UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M. FANNO"

DIPARTIMENTO DI SCIENZE STATISTICHE

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

IL MONDO DEI BITCOIN

RELATORE:

PROF.SSA Luisa Bisaglia

LAUREANDO: Luca Beda

MATRICOLA N. 2008150

ANNO ACCADEMICO 2022– 2023

Dichiaro di aver preso visione del "Regolamento antiplagio" approvato dal Consiglio del Dipartimento di Scienze Economiche e Aziendali e, consapevole delle conseguenze derivanti da dichiarazioni mendaci, dichiaro che il presente lavoro non è già stato sottoposto, in tutto o in parte, per il conseguimento di un titolo accademico in altre Università italiane o straniere. Dichiaro inoltre che tutte le fonti utilizzate per la realizzazione del presente lavoro, inclusi i materiali digitali, sono state correttamente citate nel corpo del testo e nella sezione 'Riferimenti bibliografici'.

I hereby declare that I have read and understood the "Anti-plagiarism rules and regulations" approved by the Council of the Department of Economics and Management and I am aware of the consequences of making false statements. I declare that this piece of work has not been previously submitted – either fully or partially – for fulfilling the requirements of an academic degree, whether in Italy or abroad. Furthermore, I declare that the references used for this work – including the digital materials – have been appropriately cited and acknowledged in the text and in the section 'References'.

Firma (signature) Luca Beda

Abstract:

Il presente elaborato, dal carattere precipuamente descrittivo, si pone l'obiettivo di fornire una sintetica panoramica sul mondo dei bitcoin nei suoi aspetti teorici e reali.

Il primo capitolo introduce i caratteri essenziali del sistema Bitcoin mediante l'analisi dei suoi obiettivi antistituzionali e delle più fondamentali soluzioni tecniche adottate per pervenirvi, rivelando come talvolta queste ultime non riescano ad adempiere in toto agli scopi prefissatisi; è il caso del protocollo *Proof of Work*, che causa la concentrazione dell'attività di *mining*.

Il secondo capitolo si occupa della percezione che il mondo ha del bitcoin, indagata attraverso sondaggi diretti circa l'utilizzo della criptovaluta come mezzo di scambio da utenti e cittadini e tramite un'analisi della storia del bitcoin. Alla luce dei dati disponibili, si è concluso che il bitcoin, nonostante il suo scarso impiego come moneta e la somiglianza tra l'andamento del suo prezzo con quello di alcune classi di asset, non può dirsi del tutto ascrivibile ad alcuna categoria tradizionale (moneta, asset o *commodity*) in virtù della strutturale polivalenza che rende questa criptovaluta unica e difficilmente etichettabile.

Nel terzo capitolo è presentata una selezione di legislazioni nazionali riguardanti il bitcoin che palesa la pluralità di idee ed opinioni -talvolta divergenti- concernenti le criptovalute.

Vengono infine introdotte le nascenti *Central Bank Digital Currencies*: criptovalute Fiat dall'immenso potenziale, ideate sul modello delle criptovalute dalle quali però differiscono per la loro appartenenza ad un'istituzione.

Indice dei capitoli:

1 - I bitcoin

I bitcoin rappresentano il primo successo globale di una moneta digitale decentralizzata, ovvero svincolata da un'autorità centrale: dal conio, al controllo della valutazione, alla validazione delle transazioni e alla loro registrazione non v'è alcun intervento di qualsivoglia istituzione o figura terza investita d'autorità. Tale innovazione venne presentata al grande pubblico con il celebre manifesto di Satoshi Nakamoto[1] (2008): "Bitcoin, A Peer-to-Peer Electronic Cash System", nella quale si enunciò l'ambizioso progetto di affrancare le transazioni online dall'esigenza di una figura fededegna.

L'assenza, nel mondo Bitcoin, di figure terze autorizzate viene colmata da una rete *peer-to-peer*: un'architettura di rete ove alle richieste dei *client*[2] rispondono nodi[3] ad essi gerarchicamente paritari -che in quel momento si comportano da *server*- fornendo loro un servizio (ciascun nodo può dunque fungere sia da *client* che da *server*). Si parla pertanto, nel caso della rete Bitcoin, di un sistema distribuito avente la funzione di creare transazioni, di verificarle ed infine di divulgarle iscrivendole nel *network*.

Nascendo sotto tali premesse, la rete Bitcoin[4] è stata disegnata per farsi carico di potere e responsabilità abitualmente propri delle istituzioni del campo: Nakamoto non nega l'esigenza di un'entità garante del buon fine della transazione, ma suggerisce per tale ruolo non già una figura più o meno personale -come possono esserlo gli intermediari finanziari- bensì una regolamentazione applicata in maniera automatica e deterministica. Se è vero che presupposto irrinunciabile per ogni transazione è la fede nel rispetto delle "regole del commercio" da parte dei contraenti, garante di tal ossequio diviene a questo punto la prova criptografica -ottenuta mediante l'omonimo software *Bitcoin*- proposta come alternativa ai tradizionali intermediari, azzerando al contempo i costi di transazione propri di qualunque mediazione e così candidandosi come reale concorrente degli attuali metodi di pagamento.

L'operatività del sistema Bitcoin si basa sul lavoro dei nodi, ed in special modo di nodi particolari: i cosiddetti *miners*. Il contributo dei nodi consiste nell'utilizzo del suddetto software Bitcoin e nell'impiego di risorse private per validare le nuove transazioni occorse, che poi i miners, apportando ingenti quantità di capitale in termini di energia elettrica, computer dall'altissima capacità computazionale ed internet a banda larga, uniscono insieme sottoforma di blocchi componenti il libro mastro (la *blockchain* di cui si parlerà a breve). La costante offerta, da parte dei nodi, di un sì fondamentale servizio è garantita dai vantaggi

[1] Tal "Satoshi Nakamoto" è il nome fittizio col quale si firmò l'autore del manifesto dei Bitcoin.
[2] "Un programma che dà accesso a dati o servizi resi disponibili da un server" Summers (2022).
[3] "Nodo" è una qualunque periferica direttamente collegata alla rete.
[4] "Bitcoin", con la lettera maiuscola, indica il metodo di pagamento; con la lettera minuscola, la valuta.

assicuratigli dal sistema: più nodi saranno operativi più le transazioni risulteranno sicure; inoltre i miners, che investono una quantità considerevole di capitale per svolgere le operazioni richiestegli, in caso di avvenuta registrazione delle transazioni vengono remunerati con bitcoin di nuovo conio in un sistema di ricompensa valido fino al raggiungimento del numero massimo di bitcoin emettibili, fissato a 21milioni. Grazie a tale architettura d'incentivi, che sfrutta gli interessi egoistici degli utenti per alimentare i processi necessari al funzionamento della rete Bitcoin, il mantenimento ed aggiornamento della blockchain non costituisce costo per il sistema[5].

1.1 - Il funzionamento del Bitcoin

Un sistema di pagamento decentralizzato, per poter essere affidabile, deve essere resistente ai tentativi di spesa indebita; serve, cioè, che riesca a riconoscere e ad impedire spese di bitcoin d'altrui proprietà e i tentativi di pagamento di due transazioni con la medesima moneta. Nel mondo Bitcoin i controlli propedeutici al contrasto di queste frodi dovranno inoltre essere effettuati prescindendo dal ruolo abitualmente rivestito, nelle istituzioni, da un amministratore (la figura preposta, tra le altre cose, all'assegnazione dei numeri di conto, al rilascio delle autorizzazioni di pagamento e al calcolo dei bilanci dei conti).

Tale problema viene risolto, nel sistema Bitcoin, grazie alla conservazione diffusa d'archivi di documenti con marca temporale[6] non alterabili[7]: la blockchain, della quale si illustrerà sinteticamente il funzionamento nei seguenti paragrafi.

1.2 - La gestione decentralizzata delle identità e dei conti

Per poter permettere delle transazioni in bitcoin è necessario che a ciascun utente sia assegnata un'identità, affinché si possa ricondurre ciascuna moneta al rispettivo proprietario. La creazione delle identità, in Bitcoin, è affidata agli utenti, che dovranno seguire pochi e semplici passaggi prestabiliti dal sistema.

Anzitutto, per poter possedere bitcoin serve generare una *chiave privata* (*sk*: *secret key*, di 256 bit): una stringa alfanumerica di 64 caratteri casuali che dev'essere conservata -pena la perdita del conto- e taciuta agli altri utenti, poiché necessaria per autorizzare esborsi.

Dalla chiave privata viene derivata la *chiave pubblica* (*pk*: *public key*, di 512 bit decompressa, 257 bit compressa): un'altra sequenza alfanumerica che funge da identità con la quale l'utente possa essere riconosciuto dagli altri; il sistema crittografico Bitcoin sfrutta infatti uno

[5] I miners vengono remunerati mediante monete di nuovo conio -che non costituiscono passività per Bitcoin- e mediante una parcella associata a ciascuna transazione concessa su base volontaria. John K. Et al. (2022).

[6] La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005). Per la fonte vedere "Marche temporali" in sitografia.

[7] M. Di Pierro (2017).

"schema asimmetrico": la chiave privata serve a criptare un messaggio, mentre quella pubblica è ricavata affinché le persone esterne possano verificare che il suddetto messaggio sia stato effettivamente creato dal proprietario di quella specifica *sk*, senza con questo poter ricavare la *sk* di quell'utente. Essendo assai facile aprire un conto bitcoin, è altrettanto facile creare nuove coppie di chiavi (privata e pubblica) a proprio piacimento, tutelando così la propria vera identità.

L'*indirizzo* (160 bit), infine, è un analogo del codice IBAN, e viene derivato come hash[8] della chiave pubblica.

Tutti questi codici vengono impiegati nei processi operativi che vanno dalla creazione di una transazione alla sua approvazione ed iscrizione nella blockchain: nella spesa di bitcoin sono richieste informazioni private (la *sk*) che rimarranno celate agli altri nodi, e dati pubblici, che figureranno invece nella blockchain.

L'obiettivo della rete Bitcoin è di rendere le transazioni facili da effettuare, di rendere difficile il furto della chiave privata e di rendere semplice per gli utenti la gestione delle chiavi. Per effettuare un pagamento in bitcoin si deve anzitutto creare il messaggio della transazione che si vuole condurre; esso è composto dalla chiave privata del pagante[9], dall'indirizzo del beneficiario, dall'hash della precedente transazione-output, dall'ammontare di bitcoin da movimentare e dal valore della parcella che si è disposti a corrispondere ai miners (che può anche essere nulla). Per attestare la volontà di procedere con l'esborso serve poi che il pagante apponga una firma sul messaggio di transazione così creato; tale firma digitale è ottenuta con metodo crittografico ECDSA[10] partendo dalla chiave privata dell'acquirente e dall'hash del messaggio della transazione[11]. La firma elettronica non è mai uguale a se stessa, in virtù della presenza del messaggio tra le componenti utili alla sua creazione, evitando il rischio che la si possa semplicemente copiare ed incollare a scopo di frode; chiunque conosca la chiave pubblica del pagante può matematicamente verificare (anche offline) che la firma provenga effettivamente del possessore dei bitcoin, senza per questo ricavare alcuna ulteriore informazione sul pagante o sulla transazione. La presenza della firma digitale rappresenta inoltre prova per il non ripudio: in Bitcoin le transazioni che vanno a buon fine non sono annullabili, e per questo la segretezza della *sk* è tanto fondamentale: in caso di furto non ci sarà alcuno sportello o servizio d'assistenza a cui rivolgersi.

---

[8] La funzione hash è una funzione criptografica matematica che produce una stringa di predeterminata lunghezza partendo da una stringa di lunghezza qualunque. Narayanan et al. (2016) cap. 1.1

[9] Esistono anche conti posseduti congiuntamente, che per autorizzare un pagamento necessitano delle chiavi private di tutti gl'intestatari del conto, e ancora altri tipi di conto che però esorbitano dagli interessi di questa tesi, che si limita a presentare il caso più fondamentale.

[10] Elliptic Curve Digital Signature Algorithm: una funzione il cui input non può essere ottenuto mediante "forza bruta".

[11] Dato che l'hash ha lunghezza predefinita, il messaggio di transazione può essere di qualunque lunghezza.

Una volta firmata, la transazione viene inoltrata ai nodi della rete, dove attende la propria conferma in un limbo chiamato *memory pool* (talvolta contratto nella forma *mempool*), dal quale i miners attingono le transazioni da inserire nei blocchi.

Se il blocco creato da un certo minatore verrà accettato e confermato anche dagli altri miners, allora sarà aggiunto alla blockchain.

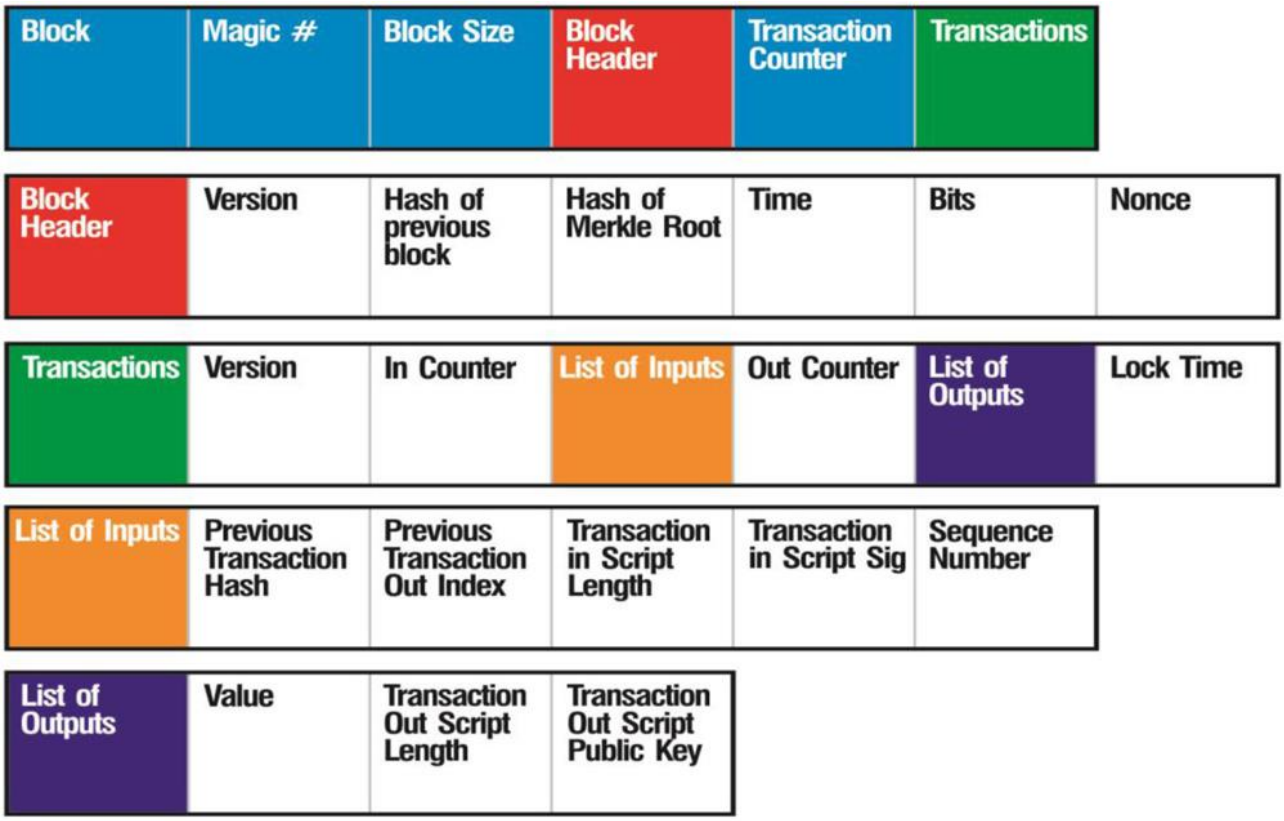

Figura 1: la struttura di un blocco.

Fonte: A. Turner & A. Irwin (2018)

1.3 - UTXO, ovvero il metodo di contabilità dei conti bitcoin

Il sistema Bitcoin non ragiona in termini di saldo conto, bensì secondo un bilancio di transazioni in entrata ed uscita (*input* e *output*) chiamato UTXO ("Unspent Transaction Outputs"), che consiste nel consulto della blockchain per individuare le transazioni in entrata non ancora spese da un certo utente e per calcolarne l'ammontare, ovvero il saldo residuo. In Bitcoin ogni asset ha la propria storia iscritta nella blockchain, il che rende possibile il completo tracciamento di ogni singolo bitcoin, del quale sono noti tutti gli spostamenti sin dal conio; per questo si definisce ogni moneta elettronica come catena di firme elettroniche (Nakamoto, 2008): perché nessun bitcoin esiste al di fuori della blockchain che ne registra i movimenti. I bitcoin non sono pertanto un bene fungibile: un bitcoin non ne vale un altro, poiché la discriminante tra di essi è la loro storia. Proprio come fossero monete fisiche, per ogni transazione non viene scelto semplicemente un ammontare da trasferire da un conto ad

un altro, ma vengono selezionate delle monete specifiche, ciascuna, appunto, con la sua propria storia. I bitcoin scelti per effettuare il pagamento vengono nominati mediante il codice identificativo della transazione che li ha portati ad essere dell'attuale possessore; tale identità ("Transaction ID" o "TXID") consiste nell'hash della suddetta transazione. Per amor di completezza bisogna aggiungere che non basta, per definire l'input, riportare il TXID, poiché una certa transazione occorsa nel passato potrebbe anche aver avuto più beneficiari; per indicare l'input, dunque, si dovranno indicare congiuntamente TXID e quale output di quella transazione intendiamo spendere: l'indice della transazione, appunto (cfr. *Figura 1*, riga 4). Nel caso sotto riportato in *Figura 2*, questo dovrà accadere per la transazione che ha fruttato a Tizio 0,2 bitcoin: se Tizio si limitasse a citare l'ID dell'anzidetta transazione -che aveva come output anche Caio- potrebbero esservi fraintendimenti tantopiù complessi quanto maggiore il numero dei beneficiari.

Nel trasferimento di bitcoin, l'input, ovvero l'importo che si vuole sborsare, è sempre uguale all'output della transazione dalla quale sono provenute le monete che ora ci si accinge a spendere[12]; qualora si voglia utilizzare solo una parte dei soldi ottenuti dalla precedente transazione (che, ricordiamo, costituiscono l'input dell'attuale transazione), bisognerà creare una transazione con output multipli, ovvero con diversi beneficiari per importi differenti, avente come destinatari la controparte e se stessi.

Gli output consistono nell'indirizzo del beneficiario, nella dimensione della transazione e nell'ammontare della somma da versargli (cfr. *Figura 1* riga 5). Per semplificare questo processo vengono adottati dei portafogli digitali (*wallet*): programmi che custodiscono le chiavi e facilitano l'effettuazione di movimenti in entrata ed uscita mediante interfacce ergonomiche.

In *Figura 2* è esemplificato un caso nel quale Tizio, disponendo di tre pacchetti di bitcoin provenienti da precedenti transazioni a noi sconosciute, vuole pagare 0,8BTC a Sempronio. Tizio utilizzerà i tre pacchetti di bitcoin come input multipli, mentre gli output consisteranno in 0,8BTC per Sempronio e in 0,09BTC per se stesso (in quest'esempio una parte della transazione verrà tributata ai miners come commissione volontaria). Le commissioni corrisposte ai miners variano non sulla base dell'importo della transazione, ma sulla base dei *byte* che la transazione occuperà nella blockchain (dimensione della transazione); la parcella corrisposta nel nostro esempio, dunque, sarà superiore a quella che converrebbe pagare ad un uomo che abbia trasferito -diciamo- 5BTC appartenenti tutti ad un medesimo blocchetto di bitcoin ottenuti da una sola precedente transazione.

Dato che nella creazione dei blocchi i miners priorizzano transazioni associate ad alte

[12] L'unica eccezione è nel caso di nuovo conio di bitcoin: in tal situazione non esiste input.

parcelle, è consigliato agli utenti d'impostarne una nel tentativo di sveltire il processo d'approvazione. Le commissioni vengono create rendendo l'*input* maggiore dell'*output*: a quel punto il sistema corrisponderà la differenza al miner che creerà il blocco sottoforma di *block reward*.

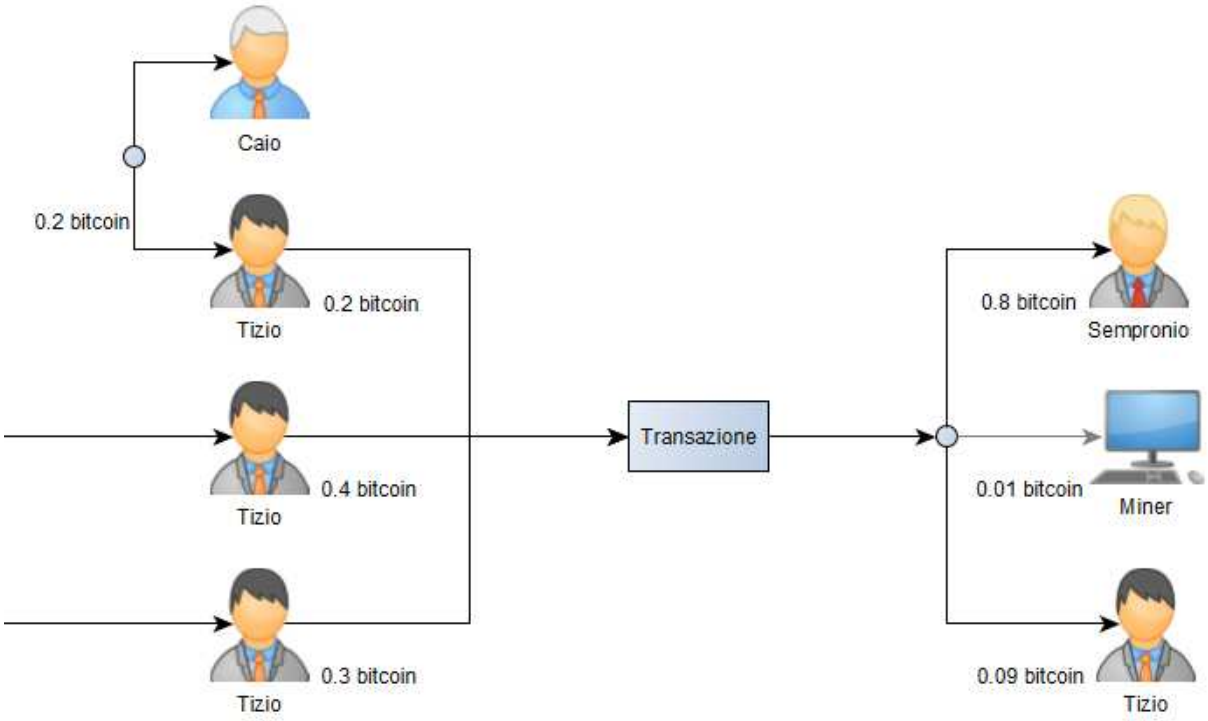

Figura 2: esempio di una transazione.

1.4 - La blockchain e il suo funzionamento

Risolto il problema della gestione delle identità, rimane aperta la questione del mantenimento ed aggiornamento del libro mastro: se si vuole evitare il problema della doppia spesa[13] è d'uopo registrare le transazioni e stabilirne il momento di generazione per poter tracciare i bitcoin e dunque decidere se validare le transazioni proposte o meno; deve inoltre esistere un sistema di sicurezza che regoli la registrazione dei blocchi e ne impedisca la modifica post iscrizione. Tutto ciò dovrà infine avvenire, come stabilito da Nakamoto, in maniera del tutto decentralizzata: chiunque potrà partecipare all'attività contabile e tutti i nodi dovranno esser trattati allo stesso modo, mancando una gerarchia. In tal contesto diviene cruciale l'efficacia del sistema contro i tentativi di sabotaggio di eventuali nodi malevoli se consideriamo che, avvalendosi Bitcoin d'identità fittizie, i malintenzionati potranno ripresentarsi sotto vesti sempre diverse.

I tentativi di manomissione della blockchain da parte dei nodi, nel sistema Bitcoin, vengono contrastati mediante un protocollo chiamato "Proof of work" (letteralmente: "prova di lavoro"), atto a regolare quei processi che vanno dalla creazione dei blocchi alla loro

[13] Il problema che gli stessi soldi vengano impiegati parallelamente in due diverse transazioni eccedendo l'effettiva disponibilità finanziaria.

approvazione. L'efficace operare di questo protocollo è fondamentale per l'esistenza stessa del sistema Bitcoin: in caso di falle, la blockchain diverrebbe vulnerabile ad attacchi e manomissioni, facendo perdere di credibilità al sistema e causando il deprezzamento della valuta; venendo meno il valore del bitcoin, con esso si svaluterebbero anche gli incentivi offerti ai miners per i loro servizi, causando lo sgretolarsi delle fondamenta della rete e dunque della rete stessa.

Le caratteristiche della prova di lavoro sono finalizzate al raggiungimento congiunto dell'affidabilità dei dati approvati e della loro inalterabilità dopo la conferma.

L'intero protocollo PoW si fonda sul presupposto -ragionevole ma non già scontato- che la maggior parte dei nodi operino in maniera onesta[14] registrando le transazioni senza contraffarne i dati: la versione di un certo movimento attestata dalla maggior parte dei nodi verrà considerata veritiera poiché, come poc'anzi postulato, la maggior parte di essi non ha ragione di manipolare le informazioni.

Il libro mastro elettronico dove vengono registrati i movimenti è la già citata *blockchain*, aggiornata e conservata grazie ai software operanti sui vari nodi.

Nonostante la crucialità del ruolo che questa tecnologia riveste per il sistema, essa -che peraltro non viene mai esplicitamente citata nella pubblicazione di Nakamoto- non rappresenta il fine del progetto Bitcoin, ma la soluzione tecnica adottata per giungere ad esso[15]. L'unità minima costituente la blockchain è la singola transazione; le singole transazioni vengono legate insieme tra loro in numero medio di 2000 circa formando un blocco; l'unione dei blocchi forma la catena (*block-chain*, appunto). La ragione per la quale nella blockchain non vengono iscritte direttamente le transazioni, bensì i blocchi, è che la verifica di un blocco risulta molto più veloce ed efficiente della verifica di ciascuna transazione in esso contenuta presa singolarmente.

Figura 3: Modello illustrativo della blockchain e delle unioni tra blocchi. I colori sono quelli della Figura 1.

[14] Nakamoto (2008): "The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes".

[15] Lewis (2018), pag. 159.

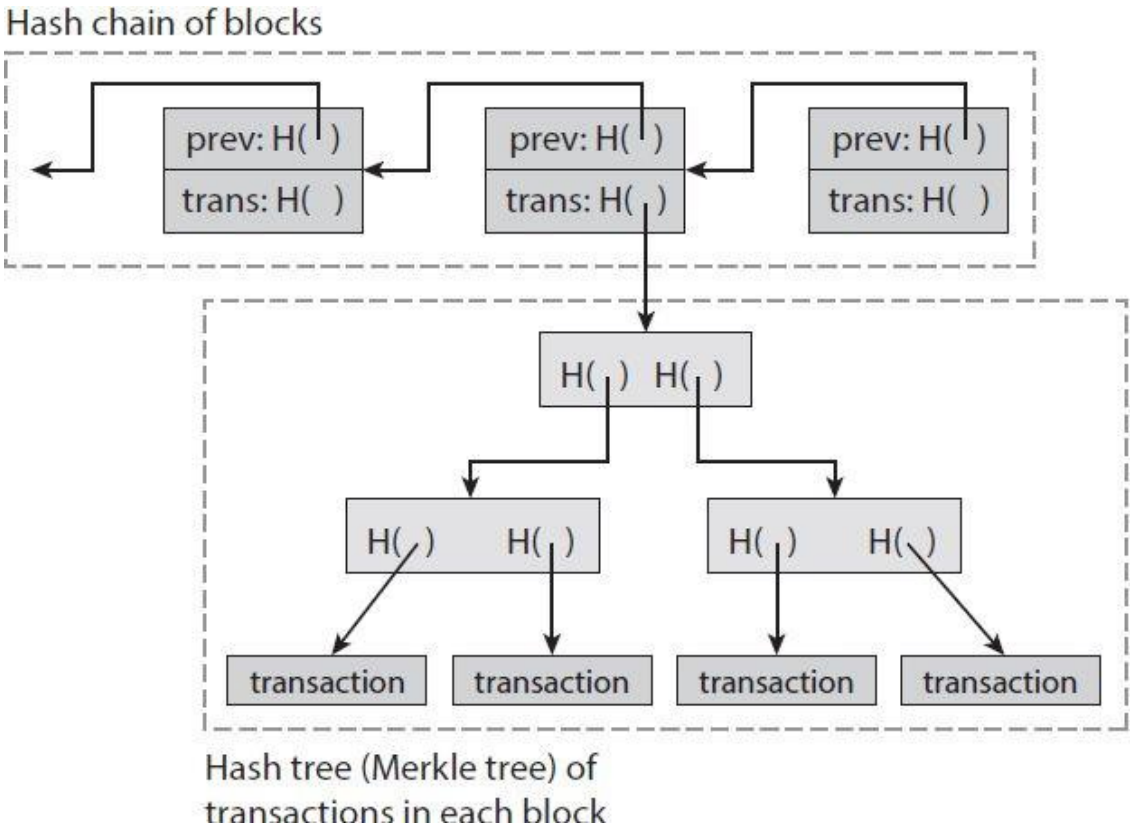

Figura 4: struttura di un blocco. I blocchi si legano tra loro mediante le proprie testate, contenenti l'hash del blocco precedente; al tal ID si agganciano a loro volta i Merkle tree interni al blocco: "alberi" di transazioni disposte in forma piramidale la cui base è costituita dalle singole transazioni ed i cui livelli più alti sono calcolati mediante le hash delle varie "foglie", prese in coppia.
Fonte: Narayanan et al. (2016), pag. 114.

Per poter aggiungere un blocco alla catena, questo dev'essere sottoposto al controllo di prova di lavoro, che, se superato, decreta la sua integrazione nel libro mastro.

La PoW viene superata mediante dei rompicapo in hash (*hash puzzle*): per creare un blocco, è richiesto ai miners di trovare una serie numerica di 32 bit (*nonce*, cfr. *Figura 3*) tale che, dopo aver calcolato l'hash del blocco, quest'ultima sia di dimensioni tali da occupare perfettamente una posizione target ad essa predisposta (*dimensione dell'hash del blocco ≤ dimensione target*). In virtù dell'alta capacità computazionale e dei consistenti apporti di capitale privato richiesti ai miners per completare il puzzle, il protocollo PoW disincentiva, mediante la difficoltà computazionale necessaria alla creazione di un blocco, la nascita e proliferazione di nodi malevoli: se non è possibile punire i comportamenti nocivi in un sistema nel quale la creazione di una nuova identità è estremamente semplice, si può evitare il problema di avere il 51% di nodi di rete impostori alzando i costi di *mining*.

Lo scopo di questa corsa al pezzo mancante è la generazione di un hash che segnali se il blocco registrato è stato modificato. Se questo dovesse accadere al blocco A -ad esempio-, per via della presenza dell'ID[16] di A nel blocco B ad esso successivo, con la modifica del blocco A verrebbe meno la coincidenza tra ID di A inscritto in B ed attuale ID di A, invalidando così

[16] Per ID di un blocco s'intende l'hash dello stesso.

tutti gli anelli della catena dal blocco B in poi. Per poter modificare un solo blocco della catena servirebbe dunque modificare anche tutti i blocchi ad esso inanellati e riuscire a far accettare tale modifica alla maggior parte dei nodi di rete.

Proprio per via dell'immutabilità dei blocchi della blockchain non è assolutamente prevista, nel sistema Bitcoin, la possibilità di annullare una transazione valida (neppure in casi estremi come il furto della chiave privata).

Il metodo più efficace per risolvere l'hash puzzle è procedere a tentoni: tentare in sequenza tutte le possibili *nonce* finché l'hash del blocco risulta essere di dimensioni accettabili. Solitamente, però, non esistendo una *nonce* possibile per ciascun potenziale blocco, i miners procedono a modificare l'ordine delle transazioni o a cambiare le transazioni incluse nel blocco finché non viene individuata una nonce valida tra le 2^{32} possibili. Il miner che riesce ad ottenere l'iscrizione del blocco nella catena riceve, oltre a tutte le commissioni annesse alle transazioni in esso contenute[17], anche il diritto di aggiungere al suddetto blocco una nuova transazione *coinbase*, consistente in bitcoin di nuovo conio destinati ad un indirizzo a scelta. Il valore della coinbase è predefinito dal sistema e varia nel tempo dimezzandosi ogni 210mila blocchi aggiunti alla catena (ogni 4 anni circa); attualmente essa è pari a 6,25BTC.

Per garantire una costante registrazione delle transazioni, dal momento che i nodi sono liberi di connettersi e disconnettersi liberamente dalla rete, la difficoltà del puzzle viene calcolata in funzione del tempo medio impiegato per la produzione di un blocco, a sua volta associato con l'*hash rate* disponibile[18], per far sì che vengano registrate le transazioni ad un ritmo che consenta anche la diffusione del blocco in tutte le versioni locali della blockchain, evitando così perniciosi difetti del libro mastro (come le biforcazioni accidentali[19]). Per questa ragione solo un blocco ogni 10 minuti circa può essere aggiunto alla catena, accordando ai nodi un tempo sufficiente per comunicare tra di loro gli aggiornamenti e concordare sulla forma della catena, limitando così i potenziali danni derivanti dai difetti delle telecomunicazioni[20].

Per far sì che quest'intervallo rimanga costante si imposta la difficoltà dei puzzle ogni due settimane circa (2016 transazioni) secondo la seguente formula matematica[21]:

$$nuova\ difficoltà = \frac{difficoltà\ passata\ \cdot\ 2016\ \cdot\ 10\ minuti}{tempo\ impiegato\ per\ minare\ gli\ ultimi\ 2016\ blocchi}$$

[17] Studi come quello di Easley et al. (2019) sottolineano l'importanza delle commissioni nel raggiungimento dell'equilibrio dell'ecosistema Bitcoin, e la loro screscente preminenza alla luce della progressiva diminuzione della coinbase.

[18] Hash rate: tasso di calcolo dei codici hash, che riflette la capacità computazionale dell'*hardware* utilizzato.

[19] La biforcazione è un fenomeno nel quale ad un blocco ne vengono collegati contemporaneamente due o più, creando versioni parallele della blockchain tra loro differenti ed antagoniste.

[20] Grazie allo scandirsi del conio di bitcoin in lassi di tempo definiti si contrasta inoltre la fluttuazione del valore della valuta che un'emissione di monete in quantità eccessiva o variabile (anche temporalmente) causerebbe.

[21] Da: Narayanan et al. (2016), pag. 170.

La verifica, da parte degli altri miners, del corretto svolgimento del Proof of Work è stata pensata per essere semplice e veloce: basta calcolare l'hash del blocco e accertarsi delle sue adeguate dimensioni; così facendo si favoriscono efficacia dei controlli e trasparenza.

L'ultima questione che il protocollo Proof of work dirime è la nascita parallela di nuove blockchain: mancando un'autorità centrale detenente una versione ufficiale e univoca della blockchain, ogni nodo ne conserva una propria nella memoria locale; il grande problema che il protocollo si prefigge di risolvere è la sincronizzazione delle versioni della blockchain anche tra nodi di rete non collegati tra loro, ovviando così a difetti di *network* e a tentativi di sabotaggio. Una volta fabbricato il blocco, chiamato *blocco candidato*[22], i dati in esso contenuti vengono sottoposti al controllo degli altri nodi[23]. La diffusione delle informazioni avviene mediante un *protocollo gossip peer-to-peer*: quando un minatore crea un blocco con successo, questo viene inoltrato a tutti i nodi collegati al miner, ciascuno dei quali procederà individualmente alla verifica della sua validità per controllare che non presenti casi di doppia spesa o difetti simili. Se il blocco supera questa prova, i miners che l'hanno ricevuto lo accettano aggiungendolo al proprio libro mastro locale agganciandovi i blocchi di nuova fabbricazione ed inoltrandolo agli altri nodi ad essi collegati.

L'approvazione della transazione contenuta in un blocco avviene dopo che, aggiunto il blocco nella blockchain, su di esso gli altri miners legano i propri bocchi; generalmente dopo sei blocchi legati si considerano definitivamente approvate le transazioni in esso contenute.

Queste precauzioni servono ad evitare il fenomeno delle biforcazioni della catena: vista l'alta competitività della corsa alla costruzione di un blocco, può accadere che ad un certo blocco ne vengano collegati contemporaneamente due o più, tutti potenzialmente validi, generando nella rete diverse versioni della blockchain. In tal caso, il blocco da integrare nella catena -e per converso quelli da abbandonare- viene scelto sulla base della lunghezza della catena ad esso inanellata, dacché il PoW stabilisce che si debba sempre costruire sulla versione della catena più lunga tra quelle disponibili (LCR: *Longest chain rule*). Si genera insomma una gara tra nodi: la versione della catena che per prima supera le altre in lunghezza viene accettata dai nodi ai quali viene proposta, rubando capacità computazionale alle proprie versioni concorrenti che, crescendo a ritmo inferiore, sono destinate ad essere rigettate in favore della catena più lunga.

Per quanto riguarda i blocchi non integrati nella catena, essi andranno perduti divenendo

[22] Antonopoulos (2010).

[23] Non sono solo i miners a validare i blocchi: esistono *client* SPV ("Simplified Payment Verification") -che costituiscono la maggior parte dei nodi di rete- che conservano localmente non tutta la blockchain, come fanno i miners, ma solamente quelle parti di essa utili alla validazione delle transazioni che li coinvolgono in prima persona. La capacità computazionale richiesta ai nodi SPV è tale che persino un telefono cellulare risulta adeguato al compito.

"blocchi orfani", i cui autori non riceveranno ricompense per la loro creazione e le cui transazioni non verranno eseguite finché non figureranno nella catena accettata.

1.5 - Il software Bitcoin e le biforcazioni

Come già diffusamente detto, Bitcoin è una rete priva di figure centrali, rimpiazzate da formule matematiche e *software* informatici, considerando la natura dei quali diviene lampante il rischio di obsolescenza del sistema, minacciato internamente da difetti di programmazione ed esternamente da attacchi hacker in costante evoluzione; a tali problemi si ovvìa mediante il rilascio di aggiornamenti ai software. La questione pratica, però, visto il tipo di organizzazione decentralizzata e distribuita del sistema, verte sulle modalità con le quali gestire, proporre ed attuare una siffatta transizione.

La minaccia maggiore, per Bitcoin, è che i vari nodi, operando mediante software diversi, sviluppino problemi di comunicazione reciproca rendendo la blockchain vulnerabile a sabotaggi o a biforcazioni permanenti.

L'aggiornamento del software può implicare variazioni del protocollo di gestione della blockchain: possono essere modificate, tra le altre cose, le dimensioni dei blocchi, la struttura delle commissioni ed il protocollo Proof of Work, alterando così la definizione stessa di "blocco valido" e dunque minando i presupposti comunicativi tra nodi aventi versioni diverse del software. È bene, a questo punto, specificare che non tutte le versioni dei software Bitcoin sono incompatibili tra loro, come traspare dalla *Figura 5*, ma che possono occorrere aggiornamenti che estromettono versioni del software favorendone altre.

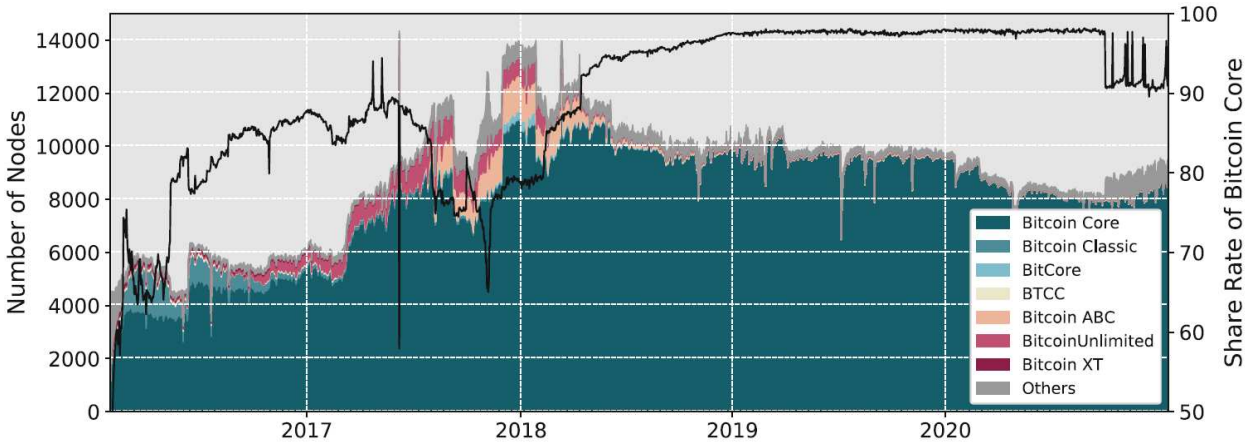

Figura 5: serie temporale delle versioni software adottate dai nodi di rete dal 2016 al 2021. Il grafico rivela l'ampiezza della gamma di software utilizzati dai nodi. La riga nera rappresenta la percentuale di adozione di Bitcoin Core.
Fonte: Imamura & Kazumasa (2021).

Dall'aggiornamento dei sopracitati aspetti della blockchain, con le annesse difficoltà comunicative tra nodi aggiornati e nodi con differenti ed incompatibili versioni, traggono origine le cosiddette "*soft*" ed "*hard forks*": dei particolari tipi di biforcazione della blockchain.

Le *soft forks* vengono causate dall'introduzione, nel software aggiornato, di nuove restrizioni: blocchi costruiti secondo criteri prima validi ora divengono inaccettabili ai sensi delle nuove regole (es: la dimensione massima di un blocco valido viene dimezzata).

Questi sono i presupposti per la nascita di un contrasto tra nodi aggiornati e non: i nodi aggiornati potranno proporre ai nodi non aggiornati blocchi validi secondo i parametri di questi ultimi, mentre i blocchi prodotti dalle vecchie versioni del software risulteranno inaccettabili agli occhi del software aggiornato.

L'accettazione della versione aggiornata viene decretata mediante la regola della catena più lunga: il software aggiornato prevarrà se impiegato dalla maggior parte della capacità computazionale del sistema, poiché avvalendosi di un alto hash rate la versione della blockchain costruita secondo il criterio restrittivo crescerà più velocemente della catena costruita secondo il criterio rivale, impossibilitando infine i nodi adoperanti i vecchi software ad iscrivere i propri blocchi nella blockchain (costruita secondo criteri più rigidi). Se questo non dovesse avvenire, invece, sarà decretato il rifiuto dell'aggiornamento.

Nel mondo Bitcoin, evidentemente, la scelta del software da adottare -o, per meglio dire, delle regole di costruzione della blockchain, poiché come abbiamo visto sono queste a contare piuttosto che l'adozione di un software specifico, che ne è solamente espressione- è imposta ai nodi dalla dittatura della maggioranza (maggioranza non dei nodi ma del potere computazionale, il che circoscrive ulteriormente la cerchia d'influenti in questo ambito[24]). Se si vuole continuare ad iscrivere blocchi nella catena bisognerà attenersi alle nuove regole.

Le *hard forks*, a differenza delle *soft forks*, nascono all'introduzione di un aggiornamento che rende le regole sulla formazione dei blocchi meno stringenti (es: le dimensioni di un blocco ora possono essere anche doppie rispetto a prima). Se un miner col software aggiornato produrrà un blocco di dimensione doppia, questo sarà accettato dai nodi aggiornati e rifiutato da quelli non aggiornati, mentre i blocchi prodotti dai miners non aggiornati risulteranno accettabili agli occhi dei *client* aggiornati. I nodi aggiornati, dunque, lavoreranno sulla propria versione della blockchain che non verrà mai accettata dai vecchi *client*, i quali a loro volta elaboreranno una propria versione della catena.

Nel caso delle *hard forks*, le due versioni possono anche continuare a coesistere per tempo indefinito, causando problemi alla blockchain (ovvero raddoppiando i bitcoin esistenti[25]) e

[24] Il mining è un'attività estremamente centralizzata: il 10% dei miners controlla ben il 90% del potere computazionale, e lo 0,1% dei miners (in numero di una cinquantina circa) controlla quasi il 50% della capacità computazionale totale. Questi dati empirici sono tali da mettere in quesitone la stessa validità della teorica decentralizzazione Bitcoin. Makarov & Schoar (2021).

[25] Come quando, il primo agosto 2017, una *hard fork* generata da un gruppo scissionista causò la separazione tra bitcoin (BTC) ed il tuttora esistente frutto della biforcazione: la nuova criptovaluta "bitcoin Cash" (BCH). Atik & Gerro (2018).

diminuendo l'hash rate complessivamente disponibile, poiché una parte di essa sarà impiegata a lavorare su una blockchain e l'altra parte lavorerà su un'altra catena divergente dalla prima. La difficoltà di progettare un cambiamento nella rete e ancor più i danni che questo può cagionare sono le principali ragioni per le quali nella storia di Bitcoin non sono mai avvenute trasformazioni davvero degne di nota, che forse mai accadranno.

2 – I bitcoin nell'economia reale

Nel presente capitolo, oramai illustrati i principali meccanismi tecnici che permettono a Bitcoin di funzionare come rete e criptovaluta, si procederà a trattare il tema del reale utilizzo del bitcoin nell'economia, e dunque della sua vera natura.

2.1 – Le persone che utilizzano Bitcoin come metodo di pagamento

Non è possibile stimare, mediante consultazione della blockchain, il numero di persone che effettivamente utilizza il bitcoin come moneta di scambio: la catena riporta infatti -secondo il principio di pseudonimia- indirizzo e chiave pubblica delle controparti, ma non risponde al principio di "un uomo un conto", tantomeno se si considera che molte persone acquistano bitcoin da privati che adoperano un unico conto per effettuare pagamenti per conto di molte persone diverse[26].

Sotto questo aspetto, dunque, l'unico modo per procedere è mediante sondaggi diretti, il più recente dei quali proviene dalla Banca Centrale australiana: "Consumer Payment Behaviour in Australia"[27], condotto tra ottobre e l'inizio di dicembre 2022 su un campione di mille persone circa. Tale studio, in un contesto di grande crescita dei pagamenti digitali dovuto alla pandemia e alla quarantena, conclude lapidariamente che: *molte persone erano a conoscenza delle criptovalute, ma solo una minuscola frazione di esse le ha impiegate per condurre un pagamento nell'ultimo anno*.

Un secondo e forse più significativo contributo proviene dallo studio di Alvarez et al. (2022), condotto nello stato di El Salvador (stato in cui il bitcoin ha corso legale e l'accettazione del quale è pertanto obbligatoria). Secondo tale studio, condotto mediante interviste faccia a faccia con 1800 famiglie, in media solamente il 4,9% degli acquisti vengono pagati in bitcoin, e l'88% delle attività converte immediatamente i bitcoin ricevuti in USD, con un'accumulazione di bitcoin nei portafogli tendente allo zero. In questo studio uno dei principali problemi è costituito dallo scarso tasso d'alfabetizzazione digitale salvadoregno, che tuttavia non inficia l'indicatività dei risultati ottenuti.

Sembrerebbe insomma che le persone non percepiscano il pagamento con bitcoin come una valida alternativa ai metodi tradizionali.

2.2 – I bitcoin che vengono utilizzati come mezzo di pagamento

Una conferma di quanto prospettato nel precedente paragrafo può esser ottenuta dallo studio della blockchain per esaminare la composizione dei movimenti in essa registrati.

---

[26] Makarov & Schoar (2021): "Bitcoin addresses can be generated freely, so [in some cases] the same entity controls […] even tens of millions of different addresses".

[27] Thuong & Benjamin (2022).

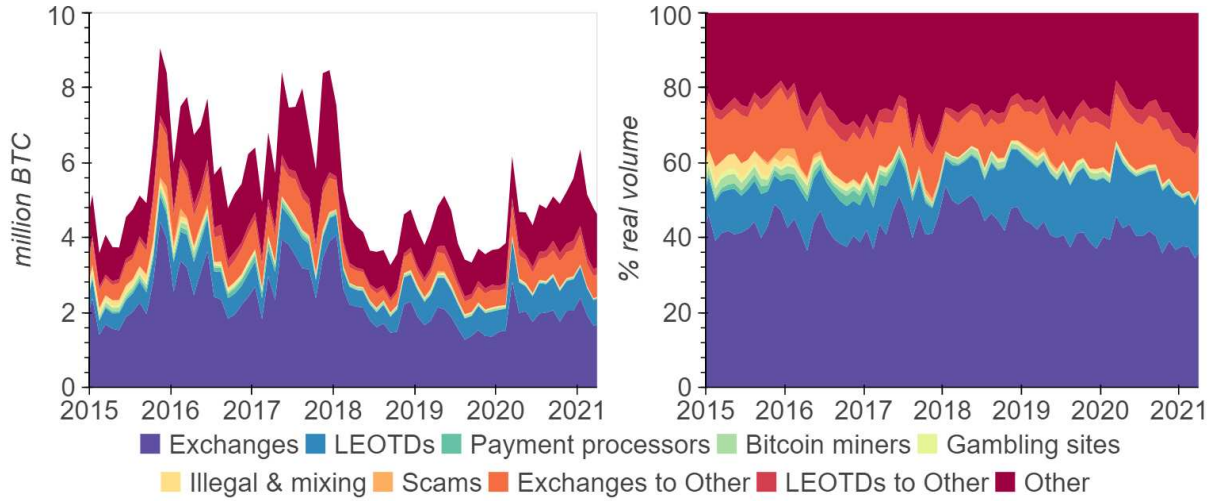

Figura 6: composizione delle transazioni economicamente rilevanti iscritte nella blockchain tra gennaio 2015 e maggio 2021.

***LEOTDs**: Likely Exchanges, OTC brokers, Trading Desk*

***Bitcoin miners**: block reward = coinbase + commissioni*

***Other**: pagamenti vs indirizzi non classificati. Una parte di questa categoria è costituita da transazioni tra persone diverse.*

Fonte: Makarov & Schoar (2021).

Stando allo studio di Makarov & Schoar (2021), la blockchain è costituita per il 90% da movimenti non economicamente rilevanti, come spostamenti tra conti aventi medesima proprietà e conversione di bitcoin in altre valute. Esaminando quel 10% di movimenti occorsi tra persone diverse (cfr. *Figura 6*), invece, risulta che LEOTD e cambi valuta costituiscono insieme oltre il 60% di essi -rivelando un consistente impiego speculativo del bitcoin- e che "payment processors" (siti che facilitano le transazioni con entità accettanti il bitcoin), siti d'azzardo, truffe ed attività illegali non costituiscono che il 3% circa delle transazioni occorse. Le transazioni tra privati costituiscono una percentuale non meglio specificata certamente inferiore al 23% delle transazioni economicamente rilevanti occorse (cfr. *Other* in *Figura 6*). Il dato più inquietante, però, è rappresentato dal numero straordinariamente alto di transazioni a sfondo illecito condotte mediante bitcoin (valuta particolarmente adatta a tali scopi grazie alla sua tutela della privacy); è stato stimato da Foley et al (2017) che nel 2017 il 26% degli utenti bitcoin ed il 46% delle transazioni tra persone diverse fossero collusi in attività illecite per un valore totale di 27milioni di bitcoin (7miliardi di USD).

È altresì probabile che il bitcoin sia sempre stato considerato, dalla maggior parte dei suoi possessori, come investimento speculativo: già nel 2013, infatti, Ron & Shamir (2013) affermavano: *la maggior parte della moneta coniata rimane dormiente in indirizzi che mai hanno partecipato ad operazioni in uscita* e che costituiscono il 73% dei conti totali. Sembra insomma che il bitcoin non venga particolarmente impiegato nella sua funzione di mezzo di scambio.

2.3 – Una prospettiva storica sul Bitcoin

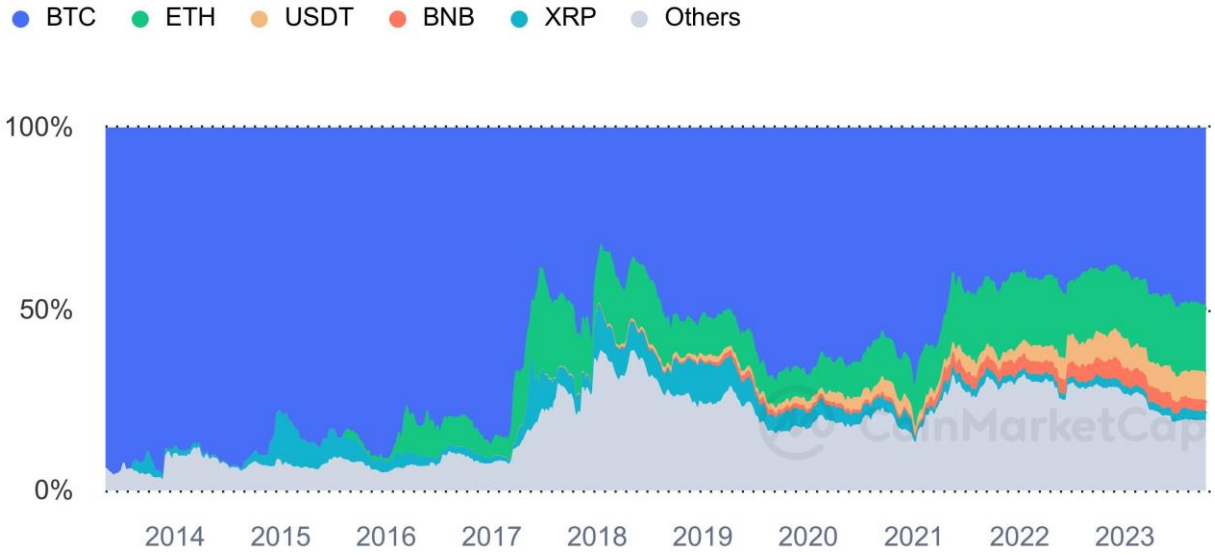

Figura 7: Serie storica sulla composizione della capitalizzazione del mercato delle criptovalute.
Per la fonte vedere: "Composizione market cap criptovalute" in sitografia.

Considerata "la" criptovaluta per antonomasia, il bitcoin, nella sua vita poco meno che quindicennale, ha vissuto da protagonista tutte le evoluzioni del settore delle monete digitali decentralizzate, di cui è il più eminente rappresentante (cfr. *Figura 7*).

La suddivisione dei periodi qui sotto proposta è tratta da Chohan (2022).

2008 - 2010: la nascita

L'anno seguente alla pubblicazione del manifesto del 2008, Bitcoin entrò in funzione con la creazione del primo blocco della catena, minato da Nakamoto stesso. In quegli anni, rimanendo pur sempre un'innovazione di nicchia, il bitcoin riuscì ad attirare l'attenzione di appassionati e detrattori delle istituzioni tradizionali (sono gli anni della crisi finanziaria globale), venendo impiegata per la prima volta -nel 2010- in una transazione: due pizze acquistate indirettamente da Papa John's. L'unico altro evento significativo occorso durante questi primi anni di rodaggio fu il primo successo di un attacco hacker contro la blockchain, con l'emissione, nell'agosto del 2010, dell'esorbitante cifra di 180miliardi di bitcoin, immediatamente rimossi dal circolo; per la prima volta aggiornamenti del software divenivano necessari alla perpetuazione del sistema.

2011-2017: prima crescita e diffusione

L'ecosistema delle criptovalute iniziò ad esprimere una vitalità crescente, testimoniata dalla comparsa di nuove monete digitali ideate partendo dal codice open-source di Bitcoin, dall'accettazione di transazioni in bitcoin da parte -tra gli altri- di WikiLeaks, e dall'approdo del bitcoin ai canali di comunicazione di massa, nella neonata rivista *Bitcoin Magazine* e con una sorprendentemente lunga citazione nella celebre serie televisiva *The Good Wife*.

Nel 2012 venne istituita la "Bitcoin Foundation": un'organizzazione finalizzata alla protezione e promozione di un bitcoin la cui reputazione era intaccata dal suo consistente impiego in commerci illeciti.

Nel 2013, monitorato con sempre maggior attenzione dalle autorità politiche e giudiziarie di tutto il mondo, il bitcoin dovette affrontare problemi di natura tecnica e legale: in un contesto di crescente accentramento dell'attività di *mining*, negli USA la Financial Crimes Enforcement Network impose ai miners la registrazione per l'esercizio della propria attività (vanificando l'apprezzato principio di pseudonimia garantito da Bitcoin), mentre nel dicembre dello stesso anno, in Cina (all'epoca sede del più importante exchanger al mondo: *BTC China*), venne proibito l'utilizzo di bitcoin per ultimare transazioni online, causandone un crollo del prezzo, ulteriormente danneggiato dalla diminuzione dell'offerta di miners e dal conseguente rallentamento dei processi tecnici di aggiornamento della blockchain.

Sempre nel 2013 venne chiuso *Silkroad*: l'*e-Bay* del *DarkWeb*, causando la massiccia vendita di bitcoin da parte dei non pochi utenti del sito.

Nel gennaio del 2014 si verificò la prima hard fork scissionista, dalla quale prese vita la nuova cripto *Dash*.

All'inizio dello stesso anno, inoltre, fecero scalpore i clamorosi furti di conti subiti dai due maggiori cambiavalute al mondo: Bitstamp (britannico, derubato di 19000 BTC) e Mt.Gox (giapponese, fallito dopo la scomparsa di 744000 BTC), che causarono un secondo crollo del valore della cripto, la cui affidabilità veniva così messa nuovamente in discussione. Nonostante le avversità degli ultimi due anni, gli esercizi accettanti il bitcoin come metodo di pagamento (tra i quali s'annoverano Dell, Microsoft ed importanti siti di scommesse) continuarono a crescere in concomitanza col valore del bitcoin, per il quale le avversità del 2013 e 2014 non avevano che rappresentato un momentaneo arresto di un inesorabile processo d'espansione testimoniato anche dall'apparizione del prezzo bitcoin in siti come YahooFinance (2014) e GoogleFinance (2015).

Nel dicembre del 2017, infine, visto il dilagante interesse verso questa innovazione, il costo della cripto si gonfiò in breve tempo, toccando la cifra record di 19475 $/BTC il 17 dicembre. Tali risultati non erano però destinati ad esser mantenuti: in due settimane soltanto bitcoin vide il proprio prezzo calare del 33%, assumendo un andamento al ribasso conservato anche nella prima parte del 2018.

Di seguito è proposto un sintetico studio grafico dei bitcoin. I dati, provenienti dalle serie storiche a cadenza giornaliera di YahooFinance, sono stati selezionati prendendo ispirazione da Dirk G. Baur et al. (2018, capitolo 3.1).

BTC (criptovaluta): prezzo di un BTC in USD, confrontato con:

Gold (asset, metallo prezioso): prezzo in USD.

Pd (futures sul palladio: asset, metallo prezioso): prezzo in USD; quello del palladio è un mercato ad alta volatilità[28].

SPHY (SPDR EFT high yield: bond): indice rispecchiante le prestazioni di corporate bond under investment grade denominati in USD.

CNY (valute): tasso di cambio USD/Yuan-Renmimbi per scambi interni alla Cina continentale.

EUR (valute): tasso di cambio USD/EUR.

SeP500 (S&P 500: indice azionario): indice delle 500 aziende statunitensi a maggior capitalizzazione.

TNX (10y treasury rate: bond): proxy del costo del capitale a rischio nullo.

FSI[29] (indice di stress finanziario): calcolato per *US*, *other developed economies* ed *emerging markets*.

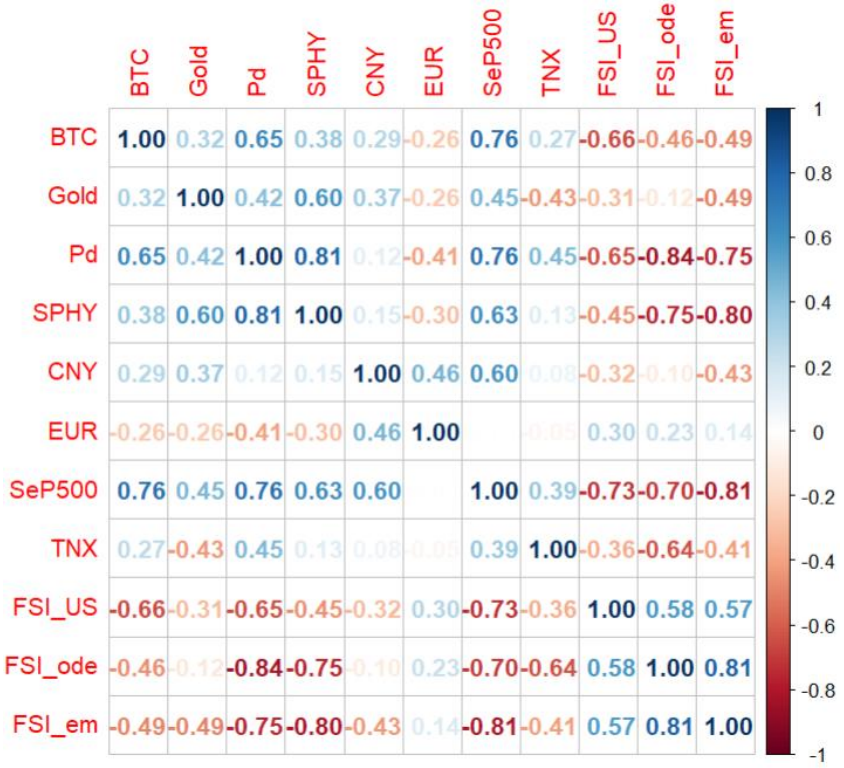

Figura 8: Correlazioni tra le variabili; dati dal 18/09/2014 al 17/12/2017.

Per quanto un semplice studio sulla correlazione non possa esser niente più che indicativo dei rapporti tra variabili, l'alta correlazione tra l'indice S&P500 ed il prezzo del bitcoin suggerisce come, in quest'arco temporale, la cripto possa esser stata percepita quale analogo degli strumenti finanziari presenti sul mercato azionario (cfr. *Figura 13*).

2018-2019: il riassestamento ed il *cryptowinter*[30]

L'esplosione della prima bolla Bitcoin, oltre ai danni cagionati dalla subitanea svalutazione della moneta, generò un senso di circospezione in quei molti investitori che in poco tempo,

[28] Mensi et al. (2019): "Palladium has the greatest influence on the good and bad volatility of BTC".
[29] La fonte per questi dati è: https://www.financialresearch.gov/financial-stress-index/
[30] Per la fonte vedere: "Cryptowinter" in sitografia.

fomentati dall'irrazionale eccitazione del settore, vi avevano perduto buona parte delle somme precipitosamente investite.

Sotto un rigenerato senso di diffidenza generale, rallentatasi la diffusione della criptovaluta tra gli sfiduciati investitori, si assistette a due anni di fluttuazioni del valore del bitcoin che, partendo dai 19mila dollari del 17/12/2017, arrivò addirittura a 3253$ il 18/12/2018. Nel gennaio del 2018 il processo di svalutazione accelerò: si diffusero voci su un possibile divieto dell'attività di *crypto trading* in Sud Corea (un paese con una giurisdizione considerata amena per il bitcoin) ed avvenne un nuovo clamoroso furto di bitcoin, per un valore di 530milioni di USD, ai danni di Coincheck: il maggiore mercato OTC del Giappone, costretto a sospendere la propria attività.

Dal punto di vista giurisdizionale, gli USA si preoccuparono di costruire una regolamentazione per le due criptovalute maggiormente capitalizzate (*bitcoin* ed *ehtereum*): esse vennero ascritte alla categoria delle *commodity* e vennero creati dei protocolli per contrastare il loro impiego in attività di riciclaggio di denaro e finanziamento d'attività terroristiche. L'approccio legislativo utilizzato dagli Stati Uniti, prudente e liberale, sortì il benefico effetto di offrire al sistema Bitcoin dei servizi -come quello di arginamento delle attività illegali- che altrimenti non avrebbero mai potuto essere effettuati, tutelando così la reputazione della criptovaluta. Un secondo effetto positivo di tali provvedimenti fu quello che, presi come esempio o quantomeno come modello di confronto da quelle nazioni che si preoccupavano di regolamentare le criptovalute, costituirono una premessa favorevole agl'interessi espansionistici del bitcoin, senza per questo determinare un appiattimento delle legislazioni sull'esempio americano. Un ultimo beneficio fu quello che molte persone interpretarono erroneamente le azioni americane come una legittimazione del bitcoin.

Questa medesima ingerenza delle autorità nazionali sul funzionamento di Bitcoin sancì al contempo una limitazione -non da tutti ben accetta- al decentramento del sistema e all'internazionalizzazione della criptovaluta.

Proliferò inoltre, in questo periodo, il fenomeno delle hard fork della blockchain con la generazione di nuove criptovalute, come la già citata *BTC Cash*, ma anche *BTC Gold*, *BTC XT* e *BTC Classic*.

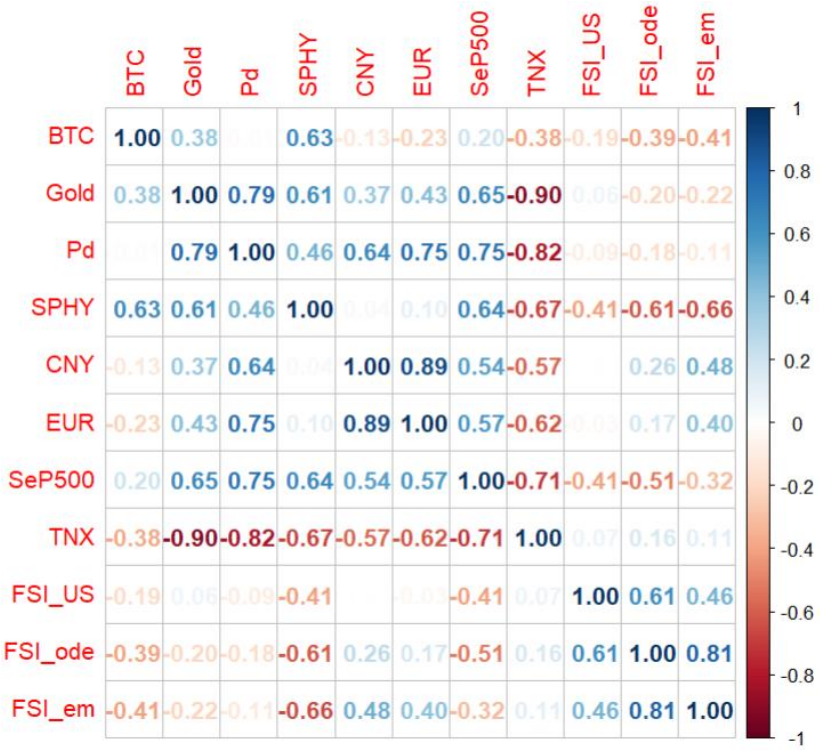

Figura 9: Correlazione tra le variabili; dati dal 18/12/2017 al 23/01/2020.

In questi due anni la maggior correlazione del bitcoin si sviluppa con l'indice SP High Yield (*corporate debt under investment grade*), che denuncia come il bitcoin, percepito come in qual modo simile a titoli di debito altamente rischiosi, fosse considerato come a sua volta rischioso.

Figura 10: Andamento congiunto ln(bitcoin) - indice SPHY. *La data è in formato:* anno-mese.

2020-2023: dall'era pandemica ad oggi

Il 24 gennaio del 2020, nella città cinese di Wuhan, venne imposta per la prima volta la quarantena preventiva alla diffusione del Covid-19; ad aprile dello stesso anno, circa metà della popolazione mondiale si trovò confinata entro le proprie case.

Tra l'inaspettata e repentina rottura delle abitudini ed il bisogno di rimpiazzare vari aspetti di esse in un contesto di isolamento, Bitcoin, riuscendo a rispondere -almeno parzialmente- a

molte di queste richieste (bisogno di trovare una nuova fonte di reddito, di una valuta di facile cambio per i crescenti commerci online, di riempire giornate vuote, di proteggere il proprio capitale dall'inflazione…), si espanse come mai si sarebbe potuto immaginare, passando da un market cap di 200miliardi di USD nel gennaio 2020 a 3trilioni nel novembre 2021. L'ecosistema delle criptovalute, inoltre, si arricchì delle neonate "stablecoin": un tipo di criptovaluta progettata per mantenere un prezzo stabile nel tempo perché ancorato al valore di uno strumento finanziario sicuro, riuscendo così ad offrire tutti i vantaggi delle criptovalute limitandone l'estrema volatilità[31].

Nel maggio del 2021 la Cina attuò misure per reprimere tutte le attività legate alle criptovalute, dal mining al trading, per evitare che i rischi cui queste attività sono soggette si ripercuotessero sull'intera società.

Vista la formidabile diffusione delle criptovalute (e in special modo del bitcoin), i problemi che esse sollevarono dal punto di vista legislativo si acuirono, portando a riposte assai diverse: dall'accelerazione del processo d'illegalizzazione delle criptovalute (Cina, con la proposta di una moneta digitale della BC), ad un'euforica accettazione del bitcoin come valuta ufficiale (El Salvador), ad approcci più prudentemente regolativi (USA ed Europa). Si segnala inoltre come, in un contesto di crescente dipendenza dalla tecnologia per la comunicazione e per l'accesso a servizi, accrescendosi il problema dei *ransomware* (attacchi hacker atti a produrre disservizi per cessare i quali vengono richiesi dei riscatti, spesso in BTC), agenzie statunitensi sottoposte a tali ricatti siano riuscite a rintracciare -mediante Bitcoin- le identità degli hacker e a riappropriarsi delle somme esborsate, mettendo in seria discussione un secondo caposaldo del Bitcoin: l'anonimia (declassata a pseudonimia).

Dopo aver raggiunto il massimo storico nel novembre 2021 (67549 $/BTC), con la fine della pandemia, negli ultimi mesi del 2022 si è assistito ad un nuovo crollo del prezzo bitcoin -aggravato dall'invasione Russa dell'Ucraina- in seguito alla quale si è entrati in un nuovo *cryptowinter*: una condizione analoga alla fase di *mercato orso*[32] vissuta da altre categorie di asset.

[31] Per la fonte consultare la voce "Stablecoins" in sitografia.

[32] "Il […] mercato orso, è contraddistinto da una progressiva diminuzione dei prezzi delle attività finanziarie e da aspettative pessimistiche". Per la fonte vedere "Mercato orso" in sitografia.

Figura 11: Correlazione tra le variabili; dati dal 24/01/2020 al 05/10/2023

Si può notare una forte correlazione positiva con l'indice S&P500, che suggerisce una volta ancora come il bitcoin possa essere stato percepito come classe di asset peculiare. Si nota anche un'insolitamente alta correlazione negativa col tasso di cambio USD/Renmimbi, che però, viste le politiche anti-cripto attuate dalla Cina e alla luce del complesso sistema di cambio impostato dalla stessa, risulta d'ardua interpretazione.

Grafici di dati dal 18/09/2014 al 05/10/2023

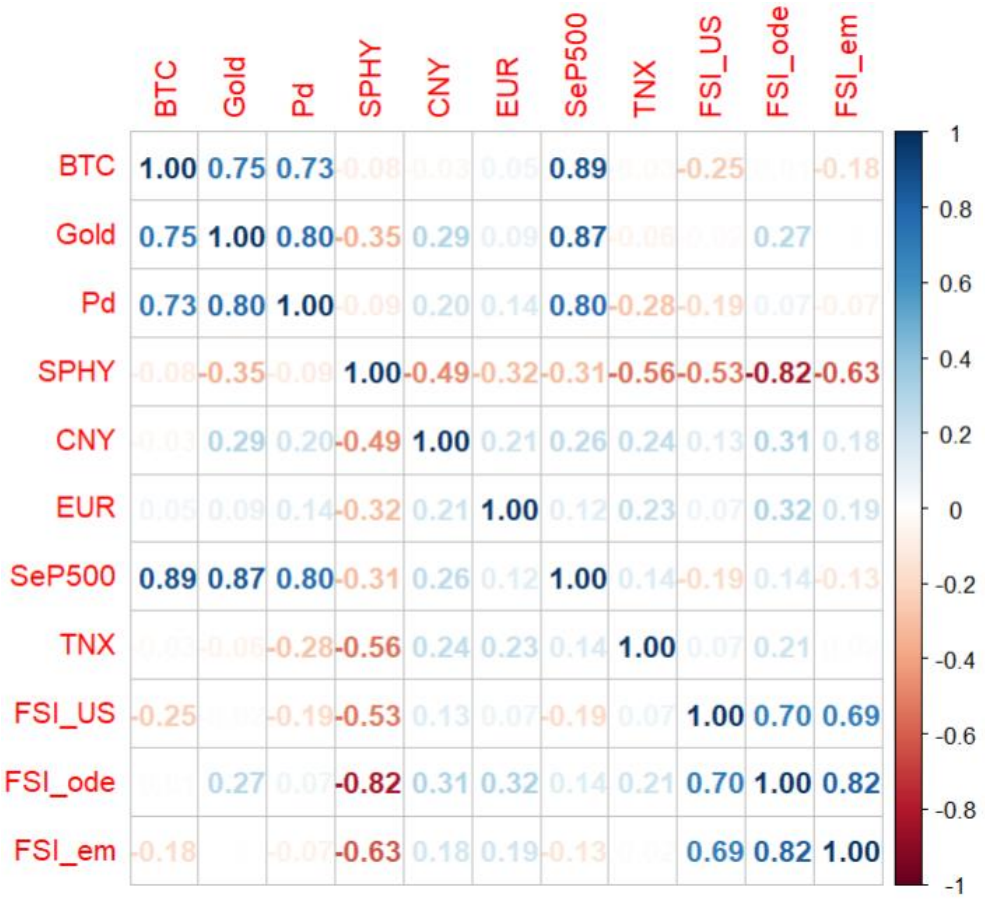

Figura 12: correlazione dei dati lungo tutto l'arco temporale.
Le correlazioni più forti sono positive e con classi di asset come Oro, Palladio e l'indice azionario S&P500.

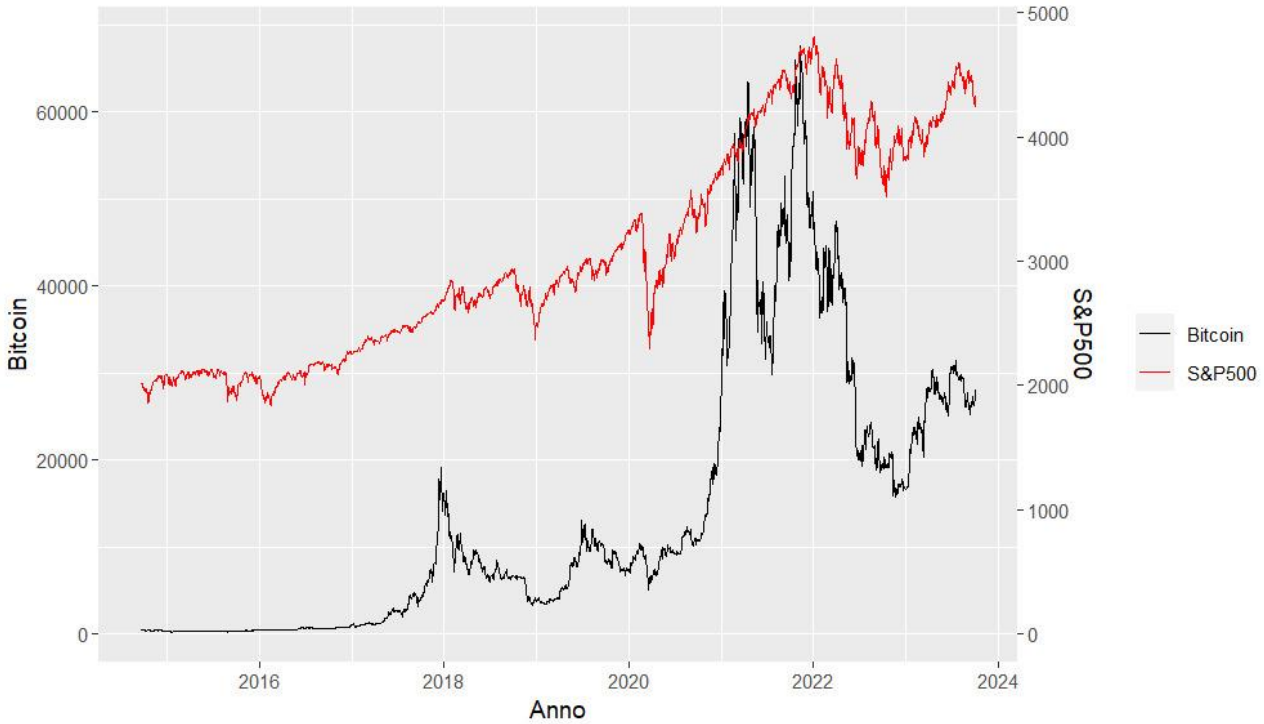

Figura 13: Andamento congiunto BTC-S&P500.

Figura 14: Andamento congiunto BTC-Oro*; la rilevata correlazione matematica, che poco emerge dalla rappresentazione grafica (inficiata forse dalle differenze di volatilità), sembra riscontrarsi nella tendenza generale accomunante le due variabili, il che suggerisce come esse possano essere mosse dalle stesse fluttuazioni di mercato ed in ultima istanza percepite come in qual modo simili.*

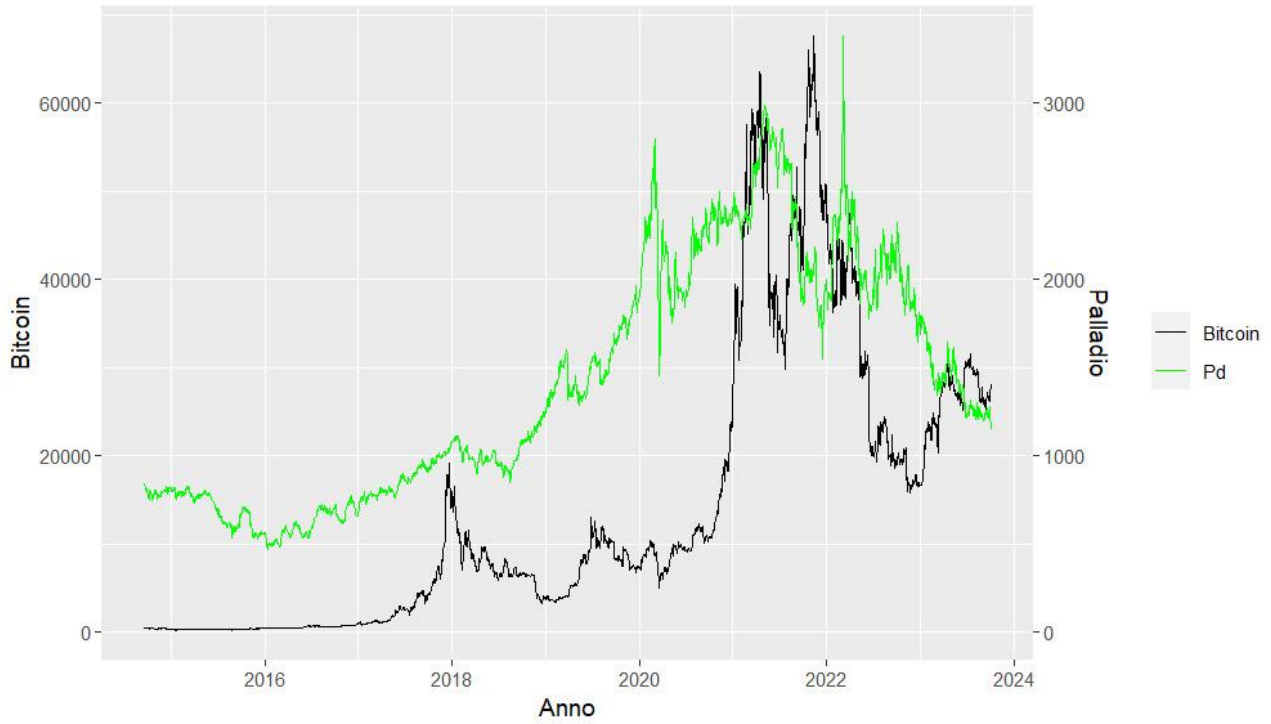

Figura 15: Andamento congiunto BTC-futures Palladio.

3 – La natura del bitcoin

Il proposito del presente elaborato non è quello di ricondurre il bitcoin ad una specifica categoria finanziaria, bensì d'illustrare gli impieghi cui questa versatile criptovaluta si presta, fungendo sia da mezzo di scambio (come una moneta) che da investimento o bene rifugio[33] (come un asset o una *commodity*). Ci si limiterà a constatare che per potersi dire a pieno titolo "moneta impiegabile in transazioni", il bitcoin esibisce una volatilità eccessivamente pronunciata, che la rende inaffidabile, ma non già inutilizzabile; mentre come asset rappresenta un investimento ad alto rischio. Eludendo le tradizionali classificazioni, il bitcoin rientra tuttavia, sotto certi aspetti, nella categoria di moneta, senza potervi però appartenere completamente, non essendo essa una moneta Fiat (una valuta istituzionale sostenuta da figure che ne garantiscono il valore e l'accettazione nell'economia). Proprio per la volontà di costituirsi quale valuta franca ed internazionale il cui valore viene determinato dal mercato, il bitcoin perde alcune tradizionali proprietà della moneta acquisendone altre degli asset, non trasformandosi propriamente per questo né nell'una né nell'altro. In estrema sintesi si può concludere che, mentre ricondurre la natura ibrida del bitcoin ad una categoria (sia essa moneta, asset o *commodity*) non può che essere uno sforzo teorico fortemente legato alle premesse poste ed il cui risultato è destinato a rimanere perlopiù nominale, a livello pratico la sua natura è definita dalle modalità entro le quali viene impiegato, che variano nel tempo anche in funzione di forze esogene (come, ad esempio, le regolamentazioni nazionali). Questa mi pare essere la principale ragione per le contrastanti tesi presenti nella letteratura e nelle legislazioni.

3.1 – Le legislazioni sul bitcoin in giro per il mondo

Come si è accennato, il bitcoin, durante la propria storia, si è più volte interfacciato con le realtà politiche dei paesi nei quali veniva impiegato, dando vita ad incontri e scontri che ne hanno alterato forma e natura. Come è già stato detto, infatti, il bitcoin ha dovuto recedere, nella pratica, da molte delle sue posizioni più estreme e caratteristiche: dall'anonimia -mito sfatato a più riprese dalle agenzie americane e vanificato per i miners con l'obbligo d'iscrizione vigente in molti paesi- all'implicito riconoscimento di regolamentazioni (istituti propri d'istituzioni centralizzate) estranee a quell'unica legge d'amministrazione della blockchain citata nel manifesto. Di seguito è proposta una selezionata fenomenologia degli approcci che varie istituzioni hanno adottato verso il bitcoin.

La principale fonte è Reuters (2022)[34].

[33] Durante la svalutazione di rublo e grivna, il ricorso al bitcoin è aumentato significativamente in questi due paesi con lo scopo di fungere da riserva di valore. Cfr. Theiri, Nekhili & Sultan (2023).

[34] Vedere "Thomas Reuters" in sitografia.

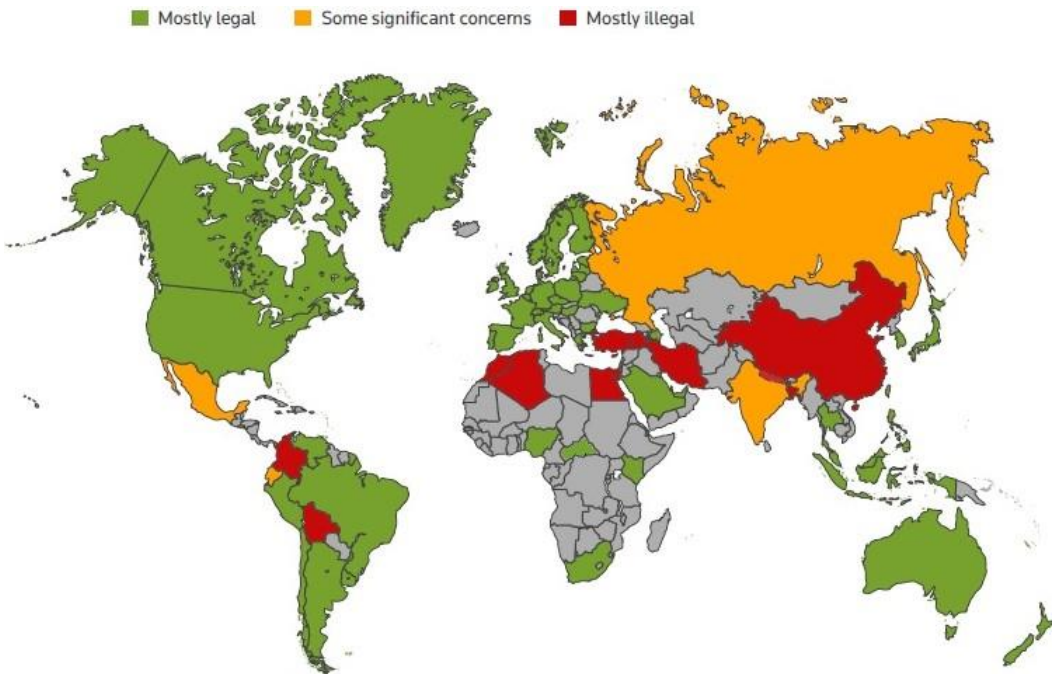

Figura 16: Mappa dei regolamenti nazionali verso Bitcoin.

Modificata partendo da: Thomson Reuters (2022). Vedere in sitografia.

Stati Uniti d'America:

Il paese che più di qualunque altro si occupa di criptovalute tra investitori, *miners*, piattaforme di trading ed *exchangers*, latita di un'univoca definizione del bitcoin, differente a seconda dell'agenzia: la Security and Exchange Commission la cataloga come *security*, la Commodity Futures Trading Commission come *commodity* ed il Tesoro come *valuta*. Ad uniformare la definizione per uno scopo tributario è infine intervenuto l'Internal Revenue Service, definendo le criptovalute come *rappresenti virtuali di valore funzionanti come mezzo di scambio, unità di misura e/o riserva di valore* […] *senza corso legale presso alcuna giurisdizione*[35].

El Salvador:

Fucina a cielo aperto per il bitcoin, El Salvador è stata la prima nazione ad aver assurto il bitcoin a valuta nazionale[36] accanto all'USD, col *Decreto n. 57* del 07/09/2021[37]. Per agevolarne l'utilizzo, El Salvador ha inoltre creato *Chivo Wallet*: un portafoglio digitale che permette sia di convertire biunivocamente USD-BTC senza imposizione che di spendere e ricevere bitcoin. Così facendo il bitcoin è divenuta valuta con la quale poter estinguere debiti ed irrefutabile se proposta come metodo di pagamento; attività cruciali all'interno dell'economia del un paese e della vita dei suoi abitanti sono stati insomma affidati ad una moneta il valore della quale è definito da un mercato decentralizzato ad alta volatilità.

[35] Per la fonte vedere: "IRS 2014-21" in sitografia.
[36] Seguita, nell'aprile del 2022, dalla Repubblica Centrafricana, sulla quale però non sono ancora stati effettuati studi approfonditi.
[37] Per la fonte vedere: "Decreto 57" in sitografia.

La spregiudicata mossa del presidente Bukele ha suscitato un diffuso malcontento e perplessità, tanto interne al paese quanto esterne, col Fondo Monetario Internazionale che ha fortemente invitato ad un'inversione di strategia per la stabilità nazionale, e con agenzie di rating che hanno degradato i *debt ratings* salvadoregni. Ad oggi l'entusiasmo verso il bitcoin del presidente sembra essersi mitigato, col fallimento del progetto dei *Volcano Bonds* (o *Volcano tokens*[38]): bond denominati in USD per un totale di 1miliardo di USD finalizzati al pagamento del debito pubblico e a sostenere la costruzione di Bitcoin City: una città dove minare cripto grazie all'energia geotermica del vulcano.

Europa:

Sebbene ciascuno stato abbia una propria regolamentazione particolare sulle criptovalute, in linea di massima si può dire che l'Europa in toto abbia completamente legalizzato il bitcoin. Con la direttiva Ue 2018/843, il Parlamento Europeo ha riconosciuto le cripto, adoperandosi però per contrastare la pseudonimia degli utenti -e con essa fenomeni come riciclaggio ed acquisti illeciti- mediante procedure alle quali sono tenuti i fornitori di servizi digitali.

Russia:

Con una legge entrata in vigore nel 2021, le criptovalute -per la prima volta oggetto di un'esaustiva regolamentazione in territorio russo- sono state riconosciute come investimento e mezzo di scambio, ma è stato contemporaneamente vietato il loro impiego come metodo di pagamento per beni o servizi, forse per far adoperare la cripto come asset o commodity e non come una valuta mentre la valutazione del rublo fluttuava per via delle sanzioni occidentali[39]. Nonostante queste limitazioni, la Russia rimane una protagonista del mondo delle criptovalute private (ma anche pubbliche, con lo sviluppo di una Central Bank Digital Currency).

Cina:

Dopo aver vietato alle istituzioni finanziarie di trattare criptovalute nel 2013, anche le attività di mining e trading -che qui, agli esordi del bitcoin, si concentravano in altissima percentuale grazie al basso costo dell'energia elettrica- sono state fortemente ridimensionate a partire dal maggio 2021, fino al raggiungimento delle attuali trascurabili dimensioni. La Cina è anche il paese che più ha investito nello sviluppo di una CBDC.

Giappone:

Con una delle regolamentazioni più avanzate, già dal 2010, col Payment Services Act, il Giappone definì le criptovalute come proprietà (crypto-asset) utilizzabile per pagamenti non denominati in valuta Fiat verso persone non meglio specificate, imponendo ai cambiavalute di

[38] I token sono generalmente ancorati al valore di qualche cripto: in questo caso il debito avrebbe dovuto essere pagato mediante l'attività di mining bitcoin. Per la fonte vedere "Volcano bond" in sitografia.
[39] Per la fonte vedere: "Russia e cripto" in sitografia.

sottostare alle comuni regole antiriciclaggio.

Nell'aprile 2020 il Giappone creò organizzazioni di autoregolamentazione utili al rispetto delle norme e all'implementazioni delle stesse.

India:

Nel 2018 il cripto-trading venne proibito dalla Banca Centrale indiana, preoccupata per l'integrità dei mercati e per la sicurezza dei consumatori, salvo essere nuovamente permesso nel 2020 dalla Corte Suprema.

L'atteggiamento dell'India verso le criptovalute è stato sovente ambiguo e soggetto a radicali inversioni, che probabilmente sono destinate a riproporsi in futuro; cionondimeno l'India si è distinta per le proprie applicazioni innovative in campo blockchain, impiegata anche nella rupia digitale: una CBDC lanciata a fine 2022.

3.2 – Brevissimo excursus sulle *Central Bank Digital Currencies*

I metodi di pagamento elettronico e digitale, oramai divenuti consueti, non hanno alterato natura o struttura del sistema monetario; una tale rivoluzione, invece, è stata rappresentata dalle criptovalute, che però non sono ancora riuscite a raggiungere un impiego tale da consentirgli d'ergersi a concreta alternativa al sistema tradizionale.

Tutt'altro che insensibile verso l'epocale proposta addotta dalle criptovalute private, il settore bancario partecipa a sua volta al processo d'innovazione dei metodi di pagamento con una proposta atta a sopperire alle mancanze delle criptovalute, la cui volatilità è specchio di vulnerabilità strutturali (Pagnotta, 2021). Le banche centrali di molti paesi si stanno adoperando per lo sviluppo ed emissione di *Central Bank Digital Currencies* (CBDC): criptovalute denominate in valuta domestica (e quindi analoghe digitali della moneta Fiat) erogate e sostenute dalle rispettive BC; come tali, le CBDC, nel loro intento, rappresentano non solamente una nuova modalità di conservazione del denaro e di pagamento, ma un'innovazione col potenziale di rivoluzionare la realtà socioeconomica. Nel mondo delle transazioni *cashless*, le CBDC costituirebbero un'alternativa inedita poiché, oltre a consentire pagamenti elettronici senza l'ausilio d'intermediari finanziari -sostituti dalla BC-, faciliterebbero di molto i pagamenti transfrontalieri azzerando al contempo il rischio di credito, giacché per definizione le Banche Centrali non possono fallire.

Non è possibile in questa sede condurre una disamina esauriente del fenomeno CBDC -peraltro divergente da BC a BC in temi essenziali dal punto di vista tecnico ed etico- quindi di seguito ci si limiterà a riportare solamente i due aspetti fondamentali di queste particolari cripto: le loro tipologie e le modalità di distribuzione.

Esistono due forme di CBDC, che rispecchiano i tipi di conti presso le CB: una d'ampia

diffusione adibita agli acquisti di piccolo taglio (*retail*) ed una per le transazioni prioritarie (*wholesale*, e.g. per trasferimenti interbancari).

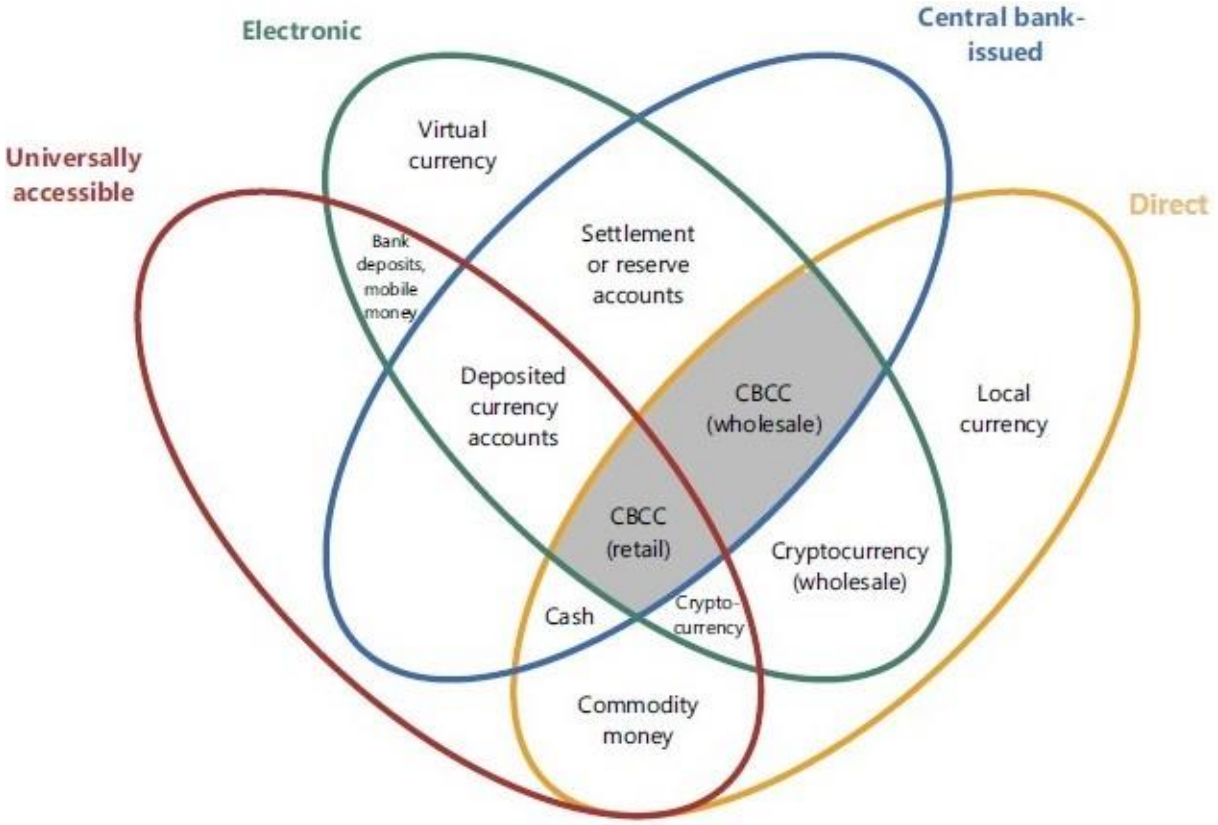

Figura 17: tassonomia delle valute.
Modificato partendo da: Bech & Garratt (2017)

Per le CBDC *retail* esistono due architetture possibili (Auer & Boehme, 2020): una ad un livello, nella quale è la BC ad incaricarsi della distribuzione della CBCD, ed una a due livelli, nella quale la distribuzione viene commissionata ad intermediari; questa seconda soluzione, secondo i sondaggi di Kosse & Mattei (2022), è preferita da oltre il 70% delle BC, poiché consente di ottimizzare processi di KYC (*know your customer*) ed antiriciclaggio.

Numero di parole totale = 9368

Riferimenti bibliografici:

Antonopoulos, A. (2010), *Mastering Bitcoin*, O'Reilly Media, Newton, MA.

Atik, J., & Gerro, G. (2018). *Hard forks on the Bitcoin blockchain: reversible exit, continuing voice*. SSRN.

Auer, R., & Böhme, R. (2020). *The technology of retail central bank digital currency*. BIS Quarterly Review, March.

Baur, Dirk G., Kihoon Hong, and Adrian D. Lee (2018) *Bitcoin: Medium of exchange or speculative assets?,* Journal of International Financial Markets, Institutions and Money 54: 177-189.

Bech, M. L., & Garratt, R. (2017). *Central bank cryptocurrencies*. BIS Quarterly Review September.

Bilotta, N., & Botti, F. (2021). *The (near) future of central bank digital currencies: risks and opportunities for the global economy and society*. Peter Lang International Academic Publishers.

Chohan, U. W. (2022). *A history of bitcoin*. Available at SSRN 3047875.

Easley D, O'Hara M, Basu S. (2019), *From Mining to Markets: The Evolution of Bitcoin Transaction Fees*, Journal of Financial Economics.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019), *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?*, The Review of Financial Studies, 32(5), 1798-1853.

Halaburda, H., Sarvary, M., & Haeringer, G. (2021). *Beyond Bitcoin: The Economics of Digital Currencies and Blockchain Technologies*, 2nd ed, Palgrave MacMillan.

Imamura M., Kazumasa O. (2021), *Empirical Study of Software Adoption Process in the Bitcoin Network*, Advanced Information Networking and Applications: Proceedings of the

35th International Conference on Advanced Information Networking and Applications (AINA-2021), Volume 1 35. Springer International Publishing.

John K., O'Hara M., Saleh F. (2022), *Bitcoin and beyond*. Annual Review of Financial Economics 14.

Kosse, A., & Mattei, I. (2022). *Gaining momentum–Results of the 2021 BIS survey on central bank digital currencies*. BIS papers.

Lewis A. (2018), *The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them*, Mango Media Inc.

M. Di Pierro (2017), *What Is the Blockchain?*, Computing in Science & Engineering, vol. 19, no. 5, pp. 92-95, 2017.

Makarov I., Schoar A. (2021), *Blockchain analysis of the bitcoin market*. No. w29396. National Bureau of Economic Research.

Mensi, W., Sensoy, A., Aslan, A., & Kang, S. H. (2019). *High-frequency asymmetric volatility connectedness between Bitcoin and major precious metals markets*. The North American Journal of Economics and Finance, 50, 101031.

Nakamoto S., (2008), *Bitcoin: A peer-to-peer electronic cash system*, Working Paper.

Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. (2016), *A Comprehensive introduction. Bitcoin and Cryptocurrency technologies*., Princeton University Press.

Nguyen, T., & Watson, B. (2023), *Consumer Payment Behaviour in Australia,* RBA Bulletin, June.

Pagnotta E. 2021. *Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security*. Review of Financial Studies.

Ron D., and A. Shamir, (2013), *Quantitative analysis of the full bitcoin transaction graph*, In 17th Financial Cryptography and Data Security International Conference.

Summers A. (2022), *Understanding Blockchain and Cryptocurrencies*, CRC Press.

Theiri, S., Nekhili, R., & Sultan, J. (2023). *Cryptocurrency liquidity during the Russia–Ukraine war: the case of Bitcoin and Ethereum*. The Journal of Risk Finance, 24(1), 59-71.

Turner A. & Irwin A., (2018), *Bitcoin transactions: a digital discovery of illicit activity on the blockchain*, Journal of Financial Crime 25.1: 109-130.

Sitografia[40]:

Composizione market cap criptovalute (u.c. 14/10/2023): https://coinmarketcap.com/charts/

Cryptowinter (u.c. 17/10/2023): https://www.forbes.com/advisor/it/investire/criptovalute/crypto-winter/

Decreto 57: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf

IRS 2014-21: https://www.irs.gov/pub/irs-drop/n-14-21.pdf

Marche temporali (u.c. 27/09/2023): https://www.pec.it/marche-temporali.aspx

Mercato orso (u.c. 17/10/2023): https://www.borsaitaliana.it/borsa/glossario/bear-market.html

Russia e cripto (u.c. 18/10/2023): https://www.cnbctv18.com/cryptocurrency/crypto-putin-bans-digital-payments-a-quick-recap-of-russia-love-hate-relationship-with-it-14170302.htm

Stablecoin (u.c. 17/10/2023): https://www.forbes.com/advisor/it/investire/criptovalute/stablecoin-cosa-sono-e-come-funzionano/

Thomas Reuters (2022): https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf

Volcano Bond (u.c. 19/10/2023): https://www.ilsole24ore.com/art/el-salvador-non-rinuncia-bitcoin-anzi-rilancia-tutte-cripto-AEniICKC

[40] *u.c.* = ultima consultazione