L’impronta ambientale del Bitcoin

Background: un po' di concetti teorici preliminari

-Il bitcoin è una criptovaluta e un sistema di pagamento creato nel 2009 da un anonimo inventore noto con lo pseudonimo di Satoshi Nakamoto (qui farò un collegamento al suo nome)

-Il bitcoin a differenza delle valute tradizionali che noi conosciamo non fa uso di un ente centrale è il suo valore viene determinato solamente dalla leva domanda e offerta. Non avendo un ente centrale significa che rende impossibile a qualsiasi autorità governativa il blocco dei trasferimenti di Bitcoin, il loro sequestro senza il possesso delle relative chiavi o la svalutazione del bitcoin dovuta all’immissione di nuova moneta.

-Il bitcoin si basa su usa struttura della rete peer-to-peer (ossia i nodi di una rete informatica non sono gerarchizzati unicamente come client o server ma posso essere nodi equivalenti o paritari.

Grazie a questa caratteristica qualsiasi nodo può completare una transazione che sarà visibile nella menpool di Bitcoin (collegamento alla mempool)

Cos’è un crypto valuta ?

Una crypto valuta e differente alla classica moneta elettronica è una unita di valore digitale movimenta online nativa online. La parola crypto indica l’utilizzo della crittografia per garantire sicurezza e impossibilità di contraffarla. E resa sicura in modo decentralizzato sulla blockchain

Una blockchain è l’infrastruttura sulla quale si muove una cryptovaluta e garantisce sicurezza e decentralizzazione alla cryptovaluta stessa.

Double spending (poter spendere la stessa unità di valore più volte) devo garantire che una volta che ho speso una unità di valore quella unità di valore non è stata duplicata e spenderla più volte (di questo di occupa la crittografia). Se c’è possibilità di dpuble spending la criptovaluta non ha valore

Una cripto valuta è un sistema aperto ossia è open source (protocollo open source su cui si può svlippare) un sistema finanziario aperto non si era mai visto prima d’ora!!!

Sistema tradizionale di moneta elettronica

Il sistema tradiziona di moneta elettronica è un sistema centralizzato prevede un intermedario (centralizzato perché si basa su qualcuno che autorizza il traferimento come una banca,paypal,satispay tutti coloro che sono intermediari finanziari)

Esempio: io invio un bonifico la mia banca lo verifica,l’approva e lo invia all’altra banca che a sua volta lo approva e accredita il bonifico alla persona a cui avevo mandato i soldi

Quindi abbiamo due approvazioni richieste quelle della mia banca e quella della sua banca e questo introduce delle tempistiche (è vero esiste anche il bonifico istantaneo ma anche qui ci possono essere delle rpoblematiche) e introduce dei costi aggiuntivi. Se l’intermediario non funziona (sistema della banca offline) ci sarà un disservizio (non posso usare carte di credito o ritirare i soldi allo sportello). In questo sistema io affido la mia “fiducia” ad un sistema centralizzato che è la banca in questo caso. Se non mi posso più fidare della banca il servizio cessa di funzionare. Inoltre io in banca non ho proprietà effettiva del mio denaro depositato ma è un credito nei confronti della banca (non posso prelevare tutto il denaro in banca in quanto buona parte della liquidità la banca la investe) non ho una proprietà diretta del denaro

Sistema decentralizzzato

Abbiamo un insieme di nodi distribuiti in giro per il mondo è noi interfaciandoci con la rete inviamo la trasfazione e il protoccolo che è decentralizzato lo invia direttamnte all’altra persona (non abbiamo un intermediario) Io ho il bitcoin e non devo chiedere ad una banca l’autorizzazione per spenderli e quanto mi porta ad avere tempi brevi, minori costi (non ho gli intermediari), e sempre fruibile (se c’ un nodo offline posso usare gli altri nodi non sono dipendente da un solo sistema) è borderless ed è sicuro grazie all’uso della crittografia

Cos’è una blockchain?

È un registro distibuito su vari nodi (i nodi sono macchine che eseguono un sowftare che li collegano al network bitcoin) ognuno dei nodi possiede tutti i dati (tutto lo storico di Bitcoin tutte le transazioni fino ad adesso)

I nuovi dati vengono sincronizzati in real time. Ogni nodo valida le transazioni (verificano che ci sia il bilancio necessario e la chiavi privata per sperderlo se cio accade la transazione viene validata)

I diversi nodi per evitare che ci sia dipendenza da un solo nodo (così da evitare di essere centralizzati) si usa il consenso distribuito (valida le transazioni in accordo con gli altri)

Alcuni esempi di consenso distribuito sono proof of work , proof of stack

Un maggior numero di nodi garantisce più decentralizzazione

La blockchain è trasparente ed immutabile tutti posso leggere dentro la blockchain

Posso vedere un address che transazioni ha fatto, vedere tutto il giro che è stato fatto da una transazione.

Come nasce Bitcoin

È la prima criptovaluta mai creata ed è la più sicura e la più decentralizzata

Non ha un “capo”: creata da satoshi nakamoto nel 2008, mai visto ed in seguito scomparso (ora Bitcoin è in mano alla community mondiale (più decentrallizata di così!)

Nasce in piena crisi economica e bailout(viene stampato più denaro per salvare le banche che rischiavano la bancarotta sscusate il gioco di parole)), con lo scopo di fornire prima o poi un’alternativa al denaro FIAT, imposto e controllato da politiche monetarie.

Come funziona?  
per usare il Bitcoin abbiamo bisogno di un wallet che è un sowtfare che mi permette di ricevere, conservare e ricevere Bitcoin. Per fare queste operazioni userò delle chiavi pubbliche e private

Il waller non è un portafoglio ma bensì è un portachiavi perché contiene le mie chiavi pubbliche e private. La chiave pubblica si ricava tramite un algoritmo crittograffico che è il ECDSA (l’algoritmo di firma digitale a curva ellittica)

La chiave privata data in pasto a questo algoritmo mi restituira la chiave pubblica. Invece se possiedo la chiave pubblica non posso ricavare la chiave privata.

Chiave pubblica la uso per ricevere i Bitcoin

Chiave privata non deve essere mai diffusa! (se proprio volete datele a noi)

Cosa da valore a bitcoin?

La sua addozione come mezzo di scambio sicuro, disintermediarlo, nativo online e borderless

Addozzione come riserva di valore (come l’oro solo che in questo caso è oro digitale)

Adozione come strumento finanziairio sul quale investire (ETF,etc)

Utilizzo di Bitcoin come collaterale (per chiedere un prestito alle banche)

Inquinamento del Bitcoin

Il mining di Bitcoin consuma una elevata quantità di energia però bisogna anche studiare lo scopo di questa energia (solitamente viene trattata come energia “sprecata” del tipo “si consuma energia che si potrebbe anche non consumare perché è sprecata non serve a niente”) Questa energia serve a mantenere sicuro il network di Bitcoin con la quale si eseguono tutte le transazioni mondiali.

Senza questa energia il network di Bitcoin non potrebbe esistere. Il mining è quel metodo usato dal network Bitcoin per rimanere sicuro e senza quella sicurezza non avrebbe senza che esistesse il Bitcoin.

Il sistema bancario tradizionale ha un consumo stimato di circa 250 Twatt/h il consumo energetico stimato dell’estrazione dell’oro è di circa 200 Twatt/h invece l’industria di bitcoin consuma circa 100 Twatt/h (questo tendenza è in crescita grazie al numero di mining che aumentano)

Le banche transitano molto più denaro di quanto faccia l’industria di Bitcoin ma qui rischiamo di cadere in uno dei “luoghi comuni” che sentiamo ai telegiornali. Stiamo confrontando due sistemi che sono del tutto differenti quante volte abbiamo sentito dire “una transazione di bitcoin consuma quanto 100 mila transazioni fatte con la carta di credito” ma è un paragone che non può stare in piedi perché il consumo energetico di Bitcoin non varia al variare del numero di transazioni sul network. Il consumo energetico di Bitcoin dipende dal numero di miner ossia dalla potenza complessiva dei miner che partecipano al network (ci sono alche altre componenti che però hanno un consumo davvero minino è per questo non le teniamo in considerazione)

Questo è un valore fisso indipendente dal numero di transazioni (il mining esiste a prescindere anche se la Blockchain fosse vuota e nessuno facesse transazioni il mining consumerebbe uguale perché deve produrre quel numero di blocchi vuol dire che se avessi una transazione di 20 dollari o 20 trilioni di dollari non cambierebbe essenzialmente nulla il consumo energetico sarebbe lo stesso) Esiste un limite di transazioni che Bitcoin può eseguire ma ci esistono metodi per scalare i volumi transati di numerosi fattori con un impatto energetico davvero basso (basti pensare che un nodo di line network può stare anche su un raspberry quindi consumi davvero minimi).

L’energia dipende dal minig

Secondo punto importantissimo “da dove viene questa energia ?” l’energia in generale andrebbe spinta verso il settore rinnovabile (è più facile a dirlo che a farlo) Bitcoin potrebbe essere un veicolo che spinge verso l’energia rinnovabile (il nemico numero 1 dell’ambiente che spinge verso l’energia rinnvaobile)

Semplicemente il minign di Bitcoin è unn buisness è tende ad approvigionarsi di energia nel modo che gli può costare di meno nel tempo . Nel caso della Cina fino a quando era all’interno dell minig si usava il combustibile fossile perché era di costo bassissimo

Dopo l’estromissione della Cina gli Stati Uniti ora hanno preso il posto come mining principali per hashpower (potenza apportata all’interno network) e gli USA sono i maggior investitori nell’area del minig Green (ci sono già numerose aziende gia quotate al NASDAQ che fanno minig Green ). In Texas esiste un problema di blackout perché alcune città aveva dei picchi di fabisongo energetico e andava quindi il blackout e di fatto le loro centrali non riuscivano a alimentare tutte le città che avevano bisogno di energia durante i momenti di questi picchi il minig di Bitcoin ha incentivato lo stato del Texas a costruire più centrali idroelettriche ed eoliche (energie rinnvabili). Così facendo il texas si è ritrovato con una eccedenza energetica ed a convertito questa eccedenza in minig (ha trasformato energia in valore!) e quindi tu non butti questa energia svendendola ma la trasformi in canali nel minig. Quindi noi abbiamo una sorta di volano che è la minig farm che nel momento in cui il fabisogno energetico dei tuoi utenti è basso incanalo più energia nella produzione di Bitcoin invece se il fabisogno energetico aumenta per ovvi motivi reindirizzo l’energia verso il fabisogno energetico degli utenti piutosto che alla produzione di Bitcoin è questo sistema porta ad non avere più Blackout. Cosi facendo viene vogliadi costruire nuove centrali risolvendo problemi energetici, investendo nell’energia rinnovabile perché tanto se hai energia di troppo non la butti la trasformi in Bitcoin dalla quale ottien dell’altro utile che può essere investito di nuovo in energia, infrastrutture o servizi (porto avanti lo sviluppo)

Tutte le attività produttive consumano energia chi più chi meno. Bisogna concentrasrsi vengo la transizione verso il rinnovabile

Che cos’è il Mining ?

E il più importante e longevo algoritmo di consenso distribuito e la colonna fondamentale del mondo crypto e Bitcoin in quanto è ciò che gli consente di esistere e ciò che si consente soprattutto di essere sicuro alla sua blockchain e al suo protocollo.

Cos’è un algoritmo di consenso distribuito?

Conoscete la storia dei generali bizantini? Probabilmente no! La storia dei generali bizantini è una sorta di indovinello da risolvere.

Ci sono un insieme di generali bizantini che si devono coordinare per attaccare una roccaforte ma c’è un problema ci possono essere tra questi generali dei traditori che sono codardi e non vogliono andare all’attacco. Un’attacco coordinato di tutti i generali bizantini porterebbe sicuramente alla vittoria ma se questi questi traditori cominciassero a mettere del dissenzio tra i generali c’è il rischio che l’attacco risulti un totale fallimento.

Quindi abbiamo due categorie di attori : i genereali che vogliono attaccare e vincere e i generali traditori che vogliono scappare e salvarsi

Questi generali non si parlano tutti tra loro e quindi ci potrebbe essere un generale traditore che comunica a gli altri che gli è stato comunicato che non bisogna attaccare e bisogna ritirarsi. Poste queste condizioni quale potrebbe essere un metodo per coordinare tutti i generali per far in modo di riuscire ad attaccare tutti insieme la roccaforte ?

Nei sistemi distribuiti (peer-to-peer)questo problema è più attuale che mai in quanto noi abbiamo una moltitudine di nodi che dobbiamo mettere d’accordo su un’unica soluzione ossia qual è la blockchain corretta perché potremmo avere alucuni nodi traditori che vogliono proporre una versione fallacea dela blockchain per andare a modificare qualche transazione e andare a fare double spending.

Per fare ciò bisogna creare degli algoritmi di consenso distribuito.

Il consenso distribuito ha come scopo quello di mettere d’accordo tutti i nodi partecipanti su una sola versione della blockchain

Ci sono alcuni problemi da dover risolvere: Come decidere chi ha ragione in caso di contenziosi ? Come definire la versione giusta della blockchain?

Come dare modo a tutti di parteciapre equamente, decentralizzandolo (tutti i nodi devono avere voce in caoitolo)? Come evitare che attori malevoli influenzino il processo? Queste solo le domande a cui devono rispondere i vari algoritmi di consenso

Esistono vari algoritmi di consenso distribuito e i più famosi sono Proof of Work, Proof of Stake, Proof oF aUHORITY (vechain), proof of history(SOLANA)

Proof of capacity (Chia)

Proof of Work ogni nodo propone la sua verisone della blockchain provandola con il lavoro che ci ha dedicato (potenza di caolcol)

I NODI competono con la loro poW per risolvere l’ultimo blocco e alla fine qualcuno riuscirà a chiudere quel blocco

Alla quel nodo creerà un blocco in più e la sua chain sarà più lunga delle altre (chi ha la chain più lunga è quella accettata dal network)

Come fa un nodo a provare di aver svolto lavoro?

La funzione hashing ? questa funzione prendere come input un qualsiasi dato e ci fornisce in output “”hashed” che è una stringa alfanumerica di lunghezza variabile. A prescindere dalla dimensione dell’input, l’output è sempre a 256 bit (nella SHA256). Lo stesso input da sempre lo stesso output (se volete potete provarlo su un qualsiasi generatore di funzione Hash.)

La funzione hashing è asimmetrica/non invertibile in quanto dall’output non posso risalire all’input

Mining

Il blocco da validare contiene tutte le transazione fatte in un lasso di tempo e poi contiene un blocco T che avrà al suo interno un riferimento al blocco T-1, il blocco T-1 avrà dentro le sue transazione è un riferimento al blocco T-2 e cosi via. Questo riferimento è in realtà hash del blocco precedente quindi io do in pasto tutto il blocco precedente eseguo la funzione di hashing che mi genera una strinfa alfanumerica (output del blocco ) e quell’output lo vado a mettere dentro al blocco T

Oltre questo abbiamo abbiamo anche una parte variabile il Nonce value al fine dì fare competizione tra tutti in modo che ognuno possa partecipare al network (produrre lavoro). Quindi l’obiettivo è trovare un hash che sia minore al hash deciso dalla difficoltà (più è alta la difficoltà più è difficle trovare l’hash)

Operazione random, di fatica (manicare hash finché non ci becchi) è questo e il modo in cui dimostri che hai consumato energia (ciè hai lavorato)

Un Miner spende energia perché fa 10^12 operazioni di hash al secondo (costo) e ne fa sempre di più per riuscire a competere e riuscire a chiudere (validare)il blocco trovando l’hash corretto, riceve BTC se valida un blocco (incentivo)

La potenza computazionale di un miner si misura in TH/s (TeraHas/secondo) la misura del netwrok è 200 milioni di TH/s Tera = 10 ^12 operazioni di hash in 1 secondo

Più miner = meno tempo per beccare il nonce giusto

Più l’hasrate totale aumneta più la difficilata aumenta e viceversa se scende l’hashrate scende anche la difficoltà (una volta si faceva mining solamente con il processore del computer ora questa idea è solamente un lontano ricordo)

Nella Bitcoin network c’è una rigida regola che deve essere sempre eseguito ciò che tra la vaildaizone di un blocco è l’altro devono passare 10 minuti

Bisogna mantenere il tempo-intra blocco costante

Minare da solo è presochè impossibile perché non riuscirò mai a minare un blocco (avrei bisogno una potenza di calcolo davvero spropositata) e per questo nascono i mining pool dove tanti piccoli miner vengono messi in una pool per avere più potenza e dopo aver minato un blocco il pool suddivide proporzionalmente la ricompensa in Bitcoin ai partecipanti (il mining pool non è un sistema centralizzato perché se mai il pool dovese comportarsi in modo malevolo i miner andrebberò via dalla pool per cercare un’altra pool)

Generali bizantini e 51% attack

La chain più lunga , la prima che valida il nuovo blocco, è quella coretta e accettata da tutti

Se un utente malevolo non ha maggioranza HP(hash power): funziona (l’utente malevolo non può avere la chain più lunga per molto tempo)

Affinchè in problema dei generali bizantini venga risolto a favore dei non traditori la percentuali di utenti non malevoli ossia non traditori deve essere maggiore del 51% . Più hashpower complessivo cresce = più Bitcoin diventa sicuro e più costoso attaccre il network Bitcoin