UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in

Economia Aziendale

La moneta 2.0: Bitcoin

The currency 2.0: Bitcoin

Relatore:

Prof. Gallegati Marco

Rapporto Finale di:

Maurizi Matteo

Anno Accademico 2021/2022

INTRODUZIONE

Il Bitcoin è la prima valuta digitale decentralizzata. Nonostante questa moneta sia in circolazione dal 2009, la sua novità non sta nella digitalizzazione dei pagamenti, che nell'era di Internet ormai tutti sono abituati, ma nel suo decentramento. A differenza di tutte le valute tradizionali, i bitcoin non sono autorizzati in alcun modo: le zecche nazionali non considerano di coniarli, non esiste una banca centrale per controllarne il valore e non esiste un intermediario finanziario per verificarne le transazioni. L'intenzione originaria di Bitcoin era quella di rendere le transazioni Internet più sicure e veloci. Si tratta di un sistema di transazione elettronica che non si basa più sulla fiducia nelle autorità di terze parti, ma su matematica e crittografia. Le banche centrali sono sostituite dalla rete Bitcoin, una rete peer-to-peer (p2p) a cui tutti possono partecipare, purché si installi il software omonimo sul proprio computer, è gratuita e open source, anche se richiede molta potenza di calcolo. I nodi della rete, "facendo funzionare" il software nei propri dispositivi, contribuiscono ad ampio raggio alla verifica e alla registrazione delle transazioni tra due utenti che vogliono scambiare unità di questo nuovo tipo di valuta, garantendone l'anonimato grazie alla crittografia insita nel sistema. L'attività di validazione e registrazione delle transazioni è chiamata "mining", in italiano miniera, termine che traccia metaforicamente

l'attività di estrazione dell'oro da una miniera, e i soggetti che svolgono questa attività sono chiamati "minatori". L'attività utilizza la potenza di calcolo delle attrezzature dei minatori e viene pagata in Bitcoin di nuova emissione secondo un preciso sistema di ricompensa. Attualmente ci sono oltre 18,81 milioni di bitcoin in circolazione e 1 BTC oggi vale $ 19.500. Questo prezzo è determinato dal mercato o dal meccanismo della domanda e dell'offerta, ma è caratterizzato da un'elevata volatilità. Lo scopo di questo elaborato è di effettuare un'analisi tecnica ed economica di questo innovativo sistema di pagamento.

CAPITOLO 1 - COS'È BITCOIN?

1.1 Cos'è il Bitcoin

Bitcoin è una valuta virtuale creata nel 2009 da uno o più hacker con lo pseudonimo di Satoshi Nakamoto. A differenza di altre valute, dietro Bitcoin non c'è una banca centrale per distribuire nuove valute, ma si basa fondamentalmente su due principi: una rete di nodi, o PC, che governano Bitcoin in un modello distribuito peer-to-peer e l'uso di crittografia forte per verificarlo e assicurarlo. Bitcoin è conosciuta come la prima valuta digitale decentralizzata. La parola Bitcoin racchiude diversi concetti: Bitcoin (la "B" maiuscola) è una rete di pagamento virtuale progettata per velocizzare e rendere più sicure le transazioni su Internet. Su questa rete viene scambiato o venduto un nuovo tipo di valuta o asset diversa dalla valuta tradizionale: bitcoin (con la "b" minuscola). La novità che caratterizza bitcoin è appunto la mancanza di un organizzazione che la controlli. Le transazioni in bitcoin non devono fare affidamento su alcun istituto finanziario che agisca come garante di terze parti, che è una presenza essenziale nel commercio online per le tradizionali transazioni in valuta. C'è comunque un controllo ampiamente distribuito su tutta la rete ed è garantito dall'adesione a un protocollo comune, un insieme di regole che definiscono il funzionamento del

sistema, espresso nell'uso del software Bitcoin. Ogni nodo della rete, ovvero ogni dispositivo hardware su cui funziona il software Bitcoin e può comunicare con altri dispositivi della rete, diventa un soggetto attivo nel processo di gestione della valuta. In conclusione, si può affermare che Bitcoin è un nuovo tipo di sistema di pagamento in cui il controllo è distribuito tra i nodi della rete in maniera decentralizzata, consentendo transazioni elettroniche nella nuova valuta digitale Bitcoin.

Le caratteristiche di Bitcoin

- Decentralizzazione - Uno degli obiettivi principali durante la creazione del Bitcoin era la totale indipendenza della valuta da qualsiasi autorità governativa. È stato progettato in modo che ogni persona, azienda o macchina coinvolta nel processo di mining e verifica delle transazioni possa far parte di una vasta rete. Anche parte del network venisse disattivato, il denaro continuerebbe comunque a muoversi.
- Anonimato - Le transazioni di Bitcoin funzionano diversamente dalle normali transazioni tra banche, in quanto il mero indirizzo del portafoglio non può essere ricollegato a nessuna informazione personale. Se da una parte alcuni individui semplicemente non vogliono che il loro denaro venga tracciato e

gestito da autorità esterne, dall'altra è possibile che l'anonimato del Bitcoin supporti attività illegali come il commercio di droghe ed il terrorismo.

- Non soggetto a politiche monetarie - L'assenza di un'autorità centrale rende impossibile per chiunque esercitare azioni coercitive sul denaro, come aumentare o diminuire unità monetarie in circolazione. L'offerta di moneta è stabilita a priori in modo che aumenti gradualmente fino a raggiungere la soglia di 21 milioni di unità. Inoltre non è soggetto a inflazione.
- Trasparenza - Tutte le transazioni sono registrate in un open al pubblico, la blockchain, ricercabile da tutti.
- Velocità - La rete Bitcoin elabora i pagamenti quasi istantaneamente: indipendentemente dalla distanza geografica, ci vogliono pochi minuti per inviare denaro a un altro utente, a differenza dei pagamenti tradizionali che richiedono giorni per essere completati.
- Non-rifiutabilità - Una volta che i Bitcoin sono stati spediti, non è più possibile riottenerli, a meno che il destinatario non decida di spedirli indietro. Questo assicura la ricezione del pagamento, vale a dire che è impossibile truffare qualcuno affermando di non aver ricevuto il denaro.

Le differenze con le altre valute legali

Il rapporto della BCE "Virtual Currency Initiative" definisce valuta legale (valuta fiat) qualsiasi valuta fiat stabilita ed emessa da un'autorità centrale che è accettata dalle persone in cambio di beni e servizi. La valuta Bitcoin appartiene alla categoria della valuta virtuale, definita come valuta digitale non regolamentata, generalmente stabilita e controllata dai suoi sviluppatori e accettata e utilizzata dai membri di determinate comunità virtuali. Esistono diversi tipi di valute virtuali basate sulla capacità di interagire con il mondo reale, il che significa che possono essere scambiate con valuta fiat o per acquistare beni e servizi nell'economia reale a un certo tasso di cambio. IL bitcoin è venduto in valuta fiat e può essere utilizzato per acquistare beni e servizi, appartenenti alla terza categoria dei sistemi di valuta virtuale. Il bitcoin, come altre valute simili nate nel 2009, rientra nella categoria delle criptovalute. Le criptovalute sono valute digitali decentralizzate che utilizzano la crittografia per verificare le transazioni e regolare l'emissione di nuove unità monetarie.

1.2 Come ottenere i Bitcoin e come spenderli

Esistono diversi modi per ottenere bitcoin, alcuni sono semplici e diretti, altri richiedono più tempo e organizzazione. Sia le attività fisiche che quelle online per le quali puoi spendere soldi sono in costante crescita. Prima ancora di pensare ad acquisire e utilizzare bitcoin, devi metterti nelle condizioni di riceverli e, dopo averli ricevuti, tenerli al sicuro dal rischio di perderli o "rubarli". Ciò richiede un portafoglio bitcoin, un portafoglio elettronico che molto metaforicamente svolge le stesse funzioni di un portafoglio fisico, come immagazzinare i nostri soldi, in questo caso digitale.

Il wallet di Bitcoin

I portafogli Bitcoin e i conti correnti non sono esattamente gli stessi. Anche se le interfacce fornite dai vari servizi di portafoglio ti consentono di conoscere l'importo totale di Bitcoin che possiedi in qualsiasi momento, nonché il movimento di depositi e prelievi, i bitcoin in realtà non si trovano nei portafogli, ma sono tenuti in un registro pubblico, una blockchain a indirizzi specifici di proprietà di utenti diversi. Gli indirizzi sono i punti di ricezione e invio, rappresentati da un codice alfanumerico a 33 o 34 bit, solitamente iniziante con 1, in modo da non includere alcun riferimento all'utente, facendo di Bitcoin uno

pseudonimo sistema di pagamento. Questi indirizzi sono derivati da altri codici, algoritmi a chiave pubblica, che a loro volta sono derivati da algoritmi a chiave privata, quindi partendo da un indirizzo è impossibile risalire alla chiave pubblica originaria e da lì alla chiave privata. Attraverso il meccanismo crittografico della firma digitale, solo il possesso della chiave privata può autorizzare l'utente ad utilizzare i bitcoin associati all'indirizzo da essa ricavato. Pertanto, la chiave privata non deve essere trapelata, ma deve essere conservata in modo tale che non vi sia il rischio che i bitcoin ad essa associati non vengano più utilizzati. I portafogli bitcoin memorizzano la chiave privata dell'utente, consentendo l'accesso ai bitcoin associati all'indirizzo esatto derivato dalla chiave pubblica da cui deriva la chiave pubblica. Il wallet, infatti, mette a disposizione dell'utente un'interfaccia intuitiva che gli consente di visualizzare i saldi bitcoin disponibili di tutti i diversi indirizzi in suo possesso, consentendogli di effettuare transazioni in uscita verso specifici beneficiari o ricevere pagamenti da specifici indirizzi. I portafogli Crypto rientrano in due grandi categorie: hot e cold. Gli hot wallet, così chiamati perché sono connessi a Internet per la maggior parte del tempo, includono tipi di dispositivi mobili, desktop e browser. I portafogli freddi includono portafogli cartacei che non sono mai "caldi" e portafogli hardware che

sono connessi a Internet solo quando sono in uso. Ogni tipo di portafoglio ha vantaggi specifici.

I tipi di Hot Wallet :

- Mobile Wallets - I portafogli mobili sono diventati il portafoglio di riferimento per i neofiti delle criptovalute, principalmente per comodità, ma anche perché i nuovi utenti possono detenere piccole quantità di monete mentre imparano a conoscere il panorama delle criptovalute. I portafogli mobili hanno problemi di sicurezza: gli smartphone sono quasi sempre connessi a Internet e sono vulnerabili ai virus e possono essere persi o rubati.
- Desktop e Browser Wallets - Sono semplici da usare, ma sono accessibili su computer desktop e portatili tramite estensioni del browser.

I tipi di Cold Wallets :

- Hardware Wallets - Sono dispositivi fisici che si collegano a un computer, telefonini tramite un cavo USB o Bluetooth.
- Paper Wallets - Utilizzati principalmente da utenti avanzati, i portafogli di carta sono i più freddi tra i portafogli freddi e sono considerati i più sicuri in quanto non sono vulnerabili agli attacchi online. Mai connesso a Internet, un portafoglio di carta è in realtà un pezzo di carta su cui sono stampate chiavi pubbliche e private, solitamente sotto forma di codice QR. Per fare trading, gli

utenti scansionano semplicemente il codice. I portafogli di carta devono essere conservati in un luogo molto sicuro.

Come si ottiene il Bitcoin

- Comprati da persone che vogliono venderli: su LocalBitcoins, persone di diversi Paesi possono scambiare la loro valuta locale in bitcoin. Permette agli utenti di creare annunci in cui possono scegliere il metodo di pagamento e il tasso di cambio per comprare e vendere bitcoin da e ad altri utenti di LocalBitcoins. Rispondendo agli annunci, si apre una chat di scambio e si attiva automaticamente la protezione escrow. L'escrow protegge sia l'acquirente che il venditore, mantenendo i bitcoin al sicuro fino a quando il pagamento non viene effettuato e il venditore rilascia i bitcoin all'acquirente. Opera in 7.600 città e 240 paesi, tra cui l'Italia. Chi vuole acquistare bitcoin può decidere se scambiare online o meno scegliendo un metodo di pagamento (bonifico bancario, PayPal...) oppure può organizzare un incontro fisico con il venditore e scambiare bitcoin con contanti, perché anche queste offerte sono relativamente vicine geograficamente.

- Comprati presso gli exchange: esistono molti siti Web su Internet che ti consentono di acquistare e vendere bitcoin con valuta fiat o altre criptovalute. Queste piattaforme agiscono come market maker impostando il tasso di cambio al quale gli scambi acquistano e vendono bitcoin contro le principali valute tradizionali o altre valute virtuali. A seconda del sito web scelto, il processo di registrazione e verifica dell'identità dell'utente potrebbe richiedere del tempo per avviare gli acquisti e le vendite di Bitcoin.
- Bitcoin ATMs: un servizio di acquisto o vendita molto più rapido rispetto agli exchange online è offerto dai Bitcoin ATMs o Bancomat Bitcoin. Il primo bancomat bitcoin, prodotto dall'americana Robocoin, è stato installato nell'ottobre 2013 presso la Waves Coffee House di Vancouver, Canada, e già nel suo primo giorno di funzionamento ha registrato ben 81 transazioni per un valore totale di oltre 10.000 $. Oggi ci sono più di 38000 bancomat bitcoin nel mondo, di cui 50 circa in Italia, ma stando alle stime dello stesso sito tale numero cresce settimanalmente di circa 8 nuove unità.
- Mining: è la verifica e la registrazione delle transazioni Bitcoin che avvengono costantemente nel sistema. Questa operazione viene eseguita da nodi di rete, cosiddetti miner, costituiti da un computer che esegue ripetutamente problemi crittografici complessi, costosi in termini di consumo energetico e usura delle

apparecchiature. Il mining è semplificato da un preciso sistema di ricompense costituito da bitcoin di nuova emissione in una quantità e tempo determinati dal protocollo, come descritto nel prossimo capitolo, ed è l'unico meccanismo attraverso il quale vengono create e inserite nuove unità di valuta.

- Vendita di beni e servizi per bitcoin: attualmente in Italia questa opzione è più pratica per i trader. Sempre più negozi, sia fisici che online, accettano pagamenti in bitcoin per beni e servizi. Il modo più semplice per un commerciante di accettare pagamenti bitcoin dai propri clienti è inserire un indirizzo e attendere che effettuino il pagamento sul proprio smartphone.

Come spendere i Bitcoin

Oggi è possibile già spendere bitcoin in cambio di prodotti e servizi? Assolutamente si, oltre ad alcuni paesi in cui è moneta legale, come El Salvador, ci sono diverse aziende che accettano pagamenti in bitcoin. Anche se in molti Stati ancora non sono pienamente regolamentate, il fenomeno crypto è troppo grande per essere ignorato. Ecco perché le aziende vogliono innovarsi e spingere verso la diffusione dei pagamenti in criptovalute e non si parla di nicchie specifiche, bensì di brand e servizi conosciuti da chiunque che fanno parte della nostra quotidianità. Molte grandi aziende ad oggi accettano pagamenti con Bitcoin come Mastercard,

Microsoft, Coca Cola, Gucci… La realtà Bitcoin non è più futuro ma presente co le criptovalute si può acquistare ormai di tutto dai voli, trasporti a buoni regalo. Le aziende che le accettano sono continuamente in crescita ed è probabile che nei prossimi anni diventerà sempre più la normalità: non solo piccole realtà, ma anche grandi colossi che inevitabilmente avranno una forte influenza su tutti gli altri.

1.3 La storia

La leggenda narra che Satoshi abbia rilasciato la sua prima dichiarazione sulla mailing list Cypherpunks l'8 gennaio del 2009, con un link a 'Bitcoin.v0.1.rar' appena caricato su SourceForge. A quel tempo minava bitcoin tramite CPU per 5 giorni, ovvero dal 3 gennaio il fattore di difficoltà era zero; quando la rete è diventata pubblica, la difficoltà è salita a 8. Per quanto ne sappiamo, queste sono le origini di Bitcoin. "Bitcoin v0.1" è stato il nome del primo software bitcoin e il suo rilascio nel gennaio 2009 ha segnato l'inizio dell'era delle criptovalute. I primi anni non sono stati molto entusiasmanti, ma il 2009 può essere visto come un anno spartiacque: da un lato ha rappresentato il raggiungimento di un importante traguardo tecnologico, derivante da numerosi progressi nel campo della crittografia e dell'informatica. D'altra parte, ha segnato la nascita di un vero e proprio ecosistema attorno a Bitcoin e la successiva proliferazione di altcoin o valute digitali alternative che hanno portato alla nascita di progetti Bitcoin.

Prima del Bitcoin

Dagli anni '70, la ricerca crittografica ha portato a sviluppi significativi in un momento in cui il graduale avanzamento verso l'era digitale sottolineava la necessità di sicurezza e privacy. La crittografia, prerogativa dei governi per la

sicurezza delle comunicazioni, è ancora una volta di dominio pubblico per garantire un elevato livello di privacy nei nuovi sistemi digitali, compresi quelli relativi ai pagamenti. Nel 1988 David Chauman considerato come l'inventore del contante digitale introduce la tecnologia delle " blind signatures" che si basano su schemi di firma digitale a chiave pubblica, come RSA. Il sistema RSA garantisce la riservatezza della comunicazione tra due parti, cifrando alla fonte il messaggio da trasmettere su un canale non sicuro e decodificandolo alla ricezione garantendo la sicurezza delle informazioni mediante la firma digitale. L'obiettivo principale delle blind signatures è far firmare il messaggio al firmatario senza rivelare lo stesso messaggio. Questo si ottiene mascherando il contenuto del messaggio prima di firmarlo. Chaum estende le sue ricerche nell'ambito dei sistemi di pagamento elettronici con la fondazione della DigiCash Inc. ad Amsterdam e il lancio del sistema e-cash nei primi anni '90. Il sistema di pagamento elettronico e-cash utilizzava del denaro virtuale da tenere nel computer, controllato crittograficamente dalle banche associate e consentiva di effettuare acquisti anonimi e sicuri su Internet o nei negozi che li accettavano, senza la necessità di scambiare le credenziali delle carte di credito. Nonostante questo sistema venne venduto a diverse banche, queste si mostrarono comunque conservative in un mercato dominato dalle carte di credito, per cui e-cash non

decollò mai in maniera significativa e fallì nel 1998. Nonostante e-cash fosse un sistema centralizzato in quanto controllato dalla banca emittente, era comunque fondato su solide basi crittografiche che avrebbero in seguito fornito degli spunti per i successivi tentativi di decentralizzazione. Nel 1998 Wei Dai con b-money progetta un'idea che esista un network anonimo in cui gli utenti siano identificati da pseudonimi, che ogni utente conservi in modo separato un registro delle transazioni (o in alternativa che lo stesso sia tenuto solo da alcuni di questi utenti, chiamati server, e che questi abbiano degli incentivi per tenerlo in modo onesto), che la creazione di moneta avvenga mediante la risoluzione di problemi attraverso l'impiego di una certa potenza di calcolo, e che infine le transazioni avvengano tra indirizzi mediante il meccanismo della firma digitale. B-money, è considerato il primo criptovaluta reale poiché le sue basi teoriche sono simili a quelle seguite dalle attuali criptovalute. A questo punto c'è da chiedersi se e in che modo il creatore di Bitcoin, Satoshi Nakamoto, ha preso spunto da queste esperienze per la creazione di Bitcoin. Va ricordato che la fine degli anni '80 ha visto la nascita del cypherpunk, un movimento incentrato sulla crittografia come tecnologia in grado di portare a cambiamenti politici e sociali. I rappresentanti del movimento hanno sostenuto lo sviluppo crittografico di quegli anni e la ricerca di Chaum. In Cypherpunk, diversi informatici ed esperti di crittografia hanno sottolineato

l'importanza e l'innovazione del contributo, inclusi i fondatori del movimento Tim May, Eric Hughes e John Gilmore. David Chaum e Wei Dai citati sopra. Cosa c'entra Bitcoin con tutto questo? Bitcoin, invece, sembra mettere in pratica le idee e gli obiettivi per i quali è nato il movimento cryptopunk, ovvero tutelare il diritto alla privacy creando un sistema di pagamento anonimo alternativo ai tradizionali sistemi di pagamento che utilizzano matematica e crittografia inoltre Nakamoto menziona sia Wei Dai su b-money che Adam Back sull'hashish nel suo articolo.

Chi è Satoshi Nagatomo?

"L'identità dell'inventore di Bitcoin rimane ad oggi un mistero". Ciò che si sa è che nell'agosto del 2008 qualcuno ha registrato in modo anonimo il dominio bitcoin.org. Nell'ottobre dello stesso anno, un autore soprannominato Satoshi Nakamoto ha pubblicato il Bitcoin whitepaper, "Bitcoin: A Peer-to-Peer Electronic Cash System" su metzdowd.com. Si tratta di un sito per gli appassionati di crittografia, nel quale il creatore di Bitcoin ha spiegato come avrebbe funzionato la valuta digitale. Ma chi è realmente Satoshi Nakamoto? Non si sa e probabilmente mai si potrà sapere l'identità dell'ideatore di Bitcoin, o forse del gruppo di persone che l'ha creato e che si nasconde dietro questo pseudonimo. Numerose ricerche sono state fatte in proposito e numerosi sono gli esperti a cui è

stato accostato, tra cui anche Nick Szabo, ideatore di bit-gold che ha comunque smentito di essere Satoshi Nakamoto. Per quasi dieci anni, Satoshi Nakamoto è stato l'unico minatore che ha creato più di un milione di Bitcoin nel tempo. Tuttavia, la prima transazione è stata effettuata con l'esperto di criptovalute Hal Finney. Lo stesso Nakamoto ha riportato l'incidente nel forum di settore bitcointalk.org, dove ha lavorato da novembre 2009 a dicembre 2010. Tanti utenti hanno utilizzato questo suggerimento per seguire le tracce del creatore di Bitcoin e rivelare la sua identità. Quest'ultimo implicava che lui e Hal Finney fossero due persone diverse. Da allora, ci sono state poche notizie su Satoshi Nakamoto. Nel 2010, ha venduto il codice sorgente di Bitcoin allo sviluppatore Gavin Andresen, che l'anno successivo ha chiarito le sue motivazioni. In un'e-mail datata 23 aprile, Satoshi ha dichiarato: "Sono passato ad altre cose. È in buone mani con Gavin e tutto il resto". La sua attività da allora è cessata. I portafogli Bitcoin a lui associati non sono stati utilizzati o toccati dalla metà del 2009 e sembrava che il creatore della prima valuta digitale non avrebbe mai più parlato ma nel 2014, il suo account P2P Foundation è stato brevemente riattivato per sfatare un articolo di Newsweek che identificava Dorian Nakamoto come l'inventore di Bitcoin. "Io non sono Dorian Nakamoto", scrisse, poi rimase in silenzio fino ad oggi.

Dalla nascita ad oggi

Bitcoin è nato ufficialmente il 3 gennaio 2009, quando è stato rilasciato il primo client per iniziare il mining e quindi creare nuove valute. Il 12 gennaio viene registrata la prima transazione sulla blockchain, in cui Satoshi invia 10 BTC al criptopunk e crittografo Hal Finney. Sono passati più di dodici anni e Bitcoin ha fatto molta strada in quel periodo. Attualmente sono in circolazione più di 18,7 milioni di BTC e sulla blockchain di bitcoin sono già state registrate quasi 60 milioni di transazioni. Nel 2009, tuttavia, non esistevano piattaforme in cui i bitcoin potessero essere scambiati, acquistati o venduti, potevano solo essere inviati o estratti da un portafoglio all'altro. In altre parole, non avevano un valore di mercato espresso in dollari, che può quindi essere valutato pari a zero. L'estrazione di BTC era molto facile all'epoca, quindi si stima che Nakamoto ne abbia estratto più di un milione lui stesso. Tuttavia, nel 2011, Satoshi ha perso le tracce ed è letteralmente scomparso nel nulla. Il 22 maggio 2010, il primo pagamento bitcoin della storia è avvenuto quando Laszlo Hanyecz ha pagato 2 pizze con 10.000 BTC. Oggi, l'equivalente di quel numero sarebbe più di $ 200 milioni, rendendo le due pizze le più costose mai acquistate. Nel luglio 2010 ha avuto luogo il primo scambio di bitcoin presso il Monte Gox, fondata da Jed McCaleb, e nell'agosto dello stesso anno iniziarono le prime transazioni regolari

di bitcoin in dollari sugli exchange ad un prezzo di circa 0,07$. In altre parole, il suo valore è già aumentato di sette volte da maggio. Il 28 novembre 2012 è avvenuto il primo split, che ha ridotto della metà il compenso del miner a 25 BTC per blocco minato e nel 2013 è stata innescata la prima grande bolla speculativa, che ha alzato il prezzo del bitcoin a più di $ 1.100. A quel tempo, il valore del bitcoin era già 110.000 volte superiore al suo prezzo iniziale nel maggio 2010. Successivamente, il 2015 è stato l'anno peggiore in assoluto per gli indicatori di prezzo BTC, con un prezzo medio dell'anno scorso di $ 272, in calo del 48% rispetto al prezzo medio dell'anno scorso. Il 9 luglio 2016 si è verificata la seconda spaccatura, seguita da un'altra grande bolla speculativa nel 2017, che ha portato il prezzo del bitcoin a $ 20.000. A quel tempo, il valore di BTC è raddoppiato di due milioni di volte rispetto al valore iniziale di maggio 2010. Nel 2018 è scoppiata un'altra grande bolla speculativa, ma l'anno successivo, il 2019, il prezzo medio è sceso. L'11 maggio 2020 si è verificata la terza divisione e nel 2021 il prezzo ha raggiunto nuovi massimi vicino a $ 65.000 il 1 aprile 2021. A quel punto, il valore del bitcoin era aumentato di 6,5 milioni di volte dal suo valore iniziale nel maggio 2010. Al giorno d’oggi Bitcoin, è sceso sotto i 18.000 dollari, con un calo di circa il 14%. Ciò lo ha portato al di sotto del livello di picco della precedente corsa al rialzo nei mercati delle criptovalute nel 2017 e ha

cancellato anni di guadagni per i detentori a lungo termine. La causa immediata di questo ultimo crollo sembra essere l'inflazione. In particolare gli investitori sembrano temere che l'attuale livello di inflazione possa continuare ad aumentare, di conseguenza facendo crescere il rischio di una recessione e più generalmente il livello di incertezza riguardo alla situazione economica globale. Tale timore è stato dimostrato dagli investitori attraverso una grande svendita dei propri asset, che ha portato il valore di bitcoin, così come della maggior parte della altre criptovalute, a crollare. Sul crollo più recente hanno presumibilmente influito i rialzi dei tassi di interesse dalla banca centrale statunitense (Fed) e dalla Banca centrale europea (Bce) e le prospettive per il settore non sembrano essere positive.

CAPITOLO 2 - COME FUNZIONA BITCOIN

2.1 Il funzionamento di Bitcoin

La funzionalità di Bitcoin è nelle mani di nodi della rete chiamati “miner" i quali raccolgono le transazioni in corso in contenitori specifici chiamati blocchi attraverso un processo di mining. Questi blocchi sono collegati tra loro per formare una blockchain che rappresenta il tema più importante e innovativo dell'intero sistema. Blockchain è un grande libro mastro aperto e condiviso dagli utenti, contenente tutte le transazioni avvenute dalla nascita di Bitcoin ai giorni nostri, e costantemente aggiornato dai miner. Chiunque può visualizzare la versione completa della blockchain online, installando il software Bitcoin o tramite un sito Web speciale chiamato Blockchain Researcher. Tuttavia, poiché le transazioni Bitcoin sono condotte tra indirizzi pseudonimi, è garantito un elevato grado di anonimato, rendendo difficile risalire all'identità di un utente. Una transazione è un trasferimento di valore tra i portafogli Bitcoin inclusi nella blockchain. Un portafoglio Bitcoin contiene una serie di dati segreti, chiamati chiave privata, che vengono utilizzati per firmare digitalmente le transazioni, fornendo una prova matematica che la transazione proveniva dal proprietario del portafoglio. Le firme digitali impediscono che le transazioni vengano alterate da

chiunque dopo la loro creazione. Tutte le transazioni avvengono tra utenti e in genere iniziano a essere confermate dalla rete entro i successivi 10-20 minuti.

La crittografia

Bitcoin utilizza una tecnica chiamata crittografia a chiave pubblica-privata. Questo approccio consente alle criptovalute di essere "trustless", il che significa che possono essere scambiate in modo sicuro tra persone che non si conoscono, senza la necessità di un "intermediario di fiducia", una banca o PayPal. Chiave pubblica o crittografia asimmetrica significa che una delle chiavi generate dall'algoritmo è casuale. Esiste una relazione matematica tra queste due chiavi per ottenere la chiave pubblica dalla chiave privata, ma il processo inverso è impossibile: la chiave privata non può essere rintracciata dalla chiave pubblica. Questo permette di assegnare diverse funzioni alla chiave e anche con qualche significato complementare, la chiave privata deve essere tenuta segreta e la chiave deve essere condivisa liberamente. Nella sua applicazione originale, la crittografia a chiave pubblica asimmetrica serviva a due scopi: crittografia e digitale. Come si realizzano queste due funzioni mediante la coppia di chiavi secondo crittografia a chiave o asimmetrica? Attraverso la Cifratura il proprietario di una coppia di chiavi mette la sua chiave disponibile a chiunque desideri un suo messaggio

crittografato. Il mittente utilizza la chiave pubblica del destinatario per crittografare il messaggio: questa può essere decifrata solo da chi possiede la chiave privata "sorella" della chiave con cui è stato crittografato il messaggio. Pertanto, solo il titolare della chiave pubblica , oltre alla corrispondente chiave privata , potrà decifrare il messaggio a lui indirizzato. La sicurezza e quindi la segretezza sta nel fatto che essa è possibile solo alla chiave privata. Successivamente, insieme alla firma digitale, entra in gioco un secondo algoritmo: l'algoritmo di hash. La caratteristica di un algoritmo di hash efficiente è quella data in input a un codice univoco: se cambia anche solo una virgola, l'hash cambierà in modo significativo e imprevedibile. Pertanto, con la firma digitale il mittente firma un messaggio, produce l'hash del messaggio che intende inviare lo cifra con la propria chiave privata infine, allega l'hash cifrato al messaggio e li invia insieme. Il destinatario verifica la firma digitale: produce l'hash del messaggio ricevuto con lo stesso algoritmo usato dal mittente decritta l'hash cifrato ricevuto con la chiave pubblica del mittente. Infine si confronta l'hash decrittato così ottenuto con la "firma" allegata al messaggio dal mittente.

La Blockchain

La blockchain come definita dal sito di bitcoin "è un registro publico e condiviso sul quale si basa l'intera rete Bitcoin". Tutte le transazioni confermate si trovano nella blockchain. In questo modo, i portafogli Bitcoin possono calcolare il loro bilancio disponibile e nuove transazioni possono essere verificate, controllando che chi spende abbia sufficiente disponibilità. L'integrità e l'ordine cronologico della blockchain sono protetti attraverso l'uso della crittografia.

Le transazioni

Le transazioni sono parte integrante del funzionamento delle criptovalute come Bitcoin. Queste rappresentano la spina dorsale di questo sistema di pagamento crittografico che ci consentono di utilizzare e godere dei nostri fondi in modo rapido, sicuro e semplice. In Bitcoin, queste transazioni possono essere intese come l'invio di Bitcoin tra persone diverse che utilizzano la rete. Tutte queste transazioni non sono altro che record salvati all'interno della blockchain di Bitcoin, cioè, un flusso di informazioni. Per effettuare queste transazioni sono necessari gli wallets che gestiscono e conservano i fondi. Gli elementi che formano una transazione Bitcoin sono quattro:

- Entrate(input) - Le entrate si riferiscono all'uscita di una transazione passata che non è stata utilizzata in nessun'altra transazione. Questi ci permettono di confermare l'origine degli asset che hanno utilizzato in una transazione e sono quelli che contengono dove sono stati originariamente ricevuti i bitcoin.
- Uscite(output) - Queste contengono l'indirizzo a cui viene effettuato il bonifico e l'importo inviato. Contengono anche indicazioni di cambio o transazione di reso che vengono inviati i resi. Una transazione può contenere più di un output.
- Identificatore - Ogni transazione effettuata avrà il proprio hash. Questo hash è generato dagli input e dagli output. Questo valore è ciò che ti consente di identificare in modo univoco e non ripetibile all'interno di una blockchain
- Tasso di commissione - La commissione è un piccolo pagamento che i miners ricevono per l'elaborazione di una transazione.

Le transazioni in criptovaluta hanno tutte una struttura di base particolare , con input e output ma con un obiettivo ben preciso: la sicurezza. In ogni momento, questi dati passano attraverso un processo crittografico di hash e crittografia asimmetrica. Questo è ciò che rende le informazioni protette e convalidate correttamente. Per eseguire transazioni sulla rete Bitcoin, i mittenti hanno accesso a indirizzi pubblici e password private associate a quei bitcoin. Non sono altro che raccolte casuali di numeri e lettere senza uno schema definito. Le password

private ci consentono di firmare e inviare transazioni come alcuni bitcoin, purché l'indirizzo pubblico funzioni come un indirizzo e-mail o un numero di conto bancario dove completeremo o riceveremo la transazione.

Il mining

Per molti il mining consiste solo nella produzione di nuovi bitcoin, tuttavia questo non è il suo scopo principale. Il vero scopo del mining è mantenere l'integrità e l'autenticità della blockchain, che per gli utenti rappresenta un vero e proprio conto bancario. Se dovessero mancare queste due caratteristiche il bitcoin perderebbe la fiducia che ha ottenuto e andrebbe contro a fallimento. Quest' attività può essere svolta da tutti che installano il client Bitcoin sul proprio computer. Il mining sfrutta la potenza di calcolo dei dispositivi messi a disposizione dai nodi della rete, ed è stato progettato dallo stesso Nakatomo come termini di elaborazione informatica difficili e dispendiosi in termini di tempo, in modo che numero di nuovi blocchi vengono prodotti in un intervallo di tempo, indipendentemente dal numero di transazioni effettuate sulla rete. "Il motivo per cui questo processo si chiami mining vuole sottolineare la relazione tra i cercatori d'oro che impiegano sempre più sforzi per trovare nuove pepite d'oro, e i nodi che impiegano sempre più potenza computazionale, costosa in termini di energia

consumata, per aumentare i bitcoin in circolazione". L'obiettivo di ogni minatore della rete è risolvere prima questo enigma. I computer dei minatori chiamati nodi, raccolgono e raggruppano continuamente in blocchi le singole transazioni degli ultimi dieci minuti. I computer competono quindi per risolvere un complesso enigma crittografico e diventare i primi a convalidare nuovi blocchi per la blockchain. Come ricompensa per i loro sforzi, il primo miner che troverà una soluzione riceverà una quantità specifica di bitcoin appena coniati. I miner sono sempre i primi a trovare la soluzione corretta per poi trasmetterla all'intera rete, dove altri nodi ne verificano la correttezza. Se tutto va bene, il nuovo blocco viene aggiunto alla blockchain. Sono necessari meccanismi di risoluzione dei puzzle per proteggere la rete Bitcoin da intrusi dannosi. Si può partecipare al mining attraverso tre alternative:

- Solo-mining: l'attività di mining viene svolta individualmente, al fine di possedere la ricompensa e la somma delle commissioni delle transazioni incluse il nuovo blocco. L'attuale elevata competitività del settore richiede una potenza di calcolo significativa per questa specifica alternativa.
- Pool-mining: Può essere fatto collettivamente aderendo a un pool minerario in cui più soggetti possono utilizzare la propria potenza di calcolo e condividere i

profitti in proporzione ai contributi forniti. Il pool mining ti consente di partecipare al mining anche senza un'elevata potenza di calcolo.

- Cloud-mining: è possibile partecipare all'attività senza possedere fisicamente i dispositivi hardware necessari, si evita cosi la manutenzione di questi programmi.

CAPITOLO 3 - L'ECONOMIA BITCOIN

3.1 L'ecosistema di Bitcoin

"Un'ecosistema è costituito da una o più comunità di organismi viventi (biotici) e da elementi non viventi (abiotici) che interagiscono tra loro". Partendo da questa semplice spiegazione di ecosistema possiamo capire che anche il bitcoin ha un proprio ecosistema che lo circonda con le sue parti che lo fanno funzionare.

Le parti dell'ecosistema di Bitcoin sono:

- Programmatori o developers: Costruiscono il software, che è open source, e ne migliorano la stabilità, le caratteristiche e fanno manutenzione.
- Minatori: si occupano della verifica delle transazioni e aggiungono i blocchi alla blockchain. Sono ricompensati con nuovi Bitcoin che sono emessi durante il processo di mining.
- Full Nodes: sono dei computer che connessi alla rete di Bitcoin, verificano e rigettano tutti i blocchi e le transazioni che non seguono le regole del consenso e rigettando le connessioni dai peer che le hanno spedite. Attualmente ci sono circa 10.000 full nodose i tutto il mondo.

- Wallet: è un portafoglio digitale, un hardware che custodisce e conserva i tuoi Bitcoin. Il wallet custodisce la chiave privata per poter spendere o inviare bitcoin.
- Exchanges: vengono utilizzati per l'acquisto di Bitcoin e sono dei siti o attività che permettono lo scambio di criptovalute per altri assets come l'euro o il dollaro.

Anche altri soggetti sono subentrati negli ultimi anni nell'ecosistema Bitcoin e sono le istituzioni finanziarie per fondi ETF, opzioni e future. Oltre a società di software come BTCPay Saver che forniscono servizi per la criptovaluta.

3.2 Le cifre di Bitcoin

Bitcoin da la possibilità ai suoi speculatori di sapere il numero di transazioni effettuate in tempo reale e il valore degli importi scambiati oltre ovviamente al prezzo di mercato convertito in valute legali. Questo sicuramente è uno degli aspetti più importanti di questa criptovaluta che gode di una trasparenza e di una pubblicità non di basso conto data dalla blockchain.

Il prezzo del Bitcoin

Oggi, 30 ottobre 2022, il prezzo di bitcoin è di 19.646$. Dalla sua nascita ad oggi il valore di mercato di questa criptovaluta è cambiato notevolmente raggiungendo in quattro anni i 1.000$, per poi impennarsi fino al 2021 raggiungendo il picco dei 60.000$. Dal gennaio 2022 tutto in mondo delle criptovalute e quindi anche bitcoin sta avendo un periodo di difficoltà dovuto alla grande inflazione e ad un notevole fattore di paura dato dagli scontri tra Russia e Ucraina che hanno portato i grandi investitori allo svuotamento dei propri portafogli digitali. Nel corso della sua vita bitcoin ha avuto molte repentine salite e successive discese di prezzo dovute al fatto che il mercato non ha ancora scoperto il reale valore di bitcoin poiché è un mercato ancora troppo giovane ed è presto per dare un valore di stabilità al bitcoin. Questo valore sarà dato soprattutto dall' utilizzo futuro che

bitcoin avrà nei pagamenti quotidiani e come e se verrà sfruttato dalle banche. La domanda che viene spontanea è : “come viene stabilito il prezzo di un bitcoin?”

Come ogni altra attività finanziaria, il prezzo di Bitcoin è determinato dagli incontri tra domanda e offerta delle varie borse su cui viene scambiato. La funzione di queste borse è quella di collegare acquirenti e venditori e fanno proposte di acquisto e vendita come qualsiasi altra borsa valori del mondo. Quando queste proposte sono d'accordo, il prezzo di Bitcoin viene stabilito. Il prezzo del bitcoin “fluttua” ogni secondo cioè cambia ogni secondo e molti speculatori utilizzano questa differenza di prezzo per comprare al prezzo più basso e vendere ad un prezzo più alto. La volatilità del bitcoin non è un fattore casuale ma viene determinata dal numero di investitori, quindi dal numero di denaro che c'è in gioco. Il futuro incerto, i rischi di valuta per grandi proprietari di bitcoin in relazione alla liquidità, violazioni di sicurezza come attacchi hacker o altri eventi dannosi o anche situazioni positive possono influenzare il prezzo di Bitcoin.

3.3 I pro e i contro di Bitcoin

Come ogni cosa anche il bitcoin presenta dei vantaggi ma anche degli svantaggi nell'utilizzare questa criptovaluta come sostituta delle valute legali. Adesso che siamo nel 2022 e che sono passati più di 10 anni dalla nascita di bitcoin, gli esperti hanno analizzato i pro e i contro nell'uso delle criptovalute.

Tra i pro troviamo:

- Protezione dalle frodi - I Bitcoin sono valute digitali. Utilizzano un algoritmo e protocolli crittografici. Questo li rende impossibili da contraffare.
- Riduzione della possibilità di furto d'identità - Le transazioni in Bitcoin sono completamente anonime. Le transazioni in Bitcoin non richiedono dati personali o informazioni sensibili da parte del mittente o del destinatario. Questo aiuta a prevenire il furto di identità.
- Regolamento immediato - I Bitcoin non coinvolgono terze parti per facilitare le transazioni. I fondi vengono regolati immediatamente e una volta avviati non possono essere messi in attesa o rimborsati.
- Trasferimento diretto - Le transazioni avvengono direttamente tra gli utenti, ovvero il mittente e il destinatario. Non sono coinvolte terze parti. In questo modo si eliminano le spese per il coinvolgimento di un intermediario.

- Maggiore liquidità - Durante la conversione in altre valute del mondo reale, il bitcoin mantiene la maggior parte del suo valore, mentre altre criptovalute perdono valore.
- Transazioni internazionali - Il Bitcoin è il metodo più semplice per avviare una transazione internazionale. Non applica alcuna commissione aggiuntiva e viene saldato immediatamente al destinatario.
- Indipendenza - Nessuna autorità politica o governativa regolamenta il Bitcoin. Non ha influenza politica. Né il governo né alcuna autorità possono bloccarlo o sequestrarlo.
- Sicurezza - Il Bitcoin ha una sicurezza molto forte ed è impossibile contraffare o imbrogliare la rete di pagamento bitcoin. Esisteranno 21 milioni di bitcoin. Questo rende il valore del bitcoin una promessa a lungo termine rispetto alle altre valute del mondo reale.
- La Blockchain - Le transazioni in Bitcoin sono a prova di manomissione grazie alla Blockchain.

Mentre tra i contro:

- Volatilità - La volatilità dei prezzi rende difficile e rischioso l'investimento in bitcoin. Non si riesce a stabilire un prezzo fisso a causa delle numerose fluitazioni di prezzo.

- Cyber hacking - Gli hacker e i siti illegali utilizzano i bitcoin come sistema di pagamento per estorcere denaro alle vittime. Questo li rende irrintracciabili grazie alla natura anonima dei bitcoin.
- Nessun rimborso - Una volta avviato e completato il pagamento, i bitcoin non possono essere trattenuti e rimborsati. Il pagamento avviene direttamente tra gli utenti, senza intermediari. Quindi i bitcoin non possono essere trasferiti indietro.
- Troppa energia - Per la creazione di bitcoin servono molti computer che devono funzionare ininterrottamente e al massimo delle loro capacità. Nonostante oltre il 40% dei minatori utilizzino energie rinnovabili, il consumo resta elevato.

3.4 Il futuro di Bitcoin

Il bitcoin è diventato un tema di carattere globale, infatti è studiato dai migliori economisti al mondo oltre che dalle autorità nazionali che cercano di prevedere il futuro di questa moneta. Per scoprire le sorti del bitcoin, bisogna tenere a mente alcune caratteristiche estremamente interessanti di questa moneta: l'offerta in quantità limitata che ne evita una svalutazione per eccesso di offerta, il fatto che sia caratterizzato da una grande semplicità di trasferimento e il fatto che non sia confiscabile. Anche il confronto diretto con l'oro viene utilizzato come strumento di paragone nonostante il bitcoin abbia alcuni vantaggi come la semplicità di deposito e la semplicità di trasferibilità. Alla luce di ciò studiato sinora, sono sostanzialmente tre i possibili scenari sul futuro del bitcoin.

1. Il Bitcoin diventa un mezzo per preservare il valore del risparmio. In questo scenario il bitcoin verrà sfruttato per proteggere i risparmi grazie alla sua conservabili, alla sicurezza nel possesso e grazie all'offerta limitata. Avrà una funzione simile a quella dell'oro ma con più vantaggi.
2. Il bitcoin si dissolve e va a zero. Il bitcoin, a causa del disuso e alla difficoltà da parte delle banche a trasformarlo in denaro ufficiale, scompare dal mercato e il suo valore va a zero. Un'altra minaccia per questa situazione può essere data

dall'evoluzione di un altra criptovaluta più avanzata che potrebbe sostituire il bitcoin del tutto.

3. Il Bitcoin diventa un mezzo di scambio. Nonostante già il bitcoin sia utilizzato per gli scambi (basta pensare al suo utilizzo tramite carta di credito), non è sviluppato del tutto. Questa soluzione potrebbe essere utilizzata dai governi che hanno interesse a controllare e tassare le transazioni.

Il rapporto con i governi

Il Financial Stability Board (FSB), organismo internazionale dei principali Paesi industrializzati che formano il G20, che monitora i sistemi finanziari e si occupa di regolamentare i mercati al fine di prevenire le crisi finanziarie, ha annunciato che presenterà una sua propria proposta di regolamentazione delle criptovalute a ottobre. L'organismo internazionale ha spiegato in un lungo comunicato stampa le ragioni e motivazioni che saranno alla base di questa proposta: "Le criptovalute e i mercati devono essere soggetti a una regolamentazione e a una supervisione efficaci commisurate ai rischi che comportano, sia a livello nazionale che internazionale. Anche se le giurisdizioni considerano potenziali modifiche ai propri framework, le cosiddette stablecoin e altri cripto-asset non operano in uno spazio privo di

normative e devono aderire ai pertinenti requisiti esistenti in cui si applicano le normative per affrontare i rischi che tali asset rappresentano".

Le criptovalute e i mercati possono svolgere una funzione economica equivalente a quella svolta da strumenti e intermediari del settore finanziario tradizionale. In quanto tali, sono soggetti alle normative pertinenti applicabili alla natura economica e finanziaria sottostante delle criptovalute, in linea con il principio "stessa attività, stesso rischio, stessa regolamentazione" .

Oltre a questa notizia a febbraio è stato pubblicato un report che evidenzia come la rapita crescita delle criptovalute potesse rappresentare un serio pericolo per la stabilità finanziaria dei mercati globali. L'Organizzazione per la cooperazione e lo sviluppo economica (OCSE) ha presentato al G20 il Crypto-Asset Reporting Framework (CARF), il primo Planning normativo cripto a livello globale per aumentare la trasparenza delle transazioni internazionali. Adesso i ministri delle finanze del G20 esamineranno il CARF che rappresenterà la prima regolamentazione delle criptovalute a livello internazionale affiancato dal common reporting standard (CRS), un sistema internazionale di scambio automatico di informazioni che raccoglie adesioni da oltre 100 Paesi del mondo per facilitare i controlli anti-evasione. Questo piano di trasparenza creato dall' OCSE, offre un paio di rendicontazione

internazionale automatica delle criptovalute che include disposizioni per il trading. L' OCSE vuole coprire e prevenire l'evasione fiscale internazionale che fino ad ora non è stata controllata da nessuno. L' industria cripto è ormai riconosciuta da tutti i leader mondiali che non accettano più scenari in cui alcuni commercianti posso abusare della natura delle criptovalute per eludere sanzioni e tasse, o per attività illecite.

La CBDC

La Central Bank Digital Currency è la valuta digitale emessa da una banca centrale e creata con la stessa tecnologia di una criptovaluta ma con uno scopo diverso. Queste CBCD sono nate per creare una sorta di quadro normativo nel contesto delle cripto. Ma cosa sono in realtà questi CBDC? In sostanza, non sono altro che token digitali che sono esattamente come le criptovalute, ma emessi direttamente dalla banca centrale di un Paese e quindi ancorati alla valuta nazionale. Sono a tutti gli effetti la forma digitale del corso legale di un Paese e sono quindi beni emessi e regolati dall'autorità monetaria nazionale.

Per fare un paragone, è come se fossero delle semplici stablecoin, ma in una forma più centralizzata, in quanto non girano su una blockchain pubblica, ma sono direttamente legate all'autorità statale. CBDC potrebbe fornire a privati,

famiglie e aziende un metodo di pagamento alternativo conveniente, veloce e sicuro grazie alle sue caratteristiche intrinseche. Ad esempio, un CBDC potrebbe ampliare l'accesso al sistema finanziario consentendo alle persone di inviare denaro online senza un conto bancario. Inoltre, una CBDC eliminerebbe i rischi di terze parti, come il fallimento o le "corse agli sportelli", mentre i rischi residui rimarrebbero nel sistema bancario centrale. Il costo delle transazioni internazionali può essere ridotto e la cooperazione giudiziaria tra i governi può essere aumentata. Inoltre, potrebbe consentire ai cittadini di accedere ai servizi finanziari senza intermediari bancari tradizionali, creando così un collegamento diretto tra i consumatori e la banca centrale.

CONCLUSIONI

In questo elaborato ho voluto descrivere la più importante valuta digitale attualmente sul mercato, il Bitcoin. Ho descritto tutte le sue caratteristiche e le principali funzioni, con i rischi che si possono correre entrando in questo "mondo" ma anche i vantaggi che può portare. Con gli anni molte criptovalute stanno cercando di emergere e molte ci stanno riuscendo ma in cima rimane sempre il bitcoin che detta l'andamento generale nel mondo delle valute digitali. L'incertezza sul futuro, la mancanza di normative e di tutela nei confronti dei consumatori stanno ostacolando la definitiva diffusione del bitcoin che viene utilizzato come strumento di speculazione anziché strumento di pagamento. Tuttavia, non possiamo escludere che in futuro sia bitcoin, sia tutte le altre criptovalute, potranno avere una maggiore diffusione globale e una maggiore sicurezza grazie alla regolamentazione da parte dei leader mondiali.

BIBLIOGRAFIA

https://cryptominded.com/it/quanti-bitcoin-ci-sono-in-circolazione/
https://www.borsaitaliana.it/notizie/sotto-la-lente/bitcoin-172.htm
https://www.blockchain4innovation.it/bitcoin/
https://it.cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin
https://blog.makerdao.com/guida-ai-diversi-tipi-di-wallet/
coinatmradar.com
https://koinsquare.com/dove-spendere-bitcoin/
https://coinmap.org
https://www.wired.it/economia/finanza/2019/01/03/bitcoin-2009-trasformazione-storia/
https://it.cointelegraph.com/news/bitcoiner-claims-to-have-found-long-lost-satoshi-bitcoin-code-with-personal-notations
https://blog.bitnovo.com/it/cosa-sono-le-blind-signatures/
https://academy.youngplatform.com/crypto-heroes/bitcoin-chi-e-satoshi-nakamoto/
https://www.startmag.it/economia/criptovalute-che-cosa-succede-ai-bitcoin/
https://www.wired.it/article/bitcoin-crollo-prezzo-cause/
https://bitcoin.org/it/come-funziona
https://youngplatform.com/exchange/btc/
https://academy.bit2me.com/it/transacciones-bitcoin/
https://www.itu.int/en/ITU-T/extcoop/dcgi/Pages/default.aspx
https://localbitcoins.com/about
https://intermarketandmore.finanza.com/ecosistema-bitcoin-facciamo-chiarezza-91713.html
https://rankia.it/criptovalute/cosa-determina-il-prezzo-di-1-bitcoin/
https://magazine.euclidea.com/il-futuro-del-bitcoin-ecco-3-previsioni-su-cosa-accadra
https://cryptonomist.ch/2022/07/12/regolamentazione-crypto-fsb-g20/
https://thecryptogateway.it/g20-crypto-ocse/
https://cryptonomist.ch/2022/07/12/regolamentazione-crypto-fsb-g20/
https://www.pagamentidigitali.it/blockchain-dlt/central-bank-digital-currency-cose-e-come-funziona-la-cbdc/
https://thecryptogateway.it/cbdc-cosa-sono/

https://cryptonomist.ch/2022/09/18/futuro-mining-bitcoin/
https://it.cryptonews.com/guides/what-is-bitcoin-mining.htm
https://www.exeo.it/Articoli/8040/punti-di-forza-e-di-debolezza-del-bitcoin.aspx
https://eternalcuriosity.it/funzioni-hash-a-cosa-servono-e-perche-dovresti-conoscerle
https://www.insidemarketing.it/glossario/definizione/bitcoin/