/news/statement/peirce-statement-spot-bitcoin-011023#_ftn2
[128] https://www.forbes.com/advisor/it/investire/criptovalute/etf-spot-bitcoin.

prevedono la vendita del prodotto finanziario ad un prezzo stabilito: i contratti, sottoscritti dai gestori dei fondi, permettono agli acquirenti delle quote del fondo di investire (indirettamente) sui sottostanti (Bitcoin) operando sulla differenza di prezzo della vendita futura.

Gli ETF spot permettono invece di seguire direttamente il prezzo attuale di mercato, senza dover operare mediante derivati o sottoscrivendo contratti a termine. I prezzi "spot" vengono adoperati come riferimento ai prezzi correnti degli asset per una vendita immediata, a differenza dei Futures, nei quali il prezzo è analizzato in funzione delle prospettive per una vendita futura.

5.5.4 Vantaggi degli ETF cripto

È necessario analizzare gli elementi[129] che hanno spinto per l'implementazione di questi strumenti finanziari:

- *Diversificazione*: Gli ETF consentono all'investitore di inserire nel proprio portafoglio asset unici come le valute virtuali. Inoltre, rappresentano un ponte di collegamento con una vasta gamma di cripto-asset e società ad essi correlate, incrementando ulteriormente la diversificazione rispetto all'investimento diretto del token;
- *Sicurezza*: l'ETF permette di possedere criptovalute senza l'intermediazione di un ente esterno quale l'Exchange, particolarmente esposto ad hacking o truffe. La responsabilità ricade nella società gestore del fondo, garantendo la protezione del patrimonio dell'investitore e una minore esposizione a rischi. Inoltre, la presenza

[129] https://www.agendadigitale.eu/mercati-digitali/via-libera-agli-etf-spot-su-bitcoin-cosa-significa-per-il-futuro-delle-criptovalute/

di una delineata regolamentazione offre un maggior grado di sicurezza e trasparenza;

- *Accessibilità:* La complessità di acquistare e gestire direttamente e singolarmente i wallet cripto disincentiva gli investitori che non possiedono le competenze tecniche necessarie. Gli ETF semplificano il processo di investimento, permettendo a chiunque di operare, ampliando le potenzialità di una vasta gamma di investitori (la semplicità nell'uso degli ETF compenserà gli svantaggi ad esso collegati);

5.5.5 Svantaggi degli ETF cripto

Un'analisi completa e oggettiva richiede anche la considerazione degli ostacoli economici[130] che caratterizzano i fondi con criptovalute:

- *Costi di gestione*: L'acquisto diretto delle criptovalute prevede una commissione verso gli Exchange, costituita da una piccola percentuale del valore negoziato. Nel caso degli ETF, i costi sono relativi sia al servizio dell'intermediario finanziario, sia alla gestione del fondo, con tassi particolarmente più elevati rispetto agli exchange. Maggiori costi di gestione riducono i rendimenti complessivi;
- *Assenza di controllo diretto*: L'investimento nell'ETF non consiste nel possesso diretto dello strumento virtuale, né del controllo e gestione diretto (se si tratta di ETF Futures, neanche il fondo è possessore del token). Inoltre, il potere esecutivo è correlato alla gestione strategica del manager del fondo, rendendo inaccessibili personali strategie mirate;

[130] https://www.investopedia.com/pros-and-cons-of-crypto-etfs-8362499#citation-7

- *Limitazioni alle possibilità di trading*: Dovendo operare in un mercato regolamento da orari di apertura e chiusura, le potenzialità di scambio di un investitore sono limitate. Gli Exchange operano costantemente 24/7. Inoltre, è possibile suddividere in frazioni i token, consentendo agli investitori di acquistare o vendere qualsiasi quantitativo desiderato;

5.6 CBDC: CENTRAL BANK DIGITAL CURRENCY

L'analisi del mercato deve tenere conto di un nuovo strumento virtuale che sta acquisendo una particolare rilevanza nel panorama finanziario: le Central Bank Digital Currency.

Le valute digitali della banca centrale (CBDC) sono ideate come complementari o sostitutive dei token peer to peer decentralizzati. Sebbene condividano elementi con l'architettura virtuale delle criptovalute, le CBDC sono lontane per finalità alle conosciute valute virtuali[131].

Come espresso in precedenza, le CBDC sono versioni virtuali delle valute tradizionali controllate dall'autorità monetaria e controllabili in tempo reale. Nonostante la somiglianza con le criptovalute, questi nuovi strumenti digitali sono rigorosamente uno strumento per la gestione e sorveglianza dei sistemi monetari. Infatti, i token delle Banche Centrali sono contraddistinti da una duplice finalità: risolvere i problemi esistenti e preparare il panorama finanziario ad un futuro digitalizzato[132].

Innanzitutto, le CBDC possono contribuire all'efficienza e stabilità dei sistemi di pagamento nazionali e internazionali, promuovendo la competizione nel mercato dei sistemi di pagamento e di conseguenza, riducendo i costi dei servizi finanziari. Inoltre,

[131] Ng, D., & Griffin, P. (2018). *"The wider impact of a national cryptocurrency".* Global Policy, 1.
[132] Internationa Monetary Fund (2023). *"Central Bank Digital Currency-Initial Considerations", Policy Papers*, *2023*(048).

potrebbe assolvere alla funzione di sistema di pagamento "back up" in situazioni emergenziali, in quanto è possibile, tramite la tecnologia blockchain, plasmare i nuovi token per essere più resilienti, operativi anche offline e immuni a potenti cyber attacchi.
Un ulteriore vantaggio è costituito dal miglioramento dell'inclusione finanziaria. I CBDC potrebbero essere utilizzati senza un conto bancario per chi opera con quantitativi ridotti e potrebbero richiedere commissioni basse se non nulle. Inoltre, l'operatività anche offline dei token potrebbe fungere da ponte al sistema finanziario tradizionale anche per popolazioni in aree rurali con connessioni instabili[133].

La principale ambizione dei CBDC è ancorata all'utopistica eliminazione del contante per i sistemi di pagamento del futuro. Il contante rappresenta l'unità di conto per eccellenza di una banca centrale, ed una sua rimozione potrebbe comportare una totale sfiducia del sistema instaurato: le CBDC potrebbero essere uno strumento per garantire la continua disponibilità di moneta della Banca Centrale in futuro. Inoltre, tali monete potrebbero rafforzare il ruolo della Banca Centrale, permettendo di interagire e controllare i consumatori senza la necessità di banche intermediarie.
Nonostante l'intenzione di presentarsi come un'innovazione dirompente nelle mani del pubblico, le CBDC restano allineate ai tradizionali modelli di pubblica amministrazione. D'altro canto, le criptovalute intese come strumento finanziario stanno ottenendo maggiore apertura normativa, ma come strumento "dirompente" rappresentano una minaccia al dominio dei sistemi finanziari tradizionali.
A tal proposito, qualsiasi autorità monetaria pone enormi aspettative sulle spalle dei CBDC: molti paesi stanno lavorando all'emissione di CBDC, tra i quali spiccano la Cina

[133] Lannquist, Ashley and Brandon Tan. (2023). *"CBDC's Role in Promoting Financial Inclusion"*. IMF Fintech Notes No 2023/011.

con lo Yuan digitale, le Bahamas con il Sand Dollar, la Giamaica con il JAM-DEX e diversi paesi Sud Americani. Più di 90 banche centrali stanno studiando o sperimentando le CBDC, tra le quali risulta anche la Banca Centrale Europea, attualmente in una fase avanzata di sperimentazione per il Digital Euro, di cui è prevista l'emissione tra il 2025 e il 2026[134].

[134] https://www.ecb.europa.eu/paym/digital_euro/

CAPITOLO 6: PROCESSO DI CREAZIONE E SVILUPPO DI UNA CRIPTOVALUTA

Lo studio svolto nei capitoli precedenti ci permette di delineare con maggiore semplicità l'iter necessario per lo sviluppo di una valuta virtuale. La creazione e gestione della moneta coinvolgono numerose figure tecniche esperte in grado di assolvere a complesse funzioni dal punto di vista crittografico, informatico, tecnico, economico e legale.

6.1 DEFINIZIONE DELL'OBIETTIVO, COSTRUZIONE DELLA BLOCKCHAIN E TOKENOMICS

Come qualsiasi progetto imprenditoriale, la creazione di una criptovaluta richiede un preliminare studio dell'essenza e finalità del prodotto. Le criptovalute possono svolgere ruoli diversi per i quali è necessaria una particolare architettura per massimizzarne l'utilità: un progetto che aggiunge valore al mondo reale, con un'effettiva utilità, è caratterizzato da una maggiore propensione allo sviluppo e probabilità di successo.
Lo step successivo è rappresentato dallo studio crittografico durante il quale il team deve delineare la tecnologia blockchain alla base del proprio progetto, scegliendo tra lo sviluppo di una nativa catena crittografica o sfruttando la possibilità di utilizzare i protocolli creati da altri sviluppatori di blockchain (il contratto ERC-20 proposto da Ethereum è il principale modello di sviluppo dei token).

A questa analisi è seguita la *"tokenomics*"[135] ovvero il complessivo studio relativo alla economicità del token. Questo processo può essere delineato come l'architettura extra

[135] https://academy.binance.com/it/articles/what-is-tokenomics-and-why-does-it-matter

crittografica della blockchain, in quanto delinea i fattori che influenzano il valore, la creazione, la distribuzione, domanda, offerta e tutti i meccanismi di incentivazione associati alla valuta digitale. Questa valutazione prende in considerazione una vasta gamma di variabili tecniche ed economiche, combinata a strumenti di analisi fondamentale per l'inquadratura delle prospettive future del progetto.

Il primo pilastro della tokenomics è rappresentato dalla "comunità": è fondamentale che alla base del progetto ci sia una massa critica in grado di supportare i principi e gli obiettivi del progetto, conservandone gli ideali, la stabilità e la crescita.

Successivamente, gli interessi degli sviluppatori si spostano verso la domanda e l'offerta del token, ovvero i fattori che influenzano principalmente l'andamento del prezzo. L'ostacolo maggiore consiste nell'eliminare gli ostacoli che comportano un'instabile fluttuazione dei valori delle monete. Esistono diversi meccanismi che permettono la gestione e un relativo controllo dell'economicità dei token: i principali sono rappresentati dall'offerta massima, una misura in grado di quantificare l'obiettivo numerico massimo di token producibili, e dall'offerta in circolazione, uno strumento che permette di monitorare, tramite coniazione e distruzione di token, i quantitativi di token in circolazione che possono influenzare l'andamento del prezzo.

Infine, il principale strumento nelle mani degli sviluppatori consiste nei meccanismi di funding e distribuzione delle monete.

6.2 FUNDING

L'ecosistema crittografico delle criptovalute e blockchain ha permesso di ampliare gli orizzonti della raccolta di capitali: le fonti da cui gli imprenditori possono attingere per

finanziare i loro progetti si sono notevolmente evolute negli ultimi anni con lo sviluppo delle piattaforme digitali di crowdfunding. Sebbene i metodi di finanziamento tradizionali funzionino ancora nello spazio Web 3.0[136], spesso vengono integrati (se non totalmente sostituiti) da approcci di finanziamento crittografico, in quanto gli investitori apprezzano la flessibilità nell'utilizzo di valute fiat e token crittografici e la rapidità con cui si svolgono i processi di funding. Tuttavia, questo nuovo settore è fortemente influenzato dall'assenza di una robusta regolamentazione che se da un lato fortifica la caratteristica decentralizzazione, dall'altro non garantisce agli investitori un'essenziale immunità in caso di fallimento o truffa.

Rispetto al boom riscontrato negli anni passati, i volumi di fondi allocati sono drasticamente diminuiti, evidenziando come sia particolarmente complesso ottenere finanziamenti concreti e stabili. Il processo di funding è infatti fondato su molteplici aspetti che ne determinano la sopravvivenza: situazione di mercato, fiducia degli investitori nel prodotto, unicità della tecnologia, efficienza del progetto, capacità del team, budget stimato e previsioni di lancio del prodotto.

Per la creazione di nuovi token sono necessarie o la costruzione di una nuova rete blockchain o l'emissione della valuta virtuale mediante la connessione con architetture blockchain esistenti. Un enorme vantaggio della raccolta fondi decentralizzata è legata alla possibilità di basare il proprio progetto su programmi già ampiamente sviluppati. Esempio lampante è la piattaforma Ethereum che permette, tramite "contratti intelligenti "(ERC-20)[137] di costruire innovative applicazioni crittografiche affidandosi alla stabile

[136] Nuova versione del World Wide Web incentrato sui principi della decentralizzazione, utilizzo di AI, connettività... La filosofia ala base del Web 3.0 consiste nella partecipazione degli utenti nei processi di sviluppo del Web e distribuzione di dati digitali.

[137] Lo standard ERC20 è uno standard per creare token sulla blockchain di Ethereum. Prima dei token ERC20, gli scambi di criptovalute dovevano costruire ponti personalizzati tra le piattaforme per supportare lo scambio di qualsiasi token.

tecnologia blockchain di Ethereum: non a caso, circa il 90% [138] delle ICO svolte con successo sono fondate sulla tecnologia Ethereum.

È opportuno analizzare e confrontare le diverse tipologie di funding che hanno caratterizzato lo sviluppo del settore cripto-centrico.

6.2.1 ICO (Initial Coin Offering)

Il primordiale processo che permette la creazione e distribuzione dei token virtuali è definito come ICO, Initial Coin Offering, e può essere delineato come il primario canale per l'allocazione degli asset digitali. Dunque, le ICO possono essere considerate come degli strumenti finanziari che introducono le valute "giovani" al panorama finanziario.

Si tratta di una forma di finanziamento tramite il quale un'azienda emette una nuova criptovaluta o token e la offre in vendita al pubblico per ottenere fondi per lo sviluppo del progetto crittografico. Tuttavia, gli investitori, a differenza delle IPO, non diventano proprietari di azioni societarie ma sono principalmente mossi o da finalità morali (es. sostenibilità del progetto) o da motivazioni prettamente utilitaristiche, quali l'incremento di valore del token per una futura vendita[139].

Anche dal punto di vista regolamentativo è necessario evidenziare una profonda differenziazione rispetto alla raccolta fondi azionaria: la versione crittografata non è delineata da una regolamentazione istituzionale o governativa in quanto totalmente decentralizzata. Pertanto, non sono previste particolari istruzioni, fatta eccezione per la presentazione del White Paper, il quale deve presentare un contenuto minimo costituito

[138] ICObench.com.
[139] Myalo A.S. (2019*) "Comparative analysis of ICO, DAOICO, IEO and STO. Case study"*. Finance: Theory and Practice ;23(6):6-25.

da: ideologia del progetto/business, descrizione del progetto, della sua architettura ed economicità, composizione del team e le tempistiche relative al lancio del token.

Il processo ICO si volge nelle seguenti fasi:

- *Preparatoria ICO*: Vengono annunciati i dettagli del progetto, viene creata la nuova criptovaluta o il token ancorata a blockchain già esistente e si svolge una fase di vendita preliminare ad un prezzo ridotto rispetto al momento del lancio;
- *CrowdFunding ICO*: Avviene l'offerta della valuta digitale durante la quale gli investitori acquistano i token al prezzo stabilito in cambio di valute fiat o altre criptovalute;
- *Post lancio*: I token vengono distribuiti in base alle regole stabilite durante la fase di vendita e viene dichiarata conclusa la ICO;

Figura 20: ICO concluse e fondi ottenuti per ogni anno

Year	ICOs Published	Funds Raised
2016	29	$90 million
2017	875	$6 billion
2018	1,253	$7.5 billion
2019	109	$370 million
2020	14	$55.6 million
2021	320	$378 million
2022	217	$117 million

Fonte: https://icobench.com/stats/ico-statistics/

Come è possibile osservare dalla Fig. 21, tra il 2017 e il 2018 si è verificata una significativa crescita delle ICO. L'innovativo processo di raccolta fondi ha suscitato interesse grazie ai numerosi vantaggi[140] proposti rispetto alla controparte tradizionale.

[140] https://icobench.com/stats/ico-statistics/

In primo luogo, le ICO sono aperte a tutti i potenziali investitori: diversamente dalle IPO, nelle quali l'accesso è limitato solo ad investitori accreditati con un determinato patrimonio, la base di acquirenti aumenta sostanzialmente nella raccolta fondi virtuale. Questo elemento è anche stimolato dalla flessibilità ed efficienza del sistema: è infatti possibile acquisire frazioni di token che possono essere scambiati con alta velocità di esecuzione, internazionalmente e, soprattutto, con la possibilità immediata di generare liquidità. È opportuno sottolineare come la libertà d'ingresso permette la partecipazione anche di soggetti inesperti o inaffidabili, che potrebbero inficiare i risultati delle ICO.
La caratteristica principale è sicuramente la decentralizzazione del sistema in quanto l'indipendenza da enti terzi permette sia di ridurre i costi del servizio, sia di incrementare l'efficienza sfruttando tutti i vantaggi proposti dalla tecnologia blockchain.

Figura 21: Benefici delle ICO

Fonte: https://icobench.com/stats/ico-statistics/

Prima di lanciare un ICO, il team di sviluppo stabilisce la finalità per cui è necessario raccogliere fondi e indica due cifre nel proprio Whitepaper: il Soft Cap e l'Hard Cap.

- L'Hard Cap definisce l'obiettivo finanziario, inteso come il limite massimo dell'importo di denaro da raccogliere. Si tratta di un indicatore molto importante

in quanto le criptovalute hanno un limite sul numero totale di unità in circolazione: questo fattore determina il valore del token oltre al meccanismo della domanda e dell'offerta.

- Il Soft Cap è l'importo minimo di investimento richiesto affinché il team possa procedere con l'implementazione del progetto secondo il piano. Se non viene raggiunto entro il periodo specificato, il contratto viene chiuso e vengono restituiti automaticamente tutti i fondi raccolti.

Se viene raggiunto l'Hard Cap, la vendita dei token si interrompe. Una ICO di successo prevede un Soft Cap di almeno 5 milioni di dollari e un Hard Cap massimo di 57 milioni di dollari per un investimento medio. Ulteriori elementi che contraddistinguono le ICO di successo sono la validità del progetto proposto e le competenze del team incaricato di costruire un business efficiente nel lungo periodo.

È opportuno analizzare anche le problematiche che hanno contraddistinto il primo processo di funding crittografico e che hanno permesso una sua evoluzione.

Nonostante la decentralizzazione sia una caratteristica innovativa e trainante lascia un vuoto regolamentativo particolarmente pericoloso per l'investitore, ma anche per il progetto stesso. La problematica principale è infatti legata alla rischiosità pura dell'investimento. Sono stati analizzati due principali aspetti di questa incertezza:

- Rischio legato all'asimmetria informativa tra gli emittenti e i potenziali investitori riguardo al contenuto, qualità e affidabilità del progetto. Per esempio, nel 2018, apice delle ICO, l'80% delle procedure si è rivelata fraudolenta[141]: il progetto Bitconnect ha frodato gli investitori per un totale di 2,6 miliardi di dollari;

[141] https://icobench.com/stats/ico-statistics/

- Rischio di mercato post emissione legato alle fluttuazioni di valore a seguito dell'inserimento del token nel mercato;

Un altro problema è legato agli attacchi informatici che hanno colpito una sostanziale fetta dei fondi ottenuti mediante le ICO. La vulnerabilità è solitamente causata sia da difetti nei codici dei contratti intelligenti sia dalle dimensioni ridotte e consistenza delle blockchain protagoniste.

La crescita globale delle ICO ha smosso anche attori politici, preoccupati dalle possibili attività illegali finanziate tramite ICO. Molte attività analizzate hanno evidenziato come i processi di funding fossero ad altro rischio di riciclaggio di denaro e/o finanziamento di attività terroristiche.

Un'ulteriore potenziale spiegazione della decrescita dei volumi delle ICO dopo il 2019 consiste nello sviluppo di nuovi modelli di crowdfunding: partendo dalle fondamenta delle ICO, hanno permesso di migliorare o rivoluzionare i processi di raccolta fondi.

6.2.2 DAICO (Decentralized Autonomous Initial Coin Offering)

Il termine "DAICO" sta per "Decentralized Autonomous Initial Coin Offering", ovvero una nuova tipologia di allocazione di fondi decentralizzata e autonoma per un token crittografato.

Proposta nel 2018 dal fondatore della blockchain Ethereum, Vitalik Buterin, il modello mira a combinare i vantaggi delle organizzazioni autonome decentralizzate (DAO)[142] con la classica ICO, al fine di coinvolgere maggiormente gli investitori al processo di sviluppo del progetto, rendendolo più trasparente e sicuro.

[142] Organizzazione la cui attività ed il cui potere esecutivo sono ottenuti e gestiti attraverso regole codificate, definite Smart Contract.

Figura 22: Combinazione tra DAO e ICO

Fonte: https://ethresear.ch/t/explanation-of-daicos/465

L' architettura di un DAICO è costituita da un contratto intelligente che regola tutte le fasi di raccolta e gestione dei fondi. Un team di sviluppatori pubblica un contratto DAICO impostato nella "contribution mode"[143], fase nella quale vengono esplicate tutte le informazioni relative alla tipologia di crowdfunding impostate e nella quale qualsiasi investitore può interagire con il progetto e contribuire economicamente al suo sviluppo in cambio i token.

Conclusa la prima fase, non è più possibile contribuire alla raccolta fondi in quanto viene impostato il bilancio dei token. Inoltre, il contratto blocca temporaneamente la vendita libera dei token al fine di evitare manipolazioni da parte del team del progetto (uno dei principali difetti delle ICO) e determina i valori del meccanismo "tap"[144]: se la contribution mode richiama cenni delle ICO, allora la "tap mode" rappresenta l'essenza delle DAO. Tale strumento permette di gestire e organizzare i fondi ottenuti permettendo gli investitori di decretare il quantitativo di fondi che gli sviluppatori possono ricevere

[143] https://ethresear.ch/t/explanation-of-daicos/465
[144] Overview of the DAICO Crowdfunding Model | HackerNoon

mensilmente dalla raccolta fondi, garantendo la sicurezza dell'investimento. Inoltre, hanno la possibilità di delineare le priorità del progetto, guidando gli sviluppatori verso il percorso più adeguato ed efficiente. Il vantaggio chiave rispetto alle ICO è rappresentato dal potere gestionale in mano ai detentori dei token, i quali con la possibilità di voto annullano il rischio di manipolazioni e frodi. Dunque, il concetto di DAICO di Buterin propone di bloccare tutti i proventi di un'ICO in un contratto intelligente di un'organizzazione autonoma decentralizzata (DAO) e lasciare la maggior parte delle operazioni decisionali nelle mani degli investitori.

Il sistema DAICO permette in sostanza di incrementare l'efficienza dei fondi raccolti migliorando la relazione tra sviluppatori e investitori. Di conseguenza, ciò permette uno sviluppo della sicurezza delle start-up basate sulla blockchain sia nella raccolta dei fondi sia nel trading dei token: tale modello ha le potenzialità di "sanificare" il crowdfunding cripto e stimolare la confidenza di futuri investitori nei confronti di progetti basati sulla crittografia.

6.2.3 IEO (Initial Exchange Offering)

IEO, l'Initial Exchange Offering, è un'innovativa metodologia per attirare investimenti nel settore blockchain, tramite la quale un Exchange è direttamente coinvolto nella selezione dei progetti, nell'organizzazione e nella vendita di token. La piattaforma di scambio funge da intermediario e facilita l'emissione e la vendita dei token e tramite le IEO, potenziali investitori possono acquistare asset virtuali prima che siano disponibili sul mercato. Essendo il processo agevolato da un Exchange che assume le principali responsabilità, le start-up che scelgono questa opzione devono soddisfare importanti

requisiti in relazione a modello di business, alle competenze del team, alla consistenza del White Paper e all'efficienza della tecnologia, ovvero elementi fondamentali per un impegno a lungo termine per il successo del progetto.[145] Le IEO sono diventate popolari come alternativa alle ICO, offrendo un processo di raccolta fondi più strutturato e gestito: tramite questo processo gli investitori trasferiscono capitali tramite i portafogli degli Exchange presso cui avviene la IEO, anzi che inviare direttamente i fondi agli sviluppatori del progetto (riducendo le possibilità di eventuali truffe da parte degli sviluppatori).

È possibile individuare molteplici vantaggi[146] delle IEO confrontandole rispetto al primordiale crowdfunding cripto:

- In primo luogo, è notevolmente ridotto il rischio di progetti fraudolenti: l'exchange intermediario assume la funzione di garante dell'investimento degli utenti partecipanti, mettendo in gioco la propria reputazione. I requisiti imposti e la vigile sorveglianza delle piattaforme rappresentano l'ostacolo principale per progetti o team inefficienti o fraudolenti;
- Semplificazione del processo di quotazione e trading: queste fasi avvengono direttamente sulla piattaforma impegnata con l'IEO, velocizzandone i processi e semplificandone la gestione. L'utente non ha la necessità di creare nuovi wallet in quanto possiede il portafoglio nell'account presso l'Exchange di riferimento: l'investitore dovrà solamente attendere che il token venga messo in vendita ed effettuare i propri ordini d'acquisto;
- I costi per la quotazione risultano minori rispetto alla ICO e la distribuzione dei token avviene in pochi minuti (differentemente dalle ICO per le quali la distribuzione può durare giorni);

[145] https://academy.binance.com/it/articles/what-is-an-initial-exchange-offering-ieo
[146] Miglo, A. (2022) *"Choice between IEO and ICO: Speed vs. Liquidity vs. Risk"*. FinTech 1, 276–293.

L'IEO permette di costruire anche un effetto sinergico aumentando l'efficacia della promozione delle monete: condurre una raccolta fondi nella propria piattaforma permette all'Exchange di incrementare il numero di utenti e offrire monete esclusive non disponibili altrove. Tutto ciò comporta un afflusso di transazioni e di conseguenza di commissioni, rappresentanti la principale fonte di reddito delle piattaforme.

Tuttavia, questo processo di raccolta fondi presenta degli svantaggi che ne influenzano l'efficienza. Per esempio, l'alta velocità di propagazione non permette a tutti gli investitori di avere un'uguale possibilità di investire su importanti progetti in quanto il numero limitato di IEO e la rigidità degli Exchange limitano le possibilità operative degli investitori. Inoltre, anche per le IEO possiamo riscontrare la mancanza di linearità normativa e legale, abbandonata alla totale discrezione degli Exchange.

Anche se ogni IEO è esaminata in maniera scrupolosa, nessun investimento è privo di rischio: è possibile che il progetto non sia in grado di realizzare la sua visione o che il prezzo del token abbia una svalutazione improvvisa non veicolata dal valore espresso durante la IEO.

6.1.4 STO (Security Token Offering)

Non tutti i token vengono creati per la stessa finalità: esistono security token, utility token e payment token[147]. Gli utility token sono costituiti dagli strumenti emessi tramite una ICO, finalizzati allo sviluppo e sostenimento di un progetto basato sulla crittografia mentre i payment token rappresentano un innovativo mezzo di pagamento in un ecosistema basato sulla blockchain. I security token delineano una classe distinta di asset

[147] Gryglewicz, S., Mayer, S., & Morellec, E. (2020). *"Optimal financing with tokens".* Journal of Financial Economics, forthcoming

digitali che si differenzia dalle precedenti in quanto è regolamentate dalle leggi dei mercati finanziari, infatti il loro processo di emissione, la STO, è il risultato di una evoluzione alternativa nelle metodologie di finanziamento per le imprese.

Definire gli asset digitali in base al loro scopo permette di evidenziare il loro contributo nell'ambito finanziario imprenditoriale.

Figura 23: Confronto Secuity Token e Utility Token

Fonte: Security token (STO) analysis (Februart 2019) Chain Partners

Lambert e al. (2022)[148] definiscono i security token come una rappresentazione digitale di un prodotto di investimento, definito in un registro distribuito, soggetto a regolamentazione ai sensi delle leggi sui titoli. La loro emissione può avvenire indipendentemente dallo stadio di sviluppo aziendale; tuttavia, la maggior parte delle STO è proposta da start-up con la finalità di lanciare i propri progetti.

La STO può essere presentata come l'evoluzione sia delle ICO che delle IPO. A differenza della prima, i security token conferiscono al possessore diritti ed obblighi in quanto rappresentano effettivamente titoli finanziari garantiti da un asset finanziario e offrono diritti e poteri legali come il voto e la distribuzione dei ricavi. Ciò sta a significare che questo processo di raccolta fondi costituisce un'evoluzione alla tokenizzazione[149]

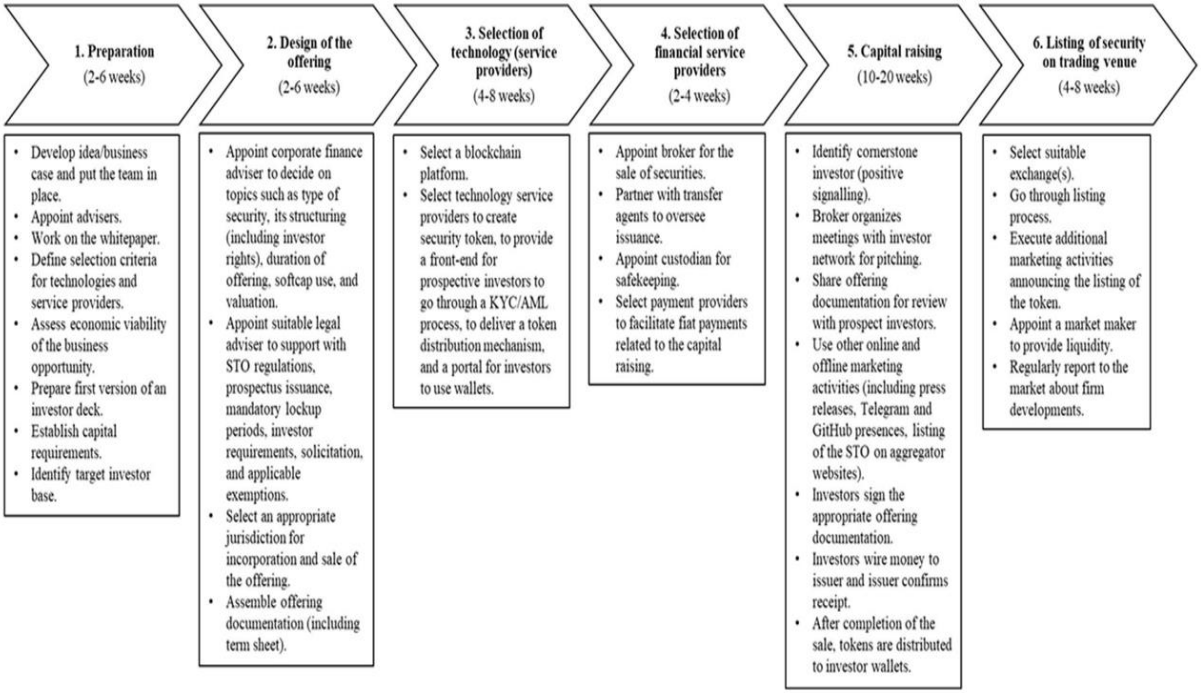
[148] Lambert T., Liebau D., Roosenboom P. (June 2022) *"Security token offerings"*. Small Business Economics, Springer, vol. 59(1), pages 299-325

[149] https://hackernoon.com/security-token-offerings-stos-what-you-need-to-know-8628574d11e2

degli strumenti finanziari tradizionali, permettendo la nascita di nuove azioni, obbligazioni, fondi e tipologie di derivati basati su blockchain e Smart contract.[150]

Il processo di crowdfunding STO prevede le seguenti fasi operative per la sua realizzazione:

Figura 24: Fasi del processo STO



Fonte: Lambert T., Liebau D., Roosenboom P. (June 2022) "Security token offerings". Small Business Economics, Springer, vol. 59(1), pages 299-32.

1. Il primo step consiste nella preparazione preliminare alla raccolta di capitale. Dal momento in cui nasce l'idea di creare un security token, il team procede con la formulazione del progetto: l'idea può ruotare attorno ad una novità imprenditoriale o alla tokenizzazione di un prodotto di investimento con la finalità di raccogliere capitali. Durante questa fase vengono incaricati i consulenti per la fattibilità economica e i tecnici per la delineazione del whitepaper. Inoltre, iniziano le prime considerazioni relative alla selezione della piattaforma blockchain e di altri servizi tecnico-finanziari;

[150] Ad esempio, un prestito tokenizzato potrebbe prevedere pagamenti automatici senza l'intermediazione di un ente bancario tradizionale.

2. Durante la seconda fase, il team nomina le figure pilastro della STO: l'avvocato e il consulente finanziario societario per assistere alla progettazione dell'offerta. Il primo rappresenta la figura di riferimento per le considerazioni legali e regolamentative; il secondo ha il compito di delineare le migliori opzioni in relazione alla tipologia e struttura del prodotto finanziario, all'inserimento di un soft cap e aspetti relativi all'emissione dei token. In seguito, il team finalizza i documenti dell'offerta.
3. Nella fase tre, vengono assunte le decisioni relative alla piattaforma blockchain (Ethereum continua ad essere la scelta più popolare tra gli emittenti) allo scopo di selezionare l'opzione in grado di ottimizzare sia l'accesso degli investitori tramite i portafogli, sia la disponibilità di sviluppatori di software. La piattaforma blockchain è fondamentale per gestire tutto il "ciclo vitale" del prodotto, dalla creazione del token alla gestione delle funzionalità e al pagamento degli interessi o dividendi.
4. Successivamente, il team seleziona i fornitori di servizi finanziari, tra cui broker, agenti di trasferimento, custodi e fornitori di servizi di pagamento. In molte giurisdizioni, la vendita di titoli è un'attività regolamentata svolta da broker autorizzati
5. La quinta fase consiste nella raccolta di capitali. Viene inizialmente delineata la figura dell'investitore ideale per avere un approccio più efficace al mercato. Il consulente organizza un "road show"[151] durante il quale viene presentato il progetto, condivisi i documenti principali e raccolte opinioni di potenziali

[151] Processo che prevede la predisposizione di una serie di incontri tra la comunità degli investitori istituzionali e il management di una società che intende realizzare un'operazione di offerta dei propri titoli (Fonte: https://www.borsaitaliana.it/borsa/glossario/road-show.html)

investitori. Di seguito avviene l'effettiva raccolta dei capitali con la firma dei documenti necessari: in base alle impostazioni della piattaforma, possono essere accettate sia valute fiat che criptovalute (solitamente BTC e ETH).

Dal momento in cui viene raggiunto il soft cap e vengono rispettate le clausole contrattuali, si conclude il funding e avviene la distribuzione dei token nei portafogli degli investitori.

6. La sesta e ultima fase è costituita dalla quotazione del token in uno o più Exchange. Il processo di quotazione necessita di ulteriore divulgazione allo scopo di attirare maggiore interesse per il prodotto quotato. È opportuno mantenere una solida rete comunicativa con protagonisti del mercato ed investitori, condividendo aggiornamenti sugli sviluppi del progetto.

La durata del processo STO in media è tra le 24 e le 56 settimane e in merito ai costi, generalmente si colloca tra 180.000 e 750.000 dollari, escludendo le commissioni calcolate come percentuale dell'offerta.

Lo studio svolto da Lambert T e al. (2022) ha permesso di individuare le variabili in grado di misurare il successo di una STO: gli elementi analizzati sono il capitale raccolto, il raggiungimento del soft cap, la condivisione del codice fonte nella piattaforma GitHub[152], la presenza in canali di comunicazione di massa[153] e i diritti di voto. In particolare, è stato evidenziato come GitHub sia correlato positivamente in modo significativo all'importo raccolto in quanto la divulgazione volontaria del codice sorgente potrebbe consentire ai

[152] È la piattaforma cloud-based che consente agli utenti di archiviare, gestire e condividere i propri progetti di coding.
[153] È stata presa in considerazione, Telegram, una delle principali piattaforme utilizzate per le ICO e STO per l'interazione con gli investitori

potenziali investitori un'adeguata valutazione della qualità strutturale dei token e, di conseguenza, del loro potenziale rendimento finanziario.

I coefficienti relativi al soft cap sono negativi ma con valori poco significativi: il risultato è coerente con la relazione tra il successo e il grado di convinzione iniziale riscosso tra gli investitori.

Anche per la variabile Telegram è stato osservato che, essendo le STO destinate ad un gruppo di investitori accreditati ed esperti, è caratterizzata da un'influenza minore rispetto alle ICO. Inoltre, la durata di uno STO è correlata positivamente con l'importo raccolto, in quanto una prolungata raccolta fondi concede agli emittenti maggiori possibilità di identificare e convincere gli investitori.

In merito ai diritti concessi agli investitori nelle STO, lo studio di Classens e al. (2002)[154] ha documentato l'effetto che la separazione tra i diritti di voto (controllo azionario) e diritti di cassa (cashflow rights) hanno sul valore societario.

I risultati hanno evidenziato come il valore societario riscontri una diminuzione nel caso in cui i diritti di voto dei membri del team siano superiori dei diritti di cassa: maggiore è il potere nelle mani degli "insiders" (manager e azionisti principali), maggiore sarà la loro capacità di ottenere valore, a spese della valutazione societaria per gli investitori esterni (azionisti minori e creditori). Dunque, riducendo la divergenza tra diritti di voto e diritti di flusso di cassa è possibile ridimensionare il problema del consolidamento di potere.

Anche progetti che svolgono le STO affrontano questioni di governance: gli investitori si dimostrano disinteressati nell'acquisto di token che non garantiscano, oltre ai diritti di cassa, anche diritti di voto. Nel caso delle STO, l'emissione dei titoli e la registrazione delle transazioni vengono effettuate su una blockchain che permette di aumentare la

[154] Claessens, S., Djankov, S., Fan, J., & Lang, L. (2002). *"Disentangling the incentive and entrenchment efects of large shareholders".* Journal of Finance, 57, 2741–2772

trasparenza della governance e di mitigare la problematica tra gli investitori insiders e outsiders. È stato osservato come associare ai security token il diritto di voto permette di migliorare significativamente l'importo raccolto poiché negare i diritti di voto rappresenta una variabile che influisce pesantemente sulla volontà d'azione degli investitori.

Tutti questi risultati ci permettono di delineare un quadro generale delle STO.
Nonostante i costi e i tempi delle STO siano decisamente più impegnativi rispetto alle ICO, tutti gli elementi innovativi trattati precedentemente rappresentano i pilastri per lo sviluppo e la diffusione del processo di raccolta fondi.
L'innovativa natura del token esalta l'economicità del processo poiché a differenza dei tradizionali strumenti finanziari, i security token non comportano costi amministrativi di acquisto e vendita, permettendo agli investitori di generare un maggiore rendimento sugli investimenti. Inoltre, la definizione di una solida regolamentazione a protezione degli investitori ha consentito a soggetti accreditati di accedere al mercato e di godere di una maggiore protezione rispetto alle altre raccolte fondi basate sui token, evolvendo ulteriormente questo scenario finanziario.

6.2.5 Confronto riassuntivo

Tabella 5: Riassunto complessivo dei processi di Crowdfunding

VARIABILI	ICO	DAICO	IEO	STO
Definizione	Raccolta fondi per l'emissione di un utility token.	Sinergia tra DAICO e ICO: gestione più sicura e controllata dei fondi ottenuti.	Versione della ICO nella quale l'emissione del token è gestita totalmente da un exchange.	Emissione di security token il cui processo di raccolta avviene seguendo le linee delle IPO.
Piattaforma per la raccolta	Sito Web dell'emittente del token.	Come per le ICO.	La piattaforma di exchange.	Piattaforma scelta dal team di sviluppatori.
Requisiti necessari	Nessuno, chiunque può avviare una ICO.	Come per le ICO.	L'Exchange svolge un controllo totale dell'azienda: requisiti da rispettare	Nessuno.
Soggetto che ottiene i fondi	Il team di sviluppo del progetto.	Il team di sviluppo e l'organo garante degli investitori.	La piattaforma exchange di criptovalute.	Il team di sviluppo del token mediato dalla piattaforma STO.
Listing automatico dopo le vendite	La start-up deve interagire con l'Exchange per inserire il proprio token; non avviene immediatamente.	Come per le ICO.	Essendo l'IEO gestita direttamente dall'Exchange, l'inserimento nella piattaforma è immediato.	Dipende dalla piattaforma utilizzata sia per la STO che come Exchange, se sono la stessa è immediato.
Difficoltà organizzative	Non sono presenti ostacoli per l'organizzazione del processo di funding.	Come per le ICO	È necessaria l'approvazione da parte dell'Exchange: successivamente l'organizzazione è affidata alla piattaforma	Il processo richiede molteplici passaggi e l'intervento di importanti figure economiche e legali: alta complessità organizzativa
Marketing	È necessario attirare l'interesse degli investitori per diffondere il progetto e incrementare la raccolta fondi: budget importante richiesto.	Come per le ICO	L'efficienza della fase Marketing è ancorata alla rilevanza sul mercato dell'Exchange	Marketing mirato ad una cerchia di investitori esperti: ampliare la portata tramite la piattaforma Exchange.
Accessibilità	Chiunque può parteciparvi	Come per le ICO	Accesso limitato agli utenti dell'Exchange	Accesso limitato ad investitori esperti e accreditati
Protezione investitore	Non garantita	Limitata	Vincolata alla regolamentazione dell'Exchange (maggiore rispetto alla ICO)	Totale protezione per l'investitore
Regolamentazione	Livello basso di regolamentazione: graduale miglioramento	Via di mezzo tra le tipologie di regolamentazione analizzate	Regolamentazione imposta dall'Exchange	Caratteristica peculiare del processo: alto grado di regolamentazione
Governance	Scarsa attenzione alla governance	L'elemento DAO caratterizza una particolare attenzione alla governance.	Media considerazione della tematica.	Ampia rilevanza alla questione governance.
Grado centralizzazione	Processo centralizzato nelle mani del team sviluppatore.	Relativamente decentralizzato: decisioni assunte secondo un sistema democratico di votazione.	Relativamente centralizzato tra sviluppatori ed exchange.	Principalmente centralizzato per gli sviluppatori: i diritti di votazione subentrano con la distribuzione dei token (STO conclusa).
Commissioni	Non presenti.	Non presenti.	Commissioni dell'Exchange.	Non presenti.
Tempistiche	Diversi mesi.	Diversi mesi.	Potrebbero servire pochi secondi, come settimane.	Circa un anno.
Costi	Tra il 5 e il 10% dei fondi ottenuti, in media attorno ai 100 mila dollari.	Come per le ICO.	Costi in funzione dell'Exchange utilizzato.	In media tra 180 e 750 mila dollari.

Fonte: Elaborazione propria

6.3 SVILUPPO E AGGIORNAMENTO

Il funding non rappresenta lo step conclusivo del lancio di una criptovaluta. Come per qualsiasi progetto, lo sviluppo, l'aggiornamento e la manutenzione del prodotto creato rappresentano elementi altrettanto importanti per la sopravvivenza del progetto.

Il seguito di investitori e sostenitori contribuisce ad alimentare le ambizioni e la costanza degli sviluppatori: il supporto offerto dalla comunità deve essere ricambiato con una costante comunicazione trasparente tramite i principali canali come forum, social media e sistemi di messaggistica. Il costante confronto con il pubblico permette di comprendere eventuali difetti o problematiche e, contemporaneamente, affrontare le preoccupazioni della comunità. Inoltre, ciò permette di investire continuamente nella promozione del proprio prodotto: è fondamentale consolidare il numero di sostenitori e ampliare il proprio seguito mediante conferenze, campagne di marketing e promozioni dei propri token virtuali.

Un altro fondamentale aspetto da considerare è l'integrazione con servizi, piattaforme e sviluppatori esistenti in quanto la robustezza dell'ecosistema crittografico si basa sull'integrazione e adozione delle proprie criptovalute da parte di un crescente numero di partecipanti, in grado di contribuire al consolidamento e sviluppo del progetto stesso. Le opportunità di Partnership possono aprire gli orizzonti di investimento, sfruttando la rilevanza economica di importanti aziende, progetti o istituzioni.

Come espresso inizialmente, la diffusione e la raccolta di capitali non costituiscono gli unici elementi da tenere in considerazione: la manutenzione, l'aggiornamento, gli sviluppi normativi rappresentano elementi chiave per la pianificazione a lungo termine del progetto. La costante manutenzione della rete blockchain permette automaticamente di aggiornare il sistema per affrontare eventuali bug e minacce alla sicurezza, per

migliorare le prestazioni e per implementare nuove funzionalità che permettono al protocollo di adattarsi alle nuove esigenze evolutive del settore.

Infine, è fondamentale osservare costantemente le evoluzioni normative che stanno caratterizzando il settore. La progressiva accettazione da parte dei governi ed enti istituzionali sta modificando le prospettive future delle monete virtuali. L'aggiornamento relativo alle nuove regolamentazioni permette sia di salvaguardare il proprio progetto da eventuali violazioni e opposizioni normative, sia di sfruttare nuove opportunità in grado di arricchire tecnologicamente ed economicamente il panorama finanziario.

CONCLUSIONE

Nonostante il successo dell'universo numismatico, le criptovalute continuano ad essere perseguitate da domande e ostacoli che offuscano il loro fondamentale intento di liberazione finanziario-digitale. Dato l'interesse condiviso per le criptovalute che ora accomuna centinaia di milioni di partecipanti, il mondo delle criptovalute è difficile da trascurare: la rivoluzione digitale ha affascinato così tante persone in cerca di un trampolino di lancio che possa spingerle verso il successo ("to the moon").

Non si può nascondere che ci sia una indifendibile diseguaglianza economica, accompagnata da un importante degrado ambientale, così come da una criminalità transnazionale alimentata dalla libera circolazione dei contanti. Tutto ciò non può essere attribuito unicamente alle criptovalute, con l'accusa di non esser riuscite a risolvere questi ostacoli, in quanto il sistema economico tradizionale è gravato anch'esso da queste problematiche.

Nonostante le criptovalute perpetuino lo stesso malessere economico del capitalismo tradizionale, devono essere considerate come uno slancio propositivo verso la risoluzione di queste falle, rappresentando uno strumento intermedio per lo sviluppo tecnologico mondiale incentrato su un nuovo equilibrio tra uomo virtuale e reale.

In conclusione, l'evoluzione delle criptovalute rappresenta una sorprendete pietra miliare nella storia finanziaria, introducendo nuove possibilità e sfide. Il processo di sviluppo delle valute virtuali è guidato dall'innovazione tecnologica e dalla volontà di superare i tradizionali sistemi finanziari.

Mentre il futuro delle criptovalute rimane dinamico e in continua evoluzione, i meccanismi, la loro comprensione e responsabile adozione possono contribuire a plasmare un ecosistema finanziario più resiliente, efficiente ed inclusivo

BIBLIOGRAFIA E SITOGRAFIA

Abadi J., Brunnermeier M. (2018). *"Blockchain economics".* Centre for Economic Policy Research. CEPR Discussion Papers.

Abbasi, G. A., Tiew, L. Y., Tang, J. Q., Goh, Y. N., Thurasami, R., & Dragan, D. (2021). *"The adoption of cryptocurrency as a disruptive force: Deep learning-based dual stage structural equation modelling and artificial neural network analysis".* PLOS One, (3), 16

Ahmed, W.M., (2021). *"How do Islamic equity markets respond to good and bad volatility of cryptocurrencies? The case of Bitcoin"*. Pac. Basin Finance J. 70, 101667.n Finance J. 61, 101326

Allen, B., Bryant, S.K. (2019). *"The market for cryptocurrency: how will it evolve?"* Global Econ. J. 19 (3), 1950019

Andrei, Daniel, and Michael Hasler. (2015). *"Investor attention and stock market volatility".* Review of Financial Studies 28,33–72.

Banca D'Italia. Le funzioni della moneta e le proposte di "moneta fiscale"

Bank of International Settlement. (2015). *"CPMI. Digital Currencies".*

Bank of International Settlement. (2018). *"CPMI. Digital Currencies".*

Bank of international settlements. *"BIS Annual Economic Report".* 2018 (dati Howmuch.net).

Boksberger, P. E., & Melsen, L. (2011). *"Perceived value: a critical examination of definitions, concepts and measures for the service industry"*. Journal of Service Marketing, 25, (3) 229240.

Bunjaku, F., Gjorgieva-Trajkovska, O., & Miteva-Kacarski, E. (2017). *"Cryptocurrencies–advantages and disadvantages. Journal of Economics".* 2(1), 31-39.

Cambridge Centre for Alternative Finance. (2023). *"Cambridge bitcoin electricity consumption index*" [Dataset]. CBECI.

Castonguay, J. J., & Stein Smith, S. (2020). *"Digital Assets and Blockchain: Hackable, Fraudulent, or Just Misunderstood?".* Accounting Perspectives, 19(4), 363-387

Chamanara, S., Ghaffarizadeh, S. A., & Madani, K. (2023). *"The environmental footprint of bitcoin mining across the globe: Call for urgent action"*. Earth's Future, 11, e2023EF003871.

Chauhan, A., Malviya, O. P., Verma, M., & Mor, T. S. (July 2018). *"Blockchain and scalability".* In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 122-128). IEEE.

Chaum D. (1983), *"Blind Signatures for Untraceable Payments"* In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds) Advances in Cryptology. Springer, Boston.

Chaum, D. L. (1979). *Computer Systems established, maintained and trusted by mutually suspicious groups* (p. 1). Electronics Research Laboratory, University of California.

Chiu, J., & Koeppl, T. V. (2022). *"The economics of cryptocurrency: Bitcoin and beyond"*. Canadian Journal of Economics/Revue canadienne d'économique, 55(4), 1762-1798.

Chohan, U. W. (2022). *"Cryptocurrencies: A brief thematic review".* Available at SSRN 3024330.

Claessens, S., Djankov, S., Fan, J., & Lang, L. (2002). *"Disentangling the incentive and entrenchment efects of large shareholders".* Journal of Finance, 57, 2741–2772

Cong, Lin William, Ye Li, and Neng Wang. (2021). *"Tokenomics: Dynamic adoption and valuation".* Review of Financial Studies 34, 1105–1155.

Davis, F. D. (1989). *"Perceived usefulness, perceived ease of use, and user acceptance of information technology*". MIS Quarterly, 13(3), 319–340.

De Vries, A. (2018). *"Bitcoin's growing energy problem".* Joule, 2(5), 801-805

Delfabbro, P., King, D. L., & Williams, J. (2021). *"The psychology of cryptocurrency trading: Risk and protective factors".* Journal of Behavioral Addictions.

Erdas, M.L., Caglar, A.E., (2018). *"Analysis of the relationships between Bitcoin and exchange rate, commodities and global indexes by asymmetric causality test*". E. J. Eur. Stud. 9 (2), 27.

European Central Bank. (October 2012). *"Virtual currency schemes"*. ECB Report. 1–55.

Furneaux N. (2018). *"Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence"*. John Wiley & Sons, 2018

García-Monleón, F., Erdmann, A., & Arilla, R. (2023). *"A value-based approach to the adoption of cryptocurrencies"*. Journal of Innovation & Knowledge, 8(2), 100342.

Gryglewicz, S., Mayer, S., & Morellec, E. (2020). *"Optimal fnancing with tokens".* Journal of Financial Economics, forthcoming

Hartman, R. S. (1967). *"The Structure of Value: Foundations of a Scientific Axiology*". Wipf and Stock. OR: Eugene

Harvey, C., Tymoigne, E. (2015). *"Do Cryptocurrencies Such as Bitcoin Have a Future".*

Hong, Harrison, Terence Lim, and Jeremy C. Stein, (2000). *"Bad news travels slowly: Size, analyst coverage, and the profitability of momentum strategies"*. Journal of Finance 55, 265–295.

Hung, N.T., (2021). *"Bitcoin and CEE stock markets: fresh evidence from using the DECOGARCH model and quantile on quantile regression."* Eur. J. Manag. Bus. Econ.

Internationa Monetary Fund (2023). *"Central Bank Digital Currency-Initial Considerations".* Policy Papers*,* 2023*(048*), A001.

International Monetary Fund. Money (2018). *"The future of currency in a digital world. Finance and development".* 55(2)

Isah, K.O., Raheem, I.D., (2019). *"The hidden predictive power of cryptocurrencies and QE: evidence from US stock market".* Phys. Stat. Mech. Appl. 536, 121032

Jeribi, A., Ghorbel, A., (2021). *"Forecasting developed and BRICS stock markets with cryptocurrencies and gold: generalized orthogonal generalized autoregressive conditional heteroskedasticity and generalized autoregressive score analysis*". Int. J. Emerg. Mark.

Jeris, S. S., Chowdhury, A. N. U. R., Akter, M. T., Frances, S., & Roy, M. H. (2022). *"Cryptocurrency and stock market: bibliometric and content analysis".* Heliyon.

Ji-Xi, J. T., Salamzadeh, Y., & Teoh, A. (2021). Behavioral intention to use cryptocurrency in Malaysia: an empirical study. Bottom Line, (2), 34.

Kim, E. (2021). *"Bitcoin mining consumes 0.5% of all electricity used globally and seven times Google's total usage".* Business Insider.

Kumah, S.P., Odei-Mensah, J., (2021). *"Are Cryptocurrencies and African stock markets integrated?"* Q. Rev. Econ. Finance 81, 330–341.

Lagos, L. and R. Wright, (2005). *"A unified framework for monetary theory and policy analysis".* Journal of political Economy, 113.3 (2005): 463-484.

Lahiani, A., Jlassi, N.B., (2021). *"Nonlinear tail dependence in cryptocurrency-stock market returns: the role of Bitcoin futures". Res*. Int. Bus. Finance 56, 101351

Lambert T., Liebau D., Roosenboom P. (June 2022) *"Security token offerings".* Small Business Economics, Springer, vol. 59(1), pages 299-325

Lannquist, Ashley and Brandon Tan. (2023). *"CBDC's Role in Promoting Financial Inclusion."* IMF Fintech Notes No 2023/011.

Lee, B. C. (2021). *"The promise of Bitcoin: The future of money and how it can work for you*". McGraw Hill Professional.

Leible, S., Schlager, S., Schubotz, M., & Gipp, B. (2019*). "A review on blockchain technology and blockchain projects fostering open science"*. Frontiers in Blockchain, 2, 16.

Liu Y., Tsyvinski A. (2018). *"Risks and returns of cryptocurrency".* SSRN Electronic Journal. DOI: 10.2139/ ssrn.3226952

Liu, Y., Tsyvinski, A., & Wu, X. (2022). *"Common risk factors in cryptocurrency".* The Journal of Finance, 77(2), 1133-1177.

Loperz-Cabarcos, M. A., Perez-Pico, A.M., Pineiro-Chousa, J., Sevic, A., (2021). "Bitcoin volatility, stock market and investor sentiment. Are they connected?". Finance Res. Lett. 38,101399

Madey, Stanley R. (20017). *"Study of the history of cryptocurrency and associated risks and threats".* Diss. Utica College.

Menkhoff, Lukas, Lucio Sarno, Maik Schmeling, and Andreas Schrimpf. (2012). *"Currency momentum strategies*". Journal of Financial Economics 106, 660–684.

Mensi, W., Rehman, M.U., Maitra, D., Al-Yahyaee, K.H., Sensoy, A., (2020). *"Does bitcoin comove and share risk with Sukuk and world and regional Islamic stock markets? Evidence using a time-frequency approach".* Res. Int. Bus. Finance 53, 101230

Miglo, A. (2022) *"Choice between IEO and ICO: Speed vs. Liquidity vs. Risk".* FinTech 1, 276–293.

Ministry of Finance of Russia (January 2018). *"On Digital and Financial Assets".* Draft Federal Law of 05.22.2018

Mishkin, Frederic S. (2006). *"The Economics of Money, Banking, and Financial Markets".* New York: Pearson Addison-Wesley.

Myalo A.S. (2019*) "Comparative analysis of ICO, DAOICO, IEO and STO. Case study"*. Finance: Theory and Practice ;23(6):6-25

Nakamoto, Satoshi. (2008). *"Bitcoin: A peer-to-peer electronic cash system."* Decentralized business review

Ng, D., & Griffin, P. (2018). *"The wider impact of a national cryptocurrency".* Global Policy, 1

O'Dwyer K., Malone D. (2014). *"Bitcoin mining and its energy footprint".* In: 25th IET Irish signals & systems conf. 2014 and 2014 China-Ireland int. conf. on information and communications technologies

Omane-Adjepong, M., Paul Alagidede, I., Lyimo, A.G., Tweneboah, G., (2021). "*Herding behaviour in cryptocurrency and emerging financial markets".* Cogent Econ. Fin. 9 (1), 1933681

Paul F. Gentle (2021). *"Stone Money of Yap as an Early form of Money in the Economic Sense".* Financial Markets, Institutions and Risks, Volume 5, Issue 2.

Rehman, M.U., Asghar, N., Kang, S.H., (2020). *"Do Islamic indices provide diversification to bitcoin? A time-varying copulas and value at risk application."* Pac. Basi

Rehman, M.U., Asghar, N., Kang, S.H., (2020*). "Do Islamic indices provide diversification to bitcoin? A time-varying copulas and value at risk application"*. Pac. Basin Finance J. 61, 101326.

Ron, D. and A. Shamir, (2013). *"Quantitative analysis of the full bitcoin transaction graph".* International Conference on Financial Cryptography and Data Security, pp. 6-24.

Rosenfeld, M. (2014). *"Analysis of hashrate-based double spending".* arXiv preprint arXiv:1402.2009.

Sinelnikova-Muryleva, E. V., Shilov, K. D., & Zubarev, A. V. (2019*). "The Essence of cryptocurrencies: descriptive and comparative analysis".* Finance: Theory and Practice, 23(6), 36-49.

Stroukal, D. (November 2016). *"Bitcoin and other cryptocurrency as an instrument of crime in cyberspace".* In Proceedings of Business and Management Conferences (No. 4407036). International Institute of Social and Economic Sciences.

Thampanya, N., Nasir, M.A., Huynh, T.L.D., (2020). *"Asymmetric correlation and hedging effectiveness of gold & cryptocurrencies: from pre-industrial to the fourth industrial revolution".* Technol. Forecast. Soc. Change 159, 120195

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). *"User acceptance of information technology: Toward a unified view"*. MIS Quarterly, 27, (3) 425478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). *"Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology"*. MIS Quarterly, 36, (1) 157178.

Vincent, O., & Evans, O. (2019). *"Can cryptocurrency, mobile phones, and internet herald sustainable financial sector development in emerging markets?".* Journal of Transnational Management, 24(3), 259-279

Vora, G., (2015). *"Cryptocurrencies: are disruptive financial innovations here?"* Mod. Econ. 6 (7), 816.

Waknis P. Competitive supply of money in a new monetarist model. Munich Personal RePEc Archive. MPRA Paper. 2017;(75401).

Wang, H., Wang, X., Yin, S., Ji, H., (2021). *"The asymmetric contagion effect between stock market and cryptocurrency market."* Finance Res. Lett., 102345

Wang, P., Liu, X., & Wu, S. (2022). *"Dynamic linkage between Bitcoin and traditional financial assets: A comparative analysis of different time frequencies".* Entropy, *24*(11), 1565.

Wang, P., Zhang, W., Li, X., Shen, D., (2019). *"Is cryptocurrency a hedge or a safe haven for international indices? A comprehensive and dynamic perspective".* Finance Res. Lett. 31, 1–18.

Yarovaya, L., Elsayed, A.H., Hammoudeh, S., (2021). *"Determinants of spillovers between Islamic and conventional financial markets: exploring the safe haven assets during the COVID-19 pandemic".* Finance Res. Lett. 43, 101979

Zhao, H. D., & Zhang, L. N. (2021). *"Financial literacy or investment experience: Which is more influential in cryptocurrency investment?"* International Journal of Bank Marketing, 39(7), 1208–1226.

https://4irelabs.com/articles/get-funding-in-crypto/

https://academy.binance.com/it/articles/what-is-an-initial-exchange-offering-ieo/

https://blogs.cfainstitute.org/investor/2022/11/16/how-do-cryptocurrencies-correlate-with-traditional-asset-classes/

https://chaum.com/ecash/

https://coinmarketcap.com/

https://coinmarketcap.com/academy/glossary/decentralized-autonomous-initial-coin-offerings-daico/

https://comparitech.com/crypto/biggest-cryptocurrency-heists/

https://ecb.europa.eu/paym/digital_euro/

https://ethresear.ch/t/explanation-of-daicos/465/

https://www.forbes.com/advisor/it/investire/criptovalute/etf-spot-bitcoin/

https://howmuch.net/articles/worlds-money-in-perspective-2018/

https://hackernoon.com/security-token-offerings-stos-what-you-need-to-know-8628574d11e2/

https://icobench.com/stats/ico-statistics/

https://www.investopedia.com/pros-and-cons-of-crypto-etfs-8362499#citation-7/

https://moneysupermarket.com/gas-and-electricity/features/crypto-energy-consumption/

https://msci.com/our-solutions/indexes/emerging-markets/

https://www.sec.gov/news/statement/peirce-statement-spot-bitcoin-011023#_ftn2/

https://spglobal.com/spdji/en/indices/digital-assets/sp-cryptocurrency-broad-digital-market-index/#overview/

https://statista.com/statistics/881541/bitcoinenergy-consumption-transaction-comparison-visa/