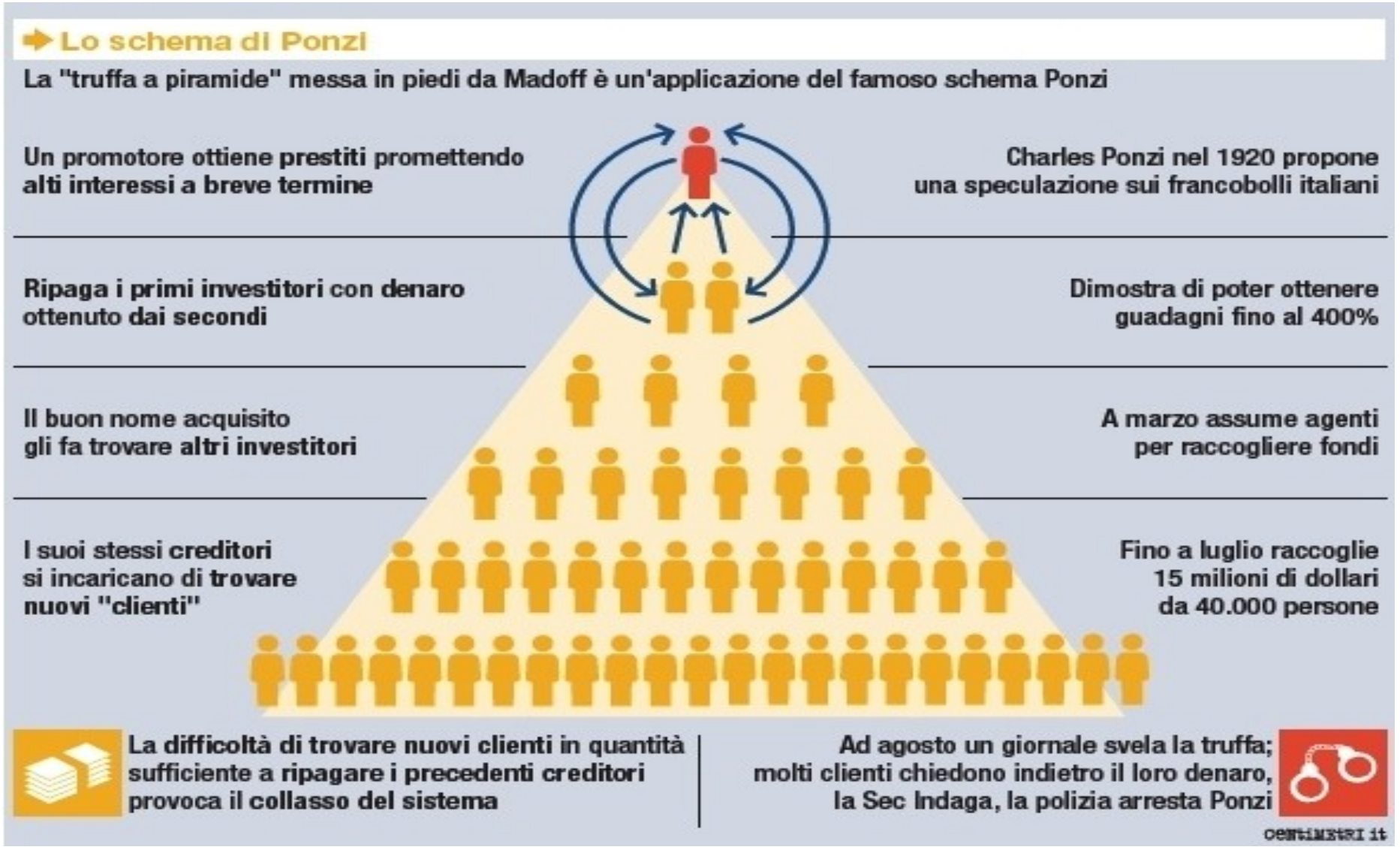
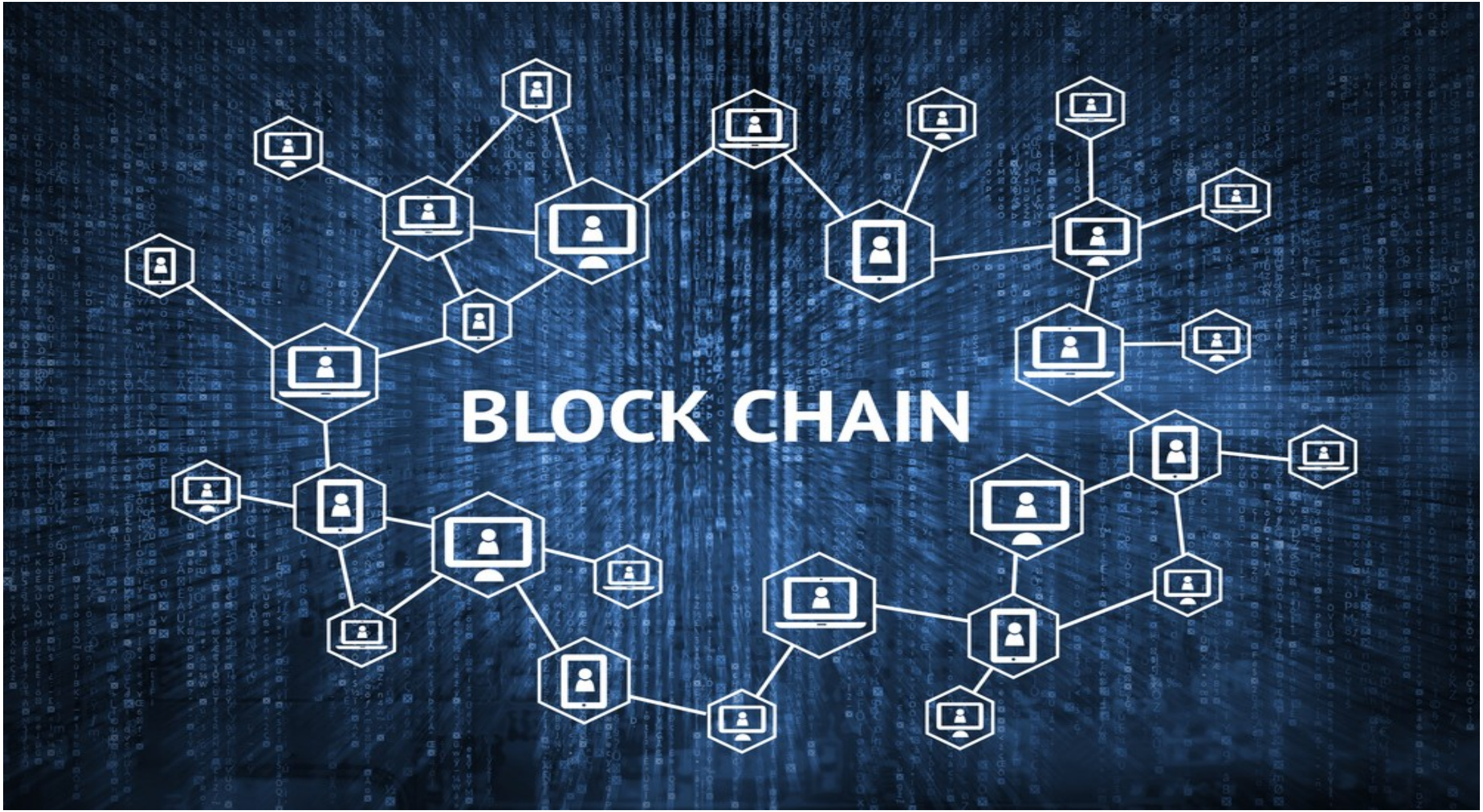
Etica e finanza – Blockchain e criptovalute

Francesco Vitelli – Perugia 8 marzo 2021

ETICA E FINANZA




BLOCK CHAIN

Eventi fondamentali

- 15.09.2008: Crack LB, inizio della Grande Crisi
- 31.10.2008: Satoshi Nakamoto scrive “Bitcoin p2p e-cash paper”
- 03.01.2009: SN lancia Bitcoin. Nel primo blocco scrive: “*Il Cancelliere sta per salvare le banche per la seconda volta*” Titolo del Times del giorno
- 12.01.2009: SN invia 10 BTC a Finney. Prima transazione al mondo.
- 18.05.2010: Primo acquisto in bitcoin: una pizza da 10.000 btc (oggi circa 404 Ml €)
- Aprile 2011: SN sparisce….*Cypherpunk*

Cosa è la Blockchain

- La Blockchain è una database decentralizzato, criptato, condiviso e distribuito tra più nodi di una rete. Chiunque può leggerlo, ma può essere modificato solo con il consenso della maggioranza dei partecipanti.
- Crittografia e decentralizzazione consentono incorruttibilità e trasparenza
- “Catena di blocchi”: ogni blocco contiene tutte le transazioni e lo storico di ogni transazione. Tutti i blocchi sono incatenati tra loro tramite la crittografia. Ciò rende immodificabili le transazioni

  → si utilizza la funzione *hash* (La parola prende il nome dal termine hash (sminuzzare, pasticciare) che designa originariamente una polpettina fatta di avanzi di carne e verdure

  →Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione.

  → doppia chiave pubblica privata (la stessa della firma digitale)

Cosa è un blocco

È un file che contiene una serie di informazioni:

1. Numero del blocco;
2. Hash univoco;
3. Timestamp;
4. Transazioni
5. Etc…

Ogni blocco contiene al proprio interno il codice hash del blocco precedente. Ciò rende particolarmente difficile “*quasi impossibile*” modificare transazioni o informazioni passate.

Smart Contract

- Uno smart contract è la trasposizione in codice di un contratto, in modo da verificare in automatico l'avverarsi di determinate condizioni e, conseguentemente, di eseguire in automatico le azioni previste e pre-accordate

- Esempi: copertura assicurativa per il ritardo di un treno o un aereo; *revenue (reddito)* di diritti intellettuali o d'autore (SIAE)

I.C.O.
Initial Coin Offering

- Un’azienda propone un progetto basato sull’emissione di una nuova criptovaluta ed offre dei token in cambio di capitali per finanziare il progetto
- Similitudine con un’IPO (OPA), ma senza un istituto di vigilanza (Consob o Banca d’Italia) a convalidare la solidità dell’azienda che richiede capitali
- Nessun tipo di regolamentazione, né garanzia

Dati sulle I.C.O.

- Prima I.C.O. nel 2013: Mastercoin (5.000 btc pari ad 420.000 €)
- 2014 la I.C.O. di Ethereum
- Ad oggi circa 20 nuove I.C.O. al mese
- Totale raccolto circa oltre 3 MLD / con i valori di oggi sono 3,000 MLD

Rischi sulle I.C.O.
I casi…negativi…e…positivi

- Tezos: una delle più attese dai tecnici, raccoglie 232 MLN, poi i soci litigano (coniugi) con chi gestiva i fondi (amico di famiglia) e vine bloccata l'emissione. Crolla del 75%. Ora in causa
- Filecoin: tra le migliori, raccoglie 257 MLN in 60minuti (c'è anche in Italia qui)
- Useless Ethereum Token (UET): inutile. Presa in giro raccoglie 40.000
- Potcoin: compravendita di marijuana, ha finanziato una spedizione in nord Korea

Nel Mondo…

- Cina: prima dichiara fuori legge le ICO e chiede il rimborso degli investimenti (400Mln), dopo una settimana cambia posizione e rimane in attesa di una regolamentazione
- Australia, Canada, Emirati, Hong Kong hanno regolamentato le ICO
- Il Belgio le ha dichiarate illegali
- La Svizzera è il regno delle criptovalute e delle ICO
- In Bangladesh si rischiano 12 anni di carcere
- In Bolivia ed Ecuador sono illegali
- U.S.A. quasi legali…dipende dagli Stati

Come valutarle

- Leggere attentamente il withepaper (documento tecnico di presentazione del progetto)
- Roadmap
- Verificare i numeri e il mercato di riferiemtno
- Controllare storia degli advisor e del team di sviluppo
- Controllare i canali di comunicazione diretti con la proprietà (telegram)

Alcune applicazioni – bc permissionless (pubblica)

- Finanziamenti trasparenti ai partiti
- Tasse
- Charity
- Assicurazioni
- Notaio
- Elezioni
- Sanità
- Diritti musicali
- Made in Italy
- Etc...

Fonti normative

ITA: decreto semplificazione 2019: validità legale a blockchain e smart contract

Agenzia delle Entrate: Risoluzione n.72 di settembre 2016 assimila btc e altre criptovalute a valute estere ma non ha valore di legge, poiché è un interpello

No tassazione plusvalenze, ma se si supera il possesso di 51.000 € per 7 giorni consecutivi è considerato speculazione finanziaria e si applica l'aliquota del 26% da pagare solo al momento in cui si vendono i btc

CASE History

- Jack Ma incide su IPO Alibaba grazie a btc
- Nel 2017 a Roma prime abitazioni al mondo vendute in btc
- 01.01.2018 a Chiasso, tasse svizzere pagate in btc
- Varie città italiane integrazioni con la smart city
- Trento, Bolzano, Milano, Genova, Torino, Pisa, Udine, Firenze, Roma, Cagliari, Parma

  → ATM € - btc e btc - €

Gli asset virtuali – le criptovalute

- Le cosiddette valute virtuali (o valute digitali o criptoattività o criptovalute) sono rappresentazioni digitali di valore, utilizzate all'interno di un network di soggetti come mezzo di scambio o detenute a scopo di investimento speculativo, che possono essere trasferite, negoziate o archiviate elettronicamente; la più conosciuta è il **Bitcoin che utilizza la piattaforma Blockchain**
- Esse sono create da **soggetti privati (Nakamoto)**, che operano sul web, e possono essere usate per trasferire valore all'interno di una comunità di persone, disposte ad accettarle come contropartita di beni o servizi; il trasferimento dei dati da un soggetto all'altro avviene sulla base di regole informatiche e crittografiche, il cui rispetto genera la reciproca fiducia dei partecipanti
- Le valute virtuali non rappresentano in forma digitale le comuni monete a corso legale (come l'euro o il dollaro); inoltre non devono essere confuse con i tradizionali strumenti di pagamento elettronici (come carte di debito o bonifici bancari). Più specificamente, le valute virtuali **non sono emesse dalla Banca Centrale**, non hanno corso legale e non devono essere obbligatoriamente accettate per l'estinzione delle obbligazioni pecuniarie; soprattutto, non sono giuridicamente tutelate da uno Stato e hanno valore solo all'interno del gruppo di persone che decide di utilizzarle

Criptovalute

- È dunque rischioso utilizzare le valute virtuali a causa dell'**assenza di tutele legali e contrattuali**, della mancanza di forme di controllo e di vigilanza su chi le emette e le conserva, di garanzia delle somme depositate, della possibilità di forti oscillazioni del "prezzo" e di perdita permanente del valore a causa di malfunzionamenti, di attacchi informatici, di smarrimento delle chiavi di accesso e altro. In conclusione, la valuta virtuale non è una rappresentazione in forma digitale di moneta a corso legale, ha valore solo all'interno del gruppo di persone disposte ad accettarla e può comportare rischi significativi per chi le utilizza.

Tradizionalmente, lo scambio di denaro tra due sconosciuti è possibile perché entrambi gli attori si fidano di una terza parte, di solito la validità di una banconota o di un intermediario, come una banca o un cambiavalute.
Il sistema di Nakamoto non prevede contanti e intermediari ma crea un sistema affidabile grazie all'uso innovativo della crittografia e del networking peer-to-peer.
Quando un utente invia Bitcoin a un altro utente, i dettagli della transazione (come gli indirizzi del mittente e del destinatario e l'importo dei fondi trasferiti) vengono trasmessi alla rete Bitcoin in modo che la transazione possa essere convalidata da tutti i "peer" (pari) della rete stessa.
Dopo essere stata convalidata dalla rete, la transazione viene inserita in un '"blocco" di transazioni e aggiunta, tramite il processo di "mining", al sempre crescente elenco di blocchi che formano il libro mastro blockchain.
Questo elenco viene conservato dai pari nella rete. Bitcoin presenta anche una funzione per mezzo della quale vengono generati e aggiunti al sistema nuovi Bitcoin, con un effetto inflazionario.
Vengono distribuiti ai miner (oltre alla somma delle commissioni delle transazioni nel blocco) come ricompensa per essere riusciti ad aggiungere le transazioni alla blockchain. Il mining può essere eseguito da qualsiasi utente dotato di un computer ma è emerso un settore di miner professionisti che utilizzano computer dedicati sviluppati appositamente per tale attività.
La struttura distribuita del sistema, insieme alla sua funzionalità crittografica, rende Bitcoin incredibilmente solido.
La fiducia richiesta per abilitare le transazioni viene raggiunta grazie alla consapevolezza che tutte le transazioni – passate, presenti e future – sono attestate (seppur automaticamente) da tutti gli utenti

Elenco criptovalute

- https://coinmarketcap.com/it/all/views/all/
- https://it.investing.com/crypto/currencies
- https://whitepaper.io/document/3/iota-whitepaper