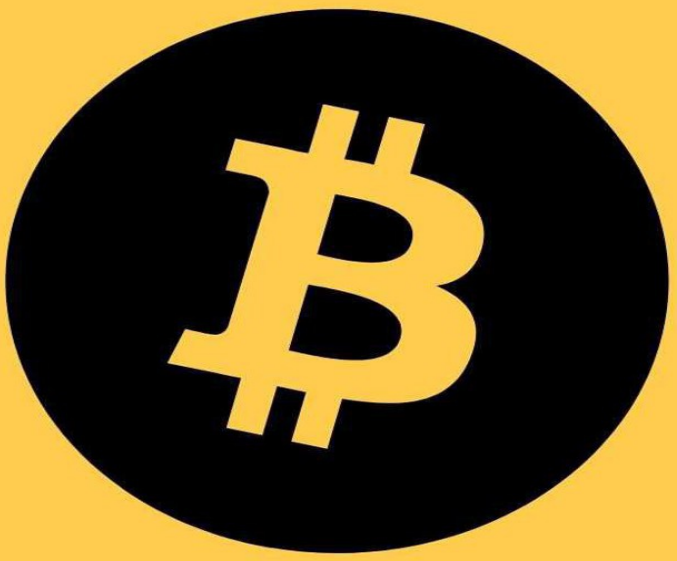
FEDERICO RUGGIERI CON
ECONOMY CAFFÈ

GUIDA INTRODUTTIVA AL MONDO DELLE CRIPTOVALUTE



UNA GUIDA PER COMINCIARE AD ESPLORARE IL MONDO DELLE CRIPTOVALUTE

GUIDA INTRODUTTIVA AL MONDO DELLE CRIPTOVALUTE

"Un piccolo esperimento che speriamo porti a qualcosa di più grande"

INDICE DEL LIBRO

SCOPO DELL'E-BOOK

Ciao,

scrivo questo eBook per introdurti ad un mondo molto discusso negli ultimi anni, quello delle criptovalute. Attenzione, non ti darò consigli su come investire poiché non sono un professionista del settore, ma mi limiterò ad esporti nel modo più completo ed organico possibile la funzione ed il funzionamento di questo tipo di “moneta”. Detto ciò, ti auguro una buona lettura.

1.0 COS'È LA CRIPTOMONETA .

Partiamo dicendo che le criptovalute sono riconosciute dall'unione europea tramite la Direttiva Ue 2018/843 come "Una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente".

La criptomoneta quindi è:

- Digitale, poiché la disponibilità liquida è memorizzata su un computer che utilizza uno specifico software.

- Decentralizzata, poiché non ha alle spalle alcun organo centrale che si occupi di coniarla.

Il termine “criptomoneta” deriva dal fatto che ad essa siano state applicate avanzate tecniche di criptografia, al fine di proteggerne le transazioni ed evitare il problema della clonazione.

2.0 COME FUNZIONA?

Premessa:

Gli argomenti trattati in questo capitolo sono abbastanza complessi, tenterò di spiegarli nel modo più semplice possibile, cercando di non scendere troppo nel dettaglio.

2.1 -PEER-TO-PEER

Per prima cosa, parlerò della tecnologia peer-to-peer e del perché permette la decentralizzazione delle criptovalute. Questo tipo di tecnologia, infatti, regola lo scambio di informazioni all'interno di una rete.

Questo, tuttavia, è un sistema centralizzato: quando, infatti, cerchiamo delle informazioni utilizzando un browser, il nostro computer è il client che richiede dei dati a un server che a sua volta li invia. Quindi, in un sistema centralizzato chi detiene il server può decidere se inviare o meno un'informazione, se modificarla o addirittura cancellarla. Ciò non succede con la tecnologia peer-to-peer poiché ogni client è anche server, dunque lo scambio di dati avviene tra tutti i dispositivi connessi alla rete. Questo vantaggio dato dalla decentralizzazione della moneta è, tuttavia, accompagnato da un aspetto negativo, ovvero la scarsa sicurezza del sistema. In un sistema

centralizzato basterebbe mettere in sicurezza il server per proteggere anche i singoli client, mentre, con questo tipo di tecnologia non si può garantire per ogni singolo client, che deve quindi provvedere alla propria sicurezza, con il pericolo di compromettere l'intera rete.

2.2 -BLOCKCHAIN

Per ovviare al problema riguardante la sicurezza, le criptomonete si servono di un altro tipo di tecnologia: la blockchain.

La blockchain è una struttura dati condivisa, composta da blocchi di informazioni. Una volta che un'informazione è inserita nella blockchain e viene validata dagli utenti della stessa, viene inviata ad ogni nodo

della rete (i possessori di criptovalute), in modo tale che un'informazione non possa essere cancellata né tantomeno modificata, a meno che non si cancelli o modifichi dagli archivi di ogni singolo utente. Nessuno ha la copia "originale" della blockchain, ma ogni utente ha la propria copia privata che viene aggiornata costantemente. A seguito di questa spiegazione della blockchain nascerà spontanea la domanda: "che cosa è un blocco?" Il blocco è la singola unità della blockchain: nello specifico, esso contiene un registro di transazioni avvenute in criptovaluta. La composizione di un blocco, tuttavia, non si limita a questo. Un'altra parte integrante del blocco, al fine della

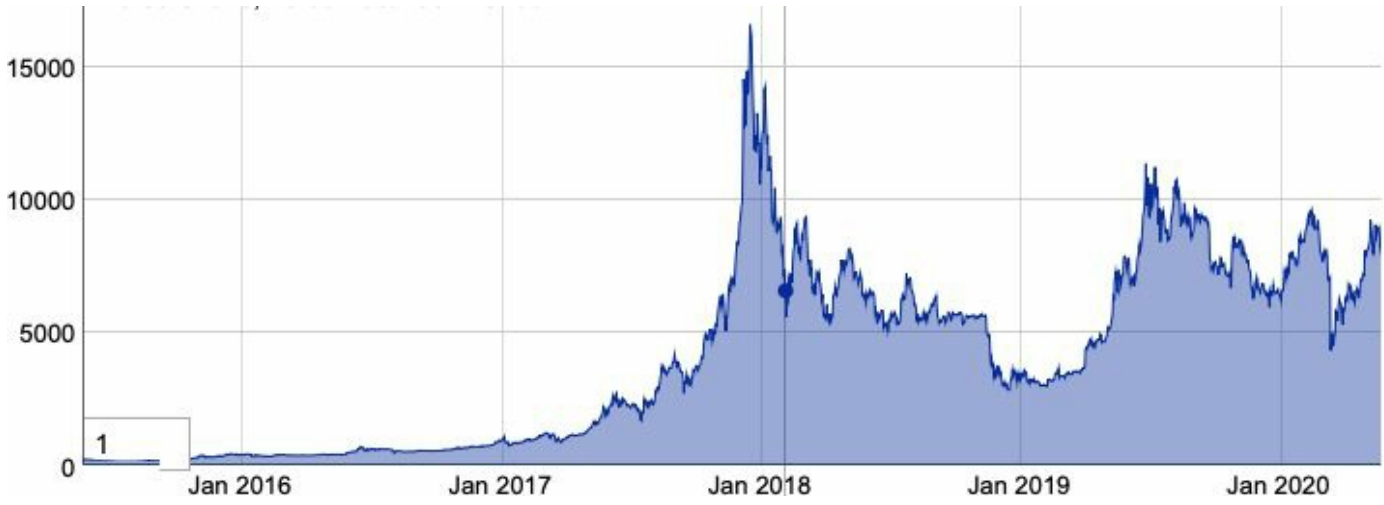
sicurezza del sistema, è l'impronta HASH, cioè un codice che viene creato con un algoritmo. La differenza principale da un altro codice identificativo è che dall'oggetto è possibile risalire al codice HASH, ma non è possibile il contrario. In parole povere, poniamo il caso in cui un soggetto X invii un'informazione con il relativo codice HASH a un soggetto Y. Come può il soggetto Y sapere se il contenuto dell'informazione è quello originario inviato da X e che non sia stato modificato? Y può ricreare il codice HASH dell'informazione e se esso coincide con quello ricevuto da X, l'informazione non è stata modificata: un minimo cambiamento del contenuto,

infatti, avrebbe variato anche il codice HASH. Le criptovalute si servono di questo meccanismo come strumento di verifica dei blocchi. L'HASH contenuto in un blocco è quello creato tramite il blocco precedente, permettendo di instaurare un collegamento tra blocchi, i quali contengono, inoltre, una marcatura temporale, che esprime la data e l'ora in cui esso viene creato. I singoli blocchi si formano grazie a degli utenti definiti "miner", che mettono a disposizione la potenza di calcolo dei loro computer al fine di costruire i blocchi, ovviamente dietro compenso in criptovaluta.

3.0 STORIA DELLE CRIPTOMONETE

Avendo parlato del funzionamento delle criptovalute nei capitoli precedenti, vorrei soffermarmi sulla loro storia, concentrandomi prevalentemente sul bitcoin. Il Protocollo Bitcoin (Il primo per una criptomoneta decentralizzata) è stato pubblicato verso la fine del 2008 su "The Cryptography Mailing list", sul sito metzdowd.com.ito, da un certo Satoshi Nakamoto (uno pseudonimo creato per coprire la vera identità del creatore). Negli anni successivi Satoshi Nakamoto ha contribuito, in via

anonima, allo sviluppo del progetto, per poi tirarsene fuori nel 2010. Sono molte le speculazioni sulla vera identità dell'inventore del Bitcoin, ma la verità è che non la si può attribuire a nessuno con certezza. Il Bitcoin è passato dal valere 0,00076$, nel novembre del 2009, a valerne circa 20.000 nel dicembre del 2017. Ad oggi (momento in cui sto scrivendo l'e-book) il valore di un bitcoin è di 9.755$ e ne esistono 18.351.912,5.



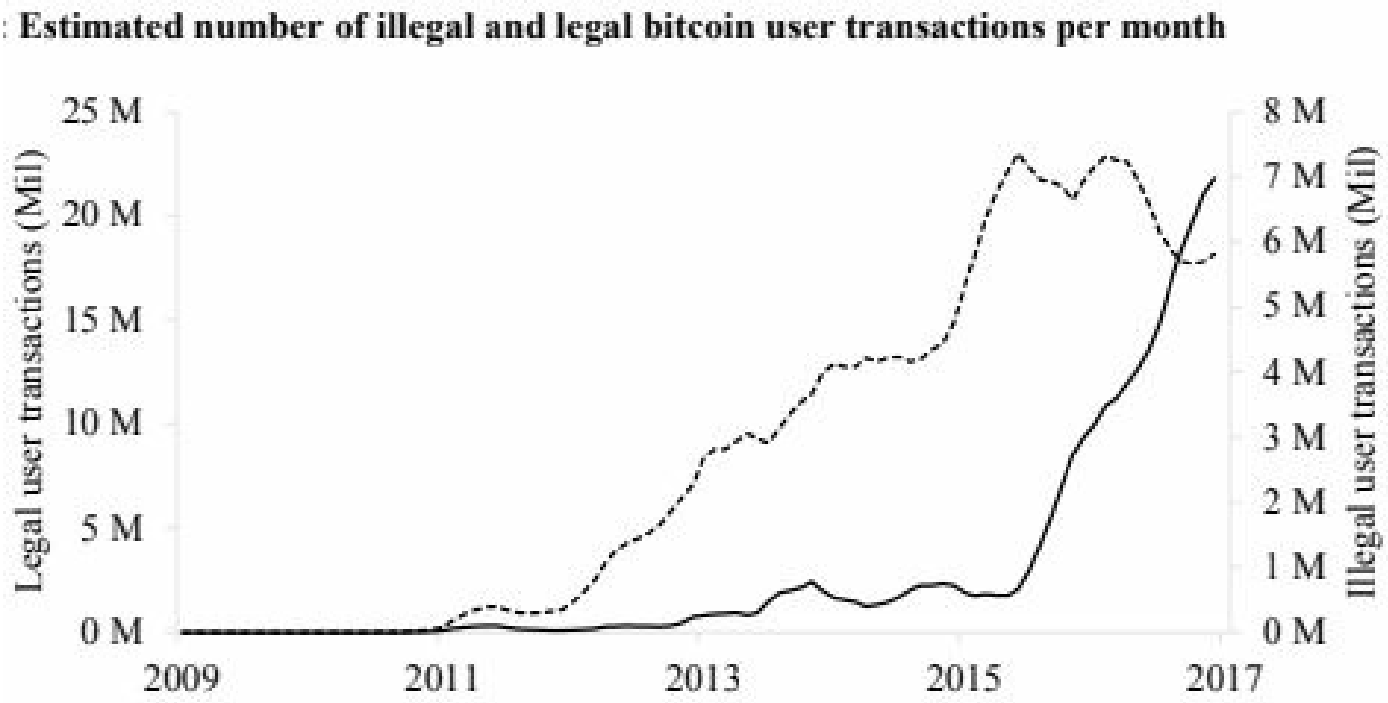
Valore del bitcoin negli ultimi 5 anni in Euro Fonte: https://www.cambioeuro.it/grafico-bitcoin/

Come ho già accennato in precedenza, non solo il valore, ma anche il numero effettivo di criptomonete varia ed esse sono in continuo aumento grazie ai miner che le "coniano". Sebbene sia innegabile l'innovazione apportata dalle criptovalute al commercio online, dobbiamo evidenziarne anche gli aspetti più opachi. L'anonimato delle transazioni in criptomoneta favorisce il commercio illegale, questo è innegabile. Una ricerca guidata da Sean Foley, un ricercatore dell'università di Sydney, intitolata "Sex, Drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies?" ha mostrato che il 46% delle transazioni e il 23% degli

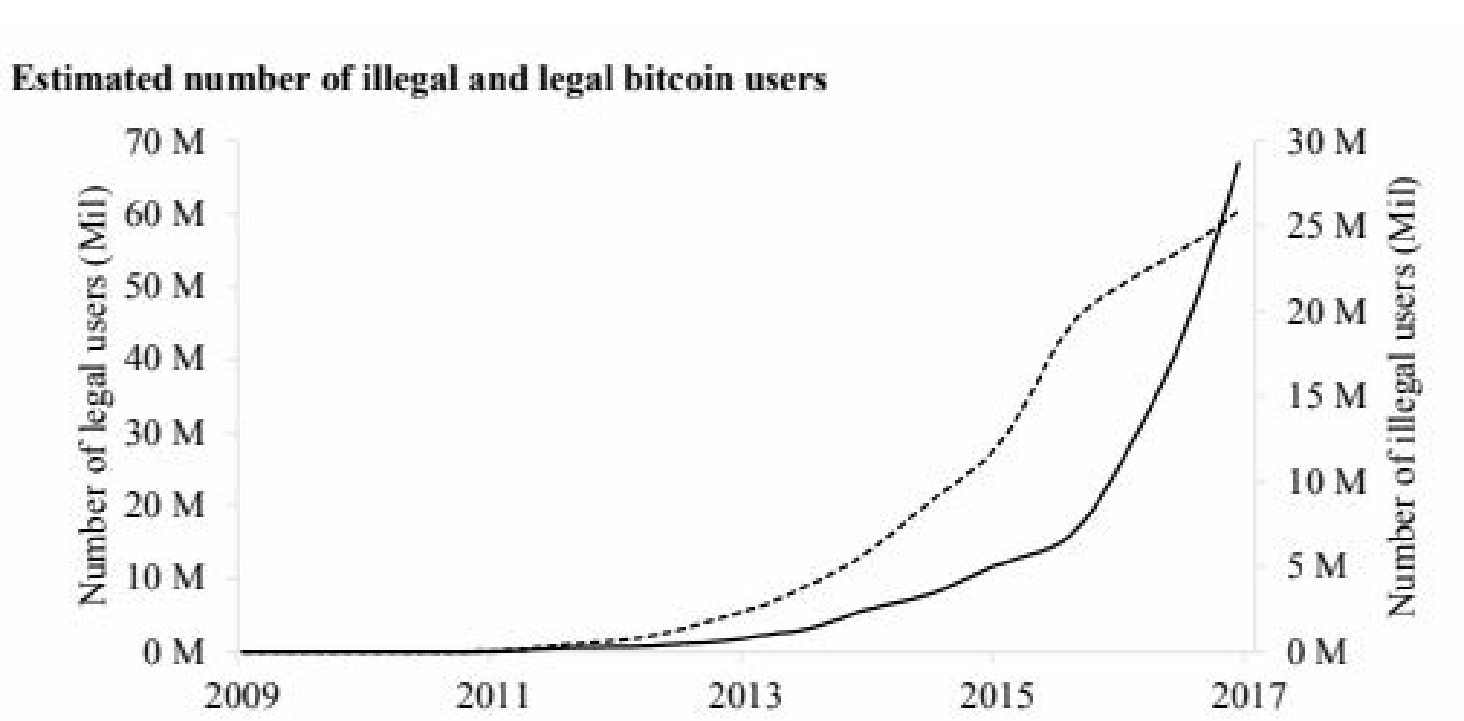
utenti bitcoin sono collegabili ad attività illegali. Secondo Foley, il valore delle transazioni illegali in bitcoin è di circa 76 miliardi di dollari, non poco, se considerato rispetto al valore complessivo dei mercati illegali europei e statunitensi, la cui stima è di 126 miliardi di dollari. Ad oggi nel mercato esistono più di 2.000 criptovalute ed ognuna differisce dall'altra per alcune sue caratteristiche, quali: la differente velocità di "conio", l'anonimato delle transazioni più o meno garantito ecc.

Nelle pagine successive inserirò alcuni grafici presi dalla ricerca svolta da Sean Foley, Jonathan R. Karlsen e Tālis J. Putniņš; *"Sex, Drugs and*

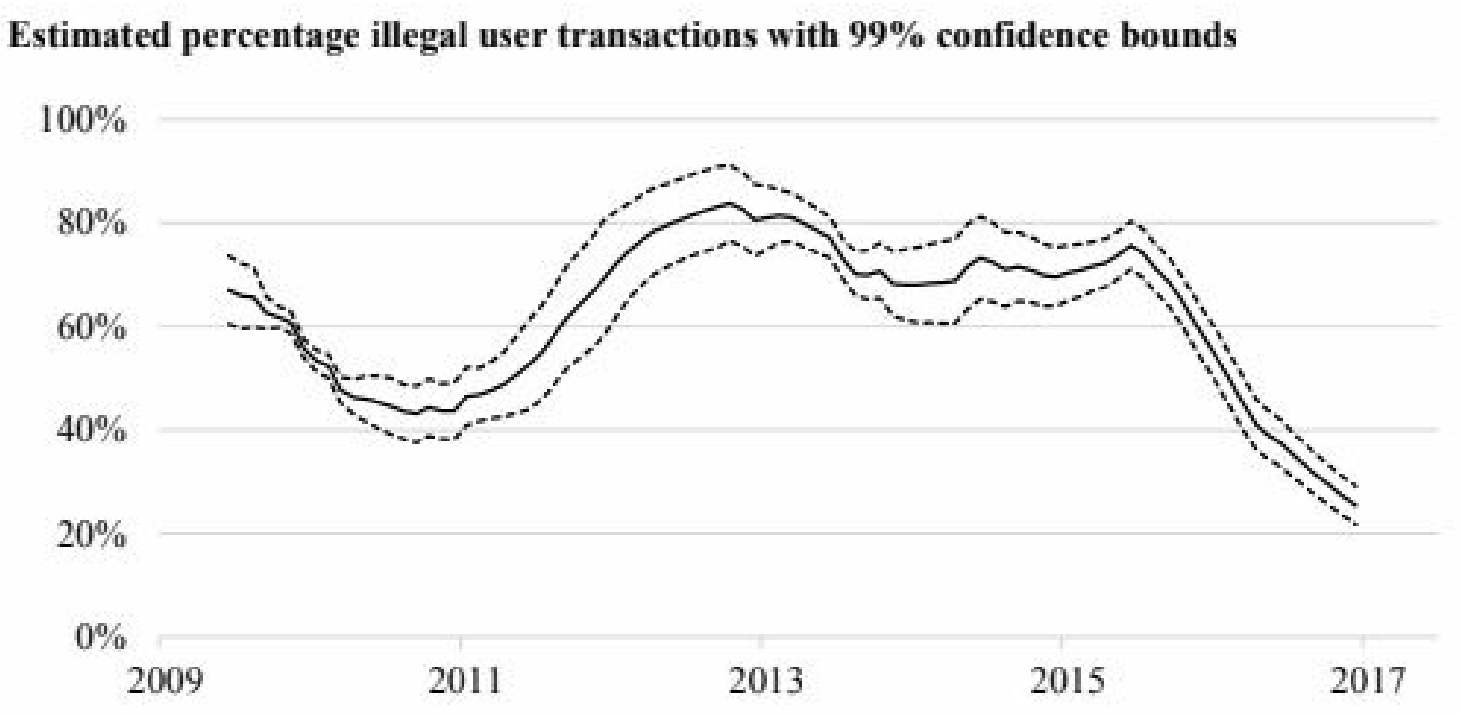
Bitcoin: How much illegal activity is financed through cryptocurrencies?"



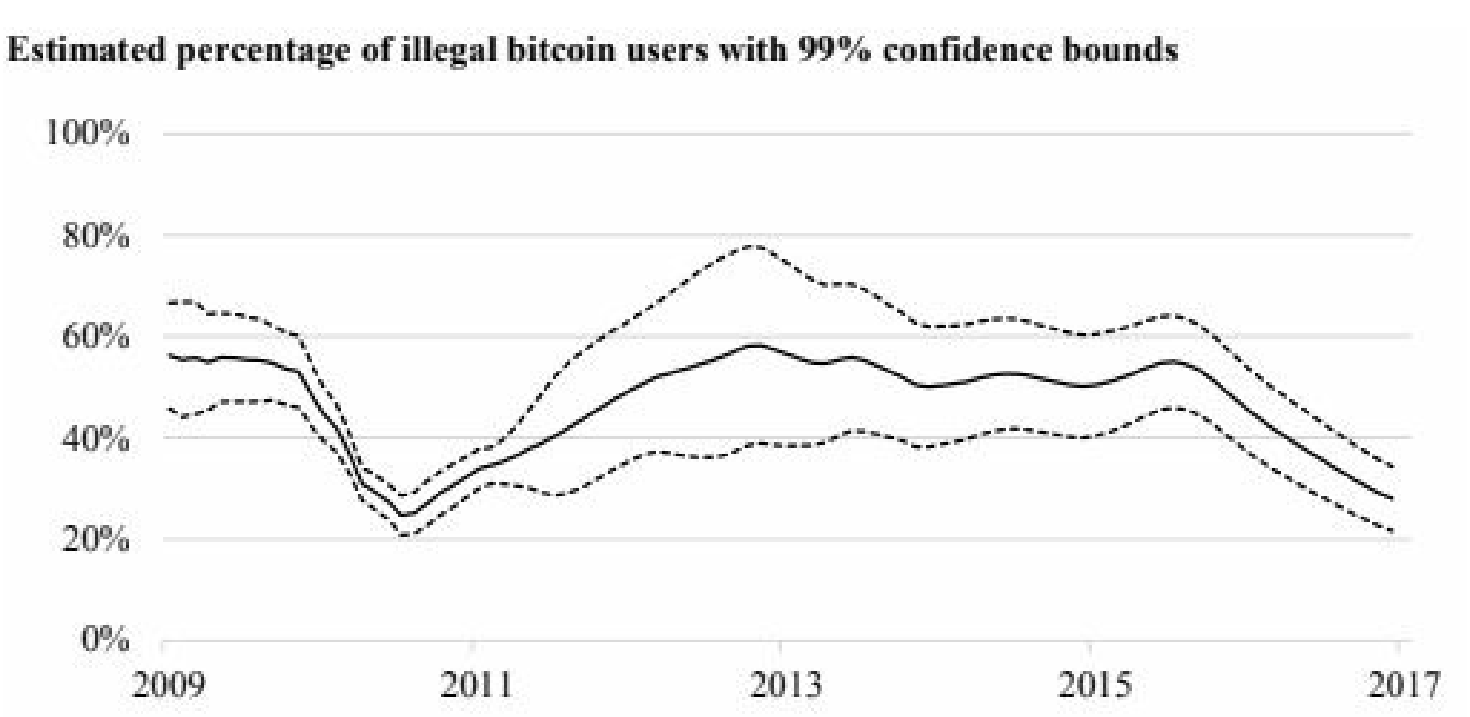
Numero stimato di transazioni legali e non con i bitcoin per mese dal 2009 al 2017



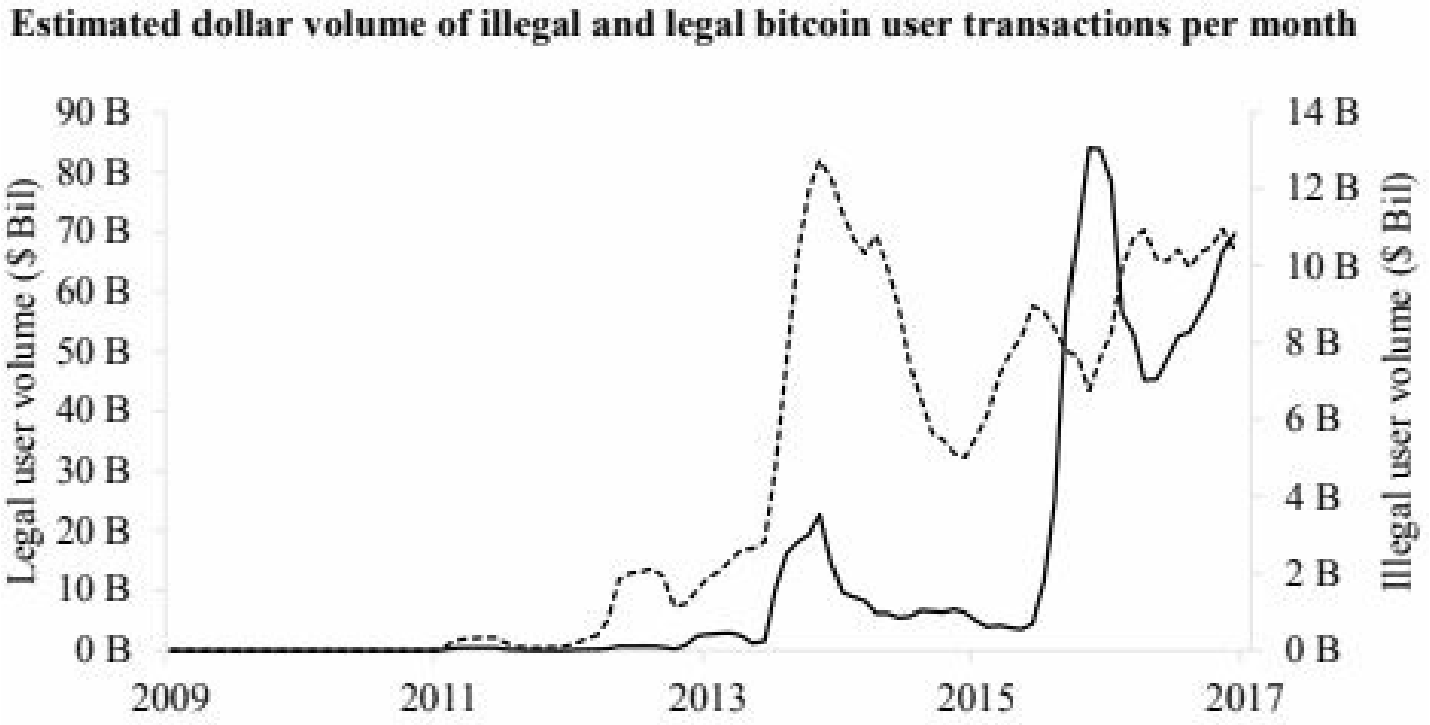
Numero stimato di utenti che utilizzano i bitcoin a fini legali e non.



Percentuale stimata di transazioni illegali in bitcoin



Percentuale stimata di utenti che utilizzano i bitcoin a fini illegali



Volume stimato in dollari di bitcoin utilizzati a fini legali e non per mese (in miliardi)

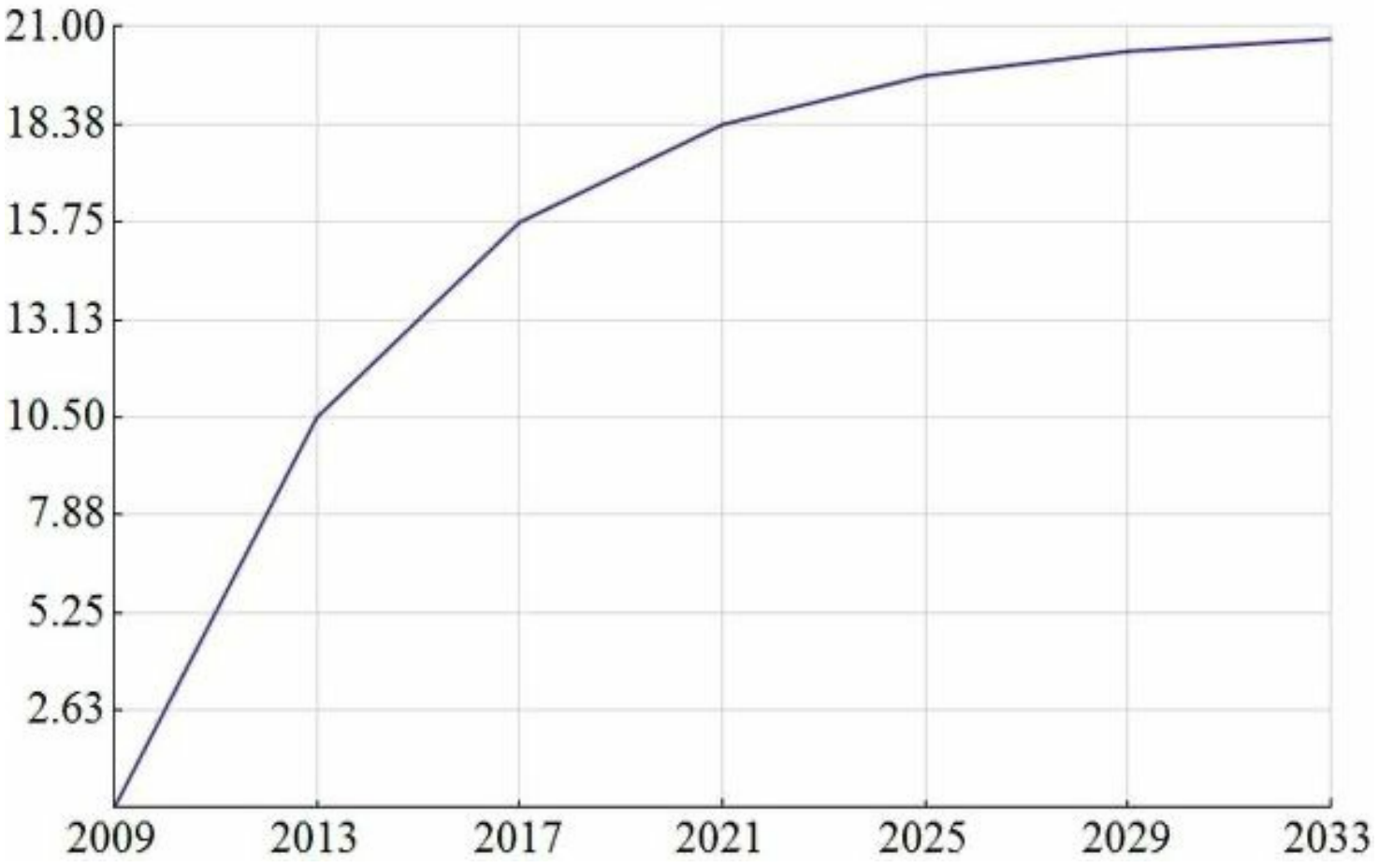
3.1 -L'ANDAMENTO DELLA QUANTITÀ DI BITCOIN

I bitcoin, come le altre criptomonete, vengono "coniati" ogni giorno, anche se la velocità con cui vengono prodotti cala nel tempo. Questo fa parte del progetto di Satoshi Nakamoto, che ha optato per una progressione geometrica per la quantità della sua moneta, fino al raggiungimento del tetto massimo di 21 milioni di bitcoin, quantità che si ipotizza verrà raggiunta nell'arco di 130 anni. Se i miner sono sempre di più e con tecnologie più avanzate, come fa l'inventore a stabilire un aumento

marginale decrescente della quantità di moneta? Ciò avviene attraverso gli halving: si tratta di eventi che si presentano ogni 40 mesi circa (ovvero ogni qualvolta vengano prodotti 210.000 blocchi). Tramite questo evento vengono dimezzati i ricavi in bitcoin dei miner, portando ad un rallentamento nel conio della moneta. Inizialmente il ricavo di un miner era di 50 bitcoin per ogni blocco emesso sul mercato, oggi, dopo 3 halving (di cui l'ultimo a maggio 2020), è di 6,25 bitcoin per blocco. Il prossimo halving è atteso per marzo 2024.

Satoshi Nakamoto ha stabilito questo andamento del bitcoin per renderlo una moneta deflazionistica, cioè che si apprezzasse nel tempo: gli halving,

infatti, causano una diminuzione dell'offerta lasciando la domanda invariata. Il bitcoin sfrutta la legge economica della domanda e dell'offerta, la quale afferma che in caso di eccesso di domanda di un bene, il prezzo dello stesso aumenta.



Quantità stimata di bitcoin esistenti dal 2009 al 2033.

Come possiamo vedere la curva non può superare il tetto massimo di 21 milioni di bitcoin. Fonte: https://images.app.goo.gl/frUWuhbBGjnTTMLu9

3.2 LE CRIPTOVALUTE PIÙ "DISCUSSE"

Le criptovalute più "importanti", cioè con un volume giornaliero di contratti scambiati più alto e con la maggiore capitalizzazione sono, in ordine, il Bitcoin, l'Ethereum, il Theter, il Litecoin e il Bitcoin Cash (Statistiche relative al giorno in cui scrivo)

-Bitcoin

Il Bitcoin ha un volume di scambi di 44 miliardi di dollari ed una

capitalizzazione di mercato di 176 miliardi. Ad oggi il valore di un Bitcoin è di 9.755$.

-Ethereum

L'Ethereum ha un volume di scambi giornaliero di 18 miliardi di dollari e una capitalizzazione di mercato che si aggira intorno ai 23. Ad oggi il valore di un Ethereum è di 210$. L'Ethereum è una criptovaluta creata nel 2013 da Vitalik Buterin e la differenza principale rispetto al Bitcoin è che il sistema creato da Vitalik, non è volto solamente allo scambio di valore monetario, ma il suo fine ultimo è l'agevolare la circolazione di smart contract, con pagamento tramite l'unità di conto del sistema, cioè "l'Ether". Gli smart

contract sono protocolli informatici che permettono la negoziazione e l'esecuzione di alcuni tipi di contratti, senza la partecipazione di intermediari, quali avvocati o notai.

-Il Theter

Il Theter ha un volume di scambi giornaliero intorno ai 53 miliardi di dollari, mentre una capitalizzazione di mercato di circa 8,7 miliardi. Questa criptovaluta è particolare, poiché è stata creata con l'idea di farle replicare l'andamento del dollaro americano, cosicché il valore di un signolo Theter sia di un dollaro.

-Il Litecoin

Il Litecoin ha un volume di scambi giornalieri pari a 4,5 miliardi di dollari

ed una capitalizzazione di mercato di 2,9 miliardi. Il valore di un Litecoin si aggira intorno ai 44$ ed il suo funzionamento è pressoché lo stesso del Bitcoin. La differenza più grande sta nella velocità di elaborazione di un singolo blocco, che per il Bitcoin è di 7,5 minuti, mentre per il Litecoin è di 2,5. In più la quantità massima di Litecoin "coniabili" è di 84 milioni, il quadruplo rispetto al Bitcoin.

-Bitcoin cash

Il Bitcoin cash ha un volume di scambi giornalieri pari a 3,4 miliardi di dollari e una capitalizzazione di mercato di 4,5 miliardi. Il valore di un Bitcoin cash è di 245$.

La blockchain costituita da blocchi di 1

MB (megabyte) consentiva circa 3 transazioni al secondo, ma la sempre crescente mole di utenti Bitcoin e di scambi richiese, nel tempo, un aumento della velocità del sistema.

Nel 2017 nacque un dibattito sul come risolvere il problema della lentezza, alcuni sostenevano un aumento di grandezza dei blocchi, altri preferivano introdurre un sistema chiamato Segwit, che alleggeriva la blockchain.

Il Bitcoin cash nasce nell' agosto 2017 proprio da questo dibattito, quando una parte di sviluppatori Bitcoin decide di creare una nuova criptovaluta con blocchi di dimensione 8MB, mentre al bitcoin viene applicato il sistema

Segwit2x, che comprende sia l'introduzione del Segwit che l'ingrandimento dei blocchi a 2 MB.

4.0 CHI E COME INVESTE IN CRIPTOMONETA

A questo punto avrete capito che la criptovaluta non è una semplice valuta virtuale, ma, grazie alla sua alta volatilità, ben più alta rispetto a quella di una normale moneta, è vista anche come un vero e proprio investimento. Di conseguenza non tutti coloro che detengono criptovaluta lo fanno con il fine di spenderla.

In questo paragrafo osserveremo vari metodi con cui è possibile investire in criptomonete.

-MINING

Il miner, come già è stato detto prima, è un utente che, mettendo a disposizione la potenza di calcolo del proprio computer, crea i blocchi della blockchain e viene ricompensato in criptovaluta. Il mining è un'attività sempre meno proficua a causa degli halving, portando i miner a dotarsi, nel tempo, di tecnologie sempre più avanzate. Ai miner la potenza di calcolo serve ad individuare un numero, chiamato nonce. Questo, se processato insieme ad altre informazioni contenute nel blocco, individua l'hash dello stesso (il blocco) e tale processo è necessario al fine della validazione di un blocco. La spesa principale per un miner è

quella in energia: infatti, al fine di massimizzare il guadagno, l'attività di mining viene svolta principalmente nei paesi dove i costi energetici sono più bassi. I più gettonati sono, in ordine, la Cina, la Georgia, la Svezia e gli Stati Uniti, più precisamente la California. Per farvi un esempio, se in Italia il costo dell'elettricità si aggira intorno ai 0,21€ per KWh (kilowattora), in Georgia scende a circa 0,05€.

-TRADING

Un altro metodo d'investimento in criptovaluta è il trading, che consiste nello speculare sulle variazioni di valore di questi asset, che molto spesso disegnano ampi grafici dovuti alla loro

elevata volatilità. Per investire in questo modo non è necessario acquistare e vendere criptovalute, ma lo si può fare attraverso i CFD (Contract For Difference), ovvero dei titoli derivati acquistabili in mercati non regolamentati, la cui funzione è quella di seguire l'andamento di borsa di un asset: in questo modo non bisogna necessariamente detenere criptovaluta per poterci investire, ma basta acquistare i CFD di una criptovaluta.

-LENDING

Il lending è un metodo di speculazione sui prestiti in criptovaluta. Il detentore di una determinata criptomoneta può prestarla chiedendo in cambio degli interessi.

-OFFERING

L'offering è simile al crowdfunding: l'investitore sostiene economicamente lo sviluppo e la progettazione di una nuova criptovaluta, in cambio di un corrispettivo (sempre in criptovaluta) quando questa sarà ultimata.

-STAKING

Come abbiamo già detto nel capitolo 2, un blocco non deve essere solo creato, ma anche validato. Quando un blocco viene ultimato, viene selezionato dal sistema un validator, cioè un utente che mette la propria "firma" sul blocco convalidando. Per poter essere un validator bisogna stoccare il proprio capitale di criptovalute, cioè tenerlo

fermo nel wallet (il portafoglio online che contiene le criptovalute) senza compiere transazioni. Per ogni blocco costituito quindi viene scelto un validator (quasi) casualmente tra i possibili candidati, e gli viene attribuito un premio in criptovaluta.

5.0 CONSIDERAZIONI FINALI

Per quanto riguarda il futuro delle criptovalute, ci sono 2 correnti di pensiero in merito: la prima ritiene che l'aumento di valore delle monete digitali sia ingiustificato e dovuto all'euforia degli investitori, vedendo, quindi, nel mondo delle criptovalute una nascente bolla speculativa, destinata ad esplodere nei prossimi anni. La seconda corrente di pensiero, sostiene che le criptovalute siano il futuro dell'economia e che si svilupperanno al punto di rimpiazzare il

denaro, diventando una moneta globale. A seguire riporterò alcune opinioni sul futuro della criptovaluta.

Peter Thiel

Imprenditore statunitense e co-fondatore di PayPal, appare sulla rivista Forbes come una delle 400 persone più ricche al mondo.

"*Bitcoin è l'inizio di qualcosa di grande: una moneta senza un governo, qualcosa di necessario e imperativo*"

John McAfee

Controverso programmatore britannico

e fondatore dell'omonima società McAfee.

"*Non puoi fermare cose come il Bitcoin. Sarà dappertutto e il mondo dovrà riadattarsi. I governi mondiali dovranno riadattarsi*" .

Warren Buffets

Imprenditore statunitense considerato il più grande value investor di tutti i tempi, nominato uomo più ricco al mondo da Forbes 2008.

"A proposito di criptovalute, in generale, posso dire con quasi certezza che finiranno male: quando o in che modo succederà, non lo so. Se potessi sottoscrivere un contratto put a cinque anni su ognuna di loro sarei felice di farlo, ma non investo neanche un centesimo su di loro. Non ne possediamo nessuna, non siamo (La Berkshire Hathaway) short su niente,

non le prenderemo mai in considerazione“.

-Joseph Stiglitz

Economista statunitense e premio nobel nella sua disciplina nel 2001.

“*Dovrebbe essere messo fuori legge. Non ha alcuna funzione socialmente utile. È una bolla che darà a molte persone un sacco di momenti entusiasmanti mentre sale e poi scend*e”.

Con questo commento finale, voglio ricordare ai lettori che questo piccolo libro non rappresenta in nessun modo una guida su come investire, e neanche una incitazione ad investire in quel mondo. Si tratta puramente di una illustrazione, una guida per capire come il mondo delle criptovalute vive ed esiste.

Fonti:

- https://www.money.it/Bitcoin-10-frasi-di-persone-famose

- https://forza-

trading.com/guadagnare-bitcoin-e-criptovalute/

- https://it.wikipedia.org/wiki/Bitcoin

- https://it.wikipedia.org/wiki/Bitcoin

- https://it.wikipedia.org/wiki/Criptovaluta

-en.bitcoin.it/wiki/Staking

- https://www.economycaffe.it

- https://www.news.mrwebmaster.it/bitcoi halving-dimezza-valore-mining_15429.html

-Sean Foley, Jonathan R. Karlsen, Tālis J. Putniņš; *"Sex, Drugs and Bitcoin: How much illegal activity is financed through cryptocurrencies?"* December 14, 2018.