UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Filosofia, Sociologia, Pedagogia e Psicologia applicata

Corso di laurea in
SCIENZE SOCIOLOGICHE

L'oro digitale come valuta di scambio

Relatore:
Prof. Mario Pomini

Laureando:
Morgan Picariello

Indice

Abstract

La mia tesi di laurea tratta della principale valuta digitale e del suo ruolo nella società.
Bitcoin è fin dalla sua invenzione un forte strumento economico e un promotore di sviluppo umano.
Ho a questo proposito analizzato la storiografia della moneta, dai suoi albori fino al tempo presente, soffermandomi in particolare sul protocollo Bitcoin, introducendo la sua tecnologia strutturale e arrivando a mettere a fuoco i vantaggi che questa innovazione può e potrà avere nella nostra società.
L'elaborato è strutturato in 3 capitoli, divisi secondo un filo cronologico: il primo analizza gli albori del protocollo Bitcoin e il passato delle differenti monete umane; il capitolo intermedio tratta i primi approcci concreti che questa moneta digitale sta subendo dalla società e come si sta interfacciando con le economie e i governi nazionali; infine il terzo proietta nel futuro tale adozione, considerando alcune possibilità in base agli attuali atteggiamenti delle istituzioni.
Il titolo della tesi si riferisce all'Oro digitale intendendo Bitcoin, facendo sottintendere come l'epilogo al quale si auspica nel mio scritto sia quello di utilizzare questa valuta come sottostante del sistema economico, la riserva di valore di tutto il denaro circolante.
Ricorrendo ad una forma di micro-transazioni derivata dalle monete digitali, ma che mantenga il meccanismo di consenso e l'ideologia del protocollo Bitcoin; riprendendo quello che, appunto, era il ruolo fondamentale dell'oro nei secoli scorsi.
Se questa intenzione venisse valutata e optata dai grandi enti bancari internazionali, il tempo necessario per Bitcoin di coprire l'intera emissione di moneta mondiale sarebbe relativamente breve ma, al contrario, essendo in disaccordo sul suo utilizzo vi sono rallentamenti e incertezze da parte della maggioranza della popolazione.
Dunque, nel corso dell'elaborazione della mia tesi, prenderò in considerazione la possibilità che vi sia un approccio propositivo e aperto all'adozione di questo "oro digitale" come riserva di valore di riferimento, e si riassetti il paradigma economico sotto una differente prospettiva.
Allo stesso tempo tratterò la possibilità che questo sistema non venga adottato, e che i vari Stati rimangano scettici riguardo il suo utilizzo e incerti sul suo futuro.

- CAPITOLO PRIMO -
LA TECNOLOGIA

1. Le origini

La crisi del 2008, il più impetuoso crash (tracollo) economico dell'ultimo secolo, ha suscitato nella popolazione avvezza alla propria gestione finanziaria un profondo senso di distacco dal mercato in tutte le sue forme speculative: primo fra tutti quello immobiliare, successivamente azionario e bancario, poi il ramo delle materie prime etc; consolidando, al contrario, in coloro i quali il mercato lo stavano già bellamente ignorando, un rinnovato sentore di sfiducia e di discreta manipolazione da parte di un qualche "potere forte" e conseguentemente una volontà di rimanerne ancor meno permeabili possibile.
In ambedue i casi il mercato perse di credibilità e si ricercarono forme di investimento alternative e più solide, o che quantomeno più solide apparissero.
Gli individui, accomunati dall'aver perso un valore monetario di qualche genere, sfogarono dunque questa evidente scontentezza tramite diversi metodi: chi smise di investire, chi cambiò settore o strumento finanziario, chi perse tutto, chi protestò tramite differenti canali.
Da quest'ultimo punto nasce il tema proprio di questa tesi.
La protesta che seguì la crisi del 2008 ebbe diversi vettori, primo fra tutti quello che più negli ultimi anni si era affermato nei grandi paesi civilizzati di tutto il mondo: Internet.
Questo artificio, che per la maggioranza rimaneva ancora avvolto da mistero, ha veicolato in questo senso una delle più grandi risposte della società al sistema economico: un cambio di paradigma.
Un forum a tema crittografia chiamato metzdowd.com ospitava molti interessati alla sicurezza e riservatezza online.
In questo forum, che divenne nel tempo una mailing-list e che ora non è nemmeno più raggiungibile/ esistente, un programmatore informatico tra i fruitori abituali pubblicò il 31 Ottobre 2008 un articolo riguardante una nuova forma di pagamento, inizialmente non meglio definita di: "A Peer-to-Peer Electronic Cash System".
Satoshi Nakamoto, pseudonimo simil-orientale utilizzato da questo account (non desueto l'utilizzo di un alias nell'ambito di internet, specialmente in contesti in cui la crittografia e la riservatezza sono i temi di maggiore interesse), in pratica programmò e in seguito pubblicò in Internet un circuito di pagamento con la relativa valuta di riferimento, utilizzando dei sofisticati metodi che illustrerò al mio meglio nei paragrafi successivi; come prova di sicurezza del network non vi erano e non vi sono tuttora imposizioni sovrane o centralizzate, bensì algoritmi spersonalizzati e la pura psicologia umana.
Nakamoto in realtà ideò già da tempo questo progetto, si evince dal fatto che il dominio web "www.bitcoin.org" fosse già stato tacitamente registrato mesi precedenti la data del rilascio di tale articolo, già dal 18 agosto 2008 infatti tale sito iniziò ad esistere.[1]
È un ottimo punto di partenza per tutti coloro i quali non abbiano dimestichezza con la tecnologia o ne siano semplicemente curiosi al riguardo.
Questo sito è poi passato in gestione di diverse associazioni e tutt'ora nel 2023 viene amministrato da alcune di loro.
Nei primi periodi, per come era stato concepito, questo sito non era nulla più che meramente descrittivo riguardo al funzionamento del protocollo Bitcoin, in più dava un'identità a questo progetto anche all'esterno del forum all'interno del quale è stato presentato.

Via via negli anni, di gestione in gestione, è stato implementato e ora offre diverse possibilità: di comprare bitcoin in proprio, un manuale specifico illustrato alla tecnologia sottostante e numerose altre comodità che vanno a completare il pacchetto "Guida introduttiva", un manuale su come gestire un intero nodo nel network bitcoin (che approfondirò in seguito) e addirittura su come un individuo, o incredibilmente anche un'azienda, possa adottare bitcoin come circuito di pagamento al posto dei più diffusi Visa e Mastercard.
Un vero e proprio reperto che è rimasto la branca più visualizzata di questo sito è il White Paper di Bitcoin[2] , il documento originale (tradotto in oltre 40 lingue) redatto da Nakamoto stesso e che rappresenta sinteticamente tutto quello che questo progetto si prospetta di fare.
Satoshi fu il primo che, con successo, immise nel mercato questa tecnologia, ma non inventò nulla che già non fosse stato concettualizzato (e con poca fortuna tentato) nei decenni precedenti e da altri prima di lui.
Vi sono a tal proposito tracce di numerosi tentativi già dagli anni 90' del secolo scorso, il più celebre tra di essi è quello proposto dal crittografo e informatico David Chaum.

2.**Il precursore inconsapevole**

Il Dottor Chaum presentò nel 1994, alla prima conferenza del CERN di Ginevra, il progetto "eCash" e lo enunciò come rivoluzionario e utopistico.
Descrisse il sistema con queste esatte parole: "You can pay for access to a database, buy software or a newsletter by email, play a computer game over the net, receive $5 owed you by a friend, or just order a pizza. The possibilities are truly unlimited."
Prima che la maggior parte degli individui sentissero anche solo parlare di web e connessione internet, le grandi menti del settore studiavano già da tempo in questo campo.
Chaum stesso, che era professore all'Università di Berkley, non solo fu un grande appassionato e sostenitore della privacy sul web, ma ne fu un fautore attivo, si incaricò cioè di strutturare un sistema di strumenti per rendere la privacy possibile in ambito finanziario.
La privacy è un tema molto ridondante al giorno d'oggi e non vi è modo, almeno per l'individuo/ utente comune, di sapere se sia protetto o meno in termini di identità o di informazioni sensibili sul web; nonostante questo esiste quantomeno l'informazione necessaria a comprendere che vi possano essere minacce di questo genere nel caso in cui non si ponga la dovuta accortezza su internet.
Nel 1981, quando Chaum sviluppó le sue prime applicazioni teoriche al riguardo e stabilì i primi utilizzi concreti, Internet era ancora del tutto sconosciuto alla massa, per questa ragione è ancor più degna di nota la sua apprensione verso questo tema.
In quell'anno l'informatico californiano teorizzò un sistema di posta elettronica non rintracciabile in entrata (mittente) e in uscita (ricevente), e non soddisfatto annesse anche uno strato di protezione maggiore ricorrendo a pseudonimi individuali.
Questo genere di crittografia darà vita a browser di ricerca fortemente anonimi come Tor Protocol.
La priorità del professore non era però quella di creare un sistema anonimo di comunicazione, bensì di pagamenti.
Nacque così la tecnologia battezzata da lui "Blind signature", il cuore pulsante del progetto eCash.
Tratterò la "firma cieca" perché concettualmente è lo stesso tipo di misura di sicurezza adottato per il protocollo Bitcoin; le differenze stanno nella tecnologia utilizzata e

intrinsecamente nei tre decenni di distacco ed evoluzione del settore finanziario trascorsi dal 1980 al 2008.
L'assoluta innovazione presentata da Chaum fu quella di rendere le transazioni anonime ma registrate e consultabili.
Prima di addentrarmi più nello specifico nella delucidazione di eCash, è bene che io introduca brevemente il concetto di chiavi private e pubbliche nel contesto di una firma crittografata.

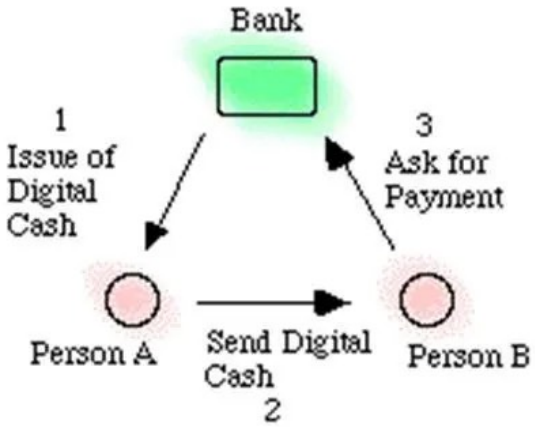
3. **Chiavi private e pubbliche**

Una chiave privata è una sequenza di lettere o cifre di lunghezza variabile e univoca; è possibile fare una sorte di similitudine presupponendo che la chiave privata di un individuo sia il suo DNA, letteralmente unico e univoco.
Dalla sequenza di chiavi private vengono algoritmicamente generate delle chiavi pubbliche, cioè semplicemente una sequenze di lettere o cifre univoche a sua volta derivanti da essa; mantenendo il nostro parallelismo metaforico la chiave pubblica è l'insieme dei tratti somatici e caratteriali derivanti dal codice genetico individuale.
Il fine di questa tecnologia è la sua stessa sicurezza, di come sia possibile da una chiave privata generarne una pubblica ma non sia possibile fare il contrario.
Il sistema è dunque stato utilizzato ai suoi albori per stabilire una comunicazione privata tra due individui, ma anche una serie più vasta di relazioni tra loro.
Ben presto prese piede attorno a questa tecnologia la funzione di sottoscrizione individuale; questa procedura tecnologicamente e statisticamente è meno fallace di una cartacea firma analogica eseguita dal suo relativo possessore in presenza di un testimone attendibile.
Il reale ostacolo è ed è sempre rimasto, la difficolta nell'applicarlo alla società comune, la quale non è così avvezza alla tecnologia da preferire una tastiera ad una penna.

4. **DigiCash e la firma cieca**

Tornando alla tecnologia di firma crittografata, era stata applicata ad alcune tipologie di dati, i quali potevano essere appunto visionati e sottoscritti dall'individuo designato; questo combinava così la sua chiave privata al dato da firmare, generando una nuova sequenza alfanumerica che in gergo specifico prende il nome, per l'appunto, di "Signature" (Firma).
Ancora una volta, è impossibile essere ricondotti alle chiavi private tramite la firma digitale, poiché la crittazione segue una direzione unilaterale.
La specificità è però la solida trasparenza di questo sistema: chi sottoscrive un certo dato lo fa in forma privata, chi però ha necessità della sicurezza che sia stato proprio quell'individuo ad apporre la sua firma digitale, l'avrà.
Questo perché la firma è direttamente riconducibile alla chiave privata univoca generata da quella nascosta chiave privata attribuita a quella specifica persona.
Questo fa sì che vi sia la totale garanzia del fatto che quella firma sia stata apposta da quell'individuo, senza però in nessun caso poterla riprodurre o falsificare.
Una "firma cieca" si basa su questi a priori ma si spinge oltre, alla parte che dovrà sottoscrivere il dato, non arriverà tale file in maniera evidente, bensì gli verrà trasmesso già crittografato da colui che gliel'ha inviato; questo fa sì che il firmatario non sia a conoscenza della reale entità di ciò che sta sottoscrivendo e questa è la ragione del termine "firma cieca".

Questo rende possibile non solo il poter ricondurre tale firma all'individuo senza conoscerne le specifiche e poterle riprodurre maliziosamente, bensì rende anche impossibile prendere conoscenza del contenuto all'interno del file.
In altre parole, grazie a questa tecnologia introdotta dal Dott. Chaum, è possibile confrontare la sicurezza e l'identità del firmatario senza poter replicare la sua stessa firma in nessuna occasione, ed è inoltre possibile crittografare l'oggetto della loro trasmissione, così da essere consapevoli di quello che si sta effettivamente scambiando ma senza poterlo riprodurre informaticamente.
Il sistema è stato concepito in ambito finanziario ed assume il suo pieno senso di esistere proprio nella sua applicazione in questo settore.
Lo esplicherò in maniera più chiara mediante un esempio: figuriamoci i soggetti Alpha, Beta e Gamma; rispettivamente Alpha e Beta siano due individui singoli e che intraprendono una transazione pecuniaria, mentre Gamma sia l'istituto bancario di credito che faccia da mediatore tra loro.
Iniziamo dal soggetto Alpha, il quale richiede un trasferimento di denaro ad opera della banca Gamma; per eseguirlo Alpha deposita in banca una somma di banconote cartacee, la quale banca poi svolge la conversione in forma di una sequenza criptata, la firma ciecamente e la ritorna ad Alpha con la garanzia di essere autenticamente corrispondente ad una somma reale nei propri depositi.
Ora che le banconote digitali sono state firmate, Alpha può trasferirle a Beta, semplicemente inviandogliele tramite le chiavi pubbliche, che ho in precedenza precisato essere quelle destinate ai terzi.
Nel momento in cui Beta riceve tali banconote in forma digitale, le inoltra alla banca Gamma (che in questo esempio si presume essere banca di riferimento per entrambi) che attesta la loro validità, in quanto anch'essa possiede l'univoca sequenza digitale di ognuna di quelle banconote e di entrambi gli attori della transazione: questo significa che non possono essere già state incassate da qualcun altro prima di Beta, ma anche che non possono già essere state incassate in generale.
La banca Gamma, essendosi assicurata della corrispondenza nei propri depositi, converte nuovamente tali banconote in denaro contante e lo consegna a Beta in modo sicuro.
La svolta fondamentale è che Gamma non ha modo di sapere che Alpha e Beta siano parte attiva della stessa transazione.
Il rapporto tra i due è *blind signed* dalla banca come garanzia ma non vi è stata intermediazione diretta: Gamma emette delle banconote digitali da essa create ad Alpha con l'obiettivo di garantire l'autenticità di quelle incassate, riceve poi in un momento successivo delle banconote digitali e firmate da Beta, che scopre essere già in precedenza nei propri e corrispondenti a delle banconote esistenti, anche se non potrà ricondurle al cliente Alpha.



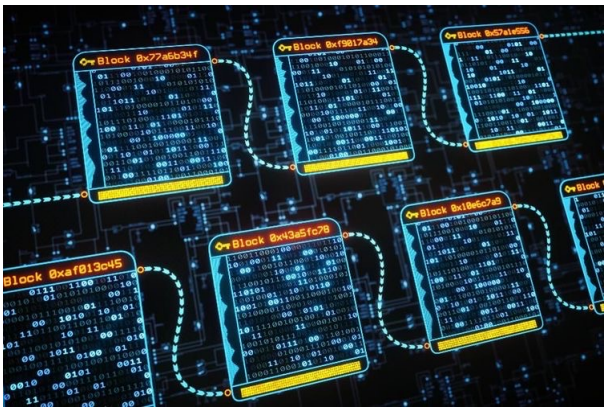
Questo era ciò che intendeva David Chaum con anonimato del sistema bancario.
L'anonimato, ovviamente, non era una novità negli scambi interpersonali in contanti di fine anni 80; divenne una grande introduzione nel momento in cui la privacy divenne saliente nel circuito dei pagamenti in versione digitale o, per riprendere il nome del progetto, in forma elettronica del contante, eCash. [3]
Chaum fondò nel 1990 Digicash, basata nei Paesi Bassi e con lo scopo di rendere più autorevole il proprio ideale finanziario mediante il loro modello di cash elettronico, oltre che per farsi portavoce di un altro paio di progetti secondari.
Il sistema venne chiamato eCash e la moneta specifica CyberBucks.

Dal momento in cui in quegli anni, quelle che sarebbero divenute poi le grandi aziende del settore (Yahoo! o Netscape) si iniziavano ad avventurare nel settore informatico e digitale, il modello di business comprendeva micro pagamenti, non ancora i banner pubblicitari.
DigiCash era considerata una promettente stella nascente nel panorama internazionale.
Le maggiori testate giornalistiche ne trattarono[4], le prime transazioni pilota vennero eseguite con successo e le prospettive per DigiCash erano di forte crescita.
Il modello era quello che le banche dovessero ottenere una licenza per utilizzare il sistema eCash, nel 1995 la prima fu la Mark Twain Bank, nel 1996 vi si avvicinarono alcune tra le altre più grandi banche al mondo, come Deutsche Bank, Credit Suisse e ING; ma non solo: Visa stessa offrì 40 milioni per il suo acquisto; Microsoft in ultima, la quale era interessata ad integrare DigiCash nel suo sistema operativo, fece un offerta di più del doppio, 100 milioni di dollari.
L'offerta non ebbe buon esito poiché David Chaum rilanciò a Microsoft 2 dollari per ogni versione di Windows 95' in commercio, famoso software di Microsoft; quest'ultima comprensibilmente rifiutò.
Nel 1996 alcuni impiegati iniziarono a lamentare una carente innovatività ai vertici dell'azienda, che passò nelle esperte mani di Michael Nash, un ex dirigente di Visa.
La sede venne trasferita nella Silicon Valley, Chaum ricopriva ancora il ruolo di CTO, il responsabile delle innovazioni tecnologiche.
La seconda ondata di risposte da parte delle banche fu debole, dalla clientela privata quasi nulla, nel 1998 la Mark Twain Bank aveva chiuso transazioni tra poco più che 5 mila utenti e in totale circa 300 esercenti.
Nel 1999 DigiCash dichiarò bancarotta, asserendo al fatto che la clientela non fosse

ancora pronta a concepire la gravità del ruolo della privacy che sarebbe avvenuta nei successivi anni.
DigiCash fallì e con esso l'utopia di un sistema che si basasse sull'anonimato scambio di denaro, ma questo cambio di progetto inspirò altri nel settore, tra i quali, forse, Satoshi Nakamoto stesso.

5. **Bitcoin e blockchain**

Alla luce del fatto che bitcoin ora sia un dato di fatto e io lo stia trattando come tale, la fondamentale differenza tra i due protocolli è abissale nel suo applicativo concreto.
Se eCash era un'ottimizzazione del sistema bancario della sua epoca, con una spiccata attenzione alla privacy dei suoi fruitori, era stata in ogni caso idealizzata come una protesi delle istituzioni bancarie; lo scopo dei suoi sviluppatori era lucrativo e il progetto centralizzato e acquistabile, ergo manipolabile sia perché venne tecnologicamente concepito in questo senso e sia nel fallace intento umano alla base, il quale spesso appone il proprio interesse a breve termine a quello del resto della società nel lungo.
Il protocollo Bitcoin, 10 anni dopo, è nato al contrario per aggirare il sistema interbancario invece che sfruttarlo, e anzi, crearne uno parallelo che non sia in alcun modo censurabile o manipolabile, seppur facendo fronte ad un metodo di crittazione delle transazioni del tutto equiparabile a quanto sviluppato da Chaum: stesso principio di chiavi private dalle quali derivano le pubbliche.
Ma in concreto il protocollo Bitcoin come funziona?
Premettendo che mi riferirò al protocollo che sorregge il sistema con la lettera maiuscola "Bitcoin", mentre con "bitcoin" mi rivolgo alla moneta di riferimento.
Il protocollo è una struttura poliedrica che attinge da diverse tecnologie e fa leva su alcuni meccanismi sociali e individuali importanti, ambedue a mio avviso degni di approfondimenti.



Il primo concetto strutturale di Bitcoin è la sua blockchain; questo termine è stato coniato e la tecnologia alla sua base sperimentata diversi anni precedenti e in ambiti anche totalmente differenti da quello finanziario.
La blockchain altro non è che un preciso e infallibile registro digitale, tramite il quale viene annotata, in questo caso specifico ogni transazione eseguita fino dalla creazione del primo blocco su tale sequenza.
Si presenta convenzionalmente come una catena di blocchi, traduzione letterale del nome anglofono.

In concreto può essere meglio interpretata come una generica rete (network) di terminali in collegamento tra loro, tramite i quali si istaura una comunicazione perpetua e che devono coesistere simbioticamente.
Vi sono blockchain pubbliche e private:
- quelle private trovano il loro utilizzo in certi contesti aziendali di una certa entità che richiedono un alto livello di sicurezza dei loro sistemi/ registri.
- Vi sono poi blockchain pubbliche, le quali verranno qui da me prese come modello.
Ogni blockchain richiede un applicativo per poter essere utilizzata, una sorta di programma di accesso mediante il quale affacciarsi su tale catena e poterne gestire il prossimo blocco.
La distinzione binaria sta nell'esclusività che una catena privata vanta rispetto ad una pubblica: la prima ha un circuito di terminali ben definiti e controllati; la seconda ha dei requisiti di accesso che sono pubblici e relativamente accessibili a tutti, in altre parole chiunque può entrare a far parte della categoria dei "controllori" della rete stessa.
Il fine ultimo, comune ad ogni blockchain, è quello di immagazzinare informazioni e renderle immutabili nel tempo, mantenendo un grado di sicurezza informatica al momento impenetrabile.
Ogni blocco della catena rappresenta un'azione o una serie di azioni, che varia in base al fine per il quale la chain viene impiegata; una grande azienda di macchine di lusso a livello internazionale, potrebbe utilizzare una blockchain privata per gestire il registro delle vendite e degli spostamenti, dunque il team di informatici potrebbe attribuire ad un blocco la compravendita del veicolo "X", targato "WYZ"ad opera del cliente "Epsilon" il giorno 00/00/0000 nel concessionario di Albuquerque, New Mexico; questo pacchetto di informazioni viene racchiuso in un blocco e annesso alla catena, registrandolo per sempre.
Nel momento in cui vi è una nuova vendita, un passaggio di proprietà, un cambio di residenza o una rottamazione che riguarda quel veicolo, questo verrà trascritto e un nuovo blocco seguirà all'interno della catena.
Le blockchain private sono settoriali e circostanziali, riguardano una realtà specifica e centralizzata, una singola equipe di individui può annettere o rivedere i blocchi creati in precedenza o crearne di successivi.
Minori sono i server che conducono un nodo (un terminale su cui viene processata e immagazzinata la blockchain e agenti tramite i quali si può andare ad annettervi dati) e più questo è centralizzato.
Tornando all'esempio precedente è plausibile che un'azienda abbia un unico team di sviluppo e gestisca un unico nodo internamente per coprire transazioni anche a livello internazionale, così come in qualche raro caso vi sono Factory profondamente all'avanguardia in questo tema che gestiscono i loro colossali commerci tramite innumerevoli distaccamenti, i quali sono tutti ugualmente abilitati e consapevoli delle informazioni innestate nel registro e che tutti possono ascrivere.
(Questo metodo nello specifico non prevede che tutti i nodi approvino la transazione, bensì che siano a conoscenza del suo avvenimento) [5]
Il focus della centralizzazione è ricercato in questo caso, un maggiore controllo significa tempi più rapidi e maggiore efficacia.
Walmart ha grande interesse nel gestire le consegne tramite blockchain, ma nessun interesse nel avere nodi dislocati nel mondo che hanno funzione di validare ogni transazione.
Bitcoin auspica invece al suo opposto, la decentralizzazione intesa come unico metodo di sopravvivenza del network e suo catalizzatore per contrastare il sistema bancario internazionale.
Il protocollo di Bitcoin è stato concepito dal suo creatore/ dai suoi creatori in ogni suo micro e macro aspetto funzionale.

In questo paragrafo esplicherò quello che è il funzionamento più analitico dello stesso, come funziona cioè da un punto di vista matematico e strutturale.
La blockchain sulla quale si fonda il protocollo è la prima vera blockchain pubblica mai esistita; questo significa che è accessibile a chiunque sia in modalità passiva visitando siti appositi e visionando in tempo reale ogni transazione mai avvenuta fin dal primo blocco creato.[6]
Sia attivamente, cioè prendendo parte alla gestione di un nodo e diventando minatori.
I minatori di Bitcoin sono delle persone fisiche che mettono a disposizione il loro terminale per rendere più decentralizzata (e in tal senso più sicura) la rete.
Ognuno di essi ha delle condizioni da seguire per poter gestire quello che in gergo viene definito full-node.[7]
Il primo fra questi è il download[8] dell'intero network precedentemente registrato; la dimensione di questo file è meno vasta di quanto ci si potrebbe aspettare, considerando che questa blockchain è in attività dal 2009.
Scaricati i 440GB di full-node ci vorranno alcuni minuti prima che l'applicativo sincronizzi e ultimi il tutto.
Vi sono inoltre altre specifiche lievemente più tecniche che non andrò ad elencare, basti sapere che queste sono di facile copertura anche da parte di un computer portatile di livello medio-basso.
Come ultimo "contro" vi sono eventuali problematiche inerenti alla legalità dell'operazione; in alcuni paesi, di cui approfondirò seguitamente, è legalmente proibita la compravendita di bitcoin, così come ovviamente la loro messa a carico da parte altrui e il loro mining.

6. **Minatori digitali**

Il protocollo Bitcoin è per definizione un "A Peer-to-Peer Electronic Cash System", ciò sta a significare che non sono previste intromissioni da parte di organizzazioni centrali o intermediarie di alcun genere.
Uno scambio tra pari senza nessun vincolo orario, di circuito bancario o di frodi.
Il minatore, come detto in precedenza, detiene propriamente una copia dello storico di tutte le transazioni presenti nella blockchain.
Bitcoin utilizza la crittografia a base di chiavi pubbliche e private e ogni minatore dunque conosce solo le chiavi pubbliche di ogni utente, che gli consentono di visionare su quali indirizzi (Wallet) vi siano depositati bitcoin e in che quantità; però, non conoscendo l'identità collegata a tale portafoglio non possiedono i mezzi per ricollegare tale sequenza ad un soggetto, così come non conoscendo le chiavi private dalle quali deriverebbero le pubbliche, non hanno possibilità di maneggiare il contenuto all'interno dei Wallet.
I minatori sono romanticamente i custodi della storia del protocollo.
Il metodo di consenso di Bitcoin è il Proof of Work, a "Prova di lavoro", e si svolge ponendo un intricato problema matematico ai computer dei miners, i quali devono lavorarlo fino a trovarne la soluzione.
La potenza di calcolo in questo procedimento preciso viene definita "hashrate" o dai più avvezzi semplicemente "hash", i terminali devono dunque dare prova del loro "lavoro" e vengono ricompensati con la commissione specifica della transazione e un ulteriore somma per il blocco appena creato, oppure in altre parole essi vengono remunerati per aver completato interi blocchi di transazioni verificate.
Ogni 10 minuti un blocco viene creato nella blockchain, all'interno del quale vengono accorpate tutte le transazioni richieste ed eseguite in quel lasso di tempo.
Ogni blocco occupa un megabyte di spazio all'interno della blockchain, appositamente

concepito in questa misura da Nakamoto stesso per rendere l'intero registro relativamente leggero e operabile su quasi la totalità dei terminali; questo dettaglio fondamentale è stato discusso più volte dai miners, affermando che se vi fossero blocchi con una maggiore capienza sarebbe più rapido tutto il network, sebbene ugualmente sicuro in termini di invulnerabilità informatica.
La decentralizzazione ha avuto un maggior peso della velocità per Satoshi.

7. **Bitcoin Pizza Day**

Nel maggio 2010 un appassionato di informatica di nome Laszlo Hanyecz si collegò ad un forum dedicato a Bitcoin, non diversamente da come succedeva usualmente; ma quel particolare giorno pubblicò un post in cui chiese se fosse possibile che qualcuno gli ordinasse due pizze e gliele consegnasse a domicilio in cambio di un onesto compenso di 10.000₿ (all'epoca circa 41$).

A suo dire ricercava una "colazione da portata, come in hotel, quando ti portano la colazione o qualcosa da mangiare e tu sei contento".

laszlo
Full Member

Activity: 199
Merit: 1071

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM
Merited by EFS (100), fillippone (52), OgNasty (50), DaRude (50), Seccour (50), debuni (50), Vod (20), sapta (20), alani123 (12), LFC_Bitcoin (11), onurgozupek (11), Nomad88 (10), TimtheYoutuber (10), Totscha (10), the_poet (10), arthurbonora (10), leps (10), mnightwaffle (10), loreRex (10), suchmoon (9), tyz (7), cheefbuza (7), ETFbitcoin (6), d5000 (5), Betwrong (5), bitbollo (5), krogothmanhattan (5), ebliever (5), LiteBit (5), mia_houston (5), nutildah (3), klondike_bar (3), vapourminer (2), BitcoinFX (2), LoyceV (2), gbianchi (2), cygan (2), bones261 (2), Halab (2), ChiBitCTy (2), crypto_curious (2), ivaxmm (2), malevolent (1), JayJuanGee (1), HI-TEC99 (1), iluvbitcoins (1), batang_bitcoin (1), UnDerDoG81 (1), TheQuin (1), S3cco (1), coolcoinz (1), digit (1), Julien_Olynpic (1), imstillthebest (1), Astargath (1), o_e_l_e_o (1), AlcoHoDL (1), amishmanish (1), lukax8 (1), JanEmil (1), jacktheking (1), frankenmint (1), bitart (1), DireWolfM14 (1), Toxic2040 (1), apoorvlathey (1), bubbalex (1), BobLawblaw (1), elianite (1), VB1001 (1), GazetaBitcoin (1), pushups44 (1), chimk (1), BTCLiz (1), taserz (1), Financisto (1), nullius (1), bonfire66 (1), SimpleFX (1), tim-bc (1), invincible49 (1), fishfishfish313 (1), thirdprize (1), Toughit (1), PascalCoin (1), barjan (1), nullama (1), M-BTC (1), dektox (1), lonchafina (1), grinbuck (1), alia (1), inkling (1), Blocktables (1), Kda2018 (1)

#1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRraAKrDvGHr1Bx3vDxeMv8Rh45aUet

Data la scarsità di offerenti scrisse di seguito un secondo post, chiedendosi se la sua "modica" offerta di 10.000₿ non fosse troppo esigua.

Il 19enne Jeremy Sturdivant vide i posts di Laszlo e il 22 maggio gli ordinò e consegnò le due pizze "large" come da lui richiesto.
Laszlo scrisse un terzo post in cui ringraziò il giovane, dicendo che le pizze erano molto buone e che i suoi bambini erano contenti, dicendosi pronto a pagare nuovamente 10.000₿ una prossima volta; pubblicò la foto che rimase poi nella storia del mondo criptovalute e blockchain.
Questa vicenda rappresenta la prima transazione di bitcoin in cambio di un bene materiale, la prima forma di pagamento tramite una valuta digitale indipendente.
Tutt'oggi il 22 maggio è conosciuto goliardicamente nella nicchia di criptofili come il "Bitcoin Pizza Day", il giorno in cui due pizze sono costate circa 275 milioni di dollari (prezzo medio di meglio 2023).

Ogni anno si festeggia questa giornata, alcuni grandi enti del settore organizzano eventi in giro per il mondo in cui vengono offerte pizze e coupon in alcuni token; moltissime pizzeria i cui proprietari sono vicini a questa nicchia offrono pizze a loro volta o le scontano a chi paga in bitcoin.

Ho attinto a questo famoso esempio sia come reportage storico, sia come filo logico del discorso precedente sui minatori: essendo un pagamento tra pari e pari, la transazione che Laszlo ha richiesto di eseguire verso Jeremy è stata garantita, come qualsiasi altra precedente e successiva a quella, da un gruppo maggioritario di minatori.
Il loro compito è stato quello di controllare se il Wallet (portafoglio) di Laszlo detenesse realmente quei 10.000 bitcoin, analizzare il Wallet di Jeremy e vedere se l'indirizzo fosse realmente esistente e abilitato alla ricezione.
Il sito di bitcoin.org spiega chiaramente come chi si offre come minatore ha poi degli obblighi verso il network, di cui il più dispendioso sia quello di tempo minimo da dedicare: 6 ore giornaliere di disponibilità di validazione.
Verosimilmente non saranno tutte dedite alla validazione delle transazioni, ma questo non è pianificabile in anticipo e dunque dipende dalla giornata più o meno intensa, anche se il maggior adottamento di Bitcoin necessita di un maggior quantitativo di minatori disponibili per poter snellire il network.

8. **Network di Bitcoin**

La rete Bitcoin è la più grande rete monetaria al mondo dallo scorso anno[9], ogni giorno di media vengono registrate tra le 240 mila e le 260 mila transazioni, al cui interno il quantitativo medio di bitcoin cadauna è di 7.7 btc.
Ovviamente il valore di bitcoin è relativo, non vi saranno mai più transazioni di 10.000 bitcoin come quella eseguita da Laszlo (forse), ma se quei 10.000 all'epoca erano solo 41$, questi 7,7btc di oggi sono più di 210.000$, due somme differenti.
La media di ogni transazione, moltiplicata per il numero medio di transazioni, fa la media di dollari giornalieri mossi dal network Bitcoin per ogni singolo giorno che passa:

51.975.000.000 dollari.
Come spesso accade, un numero di queste dimensioni per un individuo comune non ha nessuna rilevanza precisa.
Non siamo bravi a concepire e figurare i grandi numeri, ma sarà più chiaro dopo aver fatto questo parallelismo.
Mettiamo in relazione 1000$ ad una bottiglia d'acqua da 1litro (1$ = 1ml, 1000 ml), se convertissimo secondo questa logica quei 51.975.000.000 in bottiglie , queste diverrebbero 51.975.000.
Lo stato africano dell'Uganda ha una popolazione stimata di circa 46 milioni di abitanti, questo paese ha 10 milioni di abitanti in meno rispetto al nostro.
I problemi legati alle scarsissime riserve di acqua potabile in questi paesi africani è risaputa, nel parallelismo citato i 51.975.000 litri di acqua giornalieri permetterebbero ai 46 milioni di cittadini di avere cadauno e quotidianamente un litro d'acqua abbondante, riuscendo così a salvare la vita alla popolazione di un intero paese.
Un secondo e più affine parallelismo alla nostra catarsi occidentale, tramite il quale non serve fare alcuna conversione.
Il network di Bitcoin, se fosse passibile a compressione ed esportazione, garantirebbe giornalmente 880 dollari al giorno ad ogni singolo cittadino italiano ogni giorno.
Ritornando al tema centrale riguardo al numero di transazioni, ognuna di queste è stata approvata da una maggioranza del 50% + 1 di tutti quei minatori attivi in quel determinato momento in qualsiasi parte del mondo.
La decentralizzazione è totale, più i minatori sono numerosi e più la rete è disinteressata, la tempistica media di lavorazione per transazione è di circa 20/30 minuti, anche se personalmente in questo periodo in cui il mercato è più in fermento e arriva fino a 50/60 minuti.
Non ci sono giorni festivi o turni, non ci sono manutenzioni o impiegati sbadati.
La transazione arriverà all'indirizzo prescelto, perché viene predisposta dall'utente e validata disinteressatamente da una serie di individui X siti in Cina, in Vietnam, in USA, Bolivia e potenzialmente in ogni altro stato.

La transazione, una volta richiesta, viene inoltrata a tutto il network di minatori, si crea una competizione tra loro e questa viene eseguita nel più breve tempo possibile; tecnicamente viene messa a disposizione la potenza di calcolo del proprio terminale, il minatore non si caricherà personalmente di eseguire i calcoli.
Non vi sono orari di riferimento o attese dovute a tempi tecnici grazie alla decentralizzazione della rete, se una transazione viene richiesta alle ore 21:00 del fuso orario di Roma (+1), molto probabilmente non sarà un minatore pechinese (+7) ad eseguirla alle rispettive ore 3:00 di mattina, piuttosto la riscatterà qualcuno temporalmente più vicino e conseguentemente geograficamente più vicino.
Quello del minatore è il grande scudo tecnologico che il protocollo utilizza; quello che ovviamente il suo ruolo non prevede è quello di ravvisare una transazione inviata erroneamente ad un indirizzo sbagliato, l'onere è del mittente esattamente come nel settore bancario tradizionale.
Ogni transazione andata a buon fine e al quale il minatore ha commissionato potenza di calcolo, viene retribuita in Satoshi, termine del quale introduco ora il significato.
Si tratta di una frazione di bitcoin, precisamente di un suo milionesimo.
Il fine all'epoca del suo concepimento è quello a cui siamo arrivati ai giorni nostri, cioè al prospetto di valore di un singolo bitcoin molto elevato e di conseguenza al fatto che un milionesimo di tale cifra sia eventualmente ciò che più si addice alle micro transazioni quotidiane; ad oggi un sat sta a 0,03$, 3 centesimi di dollaro.
Agli albori della tecnologia il numero di sat ricompensati ad ogni transazione era all'incirca dello stesso quantitativo; i primi attori facenti parte del network erano i più convinti sostenitori, quindi credevano fortemente che accumulare bitcoin e satoshi fosse una piccola ma promettente miniera d'oro.

9. **Efficacia ed efficienza**

Vi è un numero di transazioni massime che possono essere eseguite giornalmente sulla rete.
La blockchain di Bitcoin è efficace in termini di portare a compimento le transazioni in sicurezza e in maniera indipendente, ma purtroppo non così efficiente in termini di esecuzione nel minor tempo possibile, almeno al suo stato naturale.
Anche in questa casistica vi è un'unità di misura che è la "adt": average daily transactions (media di transazioni giornaliere), la media si attestava attorno alle 90 transazioni giornaliere in tutto il mondo nel 2010, arrivando a crescere di 58 volte nel 2012, con una media di 23.000; nel 2019 le transazioni arrivarono al picco massimo mai registrato di 450.000 transazioni in un solo giorno.[10]
Come ho scritto in precedenza però le transazioni sono diminuite dal 2019 ad oggi e le cause sono state il calo del prezzo e la maggiore sfiducia nei prodotti finanziari in generale; particolarmente interessante però notare come ne sia diminuito il numero ma aumentato il valore individuale, che si aggira attorno ai 7,7 bitcoin.
Il problema attuale, e per il quale alla suddetta transazione (illustrata) sono seguiti 50 minuti di attesa invece che i canonici 20/25, è riconducibile al titanico numero di transazioni e al fronte del relativamente esiguo numero di minatori disponibili, il numero di nodi Bitcoin era di poco superiore ai 13 mila[11]; nell'immaginario collettivo possono sembrare pochi o tanti, ma analizzando i fatti è possibile riscontrare un costante aumento negli anni, che provoca una sempre maggiore dispersione degli interessi e una difficoltà maggiore nella manipolazione interna o esterna ai danni del network.
Il problema delle lungaggini nelle transazioni è concreto e riscontrabile, chiaramente questa percezione prende forma perché il network viene confrontato con altri

appartenenti ad altre cripto posteriori e tecnologicamente (e precisamente solo in questo aspetto) più innovative quali Ripple o Bitcoin Cash, delle quali tratterò a breve.
Se il parallelismo avvenisse tra Bitcoin e il sistema bancario attuale al quale siamo abituati, aspettare 25 minuti o 50 non farebbe differenza al fronte dei "2/3 giorni feriali" contrapposti dall'altro lato, giustificati con: un giorno necessario alla propria banca per elaborare la richiesta, uno per la transazione e uno per riceverla.

10. **Reti rivali**

Le criptovalute presenti attualmente sul mercato sono più di un migliaio, ne nascono ogni singolo giorno e io stesso ho dedicato tempo per provare a crearne una: i requisiti d'accesso non sono elitari ed è sufficiente saper programmare ad un mediocre livello e guardare qualche blog su internet.
Ripple è nata nel 2012 come alternativa bitcoin, non mi soffermerò sui tecnicismi di questa moneta, basti sapere che se per Bitcoin ho introdotto il concetto di "adt" come transazioni medie giornaliere, per Ripple è stato coniato il termine "tps": transactions per second, Ripple è capace di processare transazioni quasi in maniera immediata, attualmente sta processando 1.500 transazioni per secondo, dichiarando che potenzialmente il loro network ne reggerebbe fino a 50.000 al secondo.
Un numero immenso che va a doppiare ciò che i grandi colossi del mercato come Visa e Mastercard eseguono ogni secondo che passa (circa 24.000 transazioni al secondo).
Quello di cui manca Ripple è l'utenza, per un motivo molto preciso e semplice: un'efficienza così elevata può essere probabilmente dovuta ad una tecnologia prestante, ma è sicuramente dovuta ad una centralizzazione totale.
Ripple non usurperà mai Bitcoin nel ruolo che intende ricoprire.
Il secondo esempio che prima ho citato è Bitcoin Cash, il richiamo è palese e la sua nascita deriva da un fork (una biforcazione del network di Bitcoin, strutturalmente la tecnologia alla base resta la medesima ma vengono apportate delle modifiche) del 2017.
Questa valuta riconosce come problema fondamentale la dimensione ridotta ad 1MB per ogni singolo blocco, la prima proposta del fork è stata dunque quella di aumentare tale spazio a 32 MegaBytes per blocco, in modo da immagazzinare un numero molto maggiore di transazioni ogni singolo blocco e rendere la rete molto più fluida.
L'idea era quella di rendere questa moneta come il denaro contante, utile a micro transazioni per affrontare acquisti di ogni giorno: banalmente un negoziante che accetta bitcoin come pagamento deve aspettare 25 minuti prima di ricevere la somma, con Bitcoin Cash il tempo si riduce ad alcune decine di secondi (la rete non è mai stata largamente adottata, non ci è possibile sapere se vi fosse stato maggiore utilizzo quanto sarebbe aumentato il tempo di attesa).
Si stima che il numero di transazioni possibili con Bitcoin Cash fosse di 25 volte superiore rispetto al suo fratello maggiore, oltre che essere considerevolmente molto più scalabile.
Come preannunciavo questo fork non ha mai realmente preso piede e le ragioni principali sono due:
- La prima è quella che riguarda, ancora una volta, la decentralizzazione.
Questo tema, se non fosse ancora chiaro, è il più rilevante e quello sul quale si fonda tutta l'ideologia di Bitcoin, è difficile da mettere in secondo piano.
Bitcoin Cash renderebbe molto più pesante l'intera blockchain, i blocchi sarebbero minori ma di 32 volte più pesanti, senza considerare che lo storico del registro deve comunque essere considerato per poter gestire un Nodo col ruolo di minatore.
- La seconda ragione era più di tipo psicologico, la società percepiva Bitcoin con un senso di riserva di valore rispetto a quello di Cash/contante, per le micro-transazioni si sarebbe auspicata una valuta con una propria blockchain e una propria economia.

Queste ragioni, assieme al fatto che Bitcoin Cash non è mai stata chiara sulle proprie intenzioni e sul proprio funzionamento, producendo al suo interno altri due sotto fork, non ha ottenuto la credibilità che avrebbe desiderato.

11. **Miglioramenti al protocollo Bitcoin**

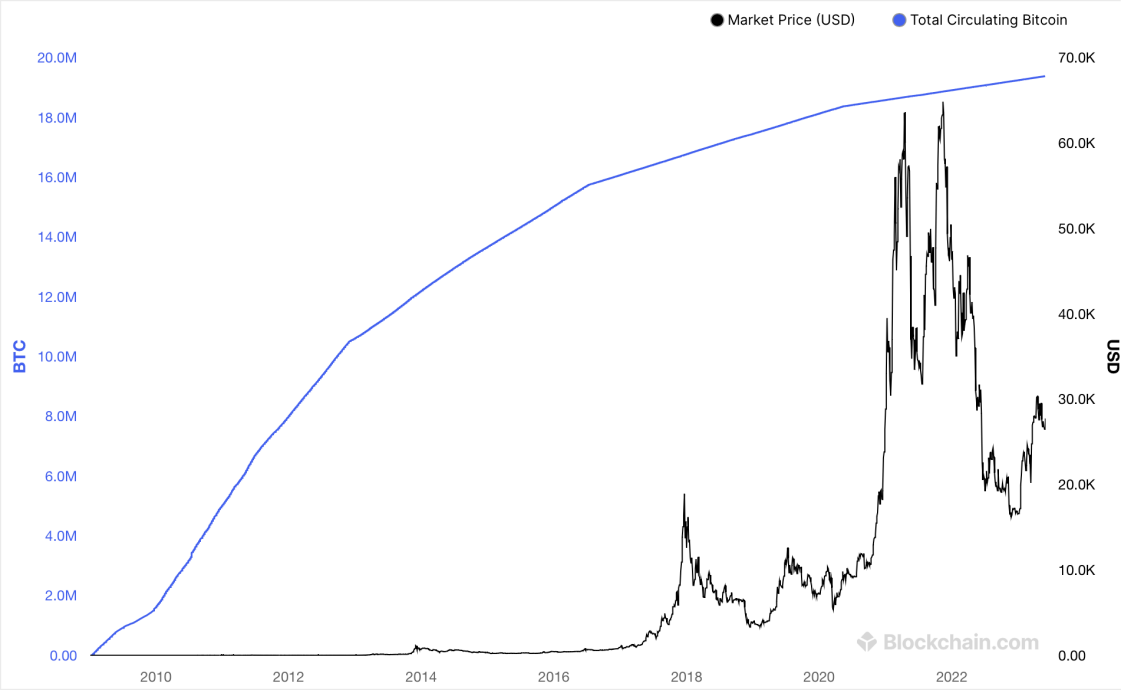
Bitcoin non è rimasto totalmente invariato in questi anni, sono state apportate alcune modifiche che hanno reso il suo utilizzo più consono al passare degli anni.
Le principali e degne di nota sono due: la prima delle quali è ormai un dato di fatto all'interno del protocollo, venendo accettata da numerosissime aziende di terze parti come unica alternativa all'invio di bitcoin "originali".
Mentre il secondo sta sfoderando le proprie peculiarità solo negli ultimi anni.
Nel 2017 il Segregated Witness, o più comunemente chiamato "SegWit" è tecnicamente un soft-fork, quindi una piccola modifica al network (che resta perfettamente compatibile) che va a migliorare in maniera alternativa la questione della rapidità e scalabilità; più nello specifico della grandezza dei blocchi, il fork agisce suddividendo la transazione in due segmenti, rimuovendo la firma di sblocco chiamata dato "testimone" dalla totalità della transazione.
La traccia contenente il dato testimone effettivamente ha una dimensione di un quarto rispetto alla sua grandezza reale.
Il Lighting Network[12] è un'applicazione proposta nel 2016 ancora una volta per aumentare la scalabilità della rete.
Tecnicamente in questa casistica il Lighting Network è un "Layer 2" di Bitcoin.
La differenza tra layer 2 e fork è che il primo si basa sulla medesima blockchain del progetto sottostante e compie operazioni più velocemente al di fuori di quella chain, per poi ritornarci appena concluso il processo; i due strati sono in continua comunicazione e condivisione tra loro e questo serve per non sovraccaricare la catena principale ed aumentarne l'efficienza delegando parte della lavorazione allo strato secondario.
Mentre il secondo, il fork, è una strada alternativa che viene presa da quel blocco in poi, la blockchain si dirama e da un capo continua il suo corso precedente, mentre dall'altro vigono le nuove regole istituite dai tecnici che hanno voluto il fork.
Il LN nasce dunque per fronteggiare la scalabilità e velocità del network, stimando che le transazioni per secondo di Bitcoin si aggirino attorno alle 3 e 7 e paragonandolo ancora una volta al colosso Visa con la fiera media di 188 miliardi di transazioni annue e 6000/8000 al secondo.
Le commissioni della rete Bitcoin inoltre teoricamente sarebbero esigue, ma la grande richiesta ha dato vita ad un meccanismo di mercato prioritario, che le ha rese talvolta esagerate: basti pensare che sono state registrate commissioni di quasi 50$ in Aprile 2021, un mese dopo erano tornate a 2,5$ come di consueto.
Per periodici spostamenti di denaro di ingenti somme Bitcoin è più performante rispetto al settore bancario, ma se inserito il suo utilizzo anche nel macro settore dei micro-pagamenti non è il principale attore consigliabile, poiché i costi d transazione arriverebbero ad essere decine di volte maggiori rispetto al bene acquistato.
Tramite Lighting Network viene creato un canale di pagamento tra due Wallet individuali; per esempio immaginiamo due soggetti, Epsilon e Delta: viene segnalato alla blockchain di registrare l'inizio del loro collegamento e la fine, trascrivendo le loro situazioni economiche nei relativi portafogli prima e dopo il loro collegamento, per cui è indifferente che vengano eseguite 43 transazioni tra le parti o una soltanto; quando il collegamento sul layer 2 viene chiuso la blockchain registra che ora le situazioni sono differenti da quelle iniziali.

Il LN è ancora in fase di testing e sta interfacciandomi con numerose sfide.
Vi sono dei Wallet creati appositamente per il suo utilizzo ma sono artificiosi e poco "a prova di utente" medio, anch'essi in fase di testing e dunque su cui è sconsigliato depositare grosse somme.
Il plus che offre questo sistema è l'immediatezza del pagamento al fronte di commissioni estremamente basse.
É un nuovo protocollo che sta riscontrando molto successo; è considerevole anche lo sforzo degli sviluppatori di integrarlo a BitcoinCore (quest'ultimo è lo strumento applicativo tramite il quale i miners scaricano l'intera blockchain e su cui analizzano le transazioni, come un Wallet potenziato e multifunzionale).

12. **L'estrazione di oro digitale e l'halving**

I ruoli di punta del protocollo restano quelli dei full-nodes dei minatori, i quali oltre a validare le transazioni hanno un forse ancor più importante compito e dal quale il loro nome figurativamente deriva: quello di estrarre nuova moneta, tramite il metodo ormai chiaro, quello della potenza computazionale (hashrate).
Il numero di bitcoin producibili è fisso a 21 milioni, non vi potrà di conseguenza mai essere inflazione, ma di questo tratterò in maniera più approfondita nei prossimi paragrafi.
In questo frangente basti sapere che il tetto massimo è fisso e che è stimato vengano prodotti gli ultimi bitcoin attorno all'anno 2140.
Nel preciso momento in cui sto scrivendo sono stati "estratti" 19.388.893,75 con un ritmo, come detto, di 10 minuti a blocco.
In questa cifra non sono inclusi ovviamente i bitcoin ancora da "sbloccare", così come quelli andati perduti; a riguardo vi sono numerose statistiche, e anche se nessuna tra loro detiene la risposta precisa è possibile stimare che un quantitativo compreso tra circa il 15% e il 25% sia stato smarrito irrimediabilmente.[13]
Fin dalla nascita dei bitcoin vi è stata una corsa ai sistemi di stoccaggio, vale a dire una ricerca continua di artefatti di sicurezza nel quale il singolo individuo potesse stivarli e conservarli.
La mente umana è più fallace di quanto non sia auspicabile, la memoria umana non è solida come quella di una macchina e disperde informazioni che non vengono richiamate da diverso tempo.
Per questa ragione alcuni portafogli sono colmi di bitcoin ma senza ormai chiave di accesso.
Vi sono ad esempio motivi fisiologici, pensiamo al caso del proprietario deceduto che non ha avuto modo di spiegare ai famigliari che in quella strana chiavetta vi fossero milioni di dollari in una criptovaluta arancione.
Il 20% di 19.388.893,75 è 3.877.778,74. Arrotondando per difetto a 3.875.000 significa che il corrispettivo di quasi 105 miliardi di dollari (ad oggi, presumibilmente cifra destinata a salire a causa del mercato) saranno persi per sempre.
Il procedimento per estrarre la moneta è letteralmente il medesimo di quello che ho descritto in precedenza, in questa circostanza mi andrò però a concentrare sul mio accenno alla doppia ricompensa che va a remunerare il minatore una volta che avrà registrato un blocco di transazioni: sia cioè per le singole transazioni e sia per la creazione del blocco stesso adibito ad immagazzinarle.
Ogni utente che vuole eseguire una transazione dovrà pagarne la commissione, la quale sarà ricevuta dal minatore che, in competizione tra tutti, risolverà per primo il difficile problema matematico.
La ricompensa che gli sarà assegnata algoritmicamente invece per la scrittura del blocco,

non sarà di matrice umana, bensì estratta dal protocollo; si tratta infatti di satoshi nuovi e di fresca immissione nel mercato circolante.
La remunerazione di ogni singolo blocco è di quantità fissa e indipendente dall'andamento del mercato o dal numero dei miners; l'unica regola che è stata programmata da Satoshi, e che è decisivo, è il sommo vincolo a quello che in gergo tecnico si chiama "halving".



L'halving è banalmente un dimezzamento della ricompensa che viene adibita al completamento di un singolo blocco.
Questo meccanismo è stato concepito proporzionalmente all'aumentare del valore di bitcoin, così da far respirare al miner un incentivo sempre abbondante ma mai esagerato.
Questo grafico rappresenta due dati incrociati: il prezzo di bitcoin dal momento della sua nascita ad oggi (linea nera) e il quantitativo di circolante nello stesso periodo (linea celeste).
Da questa illustrazione possiamo notare due fattori importanti:
- il primo (linea nera) più veniale che riguarda la grossa volatilità del prezzo di bitcoin; questo fattore genera nel grande pubblico un senso di rigetto e allontanamento, giustificato dal fatto che il mercato voglia sperimentare bitcoin come strumento di guadagno e non come alternativa al proprio sistema; una grossa percentuale di coloro i quali detengono la moneta lo fanno per il solo motivo di rivenderla non appena aumenterà di valore dal punto di vista pecuniario.
Non tutti hanno adottato l'ideologia, sebbene abbiano adottato lo strumento che ne è condotto.
- Il secondo colore (linea celeste), che è più strettamente inerente alla mia argomentazione, è la quantità di circolante immesso nel mercato negli anni: si vede chiaramente come la curva crei una pseudo-parabola che sappiamo tendere a 21 milioni.
La linea di colore blu non è però fortuita o accidentale, al contrario è matematico che ogni 210 mila blocchi prodotti, la cifra di bitcoin di ricompensa ai minatori si dimezzi.
Negli anni di prima sperimentazione della tecnologia i 210 mila blocchi sono stati prodotti

in maniera imprevedibile e difficilmente cadenzata, ma con la maturazione della rete e la lavorazione a pieno regime, è possibile predire i futuri halving, che cadranno ad una distanza temporale di 4 anni l'uno dall'altro.

Halving # (BTC)	Date	Block Number	Block Reward	BTC % Mined	Price on Halving Day (USD)
0 (Bitcoin launch)	3rd Jan 2009	0 (Genesis Block)	50 BTC	50%	N/A
1st halving	28th Nov 2012	210,000	25 BTC	75%	$12.35
2nd halving	9th Jul 2016	420,000	12.5 BTC	87.5%	$650.53
3rd halving	11th May 2020	630,000	6.25 BTC	93.75%	$8,821.42
4th halving	**between Feb to May 2024**	840,000	3.125 BTC	96.875%	?
5th halving	approx. 2028	1,050,000	1.5625 BTC	98.4375%	?
6th halving	approx. 2032	1,260,000	0.78125 BTC	99.21875%	?
7th halving	approx. 2036	1,470,000	0.390625 BTC	99.609375%	?
8th halving	approx. 2040	1,680,000	0.1953125 BTC	99.8046875%	?

Il primo blocco minato è stato proprio elaborato da Satoshi stesso, il quale ha ricevuto una ricompensa di 50 bitcoin.
Come lui, tutti coloro che abbiano eseguito blocchi da allora fino ai 210 mila blocchi hanno ricevuto lo stesso ammontare di moneta; in quei primi anni sono stati emessi il 50% dei bitcoin del protocollo.
È bene ricordare che la ricompensa dei minatori è letteralmente la medesima somma dell'immissione nel mercato di nuovo circolante, più alta è tale cifra e più il circolante aumenta velocemente.
Il 28 novembre 2012 il primo halving del network ha dimezzato a 25 il numero di bitcoin per blocco, minando in questo secondo ciclo il 75% del totale.
Così ogni 4 anni (circa) avviene questa divisione che, come preannunciavo, è stata concepita per andare di pari passo con l'aumentare del prezzo.
Basti pensare che nel 2010 creare un blocco bitcoin richiedeva (come ora) ingenti costi di energia elettrica e tempo dedicato, al fronte di 50₿ che equivalevano a pochi centesimi.
Paradossalmente ora che il guadagno è di "soli" 6,25₿ e che ognuno di essi corrisponde a 27.000 dollari, il rapporto costi-benefici è molto più alto di allora.
Faccio un appunto sulla motivazione sottostante al fatto che purtroppo molti bitcoin siano stati perduti dai propri proprietari; agli albori del protocollo vi erano un ridotto numero di minatori, e questo faceva si che vi fosse tra loro una più esigua competizione nella ricezione di quel palio di 50 bitcoin.
Era comune dunque che qualche appassionato di informatica, per gioco o per vantarsene con i colleghi, provasse a sua volta quel metodo di arrotondare con qualche spicciolo, immagazzinando quei 300/400 bitcoin dal valore di qualche dollaro.
Essendo il valore modesto e l'approccio dell'individuo al progetto molto blando, le password non vennero sempre ben conservate.
Ad oggi ci sono pagine di liste di quelli che vengono definiti "indirizzi dormienti" [14], ossia che detengono bitcoin ma che questi al loro interno non vengono maneggiati da decenni, si presume dunque che molti di loro siano ormai inaccessibili.

In questa fase conclusiva del paragrafo risponderò ad alcuni quesiti che mi sono posto negli anni e ai quali ho risposto anche grazie al lavoro di ricerca di questa tesi.

13. **Approfondimenti**

- *È possibile come individuo eseguire personalmente un nodo e validare autonomamente le proprie transazioni, senza pagare commissioni, senza passare attraverso la centralizzazione bancaria ma anche senza lasciare che sia un anonimo soggetto a prendersi la ricompensa?*
  Il network bitcoin funziona in maniera democratica, la transazione che viene richiesta deve per definizione giungere da un individuo a qualcuno che la controlli e l'unica via percorribile è il renderla parte del network stesso, quindi visibile alla community.
  Una volta che la transazione approda nella rete, diventa di dominio pubblico e tutti i miners sono ugualmente spinti ad elaborarla per ottenere la ricompensa.
  La stessa viene infatti "messa in palio" tra i minatori e al contempo controllata da tutti alternativamente, oltre poi al fatto di rimanere registrata per sempre una volta eseguita.
  Quindi no, non vi è modo di gestire un full-node con l'intenzione di esitare positivamente le proprie transazioni.

- *È possibile frodare Bitcoin, modificarne/raggirarne il codice sorgente o prevederne il prezzo?*
  Le risposte sono rispettivamente: no, no e no.
  Inizio però a spiegare l'ultima delle tre; bitcoin è un asset di mercato e il suo prezzo è dato interamente dalla prospettiva che la società assume di esso.
  Il prezzo non è però indicatore del valore reale del titolo, e il meccanismo di mercato (dell'investitore assennato) non è altro che comprare asset svalutati e quindi a buon prezzo, per poi rivenderli quando il loro prezzo oltrepassa il valore percepito come limite da quell'investitore.
  Bitcoin è un forte asset speculativo, che vive molti baratri e altrettanti picchi, è un asset volatile perché è molto giovane e soprattutto quasi totalmente sconosciuto dal mercato, cioè dalla massa.
  Il prezzo di per se stesso è impossibile da prevedere per ogni asset finanziario, si può solo stimare che dovutamente ad alcuni periodi storici più o meno positivi il prezzo salga o scenda.
  Se l'aspetto perseguito dal mercato fosse il valore invece che il prezzo, e soprattutto alle basi dell'investimento vi fosse uno studio approfondito e di lungo periodo invece che una progredita avidità istantanea, il prezzo di bitcoin matematicamente non dovrebbe più scendere, anzi impennerebbe proporzionalmente al numero di nuovi fruitori.
  Teniamo a mente che gli indirizzi bitcoin assegnati ad un soggetto a non avere zero come contenuto di moneta, sono circa il 4,2% della popolazione mondiale: c'è ancora molto margine potenziale.[15]
  Per rispondere poi a ritroso alla seconda domanda, non è possibile modificarne il codice singolarmente, poiché il codice sorgente di Bitcoin è open source, cioè significa che qualsiasi persona che lo voglia può prenderne visione e costruirvi attorno applicazioni con esso profondamente compatibili (metodo su cui si basano i vari Lighting Network, SegWit e forks).
  Il codice può essere dunque modificato sì da chiunque, ma deve essere accettato comunitariamente da tutta la rete di miners, la quale avrà sempre tutto l'interesse a rendere il protocollo più efficiente e sicuro possibile, sia nel breve ma anche in quanto a longevità del progetto.

La domanda alla quale dedico più importanza riguarda le frodi o la manomissione più in generale.
Un sistema di qualsiasi ambito che dia importanza all'equità, alla democrazia e alla giustizia, quasi non si addice alla individualità umana e ancor meno alla nostra società nel suo intricato e egoistico complesso.
Per questa ragione mi è fin da subito parso impossibile che nessun magnate si appropriasse della rete, ne delegasse la costruzione di una migliorativa, e altresì come nessun informatico hackerasse il protocollo, trovasse un metodo per appropriarsi di valute.
Un grande personaggio che disponesse di molteplici centinaia di miliardi, fondi sufficienti a comprare tutto il network, non avrebbe alcun interesse a fare questo acquisto.
Come dicevo prima il bitcoin esprime il suo utilizzo o tramite un uso speculativo o uno più idealistico. In ambedue i casi funziona perché una diversità di individui ne possiede e può permettersi di eseguire scambi di mercato, monopolio e libero scambio non sono mai coesistiti.
In un primo momento, certo, il prezzo salirebbe perché numerosi bitcoin starebbero venendo sottratti dalla disponibilità collettiva, aumentandone le scarsità e dunque il prezzo; continuando ad appropriarsene si arriverebbe ad un crash, molto banalmente il prezzo salirebbe fino agli ultimi sgoccioli di moneta rimasta in circolazione, ma già a questo punto l'economia di Bitcoin sarebbe terminata, non avrebbe più il fine per cui è stato creato e il prezzo inizierebbe ad essere solo un numero.
La forza di Bitcoin sta nella sua concretezza nel mondo e nella società, far confluire tutta la moneta o la maggior parte di essa in un unico ente, significherebbe da un punto di vista sia economico che ideale, sopprimere il protocollo.
Fermare gli scambi tra le persone che lo posseggono, arrogandosi l'intero ammontare, significa disporre di una fortuna incredibile in teoria, ma non nella pratica, perché nessuno li accetterebbe più perché non sarebbero poi a loro volta spendibili.
I miners a loro volta non avrebbero iniziativa di creazione, non avrebbero più intanto ricompensa dalle transazioni in quanto non ve ne sarebbero più tra Wallet, in più essendo il protocollo tecnicamente centralizzato, verrebbe a mancare totalmente il motivo per cui Bitcoin è venuto alla luce nel 2008; sono fortemente convinto che la maggior parte dei miners abbandonerebbe l'intero progetto.
Quei pochi rimanenti non sarebbero sufficienti a creare un'economia comprensiva di un individuo fortemente superiore e poche centinaia di persone che alla base producono una moneta che non ha valore sul mercato.
Alla luce di tutto ciò, si deve considerare inoltre il fatto che nessun magnate (figurativo, dato che al momento non esistono individui singoli o collettivi che posseggano una disponibilità tale da poter comprare l'intero numero di Bitcoin) scambierebbe una somma di ricchezza reale con una non liquidabile, in altre parole non scambierebbe la sua ricchezza con il nulla.
Un'alternativa più plausibile sarebbe quella in cui il suddetto miliardario comprasse invece che direttamente la moneta, un enorme quantitativo di terminali di mining tale da garantirgli il 50% + 1 della rete, questo gli garantirebbe un grosso peso nel ricavo di nuovo circolante, che potrebbe far suo, ma essendo attore di maggioranza anche nel ruolo di giudice dell'intero network, a livello pratico però la lavorazione dei blocchi richiede costi importanti per il singolo individuo e possedere un così elevato numero di terminali di lavorazione spingerebbe a dei costi elevatissimi al fronte di ricompense estremamente esigue.
Basti pensare che per accertare una transazione tutti i terminali della rete lavorano per risolvere il problema, consumando e costando energia ai singoli proprietari, i quali la compensano ottenendo qualche satoshi ogni transazione e quella rara volta la grossa

somma di completamento del blocco.
Essendo un così elevato numero facente parte di un unico ente, vi sarebbe più possibilità di aggiudicarsi tale premio, ma si finirebbe per far competere le proprie macchine tra loro, spendendo buona parte o addirittura tutta la ricompensa prima ancora di ottenerla.
Possedere la maggioranza dei server era possibile agli albori del protocollo, momento in cui vi erano poche dozzine di minatori e il procedimento non era realmente competitivo come oggigiorno.
Per quanto concerne le penetrazioni malevole, non sono mai stati sottratti bitcoin senza che l'utente eseguisse un qualche tipo di azione.
Vi sono state sì delle truffe di moneta, ma dovute all'inconsapevolezza o all'errore umano, non dovuto a falle nel sistema del protocollo.
Quest'ultimo non è rimasto del tutto invariato dal 2008 ad oggi, come ogni codice di grandi dimensioni richiede qualche dritta, che è stata prontamente data da team di sviluppatori volontari sparsi per il mondo.
Il punto forte non è il non avere nessuna fallacia tecnica, ma nel colmarla nel più breve tempo possibile.

- *Se le commissioni sono relativamente alte, perché dovrebbe essere conveniente usare Bitcoin invece che il sistema bancario?*
  La discriminante, come fino ad ora spesso, è quella della libertà e della non dipendenza.
  Il sistema bancario, così come per certi versanti il sistema economico su cui esso e noi tutti ci basiamo, ha delle falle strutturali, che non approfondirò in questa sede perché risulterebbe fuorviante dal tema principale.
  La società ha adottato questo sistema già da 400 anni, rendendolo un anello fondamentale della concezione del mondo così come lo conosciamo.
  Il sistema bancario all'atto concreto funziona bene, permette spostamenti di denaro da un soggetto all'altro, rilascia prestiti e garantisce finanziamenti, oltre che ad altre funzioni importanti e caratterizzanti.
  Quello che fa però è anche decidere al posto del detentore della ricchezza che essa custodisce.
  Controlla i fondi, impone delle scadenze entro le quali sia possibile o meno richiedere prestiti, appone l'interesse dell'istituzione prima di quella dei clienti e per farlo utilizza i fondi di questi.
  Ma come ho detto, il sistema funziona per coloro che non vanno a fondo delle cose e non si pongono questo genere di domande, non importa se il debito pubblico del nostro paese è di quasi 3 triliardi[16] (3.000.000.000.000) e aumenta ogni mese, se fossimo un'azienda saremmo falliti miseramente.
  Il cittadino medio non riscontra questo genere di cose, piuttosto nota che se va dalla propria banca ha possibilità di ottenere un prestito;
  culturalmente per gli individui in epoca contemporanea l'istituzione bancaria è sempre esistita, non è stata introdotta da pochi decenni e non deve affermarsi, è totalmente normale che non venga considerata una forma alternativa, specialmente se di più "difficile" accesso al giorno d'oggi.
  Le commissioni bancarie sono per la maggior parte nulle per le operazioni basilari, la maggior parte di esse richiedono però un costo mensile (mi riferisco a banche italiane, il costo è variabile da banca a banca) e un costo annuale di mantenimento del conto corrente.
  Il costo di Bitcoin è variabile a sua volta, ma come ho già fatto presente può arrivare anche a 50$ per singola transazione.
  Questo fa sì che a monte dello stesso prezzo possano essere configurate 2 transazioni all'anno al fronte di potenzialmente infinite operazioni dall'altro.

Torno a dire che vi è un'ambivalenza:
- Chi è più attento e fornisce più valore alla libertà individuale in questo settore adotta Bitcoin, o quantomeno ne è sostenitore, sminuendo il costo delle transazioni e giustificandolo come costo da affrontare per decidere per il proprio denaro.
- Chi non attribuisce valore a questi aspetti non ha reale motivo di cambiare un paradigma che apparentemente funziona per uno quasi o del tutto sconosciuto.
In questo paragrafo dunque ho cercato di essere il più esaustivo possibile riguardo la tecnologia di Bitcoin, accensando brevemente alla sua storia e ad un primo approccio pratico alla realtà della regina delle criptovalute.

L'intermediazione degli exchanges

La reputazione di Bitcoin ha negli anni subito differenti risposte e interpretazioni da parte degli stati, dei media e di conseguenza dei singoli individui; non bisogna però dimenticare che sia i primi che i secondi sono interamente il risultato della somma dei terzi.
Gli stati, sociologicamente parlando, non sono niente più che un gruppo di persone al governo, incaricate da un gruppo più numeroso di individui di fare quello che viene reputato il "bene comune" per l'intera comunità di individui.
Bitcoin non è stato inventato per essere oggetto di stato, di proibizioni e limitazioni; piuttosto è stato concepito per aggirare tali istituzioni.
Il protocollo come accennavo in precedenza si compone ed è vincolato per sempre ad essere di 21 milioni di Bitcoin disponibili, non è impugnabile in nessun modo o da alcun individuo singolo o ente aggregato.
Per l'algoritmo non vi è un soggetto più forte e uno più debole, non vi sono governi o banche centrali che tengano; vi sono solo richieste ed ordini, tutti uguali e dei quali la priorità è decisa sulla base di minime commissioni operabili da chiunque.
Il network Bitcoin interpreta tutti come indirizzi equi, non importa se lo si stia acquistando dal network per uso privato, per conto di un'azienda o per conto della Banca Centrale Europea.
Per esplicitare meglio questo concetto voglio trattare come esempio quelli che in gergo si chiamano exchange: che sono le piattaforme di scambio dalle quali si possono acquistare e vendere Bitcoin e la maggior parte delle altre altcoins, in particolare utilizzerò come vettore della mia stesura il più grande e fornito exchange al mondo.

1. **Gli exchanges**

Gli exchanges sono tecnicamente i portali sui quali vengono depositati enormi quantitativi di valuta FIAT, che nella nicchia dei cripto investitori è intesa come denaro contante, intercambiabile tramite circuito bancario classico e soprattutto direttamente ancorata ad una materia prima di riferimento con funzione di riserva di valore (dollaro, euro, rublo etc. sono etichettate come valute FIAT, non cripto).
Questa valuta tradizionale viene appunto usata da tramite dai più per poter accedere al più vasto e colorito ambiente delle valute digitali, chiunque può comprare valute a commissione diverse in base all'exchange di riferimento, al periodo di riferimento e ai tempi dei quali ha necessità di aspettare (anche altre monete, proprio come bitcoin,

hanno la possibilità di favorire la propria transazione a scapito delle altre aumentando leggermente la propria commissione offerta al miner o validatore).
L'exchange cripto più grande al mondo si chiama Binance, fondato nel recente 2017 dal multi-miliardario cinese ChangPeng Zhao (11° persona più ricca al mondo e prima in Asia,[17] e il nome deriva dall'unione di "Bitcoin" e "Finance".
Questo colosso ha un volume giornaliero di scambi di $13,086,513,483.75, mentre una riserva di valore complessivo stivato di $74,533,277,335.51, è il maggiore del settore arrivando da solo ad avere maggiori scambi giornalieri dei primi 10 competitor messi assieme (di cui uno è una società sottostante a Binance, affiliata e specializzata nelle direttive statunitensi), offre lavoro a circa 7 mila soggetti in tutto il mondo.
Per il protocollo Bitcoin però tutto ciò non fa alcuna differenza.
Binance, il quale slogan è "Exchange the world", non ha nessun merito o demerito in più rispetto ad un contadino vietnamita che sta acquistando la stessa valuta per diletto; entrambi detengono i loro Bitcoin (le altre valute funzionano a discrezione propria) su dei Wallet indipendenti, con lo stesso grado di sicurezza garantita e di privacy.
Se negli anni precedenti gli exchanges non avevano una politica chiara riguardo le loro manovre interne e l'utilizzo concreto dei fondi dei loro utenti, è stato proprio Binance a farsi carico della portata di questa nuova visione del proprio prodotto.
La comunicazione che CZ (l'amministratore delegato di Binance si fa chiamare così sui social in maniera amichevole) ha sempre tenuto verso il suo pubblico è stata di tipo diretto e (fino a prova contraria) sincera.
Non appena si aprisse uno scandalo di qualche genere non è tardata a seguire, da parte del Team di Binance, una chiarificazione che valesse la pena di sentire e che non fornisse semplici scusanti, piuttosto delle motivazioni concrete o dei metodi per rimediare e accordarsi con le autorità.
Sottolineo che in questo ambito gli scandali non sono desueti: è stata appositamente creata una parola, ancora una volta usando acronimi che somigliano agli slogan elettorali e che sui social si prestano molto bene agli hashtag, che è "FUD" (Fear, Uncertainty and Doubt) che spesso viene seguita da "SAFU", che invece è inerente ai propri beni monetari e sta ad indicare Secure Asset Fund for Users (I fondi degli utenti sono sicuri).
Un altro grande passo verso la maggior trasparenza è stato mosso nel periodo successivo il fallimento di quello che è stato per un breve periodo il secondo più grande exchange mondiale: FTX.
Quest'ultimo, crollato nei primi giorni del novembre 2022 per cause dovute a riciclaggio di denaro e ad una sovra esposizione al mercato che lo ha portato a perdere tutti i propri capitali (dei proprio clienti).
In questa sede però non tratterò delle cause che hanno portato al tracollo di FTX, piuttosto di come gli exchanges funzionino e come si approccino alle criptovalute.
Da quei giorni in avanti il mercato ha subito un forte senso di insicurezza verso entità così grandi e di cui in realtà si conosce così poco.
È stata fortemente richiesta dunque dagli organi regolatori sparsi nei diversi paesi e adibiti al settore finanziario, che la totalità dei fondi detenuti da (teoricamente) ogni exchange sia resa pubblica a tutti sia in termini di quantità che di indirizzo di Wallet.
Questo ha reso e renderà per sempre possibile tracciare ogni transazione in entrata o uscita da quei Wallet, facendo un controllo incrociato sarà poi semplice visionare se Binance (per tornare all'esempio, che è stato il primo ad introdurre questa nuova policy di fiducia) abbia per qualche ragione movimentato i suoi depositi e poter di conseguenza richiedere spiegazioni.
Torno a ripetere che Binance è per il network Bitcoin un individuo tale e quale a tutti gli altri, i Wallet di dominio pubblico sono della medesima tipologia rispetto a quello di chiunque, il contenuto certo è degno di nota, ma la tecnologia è la stessa.
Il funzionamento e la fortuna della creatura di ChangPeng sono dovute al fatto che lui

abbia visto un potenziale e creduto in Bitcoin sin dai suoi albori, comprando e accumulando tutto il possibile e arrivando a vendere la sua stessa abitazione pur di detenerne un numero maggiore.
Quell'intuizione, mista ad uno spiccato senso imprenditoriale e una serie di scelte assennate, lo hanno portato dove è ora.
La prassi di compravendita di bitcoin tramite exchance non è altro dunque che uno scambio tra pari e pari (di diverse entità e grandezze) che comprano e vendono a vicenda un bene economico.
Tornando all'esempio precedente, ipoteticamente se il contadino vietnamita avesse avuto l'intuizione di comprare 1000 Bitcoin nel lontano autunno di dieci anni fa, momento in cui il prezzo era di circa 100$ cadauno (circa 2.800.000.000 dong vietnamiti), e se al contempo avesse voluto perseguire la strada di offrire scambi tra valute; avrebbe potuto egli stesso creare/ divenire un exchange.
Bitcoin è equo con tutti i partecipanti del suo network, richiede fiducia e in cambio offre eguali opportunità e nessun rischio di manipolazione.

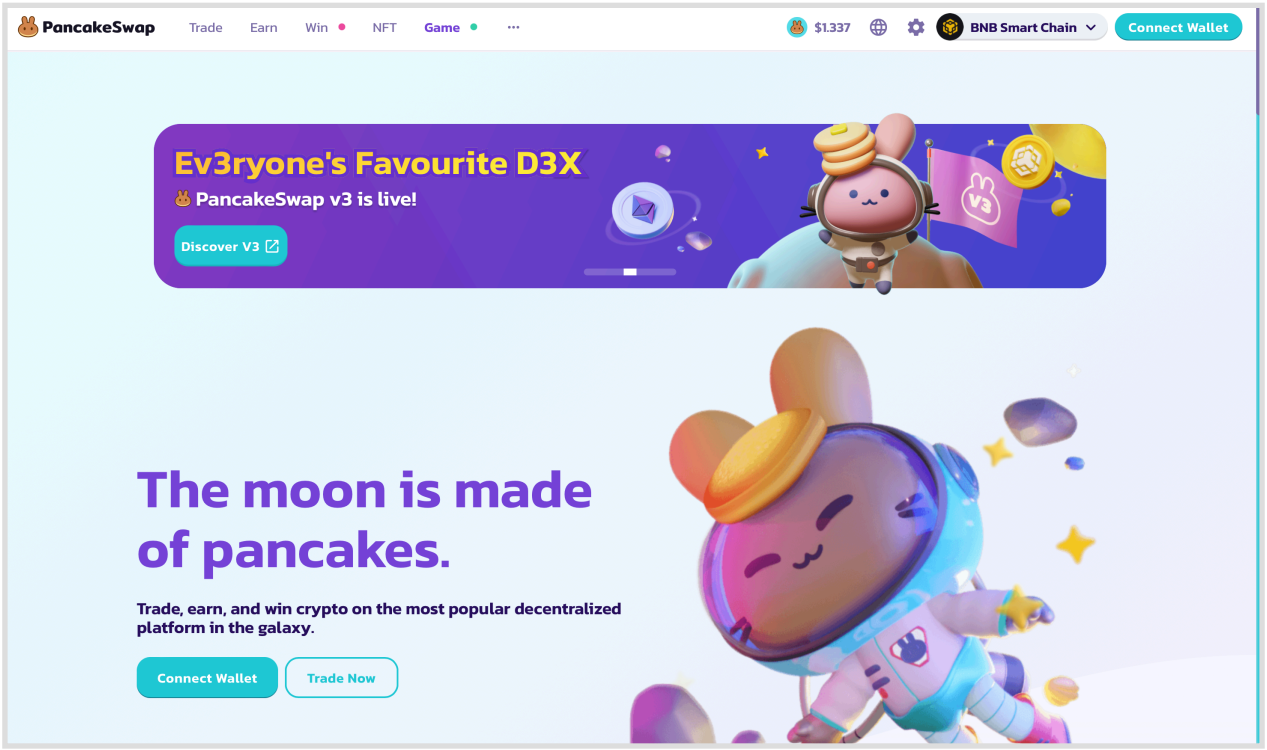
2. **Piattaforme di prestito**

Un seconda categoria di attori che esistenti in questa "comunità 3.0", anche se entrati a farne parte solo in una fase più matura, sono le piattaforme di "lending and borrowing".
Il ruolo che questi siti e applicativi ricoprono è quello di, come suggerisce la traduzione letterale, dare a prestito e prendere a prestito.
Il tutto è gestito da smart contracts (contratti intelligenti, delle clausole algoritmicamente predisposte che, allo scadere di un'azione, ne iniziano automaticamente una seconda, senza alcun intervento diretto o supervisione umana) e l'equilibro è quello che da un lato si è incentivati a prestare criptovalute, depositandole con la promessa di ricevere un interesse, dall'altro si ha la possibilità di prendere a prestito capitali ad interessi relativamente più bassi di quelli bancari tradizionali.
Le garanzie vengono saldate in anticipo, in un contesto in cui la regolamentazione è allo stato brado è dovere di ogni soggetto tutelarsi, questo significa che chi ha volontà di ricevere un prestito in una criptovaluta dovrà previamente depositare un controvalore uguale o superiore in bitcoin o valute digitali ancorate al dollaro (dipende dalle politiche delle singole piattaforme).
Il fine solitamente è quello di depositare bitcoin in modo da non doverli vendere e non perdere la probabilità che essi salgano di valore, affidandoli alla piattaforma diventa dunque possibile ricevere il controvalore e fare un acquisto importante.
Riaccreditando su base settimanale o mensile tale debito sul sito e sbloccando i propri bitcoin.
Conosco personalmente un ragazzo residente in Germania che tramite questo metodo ha comprato un'auto.
Io ho sempre e solo usufruito di tale servizio come parte che presta le proprie cripto.
Dal 2011 (anno di fondazione del primo exchange) ad oggi sono passati numerosi anni, i servizi in questo settore si sono evoluti e amplificati, la maggior parte degli exchanges di grandi dimensioni offrono ora anche il servizio di lend e borrow, così come la
maggioranza di questi ultimi hanno un servizio di scambio direttamente interno, spesso a commissioni non competitive ma sicuramente più comodo.

3. **La mia esperienza**

Gli exchanges offrono una lunga serie di servizi, opportunità e soluzioni finanziarie, il tutto però è reso facilmente accessibile sia in maniera visiva che intuitiva, venendo velocizzato tramite numerose accortezze sulla consapevolezza delle azioni che vengono intraprese in app: vi sono numerosi video corsi, post su alcuni temi salienti e soprattutto alcuni quiz obbligatori da dover superare prima di poter ricevere l'accesso a certe funzioni più rischiose.
Per esperienza personale posso confermare che non mi è stato difficile imparare ad usare la maggior parte di questi strumenti, io avevo sentito parlare di bitcoin già nel suo ultimo momento di massimo spicco mediatico del 2017[18], (Il rapporto risale a due anni fa, successivamente il prezzo di Bitcoin è addirittura triplicato e l'interesse sui social e motori di ricerca ha seguito quest'ultimo) ma non me ne ero mai interessato più approfonditamente, nel primo periodo di chiusura forzata dovuto al Corona Virus mi sono inerpicato ad esplorare nuove realtà in ambito digitale.
Nel marzo 2020 ho iniziato ad informarmi sui primi portali e dai primi influencer italiani in merito e la settimana successiva ho portato a termine la prima operazione finanziaria in bitcoin su un exchange minore che all'epoca faceva molte sponsorizzazioni sui social: ero all'oscuro di ciò che significassero e in che maniera venissero applicate le fee (commissioni) sulle operazioni, avevo sentito nominare il concetto di spread di mercato ma non avevo mai realmente approfondito, ero totalmente all'oscuro della fiscalità di questo settore.
Nonostante queste evidenti mancanze di competenza e la ridotta consapevolezza ho avuto accesso nel giro di 5/10 minuti di registrazione ad un intero nuovo mondo digitale del quale prima non conoscevo l'esistenza, in cui ora sono attivo da tre anni e che ancora alle volte è difficile da gestire.
I requisiti minimi di accesso sono tecnicamente alla portata di tutti gli individui e descriverli è quasi superfluo, è sufficiente infatti avere un conto corrente bancario in attivo, un'identità convalidata e che tale identità sia corrispondente a quella utilizzata per l'apertura del conto sull'exchange e la maggiore età in rapporto a quelle che sono le leggi vigenti nel proprio stato.
Queste sono le uniche reali barriere che un ragazzo trova nell'accedere a questo ambiente, una volta entratovi, senza le dovute precauzione, si troverà ad avere in tasca un casinò senza limitazioni od orari.
Le app di compravendita sono progettate in maniera affascinante da una prospettiva di marketing e persuasione: i colori, le forme dell'UI (User Interface: ciò che si prospetta a schermo come la forma dei pulsanti, le dimensioni etc.) sono amichevoli e del tutto simili alle "innocue" applicazioni che si usano tutti i giorni, totalmente diverse da quelle spigolose piattaforme di trading dei primi anni duemila; a questo proposito sottolineo un demerito da parte delle grandi banche o broker online che esistono da decenni ma utilizzano la stessa interfaccia di trading che si usava al momento del loro lancio.
Un esempio lampante è l'istituto di credito Fineco, una tra le migliori banche al mondo secondo il giornale Forbes; questa banca ha di recente aggiornato l'interfaccia grafica del loro strumento di punta per quanto concerne il trading, che in precedenza era stato chiamato PowerDesk, ora invece ha subito un rebranding diventando FinecoX[19], in ogni caso non c'è sfida con le piattaforme di cripto-trading.
Non mancano le possibilità, bensì manca l'intenzione di far apparire la finanza alla portata di tutti, poiché è una materia spesso percepita come noiosa, elitaria e complessa.
Il mercato delle criptovalute è, come dicevo prima, quasi sconosciuto agli occhi della popolazione globale, è importante dunque rendere il processo di compravendita più lineare e confortevole possibile.
Esempio in questo frangente diametralmente opposto a Fineco è PancakeSwap[20],

piattaforma di scambio di valute digitali disponibile al momento in due distinte e consecutive versioni che muove quotidianamente circa 130 milioni di volume in dollari nell'una e 140 milioni nell'altra.
PancakeSwap (quasi alla stregua di un "gamification" del concetto di finanza) ha già nel nome dei palesi rimandi a nulla che rientri nel ramo della finanza, lo stile grafico è tendente al bambinesco e i colori accesi sono allegri e spensierati.
Nonostante si possa dibattere sulla moralità di questo genere di raggiri percettivi, dal punto di vista a loro saliente tale manovra è profondamente efficiente.
Il sito ha un coniglietto come mascotte e indirettamente ha la medesima possibilità di prosciugare i conti correnti degli sprovveduti che vi investono.
È banalmente l'apoteosi di un tipo differente di approccio che viene adottato dalle entità operanti in questo ambito finanziario, non sto avvalorando questa manovra di giocosità inflazionata della finanza, sto costatando che sarebbe necessaria una prospettiva mediana.



La storia della moneta

1. **Proprietà della moneta**

In questo paragrafo mi dedicherò alla stesura di tutte quelle più o meno evidenti diversità tra la moneta FIAT e la base strutturale su cui si ergeva in passato, approdando seguitamente alla valuta digitale e al protocollo Bitcoin.
Questo paragrafo richiede però due premesse:
1) Prima di tutto è bene ricordare come non vi sia una regola che determini quali beni possano o non possano essere considerati "moneta".
Vi sono dunque dei canoni sulle qualità convenzionali di un determinato bene per poter essere qualificato come "moneta" di riferimento in un contesto; questi sono tre e sono in egual maniera fondamentali: scalabilità, maneggevolezza e durevolezza.
In genere i primi due primi requisiti non rendono così elitario l'accesso di un bene al ruolo di "valuta", il terzo invece è il più cruciale.
- La scalabilità o "vendibilità attraverso diverse scale", è la possibilità di un dato bene di essere suddiviso in parti più ridotte per far fronte a scambi di più esiguo valore e/o raggruppato in parti più abbondanti per scambi di più importante entità.
La divisibilità permette facilmente ad un individuo di aumentare o diminuire il proprio corrispettivo per trattare con un secondo individuo.
- La maneggevolezza o "vendibilità attraverso lo spazio" indica la facilità di trasporto fisico che tale bene possiede; gli spostamenti umani nei secoli hanno messo in risalto la ricerca della maneggevolezza e hanno portato i mezzi monetari ad avere via via un sempre maggiore valore per unità di peso.
- La durevolezza o "vendibilità attraverso il tempo" è la peculiarità di un bene di mantenere invariato il proprio stato (e verosimilmente il proprio valore di mercato) nel futuro, permettendo al suo possessore di mantenere tramite esso la propria riserva di valore negli anni.
2) La seconda premessa è il concetto di stock-to-flow: questo è il rapporto tra la moneta/ bene già circolante e presente nell'economia di uno stato, ente o realtà che sia mai stata prodotta o estratta in passato, sottratto tutto ciò che di quella sia mai stato distrutto, consumato o perduto (cioè sia rimasto in stock) e la semplicità con cui può venirne aumentato il flusso di quantità; in altre parole è la facilità di nuova immissione nell'economia di tale moneta nel periodo futuro (il flow).
L'introduzione di nuovo circolante è un equilibrio di mercato tra il valore della moneta e la spesa della sua estrazione/ creazione.
Per esempio più il valore aumenta e più si è incentivati ad estrarlo e ad aumentare il suo flow, abbassandone nuovamente il prezzo di mercato.
Un bene si dice abbia un basso rapporto stock to flow quando il suo flusso di immissione può essere facilmente aumentato, a piacimento o seguendo il mercato.
Viceversa un bene con un alto rapporto stock to flow non subisce grandi o improvvise variazioni di quantità, in quanto la possibilità di introdurre nuovo circolante è impervia o in alcuni rari casi del tutto impossibile.
La popolazione umana ha richiesto fin dall'esordio del sedentarismo, quindi della produzione circostanziale di un determinato ventaglio di beni primari e non di altri, un mezzo di scambio per appropriarsi di quelle provviste che le mancavano.

Vi sono molteplici esempi nel libro del 2018 “The Bitcoin standard” di Saifedean Ammous, che utilizza tale parallelismo per esplicare il filone storico che ha condotto il genere umano fino a Bitcoin.
Di questi esempi io ne riporterò solamente alcuni, che a mio avviso sono i più rappresentativi, poi mi concentrerò più genericamente sul percorso umano-monetario, con interesse maggiore nel continente europeo.

2. **Le perle africane**

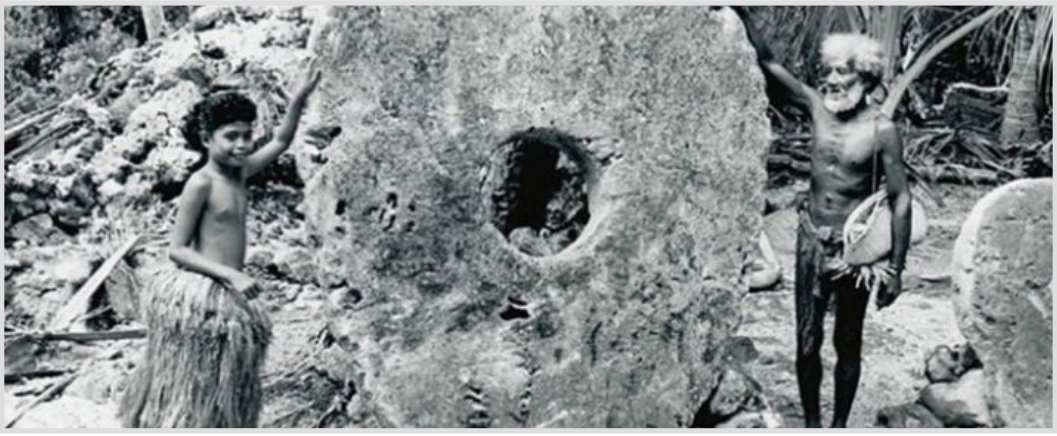
Il periodo di riferimento del primo esempio si aggira attorno al sedicesimo secolo; lo scenario storico è quello delle grandi scoperte, delle grandi tratte commerciali delle compagnie delle Indie europee e dei grandi navigatori.
Infatti, se si analizzano i commerci marittimi di quel periodo, si evince che la grande mole degli investimenti reali si concentrava sulla rotta verso le Americhe, ma un gran numero di esploratori si accinsero a percorrere vie inizialmente meno battute.
Affiancando la costa africana fino a quasi circumnavigarla si giungeva nella mitica (poi risultata la reale) India, sulle coste del Khitai (antica nomea dal quale poi deriva l’attuale “Cina”) e si ipotizza i navigatori siano approdati persino su quelle del Giappone.
I viaggi di questo tipo erano decisamente meno pericolosi di quelli oceanici, perché permettevano (in questo caso obbligavano) ai marinai di seguire la riga costiera e in qualsiasi occasione avevano la possibilità di attraccare lungo la riva africana per prendere provviste o trattare scambi con gli autoctoni.
Riguardo quelle popolazioni dell’africa occidentale non si possiedono sufficienti informazioni, ma restano alcuni reperti storiografici lasciateci dai navigatori stessi.
Tali reperti riportano di scambi e contatti periodici, ed essendo una micro economia vi era già il concetto di valuta e relativamente di “mercato”, e come tale vi era una forma arcaica moneta.

Le monete autoctone erano in realtà delle piccole perline dalla incerta provenienza, secondo alcune fonti erano di derivazione meteoritica e secondo altre discendevano da antichi residui di commerci fenici o egiziani di quelle zone in secoli precedenti il loro.
Questa valuta, dato che la lavorazione di quel particolare vetro ornato in quelle zone era onerosa e molto rara, risultava complessa da ricreare e dunque aveva un piuttosto alto rapporto tra stock e flow; un alto rapporto stock-to-flow, come suddetto, è la chiave per avere un bene duraturo e di valore nel tempo.
Gli europei, che erano stati reduci di ben peggiori carneficine e genocidi ad opera dei Conquistadores nelle Americhe, non si fecero scrupoli riguardo l'impoverimento totale di un'altra società, o forse semplicemente non si resero conto del disastroso epilogo delle loro azioni.
In breve dunque, quando si resero conto che l'economia locale si fondava su delle biglie che ai loro occhi non avevano alcuna reale valenza, ne portarono carichi pieni dall'Europa, ben più ricca di tale risorsa e di artigiani in grado di lavorarle.
Le popolazioni africane subirono un flow di immissione di liquidità enorme, e svalutandosi totalmente la loro moneta furono quindi obbligati a cambiarla.

3. **L'isola di Yap**

Un secondo esempio di manomissione del mercato locale da parte di un esterno fu quella a carico di un'antica popolazione originaria dell'Isola di Yap, sita negli attuali Stati Federati di Micronesia.
Questo piccolo arcipelago oceanico era abitato negli ultimi decenni del diciannovesimo secolo da popolazioni aborigene, in buoni rapporti le une con le altre.
L'isola di Yap e i suoi abitanti, gli yapesi, svilupparono un tipo di economia ai nostri occhi insolito, ma una più attenta analisi vi riscontrerà diverse analogie.
Alcuni studi e scritti riportano la presenza di grandi pietre cave di forma circolare chiamate Rai; queste rocce sparse per tutto il villaggio erano più o meno difficili da manovrare per via delle dimensioni e il peso ed erano la loro tipologia di valuta locale.
Queste pietre erano per lo più calcaree, materiale difficilmente reperibile in quella specifica isola, per questo si crede fossero originarie delle adiacenti isole di Palau o Guam.
La loro estrazione e il loro trasporto via mare richiedeva duro lavoro e molto tempo, specialmente con gli esigui strumenti premoderni dell'epoca.
Il flow ratio di quel contesto era dunque abbastanza alto e vennero adottate come moneta.
La dimensione dei massi era proporzionale al loro valore e data la difficoltà di trasporto fisico, per effettuare scambi interpersonali, invece che consegnarsi a vicenda tali sassi, vi era l'uso di dichiarare nella piazza del villaggio di voler eseguire la "transazione", in modo tale che la prova del loro avvenimento fosse la parola di tutto il villaggio.
Su questo particolare tipo di consenso mi soffermo brevemente per le dovute analogie e difformità con il sistema oggetto di questa tesi, Bitcoin.
Sebbene tecnicamente vi siano due secoli e mezzo di separazione, il concetto è rimasto il medesimo.
Nella popolazione degli yapesi vi era la tradizione di rendere pubblico a tutti i membri del villaggio un passaggio di proprietà di un bene da un proprietario A ad uno B perché essi facciano da garanti e testimoni.
All'interno del protocollo Bitcoin è presente una meccanica affine per far si che la transazione risulti pubblica: la blockchain (con funzione a tutti gli effetti di registro) sulla quale bitcoin si basa, ha la funzione di immagazzinare tutto ciò che tramite il protocollo

accade; è dunque possibile per chiunque visionare tutte le transazioni eseguite fino al momento presente, con tanto di quantità trasferita, codice univoco del portafoglio di invio e quello di ricezione.
La parte strutturale è che siano i membri del network stesso (cioè i membri del villaggio nel sistema degli yapesi e i minatori nel sistema Bitcoin, non un qualsiasi individuo interessato) ad approvare queste transazioni, cioè a conferire quello che in gergo tecnico viene chiamato appunto “consenso”.
Tornando però all’esempio:
Un destino non dissimile a quello delle popolazioni occidentali africane toccò agli yapesi, una seconda volta a causa dell’intervento europeo.
Un irlandese-americano di nome David O’Keefe approdò sulle coste micronesiane, tra le quali vi era anche l’Isola di Yap, con il solo scopo di commerciare delle noci di cocco con tali tribù.
Quello che egli provocò loro fu però ben più dispendioso di qualche commercio; non avendo idea di quale mezzo di scambio potesse usare per tali popoli, O’Keefe si mise a studiarli e si accorse che i massi sparsi nella zona erano molto più interessanti di quanto non sembrassero e una volta appresa la loro fondamentale funzione egli si diresse verso Hong Kong.
Nella piccola regione filo-cinese egli comprò una grossa barca e un buon quantitativo di esplosivo, con i quali poi si diresse nuovamente a sud verso la Micronesia, più nello specifico nella piccola isola limitrofa di Palau.
Lì egli usò la dinamite per accumulare pietre Rai e la capiente nave per stivarle, fece spola un paio di volte tra Palau e Yap.
Questo bastò per innescare un conflitto tra gli isolani; una parte di loro infatti reputava le pietre Rai ricavate mediante quella tecnica non propria della cultura cerimoniale yapese, come se fossero “indegne” del loro valore, mentre un’altra parte non badò alle questioni di purezza e iniziò ad accettare tali massi e a commerciarli normalmente.
All’aumentare dell’accettazione di tali Rai contraffatti, il valore di tutti i Rai diminuiva, decretando la fine di quella particolare moneta cerimoniale.



4. **Il baratto**

Le forme di moneta sono state le più disparate nel corso dei secoli, l’enjambement strutturale del loro funzionamento (che si manifesta concretamente nel mantenimento di tale forma nel tempo) è il più alto ratio possibile tra stock e flow.
Questo secondo tratto del paragrafo conterrà la storiografia della moneta nell’Antico

Continente, quello che per primo ha sperimentato i fisiologici crolli e crisi dovute alle forme di scambio economico e che per primo ha trovato metodi per arginare tali problemi e risolverli al meglio delle possibilità dell'epoca.
Le forme di scambio tra gli individui prima e i piccoli villaggi poi, accompagnano l'essere umano in tutta la sua storia.
La più intuitiva e rudimentale tra le tante era quella del baratto, che rappresenta il fulcro di un'economia di sussistenza.
Nelle piccole società, in cui i ruoli erano esigui e ben definiti tra chi svolgeva una mansione e chi un'altra, il surplus veniva barattato in cambio di altri beni dei quali si avesse maggiore bisogno.
Questa forma, in alcune sue sfumature, è presente ancora tutt'oggi, coprendo però una insignificante misura dei commerci al dettaglio e di informale entità.
Il baratto nell'antichità era per lo più composto da scambi di animali o di oggetti/ strumenti; i problemi riguardo agli animali e oggetti erano fondamentalmente rispetto a due delle tre proprietà di una moneta.
Rispetto agli animali il primo e più saliente problema era la loro deperibilità nel tempo, che non essendo beni durevoli non mantenevano lo stesso valore negli anni; ad esempio, se un carro veniva scambiato per un bue, il valore del bue negli anni diminuiva perché l'animale si indeboliva e rendeva meno al suo possessore, fino al divenire un costo.
Un secondo intoppo era la non scalabilità del baratto, sebbene si potesse scegliere in differenti zone del globo tra una vasta gamma di animali, se pensiamo ad un contesto desertico in cui il ventaglio di bestie domabili andava dal dromedario al cammello, non vi era molta scelta.
Si potevano scalare in una grezza misura, ma sarebbe come al giorno d'oggi fare la spesa con solo banconote da 100€ senza poter ricevere cambi in tagli più ridotti, si possono in ogni caso eseguire commerci ma sono approssimativi.
Il baratto di oggetti/strumenti ha invece un tempo di uso potenzialmente più lungo, un carro che viene mantenuto bene e periodicamente revisionato ha la stessa capienza che avrà 20 anni dopo.
Il problema anche in questo caso è l'indivisibilità degli strumenti e la relazione (soggettiva e individuale) con l'importanza che il compratore darà a tale scambio.
Un contadino in epoca feudale, che era obbligato a donare i 2/3 di quanto cibo producesse al proprio signore, arrivando a privare la propria famiglia di cibo, avrebbe soggettivamente dato molto più valore ad un sacco di grano in quel momento, che ad un gregge di pecore ad un anno da lì.
Un ulteriore problema è quello della ridotta trasportabilità, che non vi era tra il commercio di bestiame in quanto una fune poteva condurre 50 cammelli o un cane da pastore poteva guidare 200 pecore.
Quindi il fronte comune era quello di mettersi in comunione e formare una carovana o un possibilmente un piccolo convoglio.

5. **La coniatura**

Una successiva forma di commercio occidentale fu quella dei metalli.
Il metallo fu quindi la prima risposta ai suddetti problemi di deperimento, trasporto e scalabilità.
Di pari passo alla maggior raffinatezza nella produzione di questo a scopo produttivo, va il suo più intenso utilizzo in ogni scenario della vita quotidiana individuale e sociale, tra i quali quello qui saliente: quello monetario.
Si evidenziò come vi erano delle carenze strutturali in qualsiasi altro metodo fino ad allora utilizzato.

In particolare quindi, i metalli scelti per proprietà chimiche, durabilità fisica e di scarsità naturale erano, in quest'ordine: l'oro, l'argento, il rame e il bronzo (di derivazione dal rame e lo stagno).
Metalli più resistenti, come ad esempio il ferro, non vennero mai presi in considerazione per un'adozione più longeva, e ottennero inizialmente solo un ruolo di trascurabile entità nei primi e più esigui scambi commerciali; il motivo fu banalmente la loro tendenza alla corrosione, che disponeva di una scadenza temporale del valore anche quelle stesse monete alle quali si ricorreva per farvi fronte.
I metalli che citavo in precedenza invece hanno la caratteristica di essere più scarsi in natura e di conseguenza hanno un flow di immissione più contenuto.
L'oro e l'argento sono considerati parte dei cosiddetti "metalli nobili" (insieme a molti altri), propri cioè della particolarità di non essere soggetti a ossidazione e corrosione.
La loro scarsità e la loro durevolezza, assieme alle nuove tecniche di metallurgia che permisero di coniare delle piccole e maneggevoli forme circolari, resero così questi tre metalli i più blasonati, in particolare come tratterò di seguito, l'oro.

6. **La Monetazione Imperiale Romana**

Il grande impero che per primo introdusse la moneta in un'economia internazionale fu quello dei Romani (Monetazione Imperiale Romana), che nei secoli conquistarono un territorio ricoprente un area di circa 5 milioni di chilometri quadrati.
Ebbero così la necessita di incoraggiare e favorire il commercio interno tra popolazioni che prima di allora nulla ebbero in comune.
Egiziani e filo arabici con delle altre gaeliche e germaniche, riuscirono ad entrare in contatto, cosa che non sarebbe mai potuta avvenire senza un mezzo unitario.
La moneta di riferimento della Roma Repubblicana (509 - 31 a.C.) era il Denario, moneta d'argento di circa 4 grammi.
Successivamente, da altre zone del continente, vi furono le prime contaminazioni di monete d'oro.
Giulio Cesare, che fu l'ultimo dei famosi dittatori della Repubblica Romana, introdusse dunque l'Aureo, una moneta di 8 grammi completamente in oro.
L'aureo fu ampiamente accettato lungo tutte le coste del mediterraneo così come nelle più sperdute terre di dominio romano.
Vi fu stabilità monetaria per oltre 75 lunghi anni, fino all'assassinio di Cesare alle Idi di Marzo, data che decreterà l'inizio dell'epoca imperiale e al contempo, da un punto di vista storico, l'inizio del declino dell'onore del popolo Romano stesso.
Successivamente salì al potere Augusto, primo Imperatore romano e grande fautore del sistema monetario dell'epoca, che introdusse la Riforma Monetaria Augustea ed eresse delle regole intransigenti per scoraggiare la contraffazione.
Lo successe Nerone, che dal punto di vista numismatico apportò delle modifiche equiparabili alla riforma augustea, in quanto egli ritirò tutte le monete del regno fino ad allora coniate e le redistribuì con una grammatura minore, una dimensione precisa e standardizzata ed una minor proporzione di metalli preziosi al loro interno.
L'Impero Romano è stato per secoli uno tra i più prosperosi mai eretti, ma è crollato proprio a causa della propria cattiva gestione politico-economica.
Un Impero fiorente e ricco, abitua i propri cittadini all'agio.
Fintantoché lo Stato Romano conquistava nuove porzioni di terreno e ampliava i propri confini, i cittadini e i soldati potevano spendere i loro denari e sesterzi (gli aurei erano di grande valore, non i più comuni tra le tasche dei meno facoltosi) in quelle nuove terre, mostrando alle popolazioni locali quanto l'Impero fosse benevolo e magnanimo.

Alcuni imperatori, tra cui Nerone stesso, fecero negli anni dei periodi in cui addirittura regalarono il grano o ne dimezzarono il prezzo, chiaramente a spese dello stato.
Questi comportamenti diedero l'impressione di una ricchezza senza eguali e spinsero i cittadini delle periferie ad avvicinarsi a Roma, sperando così di essere i destinatari prioritari del prossimo favore delle élite nobiliari.
Mantenendo questo status di sfarzoso benessere, il sistema romano si ergeva ormai sull'acquisizione di nuovi territori, quasi forzata, dando speranza a loro volta agli abitanti di quei nuovi territori di poter attingere da quello stesso abbondante paniere.
Il vecchio continente però stava esaurendo i ridondanti territori conquistabili, e un'economia così imponente che trascura il sostentamento, prima o poi è destinata a crollare.
La riforma di Nerone servì in particolar modo a fronteggiare questo atteggiamento lavativo, fece diminuire il valore delle monete e così anche il salario dei contadini e dei soldati decrebbe a loro volta, dando più margine allo stato di finanziare altri versanti pubblici.
Con Nerone l'aureo pesava non più 8 grammi ma 7,2; con Caracalla sfiorò i 6,5 grammi e con Diocleziano addirittura scese a 5,5 grammi per aureo.
La popolazione certamente non rimase amorfa a tali magheggi, vi furono rivolte e ribellioni.
Diocleziano dunque cambiò di fatto nome a tale moneta, cambiando così anche la percezione dei cittadini e sulla carta coniò una nuova moneta, la quale divenne il Solido Romano, composto da 4,5 grammi d'oro.
Dal periodo dioclezianeo in poi, nel Denario non vi erano quasi più tracce di argento, se non per coprire il cuore di bronzo, fino a scomparire totalmente qualche anno successivo, decretando l'epilogo del ruolo del Denario come moneta corrente imperiale.
Il minor peso cadauna permetteva con la stessa riserva erariale di emanare il doppio del circolante, provocando un'ingente stagflazione dal quale l'Impero Romano d'Occidente non si sarebbe mai più rialzato.
Vennero eseguite altre manovre per tentare di arginare la depressione in atto: al dimezzamento del valore monetario seguì un raddoppio dei prezzi, venne di conseguenza impostato un tetto ai prezzi di mercato e questo non fece altro che impoverire ancor di più i cittadini e bloccare l'economia.
Iniziò un violento indebitamento a carico dello stato, che sprofondò in un circolo di gestione di un potere d'acquisto doppio rispetto a prima, aumentando il circolante e di conseguenza la possibilità di spesa dello stato stesso e l'inflazione e la crisi economica.
Le conseguenze a lungo termine furono devastanti.

7. **Il fiorino**

Un secondo periodo di riforme e cambiamenti in ambito monetario fu il Rinascimento, in un'Europa spettatrice del crollo dell'Impero Romano d'Occidente e che in pochi decenni si riassettò in feudi, il benessere palpabile della precedente epoca venne rimpiazzato da una sottomissione quasi totale dei cittadini, ora poco più che meri servitori, al loro signore feudale.
Le monete erano per lo più composte da bronzo e rame, poco onerose da manipolare ed incrementare da parte dei signore, grazie anche all'avanzare della tecnologia in campo metallurgico.
Non più riserve di valore e spesso differenziate da feudo a feudo spezzando la florida continuità commerciale creata in precedenza, i servitori non possedevano più patrimoni da cui poter attingere grazie ai propri avi, così come era quasi impossibile che lasciassero qualcosa a loro volta ai loro figli.
E anche se avessero avuto qualcosa, avrebbero dovuto affrontare una vorace tassazione e un'erosione dovuta all'inflazione in continua crescita.
Questa fu in generale l'atmosfera medioevale, l'epoca dei Secoli Bui.
Fortunatamente però in seguito ad un declino vi è un risorgimento, un Rinascimento culturale, artistico, politico e fisiologicamente economico.
Il Rinascimento iniziò attorno all'anno 1250 ed è interessante osservare come, ancora una volta, sia l'economia a condurre la maggior parte degli altri aspetti della vita della società.
La culla del Rinascimento fu Firenze, e con ancora una volta epicentro in Italia, dunque iniziava un'epoca di raggiante maturazione.
Alla corte fiorentina iniziarono ad essere coniati i fiorini, la valuta europea più solida dopo l'aureo romano.
La reputazione e l'autorevolezza che Firenze ottenne in quegli anni rese la loro moneta un efficace e riconosciuto mezzo di scambio in gran parte del Vecchio Continente.
Venezia, altra città che ha conosciuto nel rinascimento il suo massimo splendore, coniò dopo pochi anni il Ducato Veneziano, su dimensione e peso del Fiorino fiorentino.
Ben presto più di 150 corti in Italia e Francia coniarono la propria valuta su modello del Fiorino, le banche (istituzione già affermata in epoca romana, nel frattempo però il settore bancario era ben più capillare e prestante rispetto al passato) ritornarono a collaborare tra loro attraverso tutto il continente.
Vi fu così nuovamente modo per i popolani di accumulare benessere attraverso una valuta di riferimento spendibile su larga scala e che fosse riconosciuta ed ancorata ad un determinato valore.
Che sia Roma, Costantinopoli, Firenze o Venezia, alla base di una virtuosa economia vi sono le 3 proprietà della moneta che elencavo inizialmente: scalabilità, durevolezza e maneggevolezza.
Una volta garantiti tali attributi, è necessario che vi sia un alto ratio stock-to-flow tra il circolante e l'immissione.
L'epoca rinascimentale era però lontana dalla conclusione dell'itinerario verso l'economia autosufficiente.
Oltre il fatto che occasionalmente vi erano delle monete alternative che si introducevano nelle economie europee, vi furono delle questioni strutturali che vennero allo scoperto.
L'uso dell'oro era infatti tornato in auge, ma rimaneva elitario e spesso relegato a riserva di valore o ai grandi trasferimenti/ acquisti.
La moneta maggiormente circolante era in ogni caso argentea, di minor valore e utile anche per acquisti mondani o secondari.
Vi era un tasso di cambio tra i due metalli nobili, i quali erano complementari l'uno all'altro

nella quotidianità di corte.
Questo tasso di cambio non era fisso e seguiva la domanda e l'offerta di mercato.
La forte fluttuazione dovuta allo scambio di oro e argento creò a lungo andare delle problematiche interne, vi furono nel tempo delle precauzioni ma senza risultati in grado di migliorare la situazione.
Il duale sistema monetario perdurò per secoli in Europa e nel mondo, traversando dalle conchiglie, al sale ad altri metalli minori.

8. **La svolta del settore bancario**

Facendo ora rapidamente qualche passo avanti nei secoli, vi sono due importanti tecnologie che stravolsero la concezione di trasferimento di denaro dell'epoca: il telegrafo e i trasporti ferroviari.
Il telegrafo (1837) rese le comunicazioni tra istituti bancari di diversi paesi europei relativamente immediate, permettendo di trasferire una forma di debito/ credito da una banca all'altra senza la necessità di esporsi al trasporto fisico di un quantitativo di ricchezza.
Quando questo però era necessario, la rete ferroviaria ormai presente in maniera capillare attraverso quasi tutte le maggiori città europee lo permetteva con discreta semplicità.
Il movimento di valore reale venne rimpiazzato da assegni, fatture, ricevute e cambiali.
Il concetto di valuta nominale con un sottostante reale in metalli preziosi prese ben presto piede in tutto il continente; alcuni paesi scelsero l'oro come sottostante e altri l'argento, ma il concetto era il medesimo.
Questa scelta che di primo acchito poteva parere senza conseguenze, ben presto ne ebbe.
L'oro si rivelerà in seguito la scelta più oculata, mentre l'argento la più catastrofica.
Il primo paese ad adottare a tutti gli effetti una riserva di controvalore in oro fu la Gran Bretagna, che essendo nel 1717 il paese più ricco del globo, influenzò una schiera di nazioni a fare lo stesso.
La Gran Bretagna rimase profondamente legata all'oro fino al 1914, anno più che inedito per la storia occidentale moderna e per l'impellente necessità di enormi capitali.
Per quasi due secoli fece da traino al resto dell'occidente, vi fu solo l'intermezzo napoleonico ad interrompere tale adozione aurea, la quale venne poi ripresa attorno al 1820 al momento del loro epilogo.
Più banche nazionali adottavano l'oro come riserva di valore governativa e più questo era vendibile e diventava un asset liquido (la liquidità di un asset è la facilità con cui un venditore di questo asset riscontra un compratore nel mercato), con l'aumentare della domanda cresceva fisiologicamente anche il prezzo del metallo; il tutto dunque si muoveva ormai solamente dietro i caveau delle banche, non più agli occhi degli individui.
Le banche nazionali, a nome del paese stesso, emettevano cartamoneta in quantità equivalente alle corrispettive riserve auree fisicamente presenti nei confini territoriali, non vi era più spazio dunque nei paesi occidentali per il ruolo dell'argento.
Paesi che in precedenza adottarono la riserva nazionale in argento furono obbligati a trasferirla in oro il prima possibile e ne uscirono comunque sensibilmente impoveriti.
L'India abbandonò definitivamente l'argento nel 1898, mentre la Cina e Hong Kong sono state le ultime economie al mondo ad avere un corrispettivo in argento, fino al 1935, più di 220 anni in ritardo rispetto ai primi paesi occidentali.
La scelta di queste due super potenze ha influenzato tutto il loro ventesimo secolo, esprimendosi in un tenace inseguimento verso le nazioni occidentali arricchitesi all'inverosimile, ma questa differenza si sta appianando in questi primi decenni del

ventunesimo secolo.
La quasi totalità dell'intero ammontare delle riserve auree globali si trovava dunque stivata in questa o quella banca centrale, l'oro guadagnava così vendibilità attraverso il tempo, lo spazio e in scala, di conseguenza aveva però perso il ruolo di principale attore delle trattative interpersonali e di contante.
Le forme di pagamento non erano più materia di interesse individuale: bensì governativa, garantendo maggiore sicurezza da un lato, ma rendendo al contempo i pagamenti condizionati a quelle che erano le autorità finanziarie e politiche.
L'oro come standard nel diciannovesimo/ventesimo secolo era ciò che di più simile il mondo avesse conosciuto come "moneta ideale", ma non era ancora perfetto.
La prima ragione era quella che i governi (di ogni dimensione e tipologia) continuassero imperterriti a diffondere denaro che surclassasse le reali quantità dell'oro da essi stivato nelle proprie riserve.
L'intenzione, non volendo risultare maliziosi, era presumibilmente quella poi di ritornare al rapporto 1:1 con le proprie scorte, il surplus poteva servire temporaneamente per alcune manovre economiche "urgenti".
Resta il fatto che se il ratio non fosse rientrato il prima possibile sarebbe risultato minaccioso per lo stato stesso.
La seconda ragione era quella che le banche detenessero al loro interno non soltanto oro, ma anche un quantitativo di valuta di stati altrui.
La Gran Bretagna, che come accennavo in precedenza divenne in quegli anni la potenza economica di riferimento e dal quale il resto del mondo in maniera più o meno accentuata era dipendente, era nell'immaginario comune talmente affidabile da offrire la propria valuta stessa come riserva di valore, al pari e/o al posto del sottostante aureo, considerata la cartamoneta inglese "As good as gold": solida al pari dell'oro[21].
Considerandolo analiticamente era letteralmente impossibile che il solo Regno Unito potesse fornire alla propria sterlina un corrispettivo paritario a quello dell'economia totale o parziale di un insieme di altri stati sovrani, in quanto era letteralmente impossibile che il Regno Unito disponesse di una riserva aurea equivalente a tutto il circolante che vi era presente nel proprio regno e al contempo in molte banche degli stati altrui.
L'oro è ed è sempre stato, una moneta forte e a suo agio nei panni del ruolo che nei secoli ebbe.
Il suo problema fu l'utilizzo che ne è stato fatto dalla società, gli strumenti sui quali le banche si basavano e con i quali operavano erano più semplici da produrre di quanto il loro sottostante non fosse da estrarre.
La vulnerabilità dell'oro sta nel fatto che non sia in grado di soddisfare contemporaneamente tutta la popolazione che voglia riconvertire i propri soldi cartacei in esso come corrispettivo, per il banale motivo che non è abbastanza per tutti.
La falla di questo sistema aureo e dei due problemi suddetti, è di conseguenza sempre stata la regolamentazione governativa, macchinosa, costosa e incerta.
Le riserve d'oro sono state costrette in banche centrali dislocate in poche località dei paesi, tralasciando la comunicazione e la trasparenza con la restante società che era il vero protagonista di tali scambi.
I cittadini non avevano alcuna garanzia che vi fosse un corrispettivo, non avevano un registro affidabile che certificasse dove fossero le riserve, l'oro per sua essenza non permetteva questi meccanismi.
L'ammontare di transazioni aumentava inoltre di giorno in giorno e la loro mole comprendeva ormai trasferimenti anche di pochi centesimi.
Al giorno d'oggi sarebbe impensabile per esempio pagare un caffè 1€ e far trasferire di conseguenza dalla propria banca di riferimento della polvere d'oro del peso di 0.0173 grammi alla banca di riferimento del barista, è chiaro come sia notevolmente più immediato creare quella moneta da 1€. (Al tasso di cambio odierno)[22]

Dal momento in cui i governi hanno inglobato le riserve auree, centralizzandole, si sono diramati diversi approcci da parte della società.
- Una branca che può definirsi "Nazionalista" combatté lo status dell'oro come standard per il principale motivo di non lasciare il proprio paese alla mercé del mercato globale, volendo stabilire un'autarchia.
- Una seconda branca di "Interventisti" ritenne l'oro il più solido ostacolo al loro sforzo di manipolare i prezzi e tassi salariali.
- Un terzo gruppo di non meglio specificati "bramosi di credito" ritennero che lo sviluppo di un paese e la sua espansione creditizia fossero il rimedio univoco dei disguidi economici.
"La storia non è ciclica, gli uomini lo sono" - questa frase di provenienza sperduta nell'anonimato è valida sia per eventi storici sia per quelli a sfondo economico.
Spesso infatti si rimanda alla ciclicità della storia in ambiti belligeranti, tradimenti, tirannie, rivoluzioni etc.
Così come banalmente nel mercato, che segue un movimento ondulatorio e percorre a ripetizione periodi di forte soddisfazione e forte depressione.
I governi non sono altro che associazioni di individui, che come sempre nella storia dell'essere umano dotato di raziocinio, procacciano il proprio interesse prima di quello collettivo.
Non voglio parlare per luoghi comuni o per dati di fatto, il principio può anche essere nobile alle sue origini, come emanare moneta per saldare tutti i debiti della popolazione in un unico giorno invece che nei prossimi 15 anni.
Ma il disegno complessivo è più grande e all'interno di un'equipe governativa, in cui presumibilmente vi sono delle élite di economisti (o quantomeno qualcuno di preparato), dovrebbe essere chiaro quanto non valga mettere a rischio l'intera economia del paese per ottenere la candidatura del proprio partito o una risaltante pubblicità o non perdere la propria reputazione personale.
Deve essere chiaro al popolo quanto sia fallace questo sistema, quanto non possa reggere uno standard in cui se uno stato necessita liquidità può procurarsela autonomamente stampandosela.

9. **Il deposito aureo demaniale durante la Grande Guerra**

Il ventesimo secolo è iniziato con l'oro di dominio nazionale e che con esso provvedeva ad un circolante sulla carta equivalente.
La situazione geopolitica europea e ben presto globale divenne più concitata e grave.
La prima guerra mondiale era alle porte ed era necessario disporre di armamenti e di un'economia forte; non a caso il termine di adozione dell'oro come controvalore per molti stati coinciderà con il medesimo anno del loro ingresso nel conflitto.
Come anticipavo, era necessaria un'economia forte, resiliente a grandi contrazioni e a imminenti grandi spese, anche dalle nazioni non economicamente (e purtroppo non offensivamente, come il nostro Bel Paese) forti, era richiesta un'economia in grado di fronteggiare tale sfida, come successe in precedenza durante le guerre Napoleoniche,
occasione in cui la Gran Bretagna (ribadisco uno dei paesi più prosperosi dell'epoca) duplicò con un decreto le proprie casse statali, slacciandosi ovviamente dall'oro.
Anche durante la Grande Guerra è avvenuta la stessa manovra fiscale, mascherando tale aumento con il continuo rilevamento dell'oro rimasto ai civili da parte di forze governative, facendo risultare l'aumento di capitale come naturale, dato l'aumentare delle riserve.
L'epilogo della guerra fu da un punto di vista meramente e cinicamente economico più dannoso della guerra stessa: il settore primario di tutta l'Europa venne decimato e

divennero le donne le vere protagoniste chiamate a sostenere la patria, in patria.
Il settore industriale venne quasi totalmente focalizzato nell'industria pesante e riconvertirlo richiese spese e mesi di dedizione.
Gli stati mondiali si divisero, tranne che per qualche raro caso di neutralità o di ambivalenza, in vincitori e perdenti.
Entrambe le sponde videro in modo più o meno drammatico la loro economia sfaldarsi.
Gli unici che non ne uscirono visibilmente danneggiati, ma anzi con degli importanti creditori, furono gli Stati Uniti.
Gli USA impersonarono un decisivo contributo in questo conflitto così come in realtà in quello a venire, disponendo di un intero oceano di distacco dai missili tedeschi; non ebbero mai timore dei bombardamenti su suoli interni, ebbero al contrario sempre tempo e modo (relativamente) di gestire strategicamente le provvigioni e gli sbarchi e trovarono, giustamente, dei punti di approdo costieri dai quali non rischiassero di essere respinti.
I paesi europei originari della Triplice Intesa, cioè Francia, Gran Bretagna e Russia, si indebitarono profondamente con gli USA per ottenere rifornimenti di armi e viveri.
L'Italia poco più tardi si alleò con questo schieramento sperando di poter sedere al tavolo dei "vincitori", ed essendo tra questi il paese più povero economicamente ne uscì ugualmente indebitato, sebbene non avesse ricevuto ingenti aiuti oltreoceano.
Inoltre essendo stata per una buona parte del conflitto una parte nemica, non venne vista come alleata e non ottenne null'altro che il Trentino Alto Adige e il Friuli Venezia Giulia; per queste ragioni D'Annunzio nel 1918 la definì una "Vittoria mutilata".
Se i paesi vincitori si indebitarono sensibilmente per riuscire a prevaricare militarmente sui propri nemici, i paesi perdenti vennero multati per i loro crimini di guerra e fondamentalmente divennero a loro volta fortemente debitori verso i vincitori, oltre che verso gli Stati Uniti.
A livello economico questo si tradusse in un'inflazione madornale, specialmente per gli sconfitti.
La valuta nella quale gli Stati Uniti pretesero il loro credito fu ovviamente fine comune alla loro supremazia, il dollaro statunitense surclassò la sterlina e divenne la valuta di riferimento per gli scambi internazionali e le riserve di valore erariali.
Il dollaro assunse il ruolo di caposaldo in quasi ogni settore di mercato che uscisse dai confini nazionali, ma spesso divenne fondamentale anche in alcuni mercati nazionali, i quali ragionavano in dollari invece che nella loro propria valuta.
I paesi extra-USA sarebbero interessanti da analizzare cadauno per antecedenti storici e peculiarità sociali, ma il filo conduttore tra tutti è stato il forte indebitamento e la crescente inflazione negli anni successivi.
Un esempio peculiare e straordinario è stato quello tedesco[23].
La Germania fu una nazione che per ovvie motivazioni fu più duramente colpita dalle sanzioni dell'Intesa, condannata a pagare un debito di 22 milioni di dollari.
Per inciso, negli anni 20' il potere d'acquisto del dollaro era più di 100 volte superiore a quello di oggi, un dollaro permetteva di comprare 2,3 kg circa di zucchero (che all'epoca richiedeva molta più lavorazione del giorno d'oggi) e fino a pochi anni prima 1$ bastava per comprare un vestito per signore.[24]
Nel giro di circa due anni dalla fine della Grande Guerra vi fu la prima insolvenza, che causò la sottrazione da parte del governo francese e belga dei territori, già da anni contesi, della Ruhr, una zona molto ricca e garanzia di molti posti di lavoro e siti di estrazione per la Germania.
La Germania (o all'epoca l'Impero Tedesco) aveva sempre avuto un'economia poderosa e autosufficiente, ma non fu abbastanza per far fronte alle spese belliche e al conseguente debito attribuito dai vicini stati europei.
Per far fronte a una prima parte di questo l'Impero emanò una quantità di cartamoneta enorme, molto più di quanto possedesse nelle proprie riserve statali: questo si tradusse in

un'inflazione devastante (che iniziò a manifestarsi già negli ultimi mesi di conflitto, ma che esplose successivamente), nel ratio di cambio delle valute dollaro - marco tedesco il rapporto era di 1:35.000 nel gennaio 1923, 1:350.000 nel luglio 1923, arrivando al picco di 1 dollaro equivalente a 4.200.000 miliardi di franchi in dicembre 1923.
Il marco tedesco valeva meno della carta.[25]
Gli operai e in generale i lavoratori venivano pagati a giornata e non appena ricevevano il salario si affrettavano a liberarsene spendendolo, perché già il giorno successivo era abituale il fatto che i prezzi impennassero anche di un 100/200%.
Il tracollo pareva (e a tutti gli effetti era) ormai vicino, ma così come in ottica micro economica un individuo nulla tenente non può saldare i propri conti, così uno stato in default economico non può saldare i propri debiti di guerra.
Gli Stati Uniti considerando tale lineare logica hanno iniziato ad investire i propri capitali in Germania, sfoderando come spesso accade in queste situazioni politiche una lama a doppio taglio: mantenere in auge un intero paese così da perpetuare il flusso nelle proprie casse e al contempo assicurarsi di aver investito in uno stato con evidenti difficoltà, così da avere potere decisionale nella loro economia e avere ulteriore beneficio quando essa si riprenderà.
Dunque comprarono il loro debito e con esso una buona parte dei loro istituti bancari.
Il governo tedesco, con a capo il suo cancelliere, all'epoca Gustav Stresemann, alleggeritosi di un considerevole pegno, ebbe la forza di prospettare una manovra raramente avvenuta in epoca moderna, con il fine di cambiare la propria valuta, che ormai aveva valore pari a zero, e stabilirne una nuova.
In tutto il paese la moneta corrente passò dunque dal PapierMark al ReichsMark[26] , con un valore stabilito a tavolino di 4,2 dollari americani (un rentenmark equivaleva a 10 triliardi di papiermark).
La Germania così, lentamente, si risollevò dalla opprimente situazione nella quale si trovava.
Gli anni seguenti furono altrettanto ricchi di vicissitudini storiche, ma da un punto di vista monetario questi non afflissero molto l'economia.
È degno di nota considerare il punto di vista del mercato azionario, che in quegli anni vide la sua nascita e purtroppo anche la sua prima grande bolla speculativa.
Anche in questo caso ma in diversa forma, si nota come una ricchezza data per scontata possa rivelarsi poco certa.
La Grande depressione però intaccò in misura minore la valuta dei grandi stati, quanto piuttosto la credibilità delle grandi società per azioni e delle banche americane.

10. **Il grande indebitamento fra stati**

L'epilogo di questo paragrafo sulla storia della moneta vede come protagonista il 37esimo presidente americano Richard Nixon, il quale, essendo in carica nel bel mezzo di un conflitto armato realizzatosi nelle lande della regione indocinese contro i Vietcong di Ho Chi Minh e indirettamente con l'URSS, diede lascito a una manovra monetaria che è rimasta nella storia come "The Nixon Shock".[27]
All'inizio 1971 alcuni ricchi stati orientali come il Giappone stavano iniziando a competere seriamente con gli Stati Uniti, le spese della guerra corrente appesantivano il paese e serviva una svolta politico-economica.
La trovata del governo Nixon fu quella definitiva di auto produrre lo standard monetario, traslare dal fondare l'economia sul bene rifugio aureo ad una valuta governativa: il dollaro.
Questa non era una vera e propria novità, come abbiamo visto in altre occasioni (spesso e purtroppo simili a questa) vi è stata la medesima risposta alla situazione geo-politica; la

vera differenza in questo caso fu la consapevolezza di tale decisione: non era stata concepita come una finestra temporale fine a se stessa, in questo caso la decisione era definitiva.
Gli Stati Uniti slacciarono la loro economia da una moneta che da oltre 2000 anni aveva dimostrato di aver mantenuto la propria funzione in favore di carta filigranata stampabile tramite una zecca di stato.[28]
Nel primo paragrafo ho già affrontato individualmente il tema delle origini di Bitcoin, accodandolo però a questa esplicazione è possibile notare come il suo protocollo colga tutte le facoltà di una moneta pura e respinga tutte le possibili manomissioni umane dettate da impulsi come avarizia, egoismo o spinte offensive.
Bitcoin non è stato ideato per essere giusto o sbagliato, bensì equilibrato.
Non rincorre i bisogni di breve periodo ma ha come fine quello di mantenersi e imporsi nel lungo.
Riprendendo l'introduzione a questo paragrafo in cui mi soffermavo sulle peculiarità di una moneta, è possibile concludere come Bitcoin sia:
- scalabile (21.000.000 di Bitcoin divisibili in 100.000.000 Satoshi cadauno)
- durevole nel tempo (alcuni vengono ingannati dal fatto che il prezzo di bitcoin oscilli giornalmente, ciò accade poiché lo equipariamo al dollaro, ma anche il dollaro oscilla rispetto ad altre valute: eppure 1 dollaro oggi è 1 dollaro domani, così come 1 bitcoin oggi è 1 bitcoin domani)
- trasferibile nello spazio senza sforzi.
Queste peculiarità sono proprie anche delle valute FIAT (anche se tecnicamente FIAT sta a significare che vi sia un corrispettivo sottostante).
La reale differenza strutturale è la diversità nell'approccio stock to flow: mentre le valute tradizionali odierne hanno un ratio pari a zero, poiché il flusso di immissione non è faticoso da ottenere, bitcoin ha un flow che richiede grande potenza di calcolo giornaliera, che punisce tramite il proprio network chi cerca di raggirare il protocollo, con una "ricompensa" per potenza computazionale che ogni 4 anni viene algoritmicamente dimezzata per mantenersi equa rispetto al sottostante in dollari.
Fino ad arrivare ad un rapporto del 100%, si stima attorno al 2140, con il limite dei 21 milioni.

- CAPITOLO SECONDO -
RAPPORTI CON LA SOCIETÀ

1. **Diffusione e rapporto coi singoli paesi**

Bitcoin ha avuto, sin dalla sua immissione e albori di utilizzo, delle risposte controverse da parte di bacini di utenza di piccole e grandi dimensioni, così come da parte dei diversi stati sparsi in giro per il mondo, ognuno con una propria storia, una propria politica e delle diverse priorità.
È molto interessante notare come, analizzando alcuni giornalisti indipendenti o riviste del settore, si possa cogliere un più o meno evidente cambiamento nelle zone del mondo più affini a queste innovative forme di economia.
L'aspetto fondamentale però che accomuna ognuno di questi paesi è il seguente: lo strumento pionieristico delle criptovalute viene applicato maggiormente in due segmenti di nazioni, quelle estremamente aperte all'innovazione e all'introduzione di nuovi artefatti, che non casualmente sono spesso prime nella lista degli stati patria del maggior numero di milionari in rapporto alla popolazione, come per esempio la Repubblica di Singapore, Hong Kong e la Svizzera, le quali a livello finanziario sono tra le più all'avanguardia globalmente; viceversa invece quegli stati con un regime di discutibile o del tutto nulla libertà personale, oppure con un ratio di povertà assoluto, come la Russia, il Vietnam, alcuni paesi centroafricani.
A livello di nazioni funziona, seppur ovviamente con una prospettiva diversa, quel che affermavo in principio, ossia che le cripto vengono prese in considerazione da due tipologie di soggetti: chi crede nell'ideale sottostante e sviluppa in maniera armoniosa una serie di infrastrutture per accoglierle, e chi invece, alla guida di un paese che opprime in diverse materie si trova a doverle vietare, proibire e a "cacciarle" in quanto vanno a minare la propria supremazia.
In questo capitolo mi spingerò dunque a trattare il rapporto che a livello quotidiano Bitcoin sta riscontrando nelle diverse zone del globo, soffermandomi su alcuni esempi come unici e iconici di ognuno dei passaggi che si stanno vivendo nel tema dell'avanzamento di questa tecnologia nella società; tratterò inoltre i motivi sociologici e politici che sostengono tali approcci.
La diffusione delle valute digitali si è diffusa dal 2008 (tecnicamente il 2009) in poi, coprendo rami differenti della finanza che spaziano dalla riserva di valore del quale Bitcoin ha fatto il proprio caposaldo, agli smart contract dei quali invece Ethereum è principale attore, criptovalute per i prestiti, criptovalute per gli scambi di valuta decentralizzati ed NFT ("Non Fungible Token", delle stringhe di codice che hanno un'unico formato e si traducono in immagini ".jpeg" di elevata scarsità, alcuni le paragonano ad opere d'arte in digitale, non per l'estetica ma per il loro grande valore).
Ci sono per ognuna di queste macro categorie un numero ingente di progetti e ogni giorno ne nascono di nuovi.

2. **Prospettiva costruttivista dell'innovazione e modello di Rogers**

La prima valuta a fare breccia nel sistema è stata per banali ragioni cronologiche Bitcoin, come ho già sottolineato tramite una lunga serie di forum e anfratti di internet.
Bitcoin è stato a tutti gli effetti il progetto pionieristico che ha dato voce all'esigenza di libertà intesa in termini soprattutto di decentralizzazione; come ogni nuova tecnologia vi sono delle fasi e degli attori fondamentali facenti parte del loro processo costruttivo; il

modello in questione è riconducibile allo SCOT: Social Costruction of Technology (Costruttività sociale della tecnologia).
Questo modello esposto per la prima volta da Thomas Kuhn tra gli anni sessanta e settanta del novecento, tratta ogni artefatto o innovazione tecnologica come una sinergia di contributi dati da numerosi attori, il bisogno stesso di cambiamento è per esempio considerato una leva traducibile in "cooperazione".
Ogni innovazione mai ideata ha/ ha avuto comunque la struttura fondamentale del "Quadro tecnologico", in altre parole il contesto socio-culturale attraverso il quale tale innovazione è stata plasmata.
Ogni manufatto che oggigiorno noi utilizziamo o banalmente conosciamo è il prodotto di elaborazioni metodiche ad opera di pensatori o studiosi, i quali hanno partorito invenzioni che più si adattassero al loro quadro tecnologico di riferimento.
Il protocollo Bitcoin è stato in ogni caso l'apripista di ogni altra valuta digitale organizzata e sostenibile nel lungo periodo.
L'adozione è avvenuta gradualmente dapprima tra gli unici terminali della categoria degli "innovatori".
La prima delle fasi introdotte infatti da "Il modello di diffusione delle innovazioni" di Everett Rogers è proprio questa, si traduce nel fatto che vi siano un numero estremamente ristretto di utenti di tale tecnologia, che spesso coincide con gli inventori stessi e qualche piccola cerchia attorno a loro formata da amici e parenti.
Come ho detto in precedenza il primo blocco di Bitcoin è stato eseguito da Satoshi stesso e le prime transazioni da un numero ridicolmente ridotto di individui.
I facenti parte di questa prima fase non hanno aspettativa (o quantomeno non dovrebbero averne) sulla riuscita di tale programma; a questo proposito alcuni studi riportano non tanto le tecnologie esistenti e ancora vigenti, seppur riviste e modificate nei decenni/ secoli/ millenni, bensì le tecnologie che non hanno ricevuto un riscontro positivo dal pubblico.
A proposito di questo infatti io ho riportato l'esempio di David Chaum, di DigiCash e del suo innovativo apporto chiamato "Blind Signature" (firma cieca), questo progetto non si era fermato propriamente allo stato di "innovazione", anzi ha ottenuto diverse offerte ed era dunque approdato quasi in una diffusione di maggioranza.
Questo a riprova del fatto che in realtà in nessuna delle fasi che andrò a descrivere non vi può essere una caduta, dovutamente a cause esogene o endogene; il rischio di fallimento è plausibile all'interno di ogni realtà, anche le più affermate, dal contesto tecnologico al contesto economico/aziendale.
Le pitture rupestri di uomini impugnanti un arco risale a più di 3000 anni fa, sono state ritrovate delle pitture rupestri in alcune grotte in Asia raffiguranti queste armi in scene di caccia.
L'arco da allora ha subito numerosissime variazioni, miglioramenti al peso, all'aerodinamica e l'equilibrio dei propri materiali costruttivi e delle frecce che con esso venivano scoccate, le quali a loro volta differivano in base al filo, al materiale della punta o alla lunghezza.
Vennero ideate differenti misure e differenti accordi in base ad ogni tipologia di necessità: pesante e preciso da difesa delle mura o il più maneggevole e versatile arco da assedio.
Vi sono evidenti differenze tra gli archi corti di matrice romana, archi lunghi scandinavi, archi celtici o iberici, vi sono successe nei secoli delle diramazioni fondamentalmente diverse come la balestra e corrispettivi dardi, sulla falsa riga delle frecce.
L'arco ha avuto modo di essere analizzato e perfezionato in ogni maniera in cui potesse essere progettato. Questa tecnologia era ottimale, efficace e furtiva.
Il sistema arco e frecce funzionava alla perfezione, quanto però questa tecnologia sia stata la più performante nel proprio ambiente (frame), è improvvisamente diventata obsoleta con la scoperta di una tecnologia ancor più rivoluzionaria: la polvere da sparo.
In alcune zone del mondo le popolazioni indigene restarono a distanza da questo artefatto, sia per ragioni banalmente geografiche sia ideologiche; il progresso però imperterrito proseguiva e spodestava le popolazioni che non lo abbracciavano.
Il paradigma era cambiato, l'arco non aveva più nessun confronto con il moschetto e

passò dall'essere l'arma più tecnologicamente avanzata esistente dalla lunga gittata ad una mera disciplina sportiva di nicchia, che questo fosse evidente o meno.
Seguendo questa analogia un po' bislacca, secondo la mia visione, l'arco è il sistema bancario attuale e Bitcoin il fucile.

3. **La diffusione a goccia d'acqua**

La diffusione che sussegue la fase iniziale dell'innovazione procede figurativamente a "goccia d'acqua" o "trickle-down", citando in questo caso invece le teorie di George Simmel (definito non per niente "Il più contemporaneo dei classici") sui fenomeni sociali legati alla diffusione delle mode.
Come anticipavo e come il "modus operandi" di ogni introduzione nella nostra società, dapprima il gruppo non manifesta alcuna intenzione di avvicinarsi a tale tecnologia o, nella maggior parte delle casistiche, non è nemmeno a conoscenza della sua esistenza.
La diffusione a goccia d'acqua (su certi manuali viene etichettata anche come "a cascata") preclude il fatto che vi sia un epicentro rappresentato dal primo fruitore di tale invenzione, verosimilmente nella totalità dei casi è il suo creatore o equipe di creatori, che tramite i diversi mezzi mediali offerti in base all'epoca storica ha la possibilità e la volontà di diffondere tale manufatto al proprio pubblico di riferimento.
Il tratto inserzionistico è per molti versanti più impervio di quello della strutturazione stessa del progetto, via via però l'idea si condivide e un numero leggermente maggiore limitrofo al nucleo iniziale, incomincia ad usufruirne.
In passato Simmel teorizzò questo modello ad indice del fatto che non vi fossero mezzi mediali diffusi o digitali, bensì locali e analogici; si procedeva per passaparola, per giornali e annunci che si trasmettevano di paese in paese, di città in città.
Quindi così come una cascata nasce da un unica sorgente e si immette totalmente in uno specchio d'acqua, l'informazione viene emessa da un unico attore e si espande "a ondate".
Suppongo che con il passare dei secoli questo modello sia leggermente mutato, non vi sia più cioè un unica breccia attraverso la quale confluisce il progresso, piuttosto invece che vi siano numerose piccole gocce d'acqua che permeano la società e che si espandano.
L'utilizzo dei social e dell'informatica ha reso invisibili delle barriere che in passato erano insormontabili, come quelle morfologiche o linguistiche, permettendo ad una tecnologia come Bitcoin di provocare attrazione indipendentemente da esse, facendo perno sul fatto che vi sia un interesse comune a tutta la popolazione mondiale, cioè l'economia.
Non è difficoltoso come lo era 2 secoli fa, per un costrutto promettente e ben costruito, venire importato in altri paesi e creare un nucleo dal quale espandersi indipendentemente da quello originario.

4. **Early adopters e primi exchanges**

Dallo sporadico e superficiale interesse, l'oggetto dell'innovazione è materia di attrazione per un più folto gruppo di appassionati del settore.
Nel settore cripto è stata la differenza tra i primi fruitori in maniera goliardica e chi vi ha iniziato a costruire un piccolo impero.
Alcuni di quelli che sono riconducibili alla definizione di "early adopter", o altrimenti detti, in gergo più applicato al ramo settorialmente finanziario, "early investor".
Non è reperibile un chiaro riferimento temporale nel quale racchiudere questa seconda fase, è altresì possibile a livello intuitivo collocarla tra gli anni nei quali sono nati tutti quelli che ora, per quelli rimasti, sono progetti di successo e conclamati a livello internazionale.
Primi fra tutti sono altri progetti di valute, che indubbiamente hanno preso spunto da Bitcoin (valorizzando le differenze e sminuendone i tecnicismi) o hanno sfruttato la sua

nomea per farsi largo nel mercato con servizi affini o con funzione di protesi al suo utilizzo.
Gli esempi più evidenti, successivamente altre criptovalute stesse, sono gli exchanges, il portale di accesso più immediato e diretto al mondo delle valute digitali.
- Kraken è ufficialmente il più longevo di essi è stato fondato nel 2011 da Jesse Powell.
Questo exchange compie operazioni finanziarie nella maggior parte dell'Occidente e nel pieno della giurisdizione americana e la sua sede legale è proprio statunitense.
(Chi è nel settore finanziario è già a conoscenza del fatto che il mercato americano sia uno tra i più sostanziosi, ma anche uno con la giurisdizione, in termini di quelle che sono per noi "plusvalenze" e "minusvalenze", più intricata: in pratica operare nella piena legalità del mercato americano è un'impegno che non tutti gli exchanges si sono incaricati di sostenere).
- Coinbase Exchange è, per l'appunto, un exchange finalizzato nel 2012 da Brian Armstrong, un ex ingegnere informatico prima occupato in Airbnb.
Anch'esso nella piena facoltà di operare nella quasi totalità degli stati del mondo, è il secondo maggior exchange per scambi giornalieri dopo Binance: quasi 600.000 milioni di dollari in corrispettivo.
Come Binance e altri di questi enti, Coinbase non possiede una sede fisica dichiarata.
La grande e delineante differenza che Coinbase vanta rispetto a tutte le altre piattaforme è la sua immissione nel mercato azionario ("coin" è infatti la sigla del rispettivo titolo quotato in borsa) e tutto ciò che ne consegue, come un ferreo controllo da parte della SEC (Securities and Exchange Commission, l'ente federale statunitense preposto alla vigilanza della borsa valori) americana e la disposizione di mantenere pubblici i bilanci di mercato, gli asset allocation e le specifiche finanziarie.
Furbescamente Coinbase ha spinto la sua mission aziendale sul rendere i propri servizi più accessibili alla massa, mantenendo delle commissioni per operazioni decisamente più basse rispetto ai competitor oltreoceano.
- Gemini, nome originale dettato dal fatto che i suoi fondatori siano due gemelli, è stato sviluppato nel 2013 dai fratelli Tyler e Cameron Winklevoss, che essendo stati tra i fondatori di quella che poi sarebbe divenuta una delle aziende più influenti al mondo, Facebook, non esitarono a trasferire la loro abilità in qualcosa di più personale.
Gemini ha sede in USA e opera in tutti gli stati appartenenti alla "categoria" degli industrializzati.
- Bitfinex nasce nel 2012 ad opera di un informatico parigino, Raphael Nicolle.
Quest'ultimo basa il proprio progetto sul letterale modello di Bitcoin, offrendo la propria piattaforma come tramite per mettere in contatto i soggetti interessati nel servizio "peer to peer" (pari a pari) di Bitcoin.
Ha poi assieme al suo team aggiunto funzionalità inerenti ma innovative.
- Huobi Global di Leon Li opera principalmente nel mercato orientale, dal 2013 infatti offre servizi affini a quelli dei suddetti exchanges.
Nata in Cina, ha dovuto modificare la propria sede legale nelle isole Seychelles a causa del divieto da parte del governo cinese di operare in tale settore, sia come parte attiva che fornisce servizio, sia passiva che ne usufruisce.
Avendo composto questa lista, sottoscrivo un paio di considerazioni o postille: gli enti che ho scelto sono quelli che io personalmente ho avuto modo di utilizzare nel tempo e che combaciassero con le condizioni di origine nei primi anni successivi a Bitcoin, enti finanziari come Binance e OKX sono nati nel 2017 e quindi in una fase successiva di maggiore maturità.
Vi sono altri exchanges con i quali sono entrato in contatto ma non rientravano tra i primi 15 della classifica dei più diffusi e utilizzati, dunque non li ho inseriti.
A proposito della classifica dei più voluminosi[29] (con maggior volume di scambi) ritengo che vi sia un netto bipolarismo tra gli enti occidentali e orientali.
Tra i primi 10 exchanges della graduatoria, tutti quelli fondati nei primi anni successivi a Bitcoin si trovano in Cina e Stati Uniti d'America; i software cinesi si sono poi dovuti spostare in zone franche o banalmente meno meticolose e proibitive riguardo il settore criptovalute (e spesso finanziario in generale).

La seconda ondata di exchanges, partita invece tra il 2017 e 2018 ha vissuto le limitazioni ai danni dei loro competitor dalla prospettiva esterna, dunque nel momento in cui era necessario scegliere una località in cui innestare la propria sede legale le mete più ripetute sono state direttamente quelle facilitanti.
Un'ultima riflessione riguardo una di queste due località primarie riguarda il fatto che gli Stati Uniti fossero in una certa maniera la culla della tecnologia crittografata, la culla del progetto di Chaum e dopo l'11 settembre la più attenta nazione al mondo al tema dell'avanguardia informatizzata nel suo amplesso, che riversò lentamente nella psicologia dei suoi cittadini.
Inoltre il mercato americano è quello più regolamentato da diversi organi come la già citata SEC e Commodity Futures Trading Commission (CFTC), quindi quello offrente più garanzie e al quale seguono spesso per questa ragione un maggior numero di utenti, anche al fronte di commissioni più salate.
Molti studiosi del mercato cripto e parecchi amatori, sostengono che questo ambiente non sia mai realmente approdato ad uno stadio di "adozione di massa", il fisiologico passo successivo a quello degli "early adopters".
I numeri parlano chiaramente, premettendo che Bitcoin tecnicamente è stato progettato per ambire a soppiantare il sistema finanziario attuale che ha un riscontro del 100%, quindi tecnicamente avere come risposta più o meno lontana nel tempo un'adozione totale da parte della popolazione mondiale.
C'è da considerare come quasi la totalità dei servizi/ prodotti invece non raggiunga mai realmente quella che in linguaggio sociologico/mediatico viene definita dell'addomesticamento reciproco o dell'"appropriazione", in cui cioè l'utente plasma l'innovazione al suo utilizzo ma da essa ne viene condizionato.

5. **Il rifiuto dell'innovazione**

Tra gli individui/enti restii ad adottare tali innovazioni, possiamo distinguere due tipi di approcci all'innovazione:
- un gruppo di utenti che respingerà tale introduzione nelle maniere più o meno platoniche, reinterpretandola, adattandola sulla base della propria creatività o reinventandola totalmente.
- un secondo gruppo che tenterà volontariamente (o involontariamente) e drasticamente di sminuirla, rigettandola, escludendola dalla propria quotidianità o essendone resistenti (impermeabili al suo ingresso nella propria vita).
Facenti parte di questo secondo gruppo infine vi sono anche gli esclusi, che vengono rigettati a loro volta (questo però non può sussistere in ambito di decentralizzazione).
Torno a dire che è difficile da parte della società rifiutare l'innovazione in stretto senso economico e che spesso gli attori che più la rigettano sono, al posto che i cittadini, proprio gli enti sovrani che potrebbero farsene carico e garantirla.
Spesso la percezione degli utilizzatori di valute digitali e servizi affini, è quella che i governi (o uffici da loro designati) abbiano lo specifico compito di sabotare il progresso in questo ambito.
Bitcoin non è progettato in questi termini, come un qualsiasi sistema economico che si rispetti, viene accettato come sistema comune oppure risulta inefficiente.
Stando a questa premessa dunque, è possibile definire Bitcoin tuttora in una fase prematura e riconducibile in un "early stage" rimandando alle fasi di Rogers.
Si tratta di un progetto che verrà completato approssimativamente nel 2140, che ha delle applicazioni concrete (SegWit e Lighting Network) che sono tecnologicamente ancora in fase di beta testing, che dagli enti reggenti la società ai quali affidiamo il potere ora ne stanno (quasi uniformemente) solidamente lontani e che è adottata da una media di 4-5% della popolazione mondiale.
Con queste premesse non è verosimile definire Bitcoin come "affluito nella fase della maggioranza iniziale".

Una peculiarità alla quale però è giustificato dare atto a favore del protocollo, e più concretamente agli utenti che mantengono salde le loro credenze sullo stesso, continuando a detenere la valuta, eseguire validazioni e transazioni e soprattutto minarlo, è la persistenza.

6. **Gli exchanges come mediatori liquidi**

Gli exchanges sono la prima forma di entità organizzata che abbia sfruttato l'ondata di popolarità delle criptovalute per crearsi una nomea.
Questo ha reso questi attori come il bersaglio che poteva effettivamente offrire un volto ad un movimento, al quale le istituzioni classiche non erano (e stando ai fatti odierni non sono) pronte a condividere.
Gli exchanges, un po' come tutta la community dietro a questi ideali, hanno dovuto persistere nel loro intento ricorrendo ad una forma che si potrebbe definire "liquida" o "incorporea".
Esistono 206 stati al mondo, più precisamente 195 stati sovrani indipendenti e 11 semi indipendenti o subordinati.
Se anche solo considerassimo le nazioni prettamente autonome vi sarebbero da prendere in esame quasi 200 governi differenti, ognuno con un proprio approccio alle valute digitali.
In più per ogni singolo paese vi sarebbe da prendere in considerazione il fattore temporale, in quanto le forze politiche hanno opinioni discostanti e i cicli economici cambiano molto più rapidamente nei paesi emergenti con un tasso di industrializzazione duplice o triplice l'anno successivo rispetto al precedente.
Il rapporto che gli enti che operano nel settore hanno con questi stati è trasversale e non verticale.
Innovazione significa intrinsecamente cambiamento e incertezza ed è perfettamente plausibile che i vertici statali cerchino di tutelare i loro protetti cittadini, però meno giustificabile è il fatto che vietino tali realtà in maniera intransigente.
Non è desueto che questo accada in quei paesi in cui vige una democrazia solo formale, avendo abituato la propria popolazione ad un'autorità politica forte e ineluttabile.
Accennavo al concetto di trasversale in quanto un ambizioso e propositivo obiettivo preposto ormai dalla maggior parte delle valute immesse nel mercato, è quello che coincide con lo slogan di "senza confini", la volontà cioè di abbattere le commissioni interbancarie e nascoste dai circuiti di pagamento Visa, Mastercard o American Express.
Analizzando in modo più introspettivo si evince come in realtà sorga un altro fattore, in questo caso direttamente controproducente, cioè il fatto che il mercato Forex (il Forex o FX è una sigla che sta per "*foreign exchange market*" ed è il più grande e liquido mercato finanziario al mondo così come il più antico, si basa sullo scambio di valute governative, investendo a scopo di lucro sulla variazione che i mercati di tali valute subiscono e al valore che la loro moneta di conseguenza assume) sarebbe totalmente azzerato se non vi più fossero divise nazionali e una intercontinentale ne prendesse il monopolio.
Per di più è degno di nota come gli attori principali ed eseguire scambi nel mercato Forex non siano gli investitori al dettaglio, quanto nemmeno le grandi aziende; le maggiori entità coinvolte sono gli stessi stati, doppiamente scoraggiati a promuovere l'introduzione di criptovalute nei loro sistemi.
Proprio per queste motivazioni rimarco il vettore della liquidità settoriale, sia innescata dalla sostenuta conflittualità in termini di concorrenza interna, stimolando una sana competizione che offre nuovi servizi ai clienti.
Sia in termini banalmente di nuove funzioni introdotte, sia soprattutto di prontezza nel caso in cui lo stato X maturasse un'avversione contro l'azienda e la vietasse al suo interno.
Assicurarsi un pubblico non circostanziale ad un unica regione del mondo è fondamentale, permette all'exchange di sopravvivere in questo contesto che ad oggi non gli fornisce alcuna garanzia reale e continuativa.

Nell'esatto momento in cui sto scrivendo, a riprova della mia tesi, è stato dichiarato dalla SEC che Binance è indagato per aver commesso dei crimini di riciclaggio di denaro ai danni dei propri clienti.[30]
Accusa mossa anche precedentemente ad inizio 2023, dall'altro ufficio governativo citato in precedenza, CFTC.
A seconda riprova del fatto che non ci possa essere una permanente collaborazione, il giorno successivo della stesura delle righe precedenti, è stato dichiarato sotto indagine anche il secondo exchange più grande del pianeta per lo stesso motivo.[31]
Ricordo che Coinbase è una società per azioni, come tale è tenuta dal 14 aprile 2021 a rendere pubblici i bilanci e mantenere una certa trasparenza con tali organi tenuti alla tutela dei consumatori.
Dieci dei cinquanta stati americani hanno seguito tali accuse, con una latenza di meno di 24 ore l'una dall'altra, colpevolizzando due aziende leader del settore che collaborano con il loro governo in maniera chiara e bilaterale.
Lungi da me comprendere i reali moventi di tali attacchi, entrambe le parti sono aziende e come tali tutelano il loro interesse, spesso a discapito dei terzi.
Maggiormente di mio interesse in questa sede è ciò che accade quando un governo (o un ente super partes) si interfaccia con il settore delle valute digitali, vara le diverse piattaforme che operano nel proprio dominio e pone un veto, dato che ne detiene il potere legittimo (da noi tutti affidatogli).
A questa sentenza segue quasi simultaneamente un crollo del prezzo o una forte crescita in base al grado di compromissione che il mercato avrà da tale decisione, altra sfaccettatura di "mercato liquido" che viene spesso intesa come volatilità dell'asset, io personalmente quoto entrambe le definizioni.
La grande difficoltà e la sfida che ogni exchange deve sostenere, come ripeto, è quella di espandersi quasi al pari passo ai prodotti finanziari che propone.
Le tecnologie che offre sono la sostanza che fanno sì che sia benvoluto dagli utenti, ma ciò che gli dà reale modo di rimanere a galla è garantirsi una vastità di clienti più variegata possibile in termini geografici, cosicché se malauguratamente un paese cambiasse polo governativo e decidesse di prendere un approccio differente in termini di valute digitali, l'exchange non sia unilateralmente legato a quel singolo paese e tutti i suoi introiti non sprofondino.

7. **Le limitazioni e il rapporto con i Governi**

Esistono diversi modi con cui uno stato può effettuare limitazioni, queste usualmente vanno di pari passo all'ideologia del paese.
L'Occidente ha sempre mantenuto una posizione, seppur tradizionalista a riguardo, democratica e graduale, sebbene spesso intransigente.
L'Oriente ha posizioni contrastanti: se il Vietnam[32] dal canto suo ha un volume di transazioni che copre quasi la totalità della nazione, divenendo di fatto lo stato che più utilizza le valute digitali nell'intero globo, paesi come la Cina[33] hanno severamente proibito la prosecuzione della mansione di scambio di bitcoin, ma si sono anche spinti oltre, hanno letteralmente bandito la moneta stessa nella sua compravendita, detenzione e mining, rendendo il secondo più grande "sito di estrazione" del mondo del tutto innocuo e privo di competitività.
I cittadini che vivono in zone in cui disporre di bitcoin equivale a violare la legge, non sono stati registrati cali drastici nel numero di Wallet propri di quelle zone.
Gli exchanges di mole maggiore a matrice cinese sono emigrati in altri stati, mentre molti altri di ristrette dimensione sono stati chiusi.
Bitcoin, non essendo in alcun modo dipendente da questi attori/intermediari ha permesso di esprimere proprio in casi di estrema censura la sua natura decentralizzata, anche e soprattutto in pseudo-regimi come la Cina.
La nazioni hanno in genere rapporti diversificati con le criptovalute; nella seguente

partizione del capitolo tratterò più approfonditamente, oltre che un chiaro elenco dei singoli paesi in questi termini, di alcuni esempi più specifici in cui le valute sono state invece adottate, proibite o liberalizzate.
È importante considerare infatti che, sebbene dal debutto di Bitcoin nel 2009 esso sia stato considerato un "pari a pari" mezzo di scambio decentralizzato, quasi la totalità dei governi sovrani (molti degli stati africani e dell'Oceania non hanno l'esigenza di approvare o discutere riguardo queste tematiche) ha avuto modo di trattare questi temi per raggiungere una sorta di regolamentazione o una conclusione a riguardo; ben pochi sono infatti i paesi in cui non è chiaro l'approccio intrapreso verso le valute digitali (con approccio intendo dire che non è chiaro se siano a favore o contrari; nella maggior parte delle nazioni sono le politiche sulla tassazione, regolazione e immissione nel mercato ad essere rimaste, più o meno volutamente, vaghe.
Non esiste dunque una legge unitaria e globale per una moneta che punta a diventarlo.
Nel mondo in generale, purtroppo, vi è poca reale informazione/ formazione a riguardo, sia per il punto che ho appena espresso nei paesi più "border line" (linea di confine, zona grigia), ma anche nei paesi occidentali in cui una regolamentazione è presente da anni, sono le persone stesse spesso a seguirla malvolentieri.
Agli occhi delle persone, Bitcoin è e deve rimanere nelle proprie mani, non gestito da quelle dei governi, i quali invece dovrebbero preoccuparsi di come garantire ai cittadini il beneficio di questa "proprietà privata".
Il lato della permissione/ divieto governativo all'utilizzo inevitabilmente incide sulla portata e la dimensione che il network riscontra in quella zona del mondo, ma spesso la chiarezza normativa è ancor più fondamentale.
In Italia per esempio la regolamentazione a riguardo non è nitida, il comportamento da tenere è comprensivo di lungaggini burocratiche e termini arcaici, i quali dai più che non sono avvezzi al settore, incomprensibili.
Una trattazione non lapalissiana e che non agevola il comune cittadino, che già dal canto suo non ha l'interesse ad informarsi a riguardo, non risulterà in una maggiore
attenzione alla legalità da parte dell'utenza.
Nel Bel Paese in particolare poi è risaputo che il tema del "dichiarare" è particolarmente delicato, quasi sensibile.
L'economia sommersa in Italia è affossante:
"Nel 2020 l'economia non osservata, sommersa e da att. illegali, vale 174,6 mld di euro (-30 mld) il 10,5% del Pil, periodo di riferimento: Anni 2017-2020" - ISTAT[34]

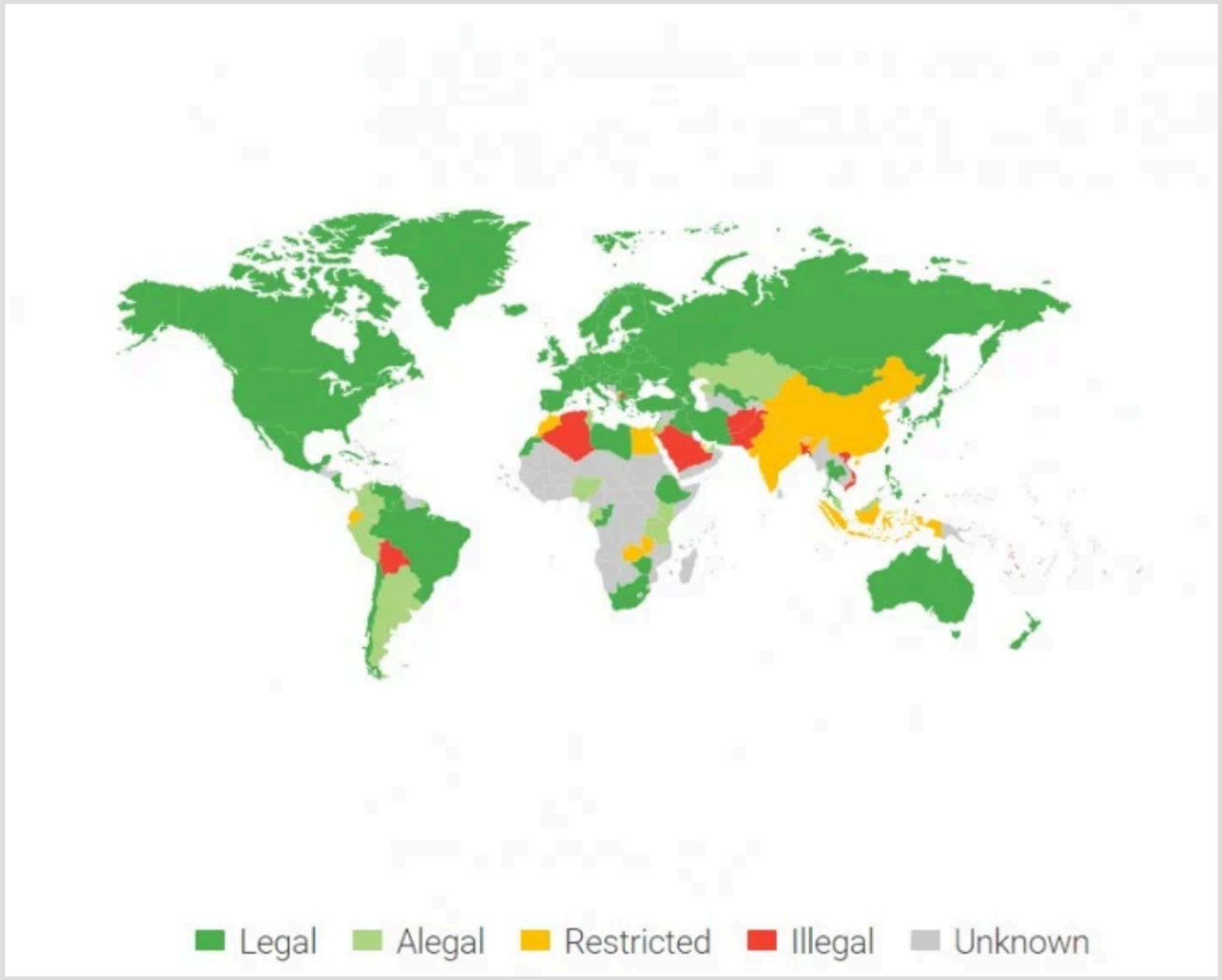
8. **Il welfare statale e la piramide dei bisogni di Maslow**

Gli stati in cui il protocollo è legale sono per lo più quelli in cui sussistono una preponderante attenzione e rigore verso un concetto profondo di cittadino e di welfare diffuso (benessere inteso come stato sociale, comprensivo di diritti e garanzie fornite dal proprio stato).
Brevemente scrivo una postilla su cosa siano questi concetti affini alla Scienza Politica e alla Sociologia e da dove derivino.
Il welfare è tradotto etimologicamente come "benessere diffuso", ma a livello sociologico ha un significato intrinseco molto potente.
Da vocabolario si traduce anche come "*sistema sociale che vuole garantire a tutti i cittadini la fruizione dei servizi sociali ritenuti indispensabili; in it. stato sociale*".
La proiezione del welfare è dunque quella primaria di tutelare il cittadino dai rischi, garantendogli la maggior protezione fisica e mentale possibile, con forze di polizia, servizi legati ad una maggior sicurezza (banalmente le luci artificiali accese negli orari notturni), servizi di pronto soccorso celeri e disponibili etc; ma anche garantendogli una sussistenza minima (per questa ragione viene anche denominato come "Stato di Sussistenza") come un reddito minimo alla popolazione considerata "debole", dando la possibilità alle famiglie così come ai singoli individui di mantenere un tenore di vita

dignitoso e che abbiano così una chance di reinserirsi nella società.
Il Welfare in generale presenta una tendenza a diminuire le grandi differenze di retribuzione tra fasce sociali diverse.
Un'attenzione di grande gravità si riversa sui due cardini di ogni istituzione sovrana, istruzione e sanità.
Ma soprattutto quello che il welfare si prepone di portare a termine è una valorizzazione individuale ed etica del singolo cittadino, non solo al tempo presente ma anche in particolare al tempo futuro.
In altre parole ciò che il welfare include è il tentare di racchiudere tutti quei bisogni che Maslow incluse nella sua omonima piramide sulla scala dei bisogni da lui teorizzata.
Questo strumento formidabilmente semplice e intuitivo è stato ideato da Abraham Maslow tra il 1943 e il 1954 e si tratta di 5 (poi prolungati a 7) scalini piramidali ordinati gerarchicamente per priorità che raffigurano i bisogni umani.
Maslow fece questa selezione a scopo soggettivo e non istituzionale; l'appropriazione del suo lavoro in questo contesto, ci tengo a precisare, la sto elaborando personalmente.
Si percorre la figura dal basso verso l'alto, con il chiaro parallelismo al fatto che lo scalino sottostante sostenga quello superiore, alla mancanza del primo il secondo non ha alcun modo di esistere.
Curiosamente (e in un certo senso naturalmente) l'ordine è anche cronologico, nella maniera in cui i primi bisogni ad essere stati riconosciuti e garantiti seguano la gerarchia della piramide e il ragionamento di sostegni precedentemente espresso.
Il bisogno di "Stima" per esempio non era nemmeno concepito nel 1920, così come in molte zone del mondo geograficamente e ideologicamente distanti da quelle che hanno adottato queste linee guida, che hanno un concetto di welfare che raramente si discosta dai primi due scaglioni.

La prima macro categoria dei bisogni di base, che comprende la "banale" volontà di sopravvivere, è quella che ci spinge ad agire e influenza maggiormente il nostro comportamento.
Una volta che i bisogni fisiologici sono soddisfatti, cioè il momento in cui abbiamo cibo e acqua, un luogo in cui dormire e tutti i bisogni che tengono letteralmente il nostro organismo in vita sono placati, viene raggiunta la condizione di omeostasi.
Il ruolo demaniale è in questo scalone quello del garantire una linea minima di autosufficienza in termini di salario per potersi quantomeno permettere il vitto quotidiano.
Giunge poi il bisogno di sicurezza, entrambi questi bisogni di base sono in auge già dai

primi imperi.
Il bisogno di sicurezza è inteso come fisica ed economica, individuale e del nucleo familiare e lavorativa.
Intesa per esempio come forze di polizia, illuminazione o sicurezza postale (in epoca contemporanea).
Con la sicurezza finiscono i bisogni definiti “da mancanza”, quelli cioè determinati dalla deprivazione di un bene o servizio e iniziano quelli “da crescita”, cioè per l’appunto alla volontà di miglioramento e crescita.
Il desiderio di appartenenza è il primo dei bisogni sociali, questo bisogno include tutte quelle minime socialità che rendono un animale sociale come l’essere umano soddisfatto.
Appartenenza intesa come relazione amicale, amorosa, famigliare e di diversi gruppi sociali di altro genere.
Disturbi sociali come la depressione, l’ansia e la solitudine sono estremamente deleteri per la psiche umana; è compito anche dello Stato fornire la possibilità ai propri cittadini di evolvere questo grado di relazioni in maniera sana e continua.
Il quarto gradino è il desiderio di sentirsi apprezzati e rispettati, tramite realizzazione nella società, autostima e rispetto reciproco.
Le persone hanno necessità di percezione di avere un valore e un significato nella società in cui vivono.
L’ultimo bisogno e il più introspettivo riguarda la sfera del sé, ed è quello di auto realizzazione.
Maslow lo spiegava dicendo semplicemente “*Quello che un uomo può essere, egli deve essere*”.
Potremmo definire questo frangente come la possibilità di esprimere le proprie potenzialità al massimo.
Ci tengo a precisare, come ci tenne lui, che non esistono distinzioni così nette, piuttosto queste sono indicative di quelle che ogni uomo o società ambisce a soddisfare in maniera generica.
Esistono tra loro moltissime sfaccettature e diramazioni; l’amplesso si basa sul fatto che un bisogno una volta appagato e dato per scontato, faccia spostare l’attenzione verso qualcos’altro, qualcosa che ancora non ci appartiene.
L’obiettivo fondamentale dello stato sociale è quello di garantire ai suoi cittadini il più alto scalino possibile in questa piramide.
Le nazioni che notoriamente più hanno un welfare prestante sono in Europa: i paesi scandinavi e a seguire gli stati occidentali centrali, poi quelli del Sud come Italia, Grecia e Spagna.
In Asia il welfare è solitamente di secondaria importanza, spesso viene sacrificato questo aspetto per un bene più “comunitario”, se così possiamo definirlo.
In America del Nord e Australia, così come in Gran Bretagna e nei paesi anglosassoni occidentali più in generale, il welfare è probabilmente ai suoi massimi livelli mai raggiunti (i paesi scandinavi vi si avvicinano molto).
In America del Sud la situazione non è ancora stabile ma in via di progressivo miglioramento.
In Italia, in particolare, il termine è stato riadattato a indicazione del fatto che l’assistenza venga erogata alle fasce più deboli come pensionati, disoccupati o diversamente abili.
Prima del termine importato di welfare questo genere di assistenza prendeva il nome di “Previdenza sociale”.
Terminata questa, non così breve, digressione sullo stato sociale, torno a trattare gli stati che abbiano o meno regolamentato Bitcoin, facendo riferimento all’immagine che mostra la cartina geografica inerente ai diversi approcci tenuti dai paesi in rapporto alle criptovalute.
Annettendo e ripetendo che l’utilizzo di un sistema di pagamento che sia meno a controllo centralizzato e più si riversi sulla piccola responsabilità interpersonale, è un tipo di servizio considerabile un plus e quantificabile all’interno del welfare di cui prima discutevo.



9. **L’approccio geopolitico**

La relazione mantenuta dai singoli stati con le criptovalute è ben mostrata nell’illustrazione annessa poc’anzi, il colore verde indica quei paesi in cui vige una serie di decreti formali che tutelino il consumatore, regolino le attività commerciali e pretendono una contribuzione.
In questi paesi le norme a riguardo non sono ugualmente all’avanguardia, tuttavia esistono e sono in vigore in quei paesi in cui notoriamente vengono rispettate (volente o nolente).
Gli stati (verde) in cui bitcoin viene regolarmente usato ed ha una regolamentazione che lo accompagna sono:
- Gli Stati Uniti dal 2013, secondo il Dipartimento del Tesoro e più precisamente il Financial Crimes Enforcement Network (FinCEN, Protocollo contro i crimini finanziari), che ha definito bitcoin come una valuta convertibile ad un equivalente in reale valuta o un suo diretto sostituto.
L’organo di Internal Revenue Service ha denominato bitcoin come una proprietà soggetta a tassazione.
Ogni entità che operi nel settore della compravendita di criptovalute, come exchange o affini, ricade nella branca dei servizi di affari monetari (MSB).
Come parte della MSB (money services business) gli exchanges sono soggetti al segreto bancario fino al corrispettivo di 10.000$ di controvalore, oltre al fatto che debbano essere riportate alle autorità le transazioni di valore superiore.

In ultima istanza la Tesoreria e il FinCEN hanno creato strategie apposite per assistere i processi legislativi negli sviluppi delle regolamentazioni più approfondite, dando priorità al tracciamento di criptovalute e alle segnalazioni.
- L'Unione Europea, la quale riconosce l'esistenza di bitcoin e di gran parte delle altre criptovalute, definendoli cripto-assets.
Non è dunque illegale acquistare e vendere bitcoin all'interno dell'Unione, ma l'Autorità Bancaria Europea ha dichiarato che le attività in questo ambito sono al di fuori del suo controllo e ha avvertito e continua a dare monito al fatto che siano rischiose per i cittadini e i business.
Nel 2020, la Commissione Europea ha ultimato una proposta sulla regolamentazione dei "cripto-assets", negli ultimi anni è stata rimandata e solo nel 2022 una bozza finalizzata è stata inviata all'intera Commissione per l'approvazione.
L'ultimazione di questa proposta, divenuta regolamento a tutti gli effetti, è avvenuta nell'aprile 2023, momento in cui il Parlamento Europeo ha approvato il MiCA (Market in CriptoAssets), norma che regola i servizi relativi ai cripto-assets e alle stablecoins (valute digitali che hanno algoritmicamente e perpetuamente un valore nominale di 1:1 con una valuta FIAT, esempio dollaro o euro) e si stima che entrerà in vigore entro il 2025.
Lo scopo non è quello di assumere il controllo di queste valute, bensì offrirvi maggior accesso, ma con più tutela ai cittadini dell'Unione.
- Il Canada, che ha sempre mantenuto una linea amichevole con Bitcoin, simile a quella del proprio vicino meridionale, gli USA.
Bitcoin è semplicemente ed efficacemente preso in considerazione come un bene qualunque dal CRA, Canada Revenue Agency (Ufficio delle "Ricompense"), che lo tratta come una categoria di altri beni per scopi tassativi.
Il Canada considera gli exchanges come servizi finanziari al pari delle banche. Questo li rende soggetti ai controlli del Proceeds of Crime per contrariare il riciclaggio del denaro e atti terroristici finanziari.
Gli exchanges devono essere iscritti al FINTRAC, cioè al Financial Transactions and Reports Analysis Centre of Canada, ente che riporta le transazioni sospette e dà voce ai reclami dei clienti.
- L'Australia, in qualità della più orientale delle nazioni occidentali, o che potremmo definire occidentalizzanti, ha una regolamentazione simile a quella del Canada al riguardo.
Lo Australian Taxation Office considera bitcoin un asset finanziario, il quale può essere tassato solo all'avvenire di specifici eventi, primo fra tutti quando le criptovalute vengono convertite in dollari, in quel preciso momento scatta il capital gain tax, cioè un corrispettivo australiano della tassa sulle plusvalenze.
Inoltre è richiesto dalle autorità che venga tracciata, per scopi legali, ogni transazione avvenuta individualmente; in Australia se possiedi bitcoin strettamente a livello individuale e fai profitto su di essi, in alcuni casi potresti anche non pagare alcuna tassa.
Altre nazioni interessate da questi canoni sono: Danimarca, Germania, Giappone, Spagna, Regno Unito e Svizzera.
Vorrei a proposito di quest'ultima percorrere un approfondimento peculiare: la Svizzera non ha mai espresso la volontà di inserimento nell'Unione Europea, così come è sempre rimasta neutrale in termini di conflitti o di legislature unitarie.
Non di meno in questo genere di politiche finanziarie, un paese come la Svizzera, che si considera la punta di diamante di tali manovre, non ha partecipato ad un fronte comune con tutti i suoi paesi limitrofi.

10. **La Svizzera**

La Confederazione Svizzera è uno stato federale suddiviso in 26 cantoni, ognuno di essi quasi totalmente indipendente dal governo centrale e a sua volta diviso in comuni con un certo grado di autonomia rispetto al cantone di appartenenza, tranne che per alcune tematiche quali la sicurezza nazionale, la politica estera e la gestione dei 3 pilastri svizzeri

(il sistema previdenziale svizzero), che sono materia nazionale, i cantoni sono semi-liberi.
I singoli Cantoni hanno sviluppato una sorta di sana competitività gli uni con gli altri, riguardo la contribuzione per esempio non tutti i cantoni hanno uguali importi di tassazione, non tutti hanno le stesse politiche sulla fiscalità, i salari orari minimi sono differenti e così via.
Ogni anno i comuni cittadini rivedono queste statistiche e le manovrano così da migliorare la loro posizione di rilevanza all'interno della Confederazione nel suo insieme.
La Svizzera è così competitiva nel mondo perché è uno stato che possiede intrinsecamente delle meccaniche di mercato.
Riguardo più nello specifico il tema di Bitcoin & Co: la Svizzera è il primo paese in Europa ad aver regolamentato le criptovalute, dal 2024 le poste permettono di acquistare e vendere valute digitali direttamente, facendo a livello governativo informazione di qualità su queste innovazioni tecnologiche.[35]
Sono stati organizzati diverse volte dei referendum[36] dediti alla piena regolamentazione di Bitcoin (accettato nel 2018 dal governo) e il Cantone di Zugo, più precisamente l'omonima città, è diventata il centro di un movimento migratorio di numerose agenzie e società operanti in questo settore, ansiose di trasferirsi in quella che viene definita "Cripto Valley", su falsa riga della Silicon Valley in California.
Da circa un anno in questo cantone nella Svizzera centrale è possibile pagare le tasse in bitcoin ed ether (criptovaluta di Ethereum).
Nel settembre del 2020, il Parlamento svizzero ha approvato all'unanimità una legge, il Distributed Electronic Registers Act, che permette alle società di criptovalute di tokenizzare azioni (suddividere azioni classiche in parti di azioni, rendendo possibile l'acquisizione di percentuali minori e non obbligando l'utente a prendere l'azione unitaria), obbligazioni e altri strumenti finanziari.[37]
Nella Confederazione non esiste una tassa sul capital gain (plusvalenze), sia in criptovalute e sia in azionario di matrice classica.
Vi è poi una grande iniziativa di fama europea che lentamente si sta facendo strada, si chiama Lugano Plan ₿[38] e si dedica da diversi anni, partendo dalla città di Lugano nel Canton Ticino, a creare una realtà totalmente sostenuta da criptovalute.
Lugano è molto attratta da ciò e ha dimostrato grande partecipazione da parte della popolazione nel tempo, la maggior parte dei negozi offrono la possibilità di ricevere pagamenti in bitcoin (Lighting network), Tether (una coin stabile ancorata al valore del dollaro) e una valuta digitale da loro coniata chiamata Lvga.
La Svizzera dunque in ambito di digitalizzazione economica è la più all'avanguardia in Europa e verosimilmente nel mondo.
Esiste soltanto una nazione che si è spinta ben oltre in quanto ad adozione di valute digitali.

11. **La Repubblica del Salvatore**

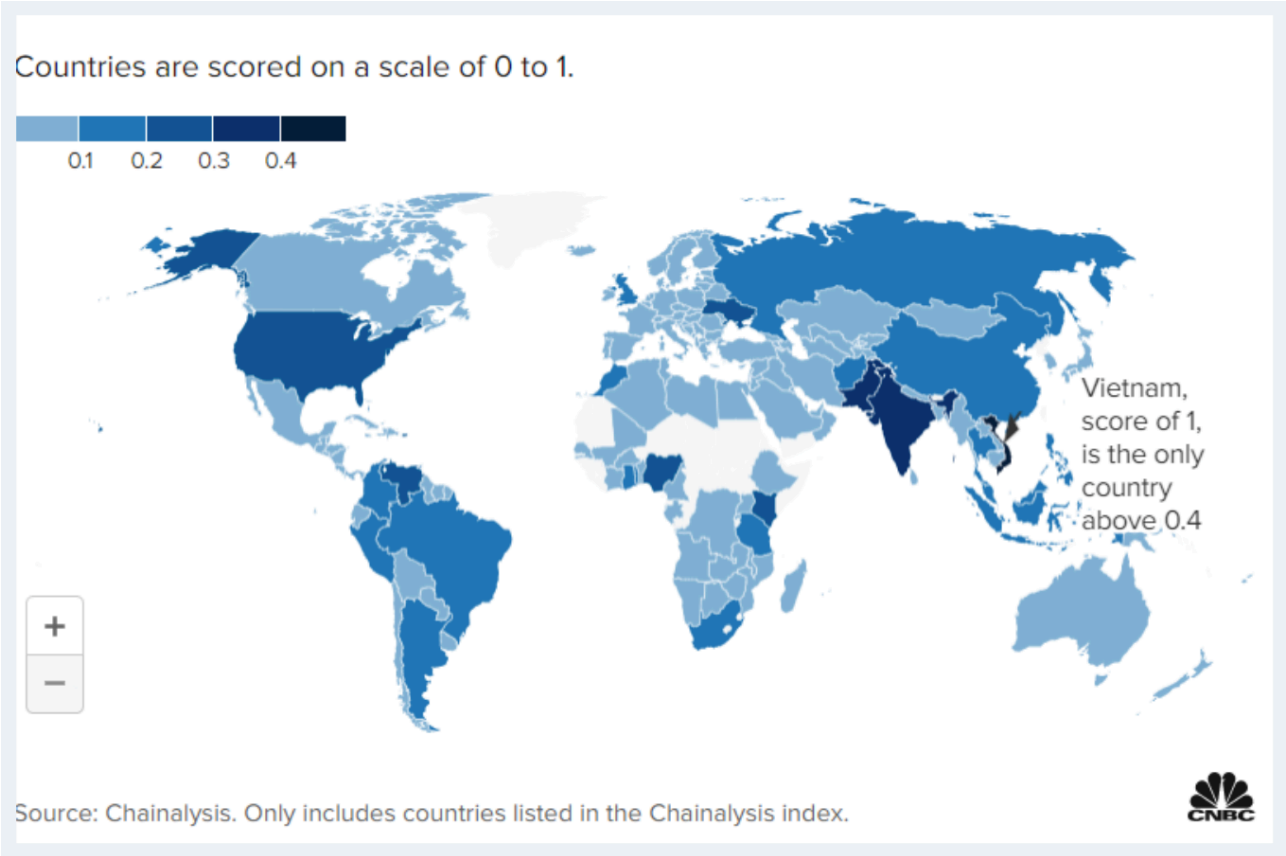
La Repubblica di El Salvador è uno stato centro americano che conta poco più di 6 milioni e mezzo di abitanti, si affaccia sull'Oceano Pacifico e io, sinceramente, prima dello spartiacque che sto per spiegare, non ero a conoscenza della sua esistenza.
Il presidente in carica Nayib Bukele ha cambiato il destino del proprio paese, allargando le proprie vedute in maniera del tutto originale: affiancato dalla propria equipe politica, il 7 settembre 2021 è stata emanata la norma tanto discussa che ha reso El Salvador un piccolo attore di un'impresa titanica.
La Repubblica è diventata il primo Paese al mondo ad avere adottato bitcoin come valuta legale, non regolamentandola e non affiancandola ad una valuta precedentemente esistente.
Gli stipendi e le pensioni vengono emanati ancora in dollari statunitensi (causa della forte volatilità), le tasse sono pagate in bitcoin, i bambini ricevono satoshi invece che monete metalliche come mancia, i prezzi nei supermercati sono in bitcoin, il carburante, la cena al

ristorante e il canone della TV, l'intera economia sta traslando su bitcoin.
Per gli appassionati, come mi ritengo io stesso, questa realtà sembrava un'utopia fino a pochi giorni prima dell'annuncio, e ancora adesso pensare al coraggio che questo piccolo stato (e che proprio per questo sta riuscendo) abbia avuto è sconcertante.
Certo, i problemi non sono tardati ad arrivare e questa assoluta nuova situazione economica è stata più difficile da gestire del previsto.
Tutto lo stato ha adottato il modulo Lighting Network, altrimenti questo non sarebbe stato sostenibile.
Ci sono state numerose proteste a seguito di questa decisione e tutta l'economia si basa ora su una tecnologia che, come accennavo, è ancora in fase di testing.
Il problema maggiore ovviamente vige quando il prezzo crolla, il governo di El Salvador ha posto grande fiducia in questa transizione, facendo presto i conti con una valuta altamente volatile (non che storicamente le valute centro e sud americane non siano affette da enorme inflazione o variazioni improvvise nei prezzi) e che dipenderà ancora per molti anni interamente da dinamiche di mercato.
Ironicamente l'8 settembre 2021 il prezzo di bitcoin crollò, così come successive altre innumerevoli volte.
Bukele ha periodicamente dato voce ai propri media, mostrando i propri acquisti al fronte del crash.
I salvadoregni dal canto loro non sono così entusiasti, probabilmente lo siamo più noi facenti parte della branca di cultori.
Loro sostengono invece vi siano problemi decisamente più concreti (tornando alla piramide dei bisogni di Maslow) come per esempio la sicurezza.
El Salvador ha un ratio di criminalità decisamente alto e questa attenzione alla loro valuta ha distolto lo sguardo dei media, a detta loro, dal vero volto autoritario e repressivo di Bukele.[39]
Questa loro esperienza però, al di là delle ripercussioni positive o negative che avrà su El Salvador e delle quali è troppo presto per fare un resoconto esaustivo, è un grande passo.
Ritengo sinceramente che se il governo e i suoi cittadini riusciranno a sostenere la criticità di questi primi anni di maturazione, El Salvador possa con la giusta saggezza e consapevolezza economica potenzialmente ambire ad essere una delle nazioni più ricche in rapporto alla popolazione.

12. **Gli Emirati Arabi Uniti**

Come ultimo esempio inerente l'adozione di criptovalute, cito gli Emirati Arabi Uniti, più in particolare la città di Dubai.
Dubai sta accrescendo negli ultimi anni la sua fama a livello internazionale di "paradiso finanziario" arabo, divenendo a tutti gli effetti un mastodontico e luccicante "parco giochi elitario e per ricchi".
Queste mie parole non le reputo estremismi, bensì banalmente un'interpretazione umanitaria della stessa città che dal punto di vista finanziario è così accattivante, direi quasi eccellente sotto certi punti di vista, ma da un punto di vista sociale è terribile.[40]
I paesi della penisola arabica (insieme a quelli dell'America latina) detengono il record di "regioni più diseguali del mondo", con una media stimata che indica che il 10-12% della popolazione detenga il 55% del reddito nazionale medio.
Con la globalizzazione e il dilagare della pandemia da Covid-19 i poveri del mondo sono diventati più poveri, mentre i benestanti più ricchi.
Al di fuori della metropoli dubaina vi sono delle baraccopoli in cui le persone patiscono la fame, ma il principale cruccio del monarca e dei suoi ministri è quello di attrarre capitali mediante le più competitive tassazioni e opportunità di business al mondo.
Rivisitando in chiave arabica la "Cripto valley" svizzera, Dubai viene definita anche una cripto Oasi, un sollievo in mezzo ad un mondo di legislazioni che non lasciano spazio alla

libertà finanziaria.
Il fondatore di Binance stesso ha scelto Dubai (da Singapore) come sede principale del proprio progetto.
Gli Emirati Arabi Uniti sono probabilmente stati il primo paese ad aver legiferato riguardo ai Non Fungible Tokens (NFT), definendoli “espressioni digitali di valore”.
Dubai è in questo ambito estremamente all’avanguardia, offrendo una burocrazia di proforma e un tetto di accesso minimo per l’inizio di attività aziendali in molteplici settori, il governo ha semplicemente applicato questa semplicità ad un settore in enorme crescita di mercato, e che a tutti gli effetti gli avrebbe condotto immensi capitali in entrata da tutto il mondo.
A proposito di queste aziende che si insediano negli Emirates per dar voce al proprio progetto, è stato appositamente creato un quartiere per ospitare tali realtà aziendali.
A Dubai si può comprare quasi tutto in cripto, dal caffè al bar fino ad un appartamento al 74esimo piano di un building miliardario.
Facendo però attenzione che quella villa in mezzo alle nuvole abbia la vetrata sulla famosa Dubai Marina, o meglio ancora sulla Palma artificiale in mezzo al Golfo Persico, e non sull’altro lato dell’edificio, quello in cui poco prima dell’orizzonte si vedono le baracche alle quali non arriva nemmeno l’acqua.
Riprendendo un concetto che ho lasciato indietro qualche capoverso fa, idealmente El Salvador è l’unico stato in cui l’innovazione Bitcoin ha raggiunto una reale maggioranza assoluta, un 100% dell’economia.



Non esiste più un modello di diffusione dell’innovazione se questa viene imposta dall’alto, però è un modo tra i tanti per cambiare uno status. (Giusto o sbagliato che sia)
Vi sono però, sebbene non siano totalmente regolamentate (e proprio per questa ragione si ha avuto modo di sperimentare le ultime tre fasi della scala di diffusione di Rogers:

maggioranza iniziale, tardiva e i cosiddetti ritardatari), delle realtà in cui si è raggiunta una certa soglia di maggioranza nell'utilizzo delle criptovalute proveniente dal basso, spontaneamente.
Queste realtà sono proprio quelle che subiscono quelle limitazioni le quali hanno dato vita all'idea portante delle valute digitali: la libertà.
I paesi che ne fanno maggiore utilizzo sono quelli emergenti, paesi quali il Vietnam (per 2 anni consecutivi il paese con adozione maggiore) in cui il rapporto è 1:1, ma anche l'India e il Pakistan.
Paesi in cui il tasso di povertà è molto alto e il sistema finanziario discutibile, si affidano alle criptovalute perché ne hanno il controllo diretto, spesso trasferiscono i loro risparmi non tanto in bitcoin o in altre valute a scopo lucrativo o speculativo, bensì in stablecoin per garantirsi che almeno mantengano un valore stabile (ancorata al dollaro americano) rispetto alla loro rispettiva valuta governativa.
Traslerò ora la prospettiva dal lato dei paesi contrari a bitcoin, che in linea più o meno marcata hanno proibito o limitato il suo utilizzo, la sua applicazione o diffusione.
Alcuni stati percepiscono più la volatilità di bitcoin (e delle criptovalute in generale) rispetto alle possibilità che può offrire, avvertono di più la minaccia che la valuta diversa e decentralizzata può provocare al sistema monetario vigente e manipolabile, additando l'utilizzo di valute digitali private (spesso denominate impropriamente come anonime, quando in realtà le valute anonime esistono ma sono relativamente poche e specifiche) come adibite al traffico di droga, di armi o di attività illecite, al riciclaggio di denaro e addirittura al terrorismo finanziario.
Le sfumature di contrarietà in materia di criptovalute sono tra loro diverse: vanno dalla proibizione implicita a quella esplicita e risoluta, si diramano in un divieto di detenere le valute digitali oppure in una limitazione al loro utilizzo in maniera indiretta, censurando tutti i servizi che permettono di comprare e vendere tali asset finanziari (exchanges).
Le nazioni dunque con un divieto implicito e restrittivo sono:
- Camerun
- Repubblica Centroafricana
- Gabon
- Guyana
- Lesotho
- Libia
- Zimbabwe

Le nazioni con un divieto assoluto sono invece:
- Qatar
- Arabia Saudita
- Cina

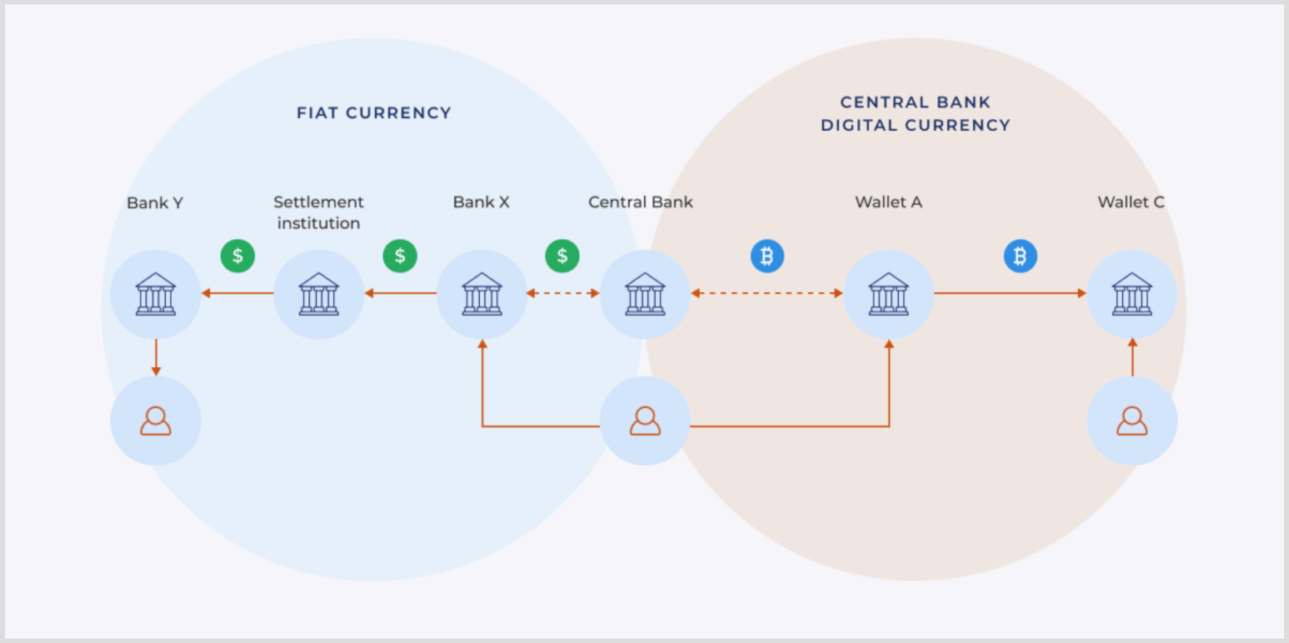
A proposito di quest'ultima faccio una parentesi che va un po' a spiegare il motivo sottostante il divieto delle criptovalute in Cina.[41]
Fin dai mesi precedenti ai quali El Salvador si è battuto per fare di bitcoin la propria valuta a corso legale, la Repubblica Popolare Cinese con a capo il presidente Xi Jinping, remava nella direzione opposta, muovendo una vera e propria guerriglia alle criptovalute, alle loro identificazioni aziendali e all'ideologia che il popolo potesse avere a riguardo.
Nel settembre 2021 la banca Centrale Cinese ha dichiarato illegali tutte le transazioni in criptovalute, impegnandosi ad aumentare drasticamente il monitoraggio su un corretto genere di comportamenti divenuti improvvisamente illegittimi.
Questo divieto informale, divenuto da quel settembre evidente e schiacciante, si è espresso (come anticipavo) in due modalità:
- La prima è stata troncare le attività a scopo di lucro vigenti e in un secondo momento bloccare quelle in prossima apertura in tal settore, privando così i cittadini di un punto di accesso facilitato al mercato delle valute digitali.
- In un secondo luogo ha poi più genericamente bandito Bitcoin, così come altre valute quali ad esempio Ethereum.

Il motivo dietro a questa interdizione non è un così misterioso segreto, la Cina ha una storia e un capitale sociale molto identitario, che mette in pratica attraverso una forma di

governo centralizzata e fortemente autoritaria.
A livello storico è possibile capirne le ragioni, non dico sia giustificabile una centralizzazione del potere in tal senso, ritengo solo che da un punto meramente cinico (ancora una volta) sia estremamente difficoltoso mantenere competitiva una nazione di 1,5 miliardi di persone tramite una democrazia reale; i cittadini cinesi, così come quelli russi di cui parlerò nelle prossime righe, hanno culturalmente assorbito l'ideologia totalitaristica nel corso dei millenni.
Parlo della forma governativa cinese per poter agganciare la ripercussione emotiva e reputazionale che essa avrebbe se perdesse il monopolio dello strumento principe di controllo societario moderno: la moneta.
A differenza di El Salvador, il quale popolo non era figlio di un economia stabile e ha colto tramite le criptovalute l'oppurtunità di un miglioramento di status, la moneta cinese è estremamente solida e di conseguenza lo stato stesso ha creato una situazione concorrenziale con le valute digitali che potremmo definire dal suo punto di vista "nomadi" o dal mio "decentralizzate", percependo da parte loro una seria minaccia.
La Cina, come si è inteso in precedenza, è stata fin dal principio un grosso bacino di utenza delle monete digitali.
Sia in ambito di fruizione che di produzione infatti essa era seconda solo agli Stati Uniti (ed è stata per diversi mesi addirittura il paese con più potenza computazionale "hashrate" al mondo).
Queste gigantesche aziende di mining sono state obbligate ad emigrare la propria attività verso paesi limitrofi o in generale più accoglienti; le destinazioni più ambite sono state il vicino Kazakistan e paradossalmente il lontano Texas in USA, cambiando addirittura del tutto bandiera. (In Texas i costi dell'energia elettrica sono notevolmente ridotti).[42]
La Repubblica Popolare però non può permettersi di rimanere nelle retrovie durante un cambiamento, lento ma inarrestabile, del sistema finanziario internazionale su movimento alla digitalizzazione compulsiva.

13. **Le valute digitali delle banche centrali**

L'alternativa istituzionalizzata dunque alla digitalizzazione finanziaria, avviene in un certo senso comparabile ad una grossa forma di stigmatizzazione del rifiuto, prospettiva alla quale sto giungendo tramite l'esempio sulla trattazione della Cina, ma sottolineo che il rapporto che i differenti paesi del mondo stanno avendo verso questa visione è all'incirca il medesimo.
In precedenza ho scritto riguardo le diverse tipologie del rifiuto di un'innovazione e tra le tante vi è la reinterpretazione personale o di gruppo di un dato progetto innovativo.
Con queste premesse introduco l'ormai palpabile contromossa concreta dei governi nazionali alle valute digitali non convenzionali.
La sigla è CBDC e sta per "Central Bank Digital Currency", cioè la valuta digitale preposta ed emanata direttamente dai governi che è ideata per essere più controllabile e riconducibile all'attuale sistema (riducendo così quello che in sociologia viene definito: cultural lag, la distanza che si contrappone tra la cultura intesa come bagaglio culturale/ capitale sociale individuale e l'introduzione di un'innovazione particolarmente rivoluzionaria).
Le CBDC sono una delle più grandi forme di reinterpretazione dell'innovazione da parte di un ente così complesso e verticale ad opera di un progetto nato dai gradini più bassi della società.
Credo per l'appunto sia successo ben rare altre volte un cambio di paradigma di portata intergovernativa in un lasso di tempo così breve.
Le CBDC[43] in breve non diventerebbero altro che forme digitalizzate delle attuali monete nazionali, concettualmente sono simili alle criptovalute, tant'è che etimologicamente prenderanno lo stesso nome di "valute digitali", ma avranno un valore fisso equiparabile a quello del riferimento corrispettivo precedente.



Queste valute governative sono in fase di test e se ne sta solo ancora discutendo nelle rispettive sedi parlamentari/ governative dei singoli paesi che intendono adottarle.
È importante sottolineare comunque come alcune di queste nazioni le abbiano già in parte adottate; la Cina per esempio, che continuo ad usare come filo conduttore, ha così fortemente invalidato l'accesso alle criptovalute che in questo frangente tratterò impropriamente come "tradizionali", con il puro fine di proporre la medesima idea in termini di tecnologia (non esattamente, successivamente ne parlerò) ma governativa e centralizzata.
La reale questione discriminante resta quella di capire come permettere che la totalità della popolazione possa avere i mezzi e le conoscenze per adottarle e in primo luogo come possano avere effetto sui network finanziari e sulla stabilità economica.
L'utilizzo delle CBDC in realtà è un naturale proseguo di quella che è l'economia per come la conosciamo oggigiorno; l'Italia per esempio è un paese ancora fortemente vicino al concetto di contante, ma altri paesi del mondo, riportando ancora una volta quelli che ho citato prima e che hanno un rapporto con la finanza più armonioso, da tempo stanno vivendo un calo abbastanza imponente dell'uso del denaro contante.
Basti pensare ai paesi scandinavi per entrare in quella che i media chiamano "cashless society", ossia società senza contanti[44].
Per queste nazioni non susciterebbe nessun drammatico cambio di paradigma l'adozione di una valuta digitale centralizzata.
Purtroppo non sussistono al momento concreti piani d'azione per le CBDC in termini di quali strumenti permetteranno il loro utilizzo e più sul particolare nell'ambito del loro funzionamento.
La mia visione a riguardo è quella che verrà fatta questa manovra per concludere quella iniziata quando sono esistite le prime forme di valute virtualizzate (virtuali e digitali sono due cose differenti), un esempio concreto che avvalora la tesi secondo la quale il sistema sul quale ci basiamo ha delle falle.
La banca ha il ruolo di prestare denaro che le viene affidato in deposito dai clienti, in questa maniera riesce ad ottenere interessi su quel prestito e ad ottenere un profitto, potendo erogare degli interessi positivi sul deposito iniziale del cliente, questo è sapere comune.

Lambda si reca in banca per versare 1000€ in contanti sul suo conto corrente per poter disporre comodamente un bonifico dal suo cellulare una volta a casa, i 1000€ vengono nel giro di qualche ora accreditati sul suo conto.
Mettiamo caso che subito dietro a Lambda entri in banca anche Kappa, che invece ha bisogno di un prestito di 1000€.
La banca eroga il prestito a Kappa di 1000€ e accredita a Lambda altri 1000€, l'unico problema è che questi sono gli stessi, sdoppiati.
Per capire meglio ipotizziamo che la banca non abbia altri clienti e altri depositi in corso, non possegga altra liquidità oltre quei 1000€ versategli, letteralmente ha creato un migliaio di euro digitali.
Il sistema esistenziale che conduce lo stile di vita su cui basiamo tutta la nostra attuale esistenza, è ricco di queste fallacie tecniche, che vengono commesse perché è così complesso e universale che non vi è modo di riassestarlo.
Un modo potrebbe risultare quello di introdurre delle valute digitali univoche, che non avranno modo di essere sdoppiate perché non vi sarà un duplice canale di spendibilità.
Le bolle speculative, la crisi immobiliare del 2008 con la quale ho aperto questo elaborato, così come moltissime altre precedenti questo secolo e moltissime altre che giungeranno sono opera umana.
La storia non è ciclica, gli uomini lo sono.
Una rivisitazione di ciò che sosteneva il grande Machiavelli.
Rimanendo e terminando l'argomentazione sulle valute digitali delle banche centrali, il loro obiettivo ufficiale riguarda una serie di funzionalità legate alla privacy, alla trasferibilità, all'accessibilità e alla sicurezza finanziaria generale.
Si auspica poi un minore costo di mantenimento, non avendo concretamente più nulla di tangibile da mantenere e rifornire, ma solo degli algoritmi da revisionare periodicamente.
Verrebbero ridotti i costi di transazione e di Forex (non eliminati come succederebbe con bitcoin, ma mantenuti e ribassatati per far contente entrambe le parti), un controllo centrale significa però anche una stabilità maggiore, una tutela più ampia e un controllo sul meccanismo economico più subdolo e fisiologico tra tutti: l'inflazione.
È sicuramente prevedibile che non vi sarà un'introduzione forzosa, a scapito di quella fascia di popolazione che a causa di agenti temporali/ biografici non avrà la volontà e la possibilità di adeguarsi a tale sistema.
Il meccanismo fondamentale di questo sistema sta però nella sua diramazione in una riserva destinata ai governi e invece un circolante adibito alla quotidianità sociale.
Ci tengo a sottolineare che questa biforcazione è ancora una volta ispirata da quelle che sono le teorie ad opera dei massimalisti di Bitcoin e che approfondirò nel prossimo capitolo.
Riproponendolo in poche righe, in pratica sono state teorizzate due forme di CBDC, non è ancora chiaro se differiscano anche nella tecnologia o solo nel nome/ ruolo.
Ma la controparte governativa farà da riserva di quella circolante, riprendendo il tema in realtà attuale delle riserve monetarie presenti in ogni banca centrale al fine di garantire un controvalore (del tutto inverosimile) alla totalità del denaro presente in un paese.

14. **I problemi delle CBDC**

Se i benefici possono essere vari, le problematiche legate a questa novità sono a loro volta molteplici, come d'altronde accade per ogni nuovo prodotto.
Primo fra tutti quello inerente al tema della sensibilità in termini di privacy, con la tecnologia odierna e i metodi che io personalmente conosco riguardo questo argomento, non esiste attualmente sul mercato una criptovaluta che abbia come caratteristiche salienti nulla che si avvicini al reale parallelismo tra controllo (o che dir si voglia tutela) e privacy.
Ancora una volta sottolineo che non intendo anonimato in senso lato, bensì una forma di reale attenzione alla riservatezza sull'utilizzo del proprio denaro.

Gli organi regolatori delle valute governative, per forza di cose, devono potersi assicurare un portale di accesso/ intrusione tra i propri utenti.
Anche in questo frangente dipende dai punti di vista soggettivi, i più tanti direbbero che quello dell'intromissione è un prezzo adeguato per una maggiore sicurezza, molto altri sosterrebbero invece che se il costo è il dover spendere il proprio denaro previa approvazione statale, preferiscono cambiare metodo o tornare al contante.
In linea generica le banche centrali devono assicurarsi che i danni e la spossatezza provocata dall'immissione nel mercato di questo progetto non superino le aspettative dei benefici, e per questo ci stanno volendo tutti questi anni: si stima che le CBDC entreranno in vigore in Unione Europea e USA attorno al 2026.
Così come al contrario è successo alla presidenza Bukele in El Salvador, credendo che il rientro finanziario dovuto a bitcoin fosse più armonioso e fisiologico, oltre che meno duraturo, l'Unione Europea non può permettersi che accada.
Non c'è confronto tra le due entità, non vi è possibilità che un così drastico cambio di paradigma nel sistema economico sia dannoso per una delle zone (a livello economico e non) più avanzate al mondo.
Un altro problema che dovrà essere sostenuto è che un così importante appoggio alle tecnologie digitali attrarrà sicuramente dei criminali informatici molto differenti dai rapinatori che ci immaginiamo ora.
Diverrà dunque essenziale dotarsi di un sistema di difesa, ad opera di umani o di sistemi operativi, molto avanzato.
In ambito criptovalute gli hacker sono sempre in attesa che vi sia un errore o una svista per poter assumere un ruolo parassitario.
È successo che ad essere veicolo inconscio della svista fosse proprio un operatore di un exchange o di un ente simil funzionante, provocando falle nel sistema anche di milioni di dollari.
In sintesi dunque le CBDC non sono criptovalute ma valute digitali e potrebbero dunque essere interpretate come un ibrido concorrenziale ad esse.
La tecnologica differenza strutturale è che, almeno nelle proposte attuali e nelle micro economie in cui già sono in parte presenti, le CBDC non hanno una blockchain sottostante.
Queste infatti non necessitano di nessuna sorta di decentralizzazione e tale "registro transazioni" assomiglia ad una blockchain privata, il punto focale è che non vi è meccanismo di consenso orizzontale da parte un minatore/ validatore, bensì verticale da parte di un ente istituzionale.
Le criptovalute sono al momento estremamente volatili e incerte, talvolta la loro creazione avviene per gioco e la loro scomparsa la segue quasi subito; è un mercato ancora parecchio acerbo e poco regolamentato e per questo motivo bisogna saper discernere i progetti validi da quelli non lo sono, è necessario stare attenti a dove sia bene destinare i propri risparmi.
Le CBDC saranno ancorate alla valuta di riferimento e sorrette da un corrispettivo, esattamente come Tether o altre StableCoin (USDC, TUSD, EURT, EURC, BUSD, solo per citarne alcune).
Il corrispettivo che sorregge tali valute non è più sicuro delle valute digitali stesse, poniamo solo più fiducia in esso. Come ho cercato di spiegare attraverso la storiografia della moneta, il dollaro è ormai la riserva di valore più gettonata e detenuta dalle banche centrali, ma lo stesso ha un valore che non si rifà al più importante dei concetti legati alla definizione di moneta, il dollaro (intendendo una qualsiasi moneta FIAT moderna) ha probabilmente il più basso ratio ratio stock to flow nella storia della moneta.
Brevemente presento un elenco di quelle realtà che hanno già iniziato a sperimentare una valuta digitale centralizzata.
Per motivi logistici sono tutte nazioni di piccole dimensioni e/o con un'economia particolarmente carente: Bahams, Antigua, Barbuda, St. Kitts e Nevis, Monserrat, Dominica, Santa Lucia, San Vincent e Grenadines, Grenada e Nigeria.
Quest'ultimo paese è l'unico di grandi dimensioni ad essersi inerpicato in questa innovazione.

Altri 18 stati hanno già un programma pilota pronto (o quasi) per l'approccio al mercato reale, tra le quali 7 fanno parte del G20.
Inoltre 32 paesi sono in fase di sviluppo.

15. **La Russia**

Nella fase finale di questo secondo capitolo voglio portare un ultimo esempio pratico ed estremamente attuale di adozione, sebbene parva del tutto estemporaneo.
La guerra in corso tra Russia ed Ucraina (in questo contesto cercherò di usare espressioni denotate da più neutralità possibile) perpetua da ormai più di un anno, più precisamente il 24 febbraio 2022 è il giorno in cui la Federazione Russa ha dichiarato stato di guerra e ha intrapreso l'offensiva.
La risposta dell'occidente non è proceduta in un fronte comune di difesa militare, quanto piuttosto nella fornitura discretamente omogenea di armi belliche e mezzi corazzati; parallelamente sono seguiti ad opera dell'Occidente, questa volta in maniera realmente unitaria, numerose limitazioni in termini di cessate trattazioni e accordi internazionali, bloccando gran parte dell'economia verso e di ritorno dalla Russia, privando gli occidentali delle riserve di gas naturale che quelle terre fornivano regolarmente alla maggior parte dei grandi paesi europei.
Le ripercussioni a danno della Russia sono sicuramente state ingenti, ma non è frequente che le informazioni trapelino fuorvianti e illusorie dai paesi che, se non sulla carta, sono totalitari.
Nonostante dopo circa un anno l'economia russa si stimi essere ritornata al principio del conflitto, anche e soprattutto grazie ad altre due potenti nazioni, non particolarmente interessate a favorire l'egemonia occidentale, quali India e Cina, è innegabile che la nazione tutta abbia risentito di tali limitazioni e ne stia accusando ancora adesso.
Per quel che interessa questa tesi, è estremamente utile ripercorrere i passi che Putin, assieme ai vertici di oligarchi e assistenti operativi, abbia seguito per rendere le criptovalute materia di stato.
Non c'è interpretazione al movente che sostiene questo repentino avvicinamento alle valute digitali, mesi antecedenti alla guerra e conseguentemente alle sanzioni, la linea dura del governo Putin su questo tema era decisamente chiara.
La Russia era prossima all'introduzione della propria CBDC[45] nella fase terminale del 2021: il Rublo digitale, causata probabilmente dalle tensioni in atto nei mesi precedenti alla guerra con Unione Europea e Stati Uniti.
Le criptovalute sono state bandite dalla Banca Centrale, sostenendo la possibilità che venissero utilizzate per scopi criminosi e spiegandone la loro volatilità rischiosa.
Un focus particolare su come, a differenza della limitrofa Cina, non siano state vietate le attività di mining di bitcoin, decisamente profittevoli sia internamente e sia come alternativa per le compagnie cinesi in cerca di un nuovo "terreno di estrazione".
Un paio di mesi dopo la prospettiva russa però cambia, contemporaneamente al mutare della situazione geopolitica e ai divieti economici posti dall'Occidente.[46]
La Russia diviene il terzo paese al mondo per utilizzo di criptovalute dopo India e Stati Uniti, la causa di questa adozione massiccia è la grande volatilità del rublo, che a quanto sembra non si è dimostrato poi una così solida alternativa a bitcoin.
Il mercato russo deteneva all'epoca il 12% dell'intero mercato cripto global, 214 miliardi di dollari. Questo esplica abbastanza palesemente perché il governo abbia cambiato rotta, approcciandosi alla regolamentazione invece che vietarle, provando a garantire un'alternativa che avrebbe reso quel momento di crisi geopolitica anche una crisi finanziaria da sommare a quella del tracollo del rublo.
Nel marzo del 2022[47], il viceministro ucraino ha fatto un appello sui social per chiedere ai maggiori exchanges internazionali di bloccare unilateralmente le transazioni cross-border (tra i confini russi).
A tutti gli effetti infatti la popolazione (e non solo) russa ha iniziato ad usare i servizi delle

valute digitali (non CBDC) per aggirare le sanzioni occidentali.
Avendo la NATO escluso la nazione dal sistema interbancario Swift e dato l'obbligo di congelare le riserve in valuta estera della Banca centrale russa.
L'8 giugno 2023, oggi, è arrivata la notizia che la maggiore banca russa offrirà servizi di compravendita di criptovaluta[48] , prendendo il ruolo di exchange ufficiale della Federazione.
Sì, questi ultimi giorni sono stati particolarmente ricchi di controversie in questo settore.
Quest'ultima vicenda dimostra ancor di più come la decentralizzazione di questi prodotti sia appositamente ideata per raggirare le censure.
L'utilizzo proprio o improprio di questa tecnologia di per sé stessa amorfa sta solo alla società.

16. **Approfondimenti**

Al pari del capitolo precedente scrivo alcune domande che mi sono posto durante la stesura o che sono semplicemente in affinità con le tematiche affrontate in queste pagine.
La prima riguarda gli exchanges:

- *Gli exchanges sono enti centralizzati, questo non è in aperto contrasto con l'ideologia fondamentale delle criptovalute?*
  Sì, la decentralizzazione pura è garantita solo mediante l'utilizzo di Bitcoin, gli exchanges sono tecnicamente enti che hanno funzione intermediaria che fanno da nodo centralizzato di scambi e opportunità secondarie su blockchain.
  Questi attori sono al momento gli unici che offrono un metodo semplice e alla portata di tutti per accedere ai servizi riguardanti le valute digitali, per queste ragioni le persone ne fanno uso.
  Ne esistono diversi come ho fatto notare, con sedi, dimensioni, politiche e interessi differenti.
  Spesso alcuni dei servizi che offrono sono associabili a strumenti finanziari derivati (che operano mediante leva finanziaria, mettendo a rischio il capitale dell'utente, il quale però ricordo essere sempre pienamente fautore delle proprie azioni).
  A mio avviso il posto più sicuro per detenere bitcoin e criptovalute resta un Wallet personale e privato; soggettivamente ritengo che sia utile depositare e far transitare i provi "averi digitali" da exchanges rigorosamente affidabili e con quelli che in gergo sono chiamati "audits", cioè certificazioni ad opera di enti appositi.
  Io detengo una parte delle mie criptovalute su diversi exchanges, avendo cura periodicamente di visionarle e tenendomi giornalmente aggiornato su ciò che accade nel mercato e se sussistono variazioni importanti.
  La branca che so che andrò a maneggiare relativamente più spesso sarà dunque alla mia portata diretta (letteralmente a portata di tap sul display del mio cellulare), la porzione che invece so che deterrò senza andare a vendere per funzione speculativa, la custodisco su un Wallet staccato da tutti i servizi terziari di exchanges o affini.

- *Tra le criptovalute alternative a bitcoin, quali sono le più importanti?*
  Esistono oltre un migliaio di criptovalute successive a bitcoin, dalle quali in misura maggiore o minore quasi tutte prendono spunto.
  Anche le valute che lo screditano, hanno basato interamente il loro progetto in funzione di proporre un progetto migliorativo di bitcoin stesso.
  La seconda e più famosa è quella programmata dal russo Vitalik Buterin, il cui nome completo sarebbe Vitaliy Dmitrievič Buterin. Questo sviluppatore e scrittore russo naturalizzato canadese è un grande appassionato di informatica e del mondo della finanza, più nello specifico del fintech.
  Nel 2013, all'età di 17 anni, ha fondato la piattaforma di Web 3.0 Ethereum (web 3.0 è utilizzato dal linguaggio dei social e ha preso piede in questo modo per intendere un modo innovativo di intendere l'interconnessione di più terminali e, la novità del web 3.0,

anche oggetti quotidiani o addirittura concettualmente intimamente i nostri stessi corpi).
Ethereum[49] è ormai arrivato a raggiungere lo stato di un'insieme di servizi finanziari, inizialmente però è nato come "smart contract", dei quali ho già trattato ma che ripeterò qui, "contratti intelligenti", ossia delle clausole algoritmicamente predisposte che, allo scadere di un'azione, ne predispongono automaticamente una seconda, senza alcun intervento o supervisione umana.
Ethereum è quello che potremmo definire come il principale attore della finanza decentralizzata e dei Non Fungible Token.
Il totale di ether presenti in circolazione hanno un controvalore di 222,720,175,009 dollari e, considerando che, come bitcoin, la nascita di questo progetto non è di portata istituzionale ed è avvenuta in anni in cui vi era un certo senso verso le valute digitali, ma era decisamente avvolto dal mistero e non definitivo, questo progetto è letteralmente strabiliante.
Ethereum è una multi piattaforma che offre l'accesso a domini internet web 3.0 e che al posto del tradizionale ".com" offre un più originale ".eth".
La maggioranza delle piattaforme di prestiti e debiti affondano su blockchain Ethereum, le quali si occupano autonomamente di bloccare il corrispettivo che viene depositato a garanzia del prestito erogato.
L'80% degli NFT presenti sul mercato sono infrastrutturalmente appoggiati ad Ethereum.
Una buona percentuale, che in realtà giornalmente è sempre minore a causa della forte competizione, di criptovalute tokenizzate, prive cioè di una propria blockchain, usufruiscono di quella di Ethereum.
Una seconda criptovaluta che vorrei trattare e che differisce in grande misura dalle altre è Monero, definita "La maggior privacy coin" (impropriamente detta "privacy coin" dai cripto amatori, in quanto solitamente loro sono a conoscenza del fatto che bitcoin come molte altre non siano realmente solide in materia di privacy, nel senso comunemente inteso)
Questa è anonima, intendo dire che si basa su un meccanismo che rende celato al pubblico l'indirizzo di ricezione e di invio delle criptovalute.
Questa valuta viene considerata letteralmente irrintracciabile e per questa ragione viene solitamente utilizzata in sezioni illegali del web, da giornalisti, soggetti sotto protezione dello stato o persone sensibilmente a rischio.

- *Nei paesi in cui bitcoin e le criptovalute non sono legali, esistono altri modi per entrarvi in contatto?*
  Nei paesi in cui tali valute sono illegali, il rischio di incorrere in pene pecuniarie e talvolta detentive è tangibile, dunque rischiare non è consigliabile.
  Non potendo fisicamente costruire fabbriche di mining di bitcoin, le persone possono solamente continuare in maniera tacita a detenere bitcoin, essendo ovviamente limitati ad operare senza approcciarsi mai ad enti che siano siti nel settore bancario e debbano dare conto ad un qualsiasi governo istituzionale.
  Negli ultimi anni è anche emerso un metodo alternativo per minare criptovalute "su delegazione"; questo metodo viene definito cloud mining e consiste nel delegare la potenza di calcolo del proprio computer ad un punto di ricezione, avendo più terminali come ho spiegato nel processo di mining, la probabilità di ottenere la ricompensa del blocco aumenta.
  Ottenuta la ricompensa essa viene suddivisa tra i portali facenti parte del processo di mining.

- *Esistono delle alternative agli exchanges?*
  La questione della centralizzazione degli exchanges ha suscitato fin da subito uno scontro di ideali tra i massimalisti di bitcoin e gli speculatori e ideatori di altri progetti e gli exchanges.
  Recentemente questo problema è stato arginato dalla svolta decentralizzata degli exchanges, chiamati DEX, decentralized exchanges.

Questi DEX non hanno un vertice e funzionano interamente tramite algoritmi e smart contratto, essi stessi essendo vincolati a smart contracts per esempio di Ethereum funzionano solo con token che abbiano la medesima struttura e blockchain (quindi di Ethereum)
Si stanno sviluppando parallelamente e secondo un gruppo sempre più sostanzioso di appassionati rappresentano il reale proseguo delle criptovalute, sono ormai ricchi di funzionalità e nell'ultimo anno si stanno diffondendo anche piattaforme decentralizzate trasversali, che permettono dunque lo scambio anche su diverse blockchain.

- CAPITOLO TERZO -
L'OPZIONE BINARIA

In questo capitolo conclusivo vorrei analizzare quelli che potrebbero divenire i diversi percorsi che le tecnologie descritte fino ad ora potranno intraprendere o meno nel corso dei prossimi anni o decenni.
Io ho ipotizzato un duplice e lineare scenario:
- Il primo in cui questa valuta perda l'appiglio ideologico su cui può far affidamento ora e cada nell'abisso di tutte quelle valute che sono decorse nella storia umana, facendo la fine delle innovazioni dimenticate a causa del loro fallimento.
- Il secondo viceversa in cui bitcoin venga accettato totalmente e divenga valuta legale della totalità (o quantomeno la stragrande maggioranza) dei paesi mondiali.

1. **Opzione in cui il protocollo Bitcoin venga abbandonato.**

La possibilità in cui il network rimanga spopolato è sempre stato di fondo un timore diffuso da parte degli appassionati di Bitcoin, e andrebbe di pari passo con la perdita di significato da parte dei minatori e di attrazione da parte del pubblico.
Bitcoin è resistito resilientemente dal 2008 ad oggi, ma si prospettano altri 120 anni prima che il suo ciclo si concluda per quello che è stato concettualizzato da Satoshi; e dato che l'essere umano tende a cambiare idea e approccio diverse volte nella propria vita, quattro generazioni risultano essere tanto tempo.
Il principale delle dinamiche che potrebbe però, a mio avviso, portare ad un bando compulsivo di Bitcoin, non sarà tanto dovuto alla sua minaccia diretta, plausibilmente a causa di computer quantistici, di crolli totali del mercato o di alternative migliori, bensì il più probabile agente di divieto internazionale e massiccio di tale tecnologia sarà la stessa Madre Natura.

2. **Le dinamiche biosostenibili**

L'attenzione alla sostenibilità in termini ambientali è nata con la consapevolezza dell'atrocità di cui l'uomo può essere capace, se spinto ad agire dai giusti interessi.
La fine dell'innocenza e neutralità della tecnologia è stata percepita per la prima volta il 6 agosto 1945 e ribadita con grande forza il 9 dello stesso mese; i bombardamenti di

Hiroshima e Nagasaki hanno palesato a tutto il mondo quanto avanzate fossero le armi di distruzione di massa già all'epoca.
Gli Stati Uniti stessi non si aspettavano una tale devastazione, e soprattutto la ripercussione che c'è stata poi negli anni a venire.
Questo fattore scatenante ha nel tempo spostato il mirino pubblico sulla scienza intesa ora come capace anche di provocare dei danneggiamenti, e non solo del benessere alla società.
Bitcoin ha scoperto il lato peggiorativo per l'ecosistema all'aumentare delle transazioni, che corrisponde all'aumentare delle emissioni.[50]
Si stima che i danni ambientali e climatici ad opera del protocollo Bitcoin dall'inizio dell'anno 2021 al suo epilogo siano di circa 11.300 dollari.
La spesa dipende dal fatto che sia necessaria molta energia per la potenza computazionale da destinarsi al suo mining.
Uno studio ha ipotizzato che circa un terzo del valore di ogni singolo bitcoin estratto è "speso" in danni di questo calibro tra il 2016 e 2021.
L'industria di estrazione di bitcoin è paragonata ad alcune tra le meno rispettose dell'ambiente, insieme a quella della carne bovina e della produzione del greggio.
In totale i danni provocati dall'azione di minare bitcoin tra il 2016 e il 2021 è stata approssimata a 12 miliardi di dollari.
Importante notare come in questo articolo venga calcolato solo il grado di inquinamento di Bitcoin, ma non sono tenute in considerazione le altre criptovalute nel loro insieme.
È fortemente prioritaria la necessità di riconoscere la non negoziabilità dell'ambiente a noi circostante, questo in termini assoluti e non solo intesi come protocollo e valute digitali.
Rischieremmo altrimenti quella che Latour definiva come "L'intrusione di Gaia", che sta a significare che prima o tardi, se la nostra specie non cambierà politiche riguardo il tema ecosostenibile, Gaia (la terra) ci inghiottirà a sua volta.
Non per una sua volontà diretta, certamente, bensì per un naturale corso della storia organica, che rispetto all'età geologica del nostro pianeta non è altro che un lungo sospiro.
L'ecosistema nella scala dei bisogni di Maslow è letteralmente ciò che rende possibile i bisogni fisiologici su cui si fondano tutti gli altri, la struttura che sorregge l'intera piramide.
La transizione verso una "finanza verde" più attenta al pianeta dovrebbe essere prioritaria, cercando, per quanto possibile, di evitare un "effetto rimbalzo": fenomeno che si presenta quando all'aumentare dell'efficienza di una tecnologia aumenta a dismisura la sua portata e fruizione, di conseguenza l'altissimo numero di richieste hanno un maggiore impatto nel totale, anche se di minore entità singola.

3. **Opzione in cui il protocollo Bitcoin venga adottato totalmente.**

Bitcoin, come ho diverse volte già anticipato, non potrà avere una nicchia di utilizzatori di minoranza in rapporto a quello che è il sistema economico mondiale, bensì per poter funzionare dovrà posizionarsi in posizione di prevalenza/ maggioranza rispetto ad altri sistemi monetari.
Non è in realtà obbligatorio, e in realtà è quasi impossibile, che vi sia un 100% del circolante in bitcoin.
Il network di Bitcoin al suo stato attuale non è in grado di superare le 500.000 transazioni in un singolo giorno, dunque mostra evidenti problemi infrastrutturali che non gli permetteranno di diventare un'efficiente valuta per l'economia quotidiana.

4. **L'oro digitale**

L'alternativa vincente richiederebbe un cambio radicale di paradigma da parte degli enti governativi, dovrebbe esserci un mutamento: dall'essere concorrenti di Bitcoin a detenerli

nelle proprie riserve dello stato.
Questo è sinonimo di centralizzare una valuta che ho per tutto l'elaborato fatto intendere non abbia volontà di essere centralizzata, in questo caso avrebbe però un fine differente.
La decentralizzazione e la sua scarsità sono ciò che rendono bitcoin diverso da qualsiasi altra valuta mai esistita prima di esso.
Ma obiettivamente parlando, è evidente quanto il singolo comune individuo non sia in grado di gestire le proprie finanze; l'educazione in questo ambito è molto diversa da famiglia a famiglia e la società finirebbe per rimanere priva di monete, indebitandosi e facendole fluire verso le poche tasche dei più talentosi uomini d'affari.
Il ruolo dello stato entrerebbe in gioco in questo frangente specifico, cioè con il preciso ruolo di detenere bitcoin con la funzione di riserva di valore: quello che fino al secolo scorso era il ruolo ricoperto dall'oro classico.
Essendo di quantità fissa non sarebbero possibili tutte le dinamiche che, all'ordine del giorno, aumentano l'inflazione, diminuiscono il circolante o saldano un debito miliardario denominato "student loan" nel giro di una decisione in parlamento.
Tutto ciò non sarebbe più possibile, il mercato diventerebbe fisiologico e legato ad un reale valore intrinseco.
Bitcoin diverrebbe il controvalore, idea che per l'appunto attrae gli economisti che stanno lavorando alle CBDC suddividendole in due utilizzi, di una moneta dedita invece a tutte le transazioni giornaliere della popolazione.
Non importa in linea di principio se vi saranno più valute nazionali, internazionali o una comunitaria: il fattore determinante diventerà il sottostante unico a tutte le banche centrali, facenti parte di un'unitaria e collettiva economia, e il vincolo assoluto a mantenere un valore totale di moneta circolante esattamente paritario alla riserva presente nel proprio paese.
Bitcoin non è positivo o negativo, il suo ruolo è stato fin dal principio quello di dare controllo agli individui del proprio denaro, affidandogli uno strumento equilibrato e che non seguirà mai gli egoismi umani improvvisi, ma solo il proprio e immutabile algoritmo.

SITOGRAFIA:

1. https://criptonomist.ch/2021/05/09/storia-bitcoin/
2. https://bitcoin.org/it/documento-bitcoin
3. https://bitcoinmagazine.com/culture/genesis-files-how-david-chaums-ecash-spawned-cypherpunk-dream
4. https://www.nytimes.com/1999/11/11/technology/what-s-next-a-cloak-for-shoppers-web-dollars.html
5. https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges
6. https://btcscan.org/tx/recent
7. https://bitcoin.org/en/full-node#what-is-a-full-node
8. https://bitcoin.org/en/download
9. https://criptonomist.ch/2022/11/04/bitcoin-metodo-pagamento-piu-utilizzato/
10. https://criptonomist.ch/2021/08/24/bitcoin-prezzo-crescita-transazioni/
11. https://it.cointelegraph.com/news/bitcoin-network-node-count-sets-new-all-time-high
12. https://lightning.network/
13. https://www.investopedia.com/news/20-all-btc-lost-unrecoverable-study-shows/
14. https://bitinfocharts.com/top-100-dormant_5y-bitcoin-addresses.html
15. https://triple-a.io/cripto-ownership-data/
16. https://www.rainews.it/articoli/2023/05/bankitalia-nuovo-record-per-il-debito-pubblico-a-marzo-ha-sfiorato-i-2790-miliardi-d26cd100-759b-4dae-a41e-c623bbd93fc1.html
17. https://it.cointelegraph.com/news/binance-ceo-cz-richest-cripto-billionaire-at-96b-bloomberg]
18. https://www.visualcapitalist.com/bitcoin-is-near-all-time-highs-and-the-mainstream-doesnt-careyet/
19. https://finecobank.it/finecoX/
20. https://pancakeswap.finance/
21. https://www.phrases.org.uk/meanings/40500.html]
22. https://www.xe.com/it/currencycharts/?from=XAU&to=EUR
23. https://www.studenti.it/la-germania-dopo-la-prima-guerra-mondiale-riassunto.html
24. https://www.visualcapitalist.com/buying-power-us-dollar-century/
25. https://viaggio-in-germania.de/inflazione-1923.html
26. https://www.hardmoneyhistory.com/rentenmark/
27. https://www.federalreservehistory.org/essays/gold-convertibility-ends
28. https://www.visualcapitalist.com/cp/how-reserve-currencies-evolved-over-120-years/
29. https://coinmarketcap.com/rankings/ exchange/
30. https://www.ilsole24ore.com/art/la-sec-accusa-binance-violate-regole-federali-finanza-AEegCiaD
31. https://www.sec.gov/news/press-release/2023-102
32. https://www.money.it/Criptovalute-chi-le-sta-usando-di-piu-nel-mondo-la-mappa
33. https://www.bbc.com/news/technology-58678907
34. https://www.istat.it/it/archivio/sommerso
35. https://www.postfinance.ch/it/privati/esigenze/guida-semplice-e-chiara-agli-investimenti/tutto-quello-che-dovete-sapere-sui-bitcoin.html
36. https://criptonomist.ch/2021/10/11/referendum-in-svizzera-per-legalizzare-il-bitcoin/
37. https://criptonomist.ch/2021/10/11/referendum-in-svizzera-per-legalizzare-il-bitcoin/
38. https://planb.lugano.ch/
39. https://time.com/6236899/el-salvador-bukele-bitcoin-crash/
40. https://www.ansa.it/ansa2030/notizie/asvis/2021/07/23/il-mondo-rischia-il-piu-grande-aumento-delle-disuguaglianze-della-storia_21371981-7766-4e58-b91d-ccdb08f6b795.html
41. https://forbes.it/2021/09/24/la-cina-dichiara-illegali-le-transazioni-di-criptovalute-il-bitcoin-precipita/
42. https://forbes.it/2021/06/23/la-cina-continua-la-guerra-alle-cripto-e-le-societa-di-mining-emigrano/
43. https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp
44. https://www.corriere.it/economia/mobile-payment/notizie/svezia-viaggio-paese-dove-denaro-contante-quasi-sparito-22492742-fd8d-11e9-8a58-4dee50fcf96c.shtml
45. https://criptonomist.ch/2021/12/20/russia-banca-centrale-ban-criptovalute/
46. https://criptonomist.ch/2022/02/03/russi-mercato-criptovalute/
47. https://forbes.it/2022/03/01/gli-utenti-russi-si-affidano-alle-criptovalute-per-aggirare-le-sanzioni-volano-bitcoin-ed-ethereum/
48. https://watcher.guru/news/sberbank-russias-largest-bank-will-offer-cripto-trading-services
49. https://ethereum.org/en/
50. https://forbes.it/2022/10/06/bitcoin-industria-inquinamento-pianeta/