Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Informatica per il Management

Il consumo energetico di Blockchain, i modelli Proof-of-Work (PoW) e Proof-of-Stake (PoS) a confronto

Relatore:
Chiar.mo Prof.
Davide Sangiorgi

Presentata da:
Filippo Brajucha

Sessione Marzo 2023
Anno Accademico 2021/2022

Dedico questa tesi
ai miei genitori, Paola e Giovanni
e alle mie sorelle, Alessandra e Ludovica.

Introduzione

La velocita' e la capillarita' con la quale l'idea di blockchain e moneta digitale di Satoshi Nakamoto e' stata sviluppata, implementata ed adottata e' a dir poco sconvolgente.
Il grande sogno di una valuta decentralizzata il cui valore viene deciso direttamente dal mercato senza l'intrusione di terze parti, come ad esempio le banche, ha reso i token digitali un paradiso per gli speculatori finanziari che negli ultimi anni hanno deciso di investire in queste nuove tecnologie.
Il recente sviluppo del settore ha portato una mole gigantesca di dati da gestire ed eleaborare; queste operazioni, ovviamente, comportano un consumo energetico al quale bisogna prestare molta attenzione. Nel momento in cui sono state sviluppati questi sistemi non si poteva certo prevedere cotanto successo pero' ora bisogna affrontare e ri-adattare le tecnologie scalandole, studiandole ed adattandole anche in questa ottica.
Il consumo resta un topic molto vociferato e discusso negli ultimi anni. Esso ci sta portando, inesorabilmente, ad un futuro in cui tutti dovremo prestare molta piu' attenzione di quanto gia' non facciamo.

Indice

Elenco delle figure

Elenco delle tabelle

Capitolo 1

La Blockchain e le Cryptocurrencies

Questa tecnologia non e' altro che un grande registro dove si tiene traccia delle operazioni che vengono eseguite. Ad esempio nel caso delle cryptovalute vengono memorizzate le transazioni effettuate, tenendo conto sia dell'importo, che dell'indirizzo del mittente e del ricevitore. Il vantaggio principale e' che tutti ipoteticamente potrebbero scrivere e aggiungere righe a questo elenco, ma il dispositivo che effettivamente si occupera' di scrivere e certificare la transazione e' solo uno e viene deciso con diverse tecniche a seconda della tecnologia adottata da quella specifica blockchain.

1.1 La Storia

La blockchain e' una tecnologia ideata da Satoshi Nakamoto all'incirca nel 2009. L'idea era quella di creare un sistema di pagamento e di scambio di denaro decentralizzato e indipendente dalle banche. Egli si ispiro' al concetto di "cryptocurrency" esposto ed elaborato per la prima volta nel 1998 da Wei Dai, un'ingegnere informatico cinese, lo adatto' alla teconologia della blockchain e sviluppo' "Bitcoin", la prima moneta digitale basata su un meccanismo di Proof-of-Work.

Satoshi annuncio' il suo progetto in un paper pubblicato tramite la mailinglist "the cryptography" in cui affermava di aver rivoluzionato il mondo della finanza ma non venne subito preso seriamente. Ci vollero anni affinche' la valuta venisse mondialmente accettata e considerata valida e il processo e' tutt'ora in corso. Nel frattempo Bitcoin aumenta il suo bacino di utenza sempre di piu', facendo aumentare anche la dimesione della blockchain sulla quale vengono annotate tutte le transazioni, essa passa infatti dai 20GB del 2014 a quasi 500GB di inizio 2022 [14].
Parallelamente allo sviluppo di Bitcoin si puo' osservare anche una proliferazione del mercato dei token digitali che adesso sono centinaia e centinaia. Molto spesso vengono sviluppate con tecnologie simili ma non proprio identiche al sistema PoW di Bitcoin. Ad esempio la moneta "Etherum" si basa sul sistema Proof-of-Stake (PoS) oppure "Solana" su Proof-of-History (PoH).

Figura 1.1: Valore del Bitcoin in Dollari dal 2018 ad oggi

1.2 Principali utilizzi

Le qualita' principali che si possono individuare nella blockchain sono l'integrita' e l'accessibilita'. Vuol dire che tutti possono leggerla o scriverci

ma nessuno e' in grado di apportare modifiche, esse sono delle rettifiche che vengono comunque scritte lasciando anche l'operazione considerata errata.
Queste qualita' la rendono una tecnologia estremamente malleabile e basilare, risulta adattabile a diversi contesti oltre che a quello finanziario. Infatti, molte aziende di consulenza e supporto tecnologico aziendale come IBM, Accenture, EY si sono affacciate a questo mondo e hanno contribuito alla ricerca e allo sviluppo producendo diversi software ad hoc basati proprio sull'idea di Nakamoto.
Essa viene largamente utilizzata nell'ambito della sharing economy o dell'archiviazione, pubblicazione e certificazione di dati, viene impiegata anche per creare e gestire i contratti elettronici (smart contracts) oppure per tracciare le supply-chains e i rapporti fornitori-venditori. Anche molti Stati si stanno adoperando per sfruttare questa tecnologia in ambito istituzionale, come ad esempio in Svezia, dove viene impiegata per gestire le informazioni catastali.

Capitolo 2

Consumi energetici

I consumi energetici di blockchain sono dovuti principalmente al mining, quindi al modello classico PoW, quello ideato da Nakamoto. Egli sicuramente non aveva calcolato che la tecnologia avrebbe ottenuto tanta notorieta' da mettere in competizione i vari "miner" per certificare le transazioni, infatti ognuno di loro cerca di avere il dispositivo piu' potente e performante per risolvere prima il calcolo che permette di validare e ottenere la ricompensa. Con la diffusione della tecnologia e' aumentato il bacino di utenza e quindi si e' passati da qualche user che cedeva la propria potenza di calcolo alla blockchain di bitcoin a vere e proprie aziende con super-computer costruiti ad-hoc con processori e/o schede grafiche in grado di eseguire i calcoli molto piu' rapidamente, rischiando quasi di perdere cosi' il concetto di decentralizzazione.

2.1 Criticita'

Il consumo dovuto al mining su blockchain aumenta sempre di piu', il mercato ha raggiunto una capitalizzazione di circa 1,75 milioni di milioni di dollari (trilions) [**?**]. Si stima che Bitcoin consumi ogni anno circa 150 TWH di energia, l'equivalente di piu' di 7 milioni di argentini che consumano circa 21 mila kWh/anno di energia [13]. La stessa moneta produce ogni anno 65

MegaTonnellate di CO2 [9], il principale gas responsabile dell'effetto serra.
Questi consumi spropositati sono dovuti alle migliaia di validazioni che vengono fatte costantemente da tutti i componenti elettronici, certamente non pensati nell'ottica del risparmio energetico ma piuttosto dell'efficienza, che lavorano freneticamente per risolvere i dilemmi crittografici che portano alla certificazione della transazione e alla ricompensa.
Attorno alla validazione delle transazioni si e' sviluppato un vero e proprio tessuto economico composto dai produttori di hardware sviluppato ad-hoc, grandi aziende che assemblano super computer e possessori di interi palazzi dedicati al mining, dei posti in zone remote e fredde della terra per facilitare il raffreddamento.
Fino a poco tempo fa era molto comune costruire questo genere di palazzi in Cina, dove non vigeva nessuna legge sulla produzione energetica e quindi si sfruttavano tecnologie a bassissimo costo come il carbone.

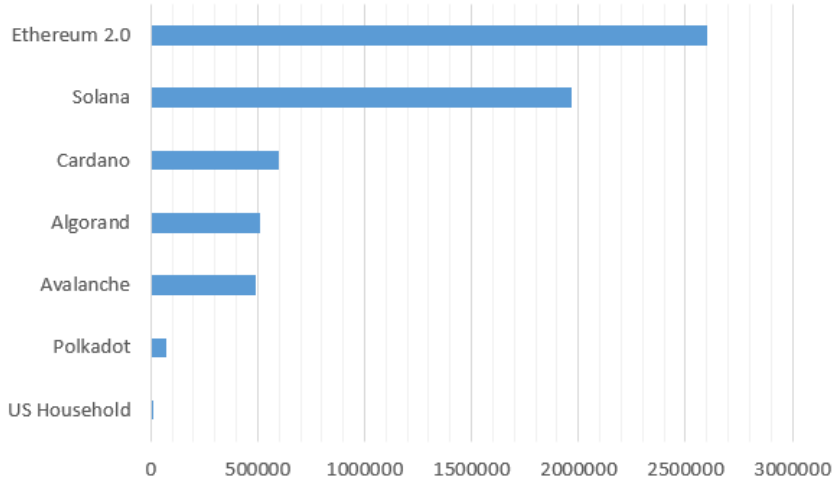

Figura 2.1: Consumo elettrico di crypto-assets PoS annuo in kWh

2.1.1 Gas Serra

Ovviamente, strettamente correlato ai consumi elettrici, possiamo parlare anche di inquinamento dovuto alla produzione di gas serra. Non e' facile dare dei numeri precisi perche' le quantita' di sostanze inquinanti emesse nell'atmosfera sotto forma di gas serra o altro vengono stimati, partendo da quanta energia viene prodotta bisogna considerare come viene prodotta e dove. Le condizioni climatiche e legislative fanno variare molto i dati che spesso oscillano.
A seconda di quanto dichiara Ethereum nel suo sito, grazie dal passaggio da PoW a PoS sono riusciti ad emettere il 99,992% di tonnellate di CO2 in meno [1], proporzionalmente e' definibile come la differenza tra l'altezza della torre Eiffel e un omino Lego.
Un report della Casa Bianca [14], invece, stima le emissioni di CO2 di Bitcoin a circa 100 Mt e accusa la moneta di provocare 2/3 dell'inquinamento globale dovuto alle crypto. Dice, inoltre, che il consumo e' aumentato di 10 volte il 5 anni (2017 - 2022). Sicuramente la colpa puo' essere attribuita anche alla Cina che e' stato per molto tempo un territorio perfetto per il mining, venivano anche impiegate molte energie rinnovabili come l'idroelettrico e il fotovoltaico, ma nel Settembre 2021 decide di mettere al bando questo business lasciando diminuire sempre di piu' l'utilizzo di energia pulita.

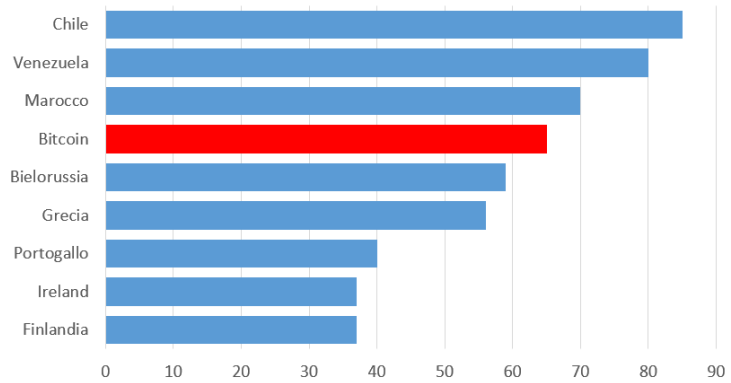

Figura 2.2: Milioni di tonnellate di CO2 emesse nel 2021

2.2 Punti di forza

Lo sviluppo repentino in un periodo storico cosi' sensibile alle tematiche ambientali ha fatto si che molti studiosi si siano adoperati per cercare di risolvere il problema del consumo energetico di questa tecnologia.
Tra le numerose idee quella che sicuramente e' stata piu' diffusa e' un'altra modalita' di validazione definita PoS, utilizzata dalla seconda moneta piu' importante: Ethereum.
Questo sistema permette di ovviare al problema del consumo energetico riducendo praticamente del 99% le emissioni di CO2. Non vengono infatti utilizzati calcoli computazionali per assegnare la ricompensa della validazione.
Nei sistemi PoS la transazione viene validata da un utente casuale che ha messo la propria macchina a disposizione posizionando in "stake" le proprie monete. La probabilita' di essere estratti aumenta a seconda delle monete che si hanno a disposizione.
L'obiettivo e' quello di eseguire una transazione verso questo sistema in modo da ridurre drasticamente l'inquinamento ed utilizzare solo il risvolto positivo della tecnologia.
Il problema sorge nel momento in cui, effettivamente, si rischia di far venire meno uno dei principi cardini di blockchain, la decentralizzazione. Esso infatti rischierebbe di essere messo in discussione dal fatto che chi ha molti token ha piu' probabilita' di essere il prescelto ad eseguire l'operazione, per questo viene inserita una variabile casuale che dovrebbe regolare e bilanciare il sistema.

2.3 Altri inquinamenti

Purtroppo l'inquinamento dovuto ai token digitali non e' fatto solo di consumi elettrici ed emissioni di gas serra, ma anche di consumi idrici e rifiuti elettronici (alcuni tra i rifiuti piu' difficili da smaltire in assoluto).
La Casa Bianca accusa i crypto-assets di danneggiare la salute umana, in-

quinando aria e acqua, producendo rifiuti solidi (come scorie e scarti) e provocando degradazione delle terre.
Stimano che un computer impiegato nel mining intensivo di Bitcoin possa consumare addirittura 63 mila galloni (290 litri ca.) di acqua per il raffreddamento delle componenti elettroniche, una cifra esageratamente alta se si pensa che e' circa il consumo annuale di acqua di una famiglia americana.
Inoltre viene considerato anche l'inquinamento acustico, infatti e' scientificamente provato che un ambiente rumoroso favorisce la diffusione di stress, disturbi del sonno e danni cardiovascolari.
Uno degli argomenti piu' sensibili, comunque, e' l'utilizzo e lo smaltimento delle famose terre rare per la produzione di hardware. Ethereum e il sistema PoS sono riusciti ad arginare abbastanza il problema aprendo la strada delle cryptovalute anche a chi utilizza dispositivi elettronici normali. Bitcoin e le altre crypto basate su sistemi PoW, d'altro canto, hanno aperto un mercato nuovo mercato di produzione in cui ogni sviluppatore cerca di produrre il dispositivo con le migliori prestazioni, utilizzando tutti i materiali come piombo, mercurio, cobalto, oro e altri che, ai giorni nostri, sono molto preziosi.
Il problema non e' tanto nell'impiego dei materiali che vengono comunque utilizzati, piuttosto nella frequenza con la quale queste macchine vengono sostituite. Viene stimato che a Giugno 2022 la produzione di materiale elettronico di scarto per il mining di Bitcoin e' di circa 35 mila tonnellate, l'equivalente dei rifiuti totali dei Paesi Bassi.
L'utilizzo dei sistemi ASIC (specifici per il mining intensivo con le blockchain di tipo PoW), in particolare, non vengono sviluppati con nessun altro scopo se non quello del mining e percio' vengono cambiati molto di frequente dalle aziende che si occupano solo di questo. Viene stimata una lungheza di vita media di circa 1 anno e 4 mesi.

2.4 Confronti

Sicuramente i consumi illustrati per quanto riguarda i crypto-assets sono spaventosamente alti. E' giusto, pero', eseguire un piccolo confronto sia con altri meccanismi di pagamento che con altre tecnologie.

2.4.1 Sistemi Finanziari tradizionali

Confrontare altri metodi di scambio di denaro o di pagamento, anche solo a livello energetico, non e' semplice. Vi sono molteplici differenze tra i sistemi tradizionali e le valute digitali che non possono essere calcolate. Come ad esempio i consumi dovuti al mantenimento delle banche che variano molto a seconda della filiale e del numero di dipendenti.
Nel 2020 i colossi bancari Visa, MasterCard e AmericanExpress dichiarano un consumo elettrico complessivo di tutte le operazioni effettuate tramite i loro circuiti di circa 0,5 miliardi di kWh [14], una cifra decisamente piu' bassa rispetto a quella di Bitcoin che, nello stesso anno, viene stimata intorno ai 100 miliardi di kWh [14].
La distanza tra i consumi aumenta ancora di piu' se si guardano i numeri delle transazioni effettuate: per quanto riguarda i circuiti di pagamento "ordinari" sono stati dichiarati 310 miliardi di operazioni, per i crypto-asset vengono sviluppati dei calcoli a partire dai consumi e dal numero di operazioni per blocco, stimando cosi' circa 460 milioni di transazioni effettutate sulle blockchain di Ethereum (ancora in fase 1.0, quindi con validazione PoW) e Bitcoin.
Eseguendo un confronto a livello matematico si puo' osservare come per effettuare lo 0,15% delle transazioni le monete digitali utilizzino 200 volte l'energia totale necessaria a tutte le operazioni tramite circuiti bancari.
Ipotizzando che i token digitali in un anno facciano lo stesso numero di transazioni delle carte di credito, proporzionalmente, il consumo elettrico dovrebbe arrivare a circa 67400 miliardi di kWh, ovvero circa 134 mila volte il consumo dei sistemi finanziari tradizionali. Una quantita' di energia veramente

esagerata e totalmente insostenibile, sia dal punto di vista delle emissioni che dal punto di vista della produzione.
Per avere un paragone piu' esaustivo e' utile prendere in considerazione anche il costo energetico della singola operazione, integrandolo anche con alcuni dati trovati nella tabella 4. Quindi con una semplice divisione si ottiene la seguente tabella:

	PoW (Bitcoin)	**PoS (low)**	**PoS (up)**	**Carta di Credito**
Transazione	217	0,00017	0,05	0,0016

Tabella 2.1: Confronto del consumo elettrico in kWh tra diversi sistemi di scambio di denaro

Per chiarezza sono stati presi dalla tabella 4 rispettivamente il consumo di Solana e Cardano, in modo da rappresentare il *lower* e l'*upper* bound dei consumi elettrici dei sistemi PoS (senza considerare il piu' comune Ethereum 2.0).
Cardano, nonstante risulti essere la crypto-valuta a validazione PoS con il consumo per transazione piu' alto, appare comunque decisamente meno dispendioso di quanto non lo sia Bitcoin ma non dei mezzi di scambio di denaro tradizionali.
Bitcoin ha dei consumi decisamente superiori di parecchi ordini di grandezza rispetto al consumo degli altri sistemi e la carta di credito, seppur con un consumo decisamente piu' basso rispetto alla celebre moenta digitale, non sembra essere il mezzo piu' ecologico per lo scambio di denaro.
Prendendo in considerazione il token Solana, infatti, si puo' osservare come una valuta digitale con validazione PoS risulti avere il consumo corrispondente a circa un decimo di quello delle carte di credito tradizionali. Risulta quindi essere il mezzo di scambio di denaro piu' "green" tra quelli presi in considerazione.

2.4.2 Altri Consumi Informatici

Il mercato finanziario e tecnologico giocano un ruolo piuttosto importante nell'inquinamento globale, tuttavia, ci sono altri aspetti dell'informatica che, purtroppo, continuano a guadagnare posizione nella classifica delle attivita' altamente inquinanti.
I Data Centres e le Reti di Comunicazione sono un esempio importante di mezzi tecnologici fondamentali che, proprio come le monete digitali, devono per forza adeguarsi e svilupparsi nell'ottica del risparmio energetico e della riduzione dei consumi.
Anche per questo molte tra le aziende tecnologiche piu' importanti hanno iniziato a produrre e utilizzare molta energia pulita come l'eolico o il fotovoltaico, facendo in modo che il settore informatico rientri tra quelli piu' sostenibili.

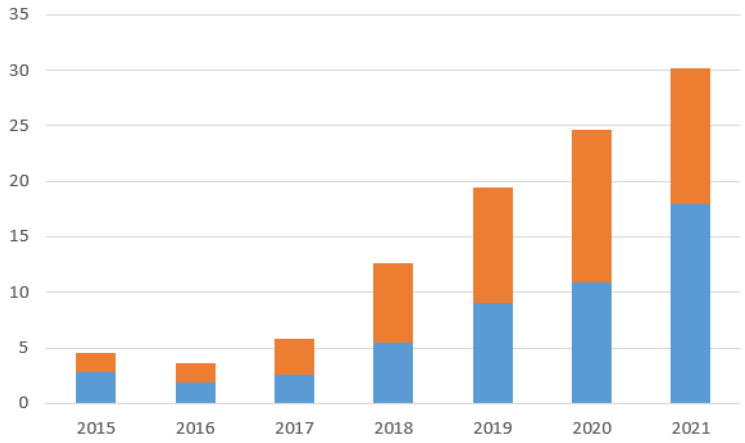

Figura 2.3: Accordi per l'acquisto di energia rinnovabile per settore (2015-2021)

In questo grafico i valori sull'asse verticale sono espressi in GW e rappresentano la quantita' di energia rinnovabile acquistata dai diversi settori, in blu quello informatico/tecnologico mentre in arancione tutti gli altri.
E' evidente che il settore IT sia quello che investe di piu' nell'acquisto di

energia pulita, sin dal 2015. Ma ecco alcuni esempi di altri consumi dovuti all'informatizzazione e allo sviluppo del settore tecnologico.

Data Centres

I Data Centres sono delle strutture fisiche che contengono una grande quantita' di strumentazione informatica messa a disposizone della rete da parte di grandi aziende per eseguire, generalemente, operazioni richiedenti una quantita' ingente di potenza di calcolo. Queste strutture possono anche contenere sistemi di archiviazione o di gestione dati e favorire lo sviluppo del cloud computing.
Essendo il mercato tecnologico sempre in fase di sviluppo e' ovvio che strutture fondamentali come queste sono sempre piu' diffuse e utilizzate. Basti pensare che l'uso di elettricita' dovuto a questi edifici in Irlanda e' triplicato rispetto al 2015 [15] e per il 2025 si prevede che verra' triplicato anche in Danimarca [15].
Un report di IEA (International Energy Agency, https://www.iea.org/) [15], spiega che nel 2021 i Data Centres hanno utilizzato 220-320 TWh di energia elettrica, costituendo circa 0,9-1,3% della domanda globale di elettricita', senza considerare tutta l'energia utilizzata per le crypto (che viene stimata a 100-140 TWh).
E' importante considerare che comunque questi consumi, aumentati del 10-60% dai 200TWh che erano stati rilevati nel 2015, non sono proporzionali alla mole di dati che devono gestire, considerando che essa e' aumentata del +300% circa, nello stesso periodo.

Reti di Comunicazione

Le reti di comunicazione sono un altro elemento che negli ultimi anni si e' sviluppato moltissimo portando con se nuove tecnologie e altissimi consumi. Viene stimato [15] che nel tra il 2015 e il 2021 il traffico di dati via internet, quindi sfruttando questi mezzi di comunicazione, sia aumento del +440%, mentre il numero di utenti e' aumentato solo del +60%.

In totale viene calcolato un consumo globale di circa 260-340TWh delle reti di comunicazione, ovvero circa 1,1-1,4% del consumo elettrico globale e ben 3 volte il consumo di Bitcoin nel 2020.
Questi numeri saranno sempre destinati ad aumentare anche perche' le tecnologie sono in continua evoluzione e diffusione, basti pensare ad alcuni settori, come lo streaming e il gaming, che dal 2015 sono cambiati radicalmente migliorando decisamente l'esperienza dell'utente ma aumentando anche il loro consumo energetico.
Anche in questo caso risulta che la quantita' di dati trattati sia aumentata esponenzialmente pero', per fortuna, le tecnologie si sono sviluppate anche nell'ottica di ridurre sprechi energetici, infatti i consumi di energia elettrica non sono proporzionali a questo aumento.
Questo e' un grande punto a favore del settore tecnologico in generale: puntare al miglioramento delle prestazioni ma sempre con un occhio di riguardo per l'inquinamento e gli sprechi.

Capitolo 3

Proof-of-Work

E' stato sviluppato per alleviare la doppia spesa nella rete. Una "prova di lavoro" richiede che i nodi che verificano le transazioni (conosciuti come miners) devono eseguire un calcolo complesso per affermare la validita' delle transazioni nella rete. In Bitcoin i nodi costituiti dai miner devono competere per convalidare le transazioni risolvendo un enigma crittografico per costruire un blocco valido da aggiungere alla catena. Quando si trova una soluzione, il nodo vincente propone un nuovo blocco di transazioni da aggiungere alla catena.
Il meccanismo PoW consuma un'enorme quantita' di energia, ad esempio il meccanismo PoW di Bitcoin (la valuta piu' importante che utilizza il sistema PoW) ha un consumo energetico stimato di 1130 kWh per transazione che e' l'equivalente del consumo di energia di una famiglia media statunitense per circa 39 giorni.
Il problema e' che e' proprio il mining computazionalmente intensivo e la competizione, responsabili dell'elevato consumo di energia e risorse, sono le stesse ragioni per cui il sistema PoW viene considerato cosi' sicuro.

3.1 Funzionamento

Il sistema Proof-of-Work nasce come deterrente per gli attacchi infromatici, non e' altro che un calcolo dal costo computazionale altissimo che permette di validare un blocco di transazioni.

3.1.1 La fase iniziale e la Validazione

Nella fase inziale le transazioni vengono raccolte in blocchi di transazioni che contengono le operazioni fatte in un determinato arco di tempo (10 minuti) e l'hash del blocco precedente, una volta che il blocco viene riempito i miner iniziano il processo di validazione.
E' proprio in questa fase che viene chiuso e validato il blocco grazie all'intervento del meccanismo di PoW. Si tiene in considerazione l'hash del blocco precedente (in modo da creare la famosa "catena" da cui deriva il nome della block-chain) e i dati delle transazioni eseguite. Viene generato un numero casuale `nonce` e viene aggiunto agli altri dati tramite l'algoritmo crittografico `SHA-256` in modo da creare un nuovo hash.
Questo nuovo hash appena generato deve rispettare un criterio, ovvero deve iniziare con un numero finito e prestabilito di zeri che cambia nel corso del tempo.
Se l'hash generato dalle operazioni non rispetta questo criterio si ripete il procedimento con un nuovo `nonce`.

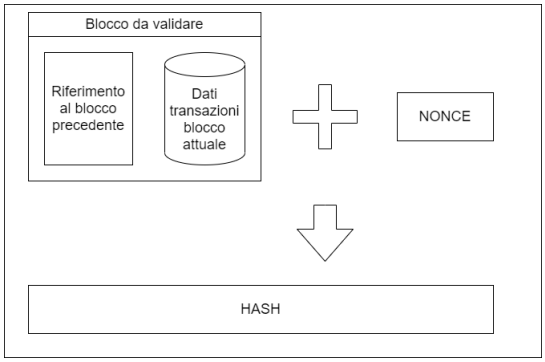

Figura 3.1: Processo di validazione di un blocco di transazioni

3.1.2 La creazione del nuovo blocco

Come visto nella validazione, una volta generato il nuovo hash, esso viene memorizzato ed inserito nel blocco successivo, in modo che nella catena di blocchi ci sia sempre un riferimento al precedente.
Quando viene validato il nuovo blocco, viene anche distribuita la nuova versione della blockchain con tutte le transazioni aggiornate.
Ipotizzando che venga introdotto un blocco estraneo il sistema e' in grado di rilevarlo molto velocemente. Anche se la modifiche apportate alle transazioni sono piccolissime, l'hash del blocco sara' completamente diverso e quindi il dispositivo del malintenzionato deve essere abbastanza potente da generare un nonce in grado di rispettare le richieste prima degli altri dispositvi che, invece, ragionano sulla blockchain corretta.
In uno scenario limite in cui la macchina dell'attaccante e' piu' potente (o piu' fortunata) di tutte le altre macchine, vuol dire che riesce ad attaccare un blocco "maligno" alla blockchain che non viene pero' riconosciuto dagli altri dispositvi e quindi non viene accettato nella catena.
La fase in cui viene utilizzata piu' energia elettrica, quindi, e' proprio quella della Proof-of-Work, ovvero il momento in cui deve essere generato l'hash con il numero di zeri prestabilito all'inizio. L'algoritmo SHA-256, infatti, risulta essere estremamente complicato e costoso a livello computazionale e quindi anche a livello di corrente elettrica.
La probabilita' che venga generato il numero corretto e'

$$\frac{1}{2^{\#zeri}}$$

. Se ad esempio devono esserci 30 zeri all'inizio dell'hash vuol dire che la probabilita' di trovare l'hash corretto e'

$$\frac{1}{1000000000}$$

ovvero ci vogliono in media 1 miliardo di tentativi per trovare l'hash corretto.

3.1.3 Ricompensa

L'unico motivo per cui il mercato del mining fa cosi' tanta gola e' perche' il validatore che riesce a trovare la soluzione corretta all'enigma crittografico riceve una certa quantita' di token "gratis". L'unica spesa che deve sostenere, infatti, e' quella energetica e quella dell'hardware.
L'ammontare di monete ricevute puo' cambiare a seconda della valuta, per Bitcoin il valore del "premio" viene dimezzato con l'aumentare del numero dei blocchi che validati e attaccati alla blockchain. Questo procedimento fara' in modo di creare un numero finito di monete (fissato gia' all'inizio a 21 milioni), dopodiche' la produzione si fermera' e il token restera' solo una moneta di scambio, teoricamente immune all'inflazione.

3.2 Consumo

Visto il funzionamento possiamo stabilire che questo sistema di validazione e' molto oneroso dal punto di vista energetico. Esso e' strutturato in modo tale da aumentare man mano la difficolata' dei calcoli computazionali da fare per impedire, o comunque disincentivare, gli attacchi dei malintenzionati.
Questo meccanismo di consenso viene utilizzato principalmente da Bitcoin e dalla prima versione di Ethereum che insieme valgono piu' del 60% della capitalizzazione di mercato delle cryptovalute, secondo un report della Casa Bianca, si stima che ad Agosto 2022 questi due token siano la causa della quasi totalita' del consumo totale di energia elettrica dovuto ai crypto-assets. Per Bitcoin viene calcolato un consumo annuale di energia elettrica tra 90 e 145 miliardi di kWh, mentre per Ethereum 1.0, nello stesso lasso di tempo, viene stimato un consumo tra 23 e 95 miliardi di kWh. Delle cifre comunque esorbitanti che sicuramente hanno delle rispercussioni a livello ambientale e sociale.
Non e' possibile, infatti, stabilire i danni ambientali che la produzione di circa 180 miliardi di kWh possono provocare in un anno, essi dipendono molto dal contesto e dalle modalita' attraverso le quali vengono prodotte. Molta

dell'energia utilizzata negli anni precedenti deriva da fonti rinnovabili come fotovoltaico o idroelettrico ma, visto l'incremento della richiesta, molte compagnie elettriche hanno deciso di riaprire delle centrali abbandonate da anni che ancora utilizzano diesel o carbone.
Si stima che nel 2021 Bitoin abbia partecipato per il 70% nella produzione di CO2, circa 100 Mt di CO2/y, una cifra altissima considerando che l'intero mondo degli asset delle crypto viene stimato a 140 Mt di CO2/y, ovvero quanto il consumo di tutte le chiatte e mezzi di trasporto marittimi degli US.
Il problema principale e' che Bitcoin e il sistema PoW sono programmati in modo tale da aumentare la propria difficolta' computazionale all'aumentare del market price. Ne consegue che aumenteranno anche le macchine utilizzate per il mining e quindi la richiesta di energia e l'inquinamento, facendo cosi' aumentare il costo della vlauta, attirando ancora piu' clientela. E' tutta una reazione a catena in un loop.
Per questo risulta necessario un cambio di rotta, verso delle tecnologie piu' sostenibili e praticabili. Il consumo energetico deve essere una priorita' anche per queste nuove tecnologie, non ancora regolamentate.

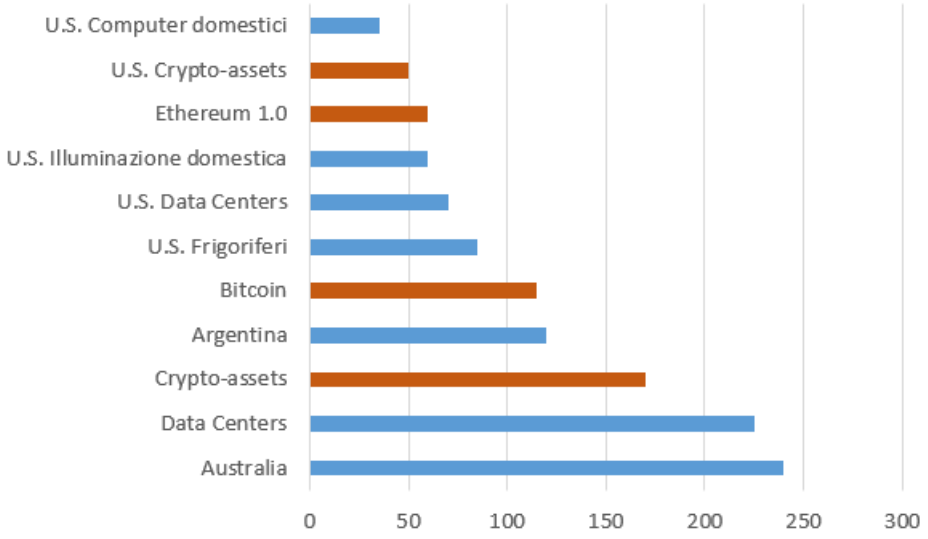

Figura 3.2: Consumo energia elettrica annuo PoW ad Agosto 2022 (prima che Ethereum passasse a PoS) in miliardi di kWh

Capitolo 4

Proof-of-Stake

PoS viene per presentato per la prima volta nel 2011 nel forum "BitcoinTalk", si tratta di un'alternativa a PoW in grado di ridurre il consumo energetico e le barriere all'ingresso costituite dalla necessita' di avere dell'hardware molto potente. Il metodo con il quale viene scelto il validatore, infatti, e' correlato piu' agli asset posseduti che alla potenza di calcolo delle macchine a disposizione.
La Proof-of-Stake e' un sistema di certificazione che sceglie il proprio validatore in modo pseudo-casuale, attraverso uno o piu' processi di verifica in cui e' necessario dimostrare anche l'ammontare del capitale investito per essere giudicati affidabili.
Questo sistema risulta talmente affidabile, pratico e conveniente che nel 2022 viene adottato da Ethereum (seconda moneta virtuale per capitalizzazione) per cercare di diminuire il proprio impatto energetico.
Secondo un report del CCRI (Crypto Carbon Ratings Institute) il cambiamento di rotta da parte di questa moneta ha portato un risparmio del 99,988% di energia elettrica e, quindi, anche una diminuzione dei consumi di CO2 stimati del 99,992%.

	ETH (PoW)	**ETH (PoS)**	**Reduction Factor**
Electric Consuption MWh/anno	22'900'320	2'600,86	0,99988
CO2 Emission t/anno	11'016'000	869,78	0,99992

Tabella 4.1: Differenza consumo elettrico ed emissioni CO2 tra Ethereum PoW ed Ethereum PoS

4.1 Funzionamento

Il processo di funzionamento del sistema PoS e' leggermente diverso rispetto a PoW, infatti gli utenti, che rappresentano i nodi dei validatori, vengono chiamati "forgers" e non "miners", perche' si occupano di creare il blocco con le transazioni piuttosto che eseguire migliaia di calcoli per certificarlo.
Anche Proof-of-Stake risulta un algoritmo molto sicuro e quasi a prova di attacco, purtroppo pero' non lo si puo' ancora affermare con certezza perche' le implementazioni e le prove su larga scala sono state fatte solo recentemente e quindi risulta essere ancora in fase di collaudo.

4.1.1 La fase iniziale e la Validazione

Essendo il sistema PoS un meccanismo in cui per verificare le transazioni il validatore deve garantire la propria affidabilita' dimostrando di possedere una certa quantita' di monete (nel caso di Ethereum minimo 32 ETH), il protocollo non puo' essere implementato nativamente. Deve esserci una fase iniziale in cui o vengono vendute delle monete (i cosiddetti pre-mined coins) oppure si parte con una validazione di tipo PoW per poi eseguire una transizione (se vogliamo anche energetica) verso il sistema PoS.
Nel momento in cui vengono eseguite un certo numero di transazioni, esse

vengono raccolte in un blocco che deve essere verificato prima di essere aggiunto alla blockchain.
Come per PoW, anche in questo caso piu' utenti concorrono per essere scelti come validatori del blocco di transazioni; nel caso di PoS, pero', la ricompensa viene ricevuta solamente sotto forma di commissioni sulle transazioni.
Per essere selezionato come validatore, l'utente deve "mettere in stake" quindi bloccare e utilizzare come una sorta di "certificazione", una quantita' della stessa valuta, come se fosse una quota di partecipazione nella rete che gli permette di essere giudicato come affidabile.
Nella selezione del validatore il sistema PoS utilizza due metodi per garantire la decentralizzazione: **Randomized Block Selection** e **Coin-Age Selection**. Senza questi metodi si rischirebbe di avere una blockchain in cui la validazione dipende solamente da chi possiede piu' monete.
Una volta scelto il blocco validante, esso controlla le transazioni e aggiunge il blocco alla catena.

Randomized Block Selection Vengono combinati l'hash value dell'utente e la quantita' di monete che ha messo in stake. Piu' alta risulta essere questa quantita', piu' si ha la possibilita' di essere selezionati.
La quantita' di monete messe in stake da parte di un aspirante validatore e' un numero pubblico quindi gli altri utenti possono vederlo e prevedere chi beneficiera' delle commissioni.

Coin-Age Selection Viene scelto chi tra gli aspiranti validatori ha la "Coin-Age" piu' elevata.
Questo valore viene calcolato moltiplicando il numero di giorni trascorsi da quando l'utente ha messo il proprio denaro in staking per il numero di monete investite.
Quando un utente viene scelto si azzera il numero di giorni in modo da garantire equita' nella comunity di validatori (e quindi decentralizzazione).

4.1.2 Ricompensa

Solo quando viene aggiunto il blocco, il validatore viene ricompensato ricevendo delle commissioni sulle transazioni controllate (Transaction Fees).
Le fees dipendono dal valore delle transazioni certificate e possono essere incassate solo quando l'utente decide di ritirare i propri risparmi dallo staking.
Al momento del ritiro vengono eseguiti dei controlli da parte di tutta la rete sulle transazioni verificate dall'utente e, solo in caso non vi siano transazioni fraudolente, vengono elargite le commissioni, in caso contrario viene sottratta all'utente una parte delle monete messe in staking, anch'essa proporzionale al valore delle transazioni e gli viene tolto il diritto di essere un validatore.
Il sistema Pos riesce, quindi, a garantire l'affidabilita' delle transazioni perche' gli utenti che mettono in staking le proprie monete non vogliono rischiare di perderle validando una transazione fraudolenta. E' come se le monete investite fossero un "financial motivator" utile ad approvare solo transazioni legittime e quindi eseguire correttamente il proprio lavoro.

4.2 Consumo

Il meccanismo PoS, come spiegato, non utilizza algoritmi ad alta complessita' computazionale per funzionare, quindi le macchine utilizzate durante il processo di validazione non sono spinte allo stremo e non consumano sicuramente quanto quelle delle cryptovalute basate su sistema PoW.
Il processo di validazione risulta essere quasi casuale ma comunque molto sicuro e decentralizzato.
E' per questi motivi che Vitalik Buterin, attuale CEO e fondatore della moneta Ethereum, nel 2022 ha deciso di cambiare il meccanismo di consenso del suo token digitale, proponendosi un po' come paladino dell'innovazione energetica di blockchain.
Nel sito di Ethereum [4], a differenza di Bitcoin infatti, si puo' trovare un'intera sezione dedicata ai consumi energetici e alla spiegazione del funzionamento del token digitale con tanto di ricerche e studi.

Alcuni degli studi proposti dal **CCRI** (Crypto Carbon Ratings Institute) si occupano di eseguire delle misurazioni precise sulla nuova rete di ETH con diversi software e hardware.
I numeri parlano chiaro: sia il risparmio energetico che le emissioni di CO2 evitate sfiorano il 100%. Seppur il cambiamento tra una tecnologia e l'altra sia decisamente significativo, la blockchain rimane comunque molto dispendiosa e inquinante visto che si parla di migliaia di MWh di energia elettrica e tonnellate di CO2 ogni anno.
Un altro grande vantaggio della rete PoS e' sicuramente la possibilita' di utilizzare hardware piu' comune. La maggior parte dei programmi piu diffusi per il forging di blocchi ETH ha dei requisiti tecnici minimi, soprattutto messi a confronto con quelli di una rete basata su Proof-of-Work come Bitcoin in cui vengono creati hardware specifici per sfruttare al massimo la potenza di calcolo.
Le basse barriere all'entrata, quindi, favoriscono l'ingresso di molti concorrenti, ma rispetto a PoW l'unico sistema per avere un vantaggio sugli altri utenti e' quello di investire piu' capitale nello staking. Quindi, sostanzialmente, non c'e' il rischio che all'aumentare della clientela aumenti anche la complessita'.
In un report della Casa Bianca sull'utilizzo di elettricita' e l'inquinamento dei crypto-assets viene citata una stima sui dispositivi utilizzati per il forging, essi richiedono tra le 10 e le 500 volte meno energia di un hardware studiato appositamente per il mining di Bitcoin.
Secondo lo stesso report, tutti i sistemi PoS insieme consumano circa 0,28 miliardi di kWh di energia elettrica all'anno (ai tempi di questo report non era ancora stata completata la transizione di ETH a PoS), che e' meno dello 0,001% del consumo globale e quasi lo 0,25% della stima piu' bassa del consumo dei sistemi PoW.
La stima che viene fatta nel sito ufficiale di Ethereum e' di circa 2,6 MWh all'anno (0,0026 TWh), a fronte dei 100 TWh all'anno consumati dalla blockchain PoW di Bitcoin che quindi risulta essere molto piu' ecologico.

Conclusioni

Dopo aver analizzato il funzionamento di blockchain e dei suoi due principali meccanismi di consenso, possiamo stabilire con certezza che e' una tecnologia con molte possibilita' di crescita e di sviluppo. Sicuramente una tecnologia utile e applicabile in diversi campi ma da migliorare dal punto di vista energetico.
Ethereum e' sicuramente un apri-pista per la rivoluzione tecnologica dei crypto-assets, dovrebbero seguire il suo esempio Bitcoin e le altre monete digitali basate su Proof-of-Work (come ad esempio Dash, DogeCoin, LiteCoin). Vitalik Buterin e la sua moneta hanno dimostrato come sia possibile adattare le proprie tecnologie, scalarle e ridimensionarle per rispettare gli obiettivi mondiali.
Se si pensa che tra gli OSS (Obiettivi Sviluppo Sostenibile) promulgati dall'ONU c'e' anche quello di diminuire il consumo energetico o comunque renderlo piu' sostenibile, e' assurdo che un mercato come quello delle cryptocurrencies non venga regolato. In questo report della Casa Bianca [5] voluto dal Presidente Biden, si stima che il mercato delle cryptovalute basate su un sistema PoW (prima che Ethereum passasse a PoS) consumi tanta energia elettrica quanto l'Argentina.
Quando si parla di inquinamento ci sono alcuni mercati che sembrano molto piu' ecologici di quanto non lo siano realmente, proprio come succede nell'universo tecnologico. Affidandosi ai grafici che si possono trovare nel sito di ETH [4] solo Youtube e Netflix insieme consumano circa 340 TWh/anno di energia elettrica che, rapportati ad un cittadino italiano (calssificato nella

top 20 dei paese al mondo per consumo elettrico), corrisponde a circa 11,4 milioni (1/5 della popolazione).
Il consumo di Ethereum con sistema PoS invece viene stimato a 0,26 TWh/anno una cifra significativamente bassa a fronte di un consumo di 78 TWh/anno con il sistema di validazione PoW.
Credo e mi auguro che la storia di Ethereum possa fungere da esempio per tutte le altre grandi cueencies.
E' inngabile ormai che la blockchain sia una tecnologia molto sviluppata e all'avanguardia, assai utile e ricca di implicazioni in ogni campo. Una tecnologia facile, immediata e sicura. Sarebbe un peccato non sfruttarla a pieno con anche i sui risvolti piu' green.
Penso che quello di Ethereum 2.0 sia un grande esempio perche' dimostra come si sia riusciti a sfruttare a pieno le potenzialita' di una tecnologia adattandola ai bisogni del Mondo odierno. Al giorno d'oggi risulta fondamentale prestare attenzione ai consumi, agli scarti ed ai rifiuti, soprattutto in un frangente come questo, in cui si possono ottenere quasi le medesime prestazioni con, letteralmente, il 99,9% dei consumi e dei rifiuti in meno.

Appendice A: Tabelle utili alla comprensione dei dati

In questa appendice sono presenti delle tabelle che possono tornare utili al fine di comprendere al meglio l'argomento trattato. I dati provengono da diverse fonti, quindi potrebbero variare a seconda del momento in cui e' stata fatta la rilevazione (per esempio i dati di capitalizzazione o di stima del consumo elettrico).
Ho preferito riportare le tabelle come trovate nei documenti ufficiali citati nella bibliografia.

Consumo con ETH 1.0

Crypto-Asset	**Capitalizzazione** (miliardi $)	Validazione **(PoW / PoS)**	**Consumo Energetico** (TWh/anno)		
			BEST	**LOWER**	**UPPER**
Bitcoin	$389	PoW	88,6	38,2	179,3
Ethereum	$185	PoW	22,9	16,5	32,2
Cardano	$15	PoS	6,0*10^-4	1,4*10^-4	4,4*10^-3
Solana	$11	PoS	2*10^-3		
Dogecoin	$8	PoW	3,8		
PolkaDot	$8	PoS	7,0*10^-5	1,4*10^-5	4,4*10^-4
Avalanche	$6	PoS	4,9*10^-4		
Algorand	$2	PoS	5,1*10^4	5,4*10^-5	1,7*10^-3

Tabella 2: Consumo elettrico stimato ad Agosto 2022

Appare evidente come il consumo elettrico delle blockchain che utilizzano un sistema PoS invece che PoW, a parita' di capitalizzazione, siano decisamente piu' bassi di molte unita' di misura. E' importante sottolineare che in questa tabella si parla ancora di Ethereum 1.0, quindi basato su sistema PoW.

Consumi PoS

Nome	**Simbolo**	**Capitalizzazione** [miliardi $]	**# Nodi**	**# Transazioni** [mTx / anno]
Cardano	**ADA**	52,8	3002	11,9
Polkadot	**DOT**	37,4	297	4,0
Solana	**SOL**	11,8	1015	11800,0
Tezos	**XTZ**	5,5	375	2,5
Avalanche	**AVAX**	4,9	1084	93,9
Algorand	**ALGO**	4,7	1190	190,0

Tabella 3: Capitalizzazione, Numero di Nodi e Numero di transazioni all'anno per crypto-valute PoS diverse da Ethereum 2.0

Simbolo	**Consumo Elettrico tot** [MWh / anno]	**Consumo Elettrico / Nodo** [kWh / h]	**Consumo Elettrico / Trans.** [Wh / Tx]	**tot Emissioni CO2** [tCO2 / anno]
ADA	598,8	199,45	51,59	284,41
DOT	70,2	236,49	17,42	33,36
SOL	1967,9	1938,85	0,166	934,77
XTZ	113,2	250,99	41,45	53,79
AVAX	489,3	451,39	4,76	232,42
ALGO	512,7	430,82	2,70	243,52

Tabella 4: Consumo Elettrico Annuo, Consumo Elettrico per Nodo, Consumo Elettrico per Transazione, Totale Emissioni CO2 Annue per crypto-valute PoS diverse da Ethereum 2.0

In questa tabella sono evidenziati i valori piu' bassi per ogni colonna, quindi gli asset con i consumi minori. Si puo' vedere come "Polkadot" sia il meno dispendioso sia nel consumo elettrico annuo che nelle emissioni totali di CO2 nonostante sia al secondo posto per capitalizzazione come si vede nella prima tabella.

Consumo per Nodo

Simbolo	PoW / PoS	Capitalizzazione [miliardi $]	# Nodi	Consumo tot [MWh / Anno]	Consumo Nodo [kWh / Anno]
ADA	PoS	52,8	3002	598,8	199,45
DOT	PoS	37,4	297	70,2	236,49
SOL	PoS	11,8	1015	1967,9	1938,85
XTZ	PoS	5,5	375	113,3	250,99
AVAX	PoS	4,9	1084	489,3	451,39
ALGO	PoS	4,7	1190	512,7	430,82
ETH 2.0	PoS	193	4755	2600	546,79
ETH 1.0	PoW	193	4755	22,9 mln	4 mln
BTC	PoW	448	15780	120 mln	7 mln

Tabella 5: Consumo per nodo di alcune famose blockchain PoW e PoS

In questa tabella vengono illustrati i consumi di energia elettrica per nodo di alcune tra le piu' famose blockchain sia PoW che PoS.
Appare evidente come le blockchain che utilizzano metodi di validazione PoS siano decisamente piu' "ecologiche" rispetto alle altre. I consumi elettrici, in generale, sono proprio su ordini di grandezza differenti.
Dalla tabella si puo' constatare che la valuta che utilizza meno energia per nodo e' Cardano con i suoi 199,45 kWh/anno, mentre quella che detiene il primato per consumi piu' alti per le tecnologie PoS e' Solana con 1938,85 kWh/anno.

Bibliografia

[1] *The Merge - Implications on the Environmental Sustainability of Ethereum*, https://carbon-ratings.com/

[2] *Energy efficiency and carbon emissions of PoS Networks*, https://carbon-ratings.com/

[3] *Determining the electricity consumption and carbon footprint of Proof-of-Stake networks*, https://carbon-ratings.com/

[4] *Proof-of-Stake (POS)*, https://ethereum.org/it/developers/docs/consensus-mechanisms/pos/

[5] *Ethereum Energy Consuption*, https://ethereum.org/en/energy-consumption/

[6] *Blockchain - Wikipedia*, https://it.wikipedia.org/wiki/Blockchain

[7] *A Very Brief History Of Blockchain Technology Everyone Should Read*, https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/?sh=36c760597bc4

[8] *History of Blockchain*, https://www.javatpoint.com/history-of-blockchain

[9] *Cryptocurrency's Dirty Secret: Energy Consumption*, https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy/

[10] *Cos'e' la tecnologia blockchain?*, https://www.ibm.com/it-it/topics/what-is-blockchain

[11] *Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption*, https://eprints.bournemouth.ac.uk/36968/1/GREEN_BLOCKCHAIN.pdf

[12] *Bitcoin - A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

[13] *Energy - OurWorldInData*, https://ourworldindata.org/energy

[14] *Climate And Energy Implications of Crypto-Assets in the United States*, https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf

[15] *Data Centres and Data Transmission Networks*, https://www.iea.org/reports/data-centres-and-data-transmission-networks

Ringraziamenti

In questa sezioni ci tenevo a ringraziare in primis il mio relatore che mi ha accompagnato nella stesura di questa tesi.
Un sentito e doveroso grazie dal profondo del cuore ai miei genitori che hanno reso possibile questo percorso, e che, insieme alle mie sorelle e ai miei parenti, hanno sempre creduto in me supportandomi psicologicamente, spronandomi e incoraggiandomi ogni giorno di piu'.
Ringrazio anche tutti i miei familiari che purtroppo non ci sono piu' ma che avrebbero tanto voluto vedermi nel momento del conseguimento del titolo scolastico.
Ci tengo particolarmente a ringraziare anche tutti i miei amici, sia quelli piu' storici di Treviso che tutte le nuove amicizie nate a Bologna. In questi anni hanno portato un sacco di gioia e felicita' nelle mie giornate di studio e nella mia vita in generale. Tra i miei amici una menzione d'onore ai miei coinquilini Michele, Youssef e Federico che oltre ad essere delle fantastiche persone e degli ottimi amici, sono stati dei compagni di percorso fondamentali durante il periodo delle quarantene e delle restrizioni dovute al Covid-19.
Grazie mille a tutti.