
Cloud Kiter
BitCoin
e i suoi
fratelli
Miniguida
introduttiva al mondo
delle criptovalute

BITCOIN E I SUOI FRATELLI

Miniguida introduttiva al mondo delle criptovalute

Gennaio 2018

Concetti simili espressi in modi diversi:

“Dicono che il denaro non faccia la felicità, ma se devo piangere preferisco farlo sul sedile posteriore di una Rolls Royce piuttosto che su quelli di un vagone del Metrò.” (Marilyn Monroe)

“La vera ricchezza non deriva dall'abbondanza dei beni materiali, ma da una mente serena.”

(Maometto)

Sommario

Introduzione

In questa mini guida cercherò di illustrare sommariamente cosa sono le criptovalute (in primis il BitCoin ma poi per analogia le tante altre in circolazione) e cos'è e come funziona la **Blockchain** il vero motore innovativo su cui sono basate le criptovalute stesse. Questo testo è pensato per chi comincia da zero sull'argomento ma ho cercato di arricchirlo di qualche approfondimento che può *intrigare* anche chi già ne sa un po'.

Puoi quindi leggerla in sequenza dalla prima all'ultima pagina ma in

alternativa, se già ne sai un po', ti propongo di seguito un indice incentrato su alcune parole chiave con il quale puoi andare direttamente all'argomento specifico.

Deep web	mining	Silk roa
Depth chart	Mining pool	Take profit Stop Lo
digest	Multilevel marketing	trading
	P2P	Valute f
	Pumping	Wannac
	Ransomware	
	virus	
	Ross Ulbricht	
	Scrypt	

P.S. ho completato questa mini guida a fine Dicembre 2017 nel pieno di quello che i media hanno

definito “**lo scoppio della bolla del Bitcoin**” questo perché in pochi giorni il Bitcoin, ma anche molte altre criptovalute, ha perso il **40%** del suo controvalore (rispetto al massimo che aveva appena raggiunto). Probabilmente (lo spero) mentre starai leggendo questa miniguida il Bitcoin avrà ripreso il suo cammino “*verso l’inifinito ed oltre!*” ma mi sembrava interessante commentare subito quello che è accaduto a Dicembre 2017: normale amministrazione! E’ normale che qualcosa che cresce con dei ritmi forsennati per mesi e mesi possa fare una “**correzione**” del 40%. A

questo proposito ho trovato questo interessante grafico che fa vedere come nella sua storia il BitCoin abbia registrato “tracolli” ben più ampi (fino al 90%!) da cui si è poi ripreso alla grande (in questo grafico si vede meglio grazie all’uso della scala logaritmica per l’asse del prezzo – non sto a spiegare cos’è la scala logaritmica perché non è importante quello che conta è che in questo modo si evidenziano meglio le correzioni % avvenute in passato, quando i prezzi erano molto più bassi dell’attuale).

History of Bitcoin's Crashes

Prices would have to drop a lot further to compare with the past

Con questo non voglio dire che il BitCoin continuerà indefinitamente questa pazzesca crescita, ovviamente non lo so. Nelle pagine che seguono cercheremo anche di ragionare insieme su cosa potrà accadere, ma mi piaceva evidenziare l'ennesimo caso in cui i media distorcono la realtà e , a voler pensar male, leggere in questa distorsione mediatica la volontà di screditare un progetto ancora poco compreso e che sicuramente da fastidio a qualche "potere forte".

Valuta digitale : prima definizione, prime considerazioni (pro e contro)

cos'è la valuta digitale?

Innanzi tutto diciamo che "valuta digitale", criptovaluta, cryptocurrency, crittovaluta, moneta elettronica,… sono tutti comunemente usati come sinonimi.

Mi piace di meno il termine

valuta/moneta “virtuale” perché questo attributo (virtuale) potrebbe evocare il contrario di “reale” mentre qui stiamo parlando di qualcosa di assolutamente concreto (va bene invece se con virtuale intendiamo qualcosa di localizzato nel “cloud”, distribuito in internet , e in questa accezione ne parleremo).
Alla parola valuta/moneta dobbiamo aggiungere l’aggettivo “digitale” per distinguerla dalle valute tradizionali (euro, dollaro, yen, …) dette anche **valute legali o valute “Fiat”** che hanno quasi sempre anche una forma fisicamente tangibile (monete e banconote).

Ma prima di affrontare la domanda “cos’è la valuta digitale” ripassiamo cosa intendiamo con valuta.

La valuta/moneta è uno strumento che ha reso possibile il commercio facendolo evolvere dal primitivo baratto.

“Grazie all’introduzione della moneta si è potuta sviluppare un’economia complessa, partecipata da persone differenti, con prodotti o servizi dalla natura più disparata, e soprattutto fu possibile introdurre scambi tra persone sconosciute” (cit.).

Inizialmente ogni stato stabiliva quale e quanta valuta fosse ritenuta legale e coniava moneta per una valore pari alle proprie riserve auree.
Nel tempo questo concetto della "convertibiilità" (il cosiddetto Gold Standard per cui ad ogni moneta corrisponde dell'oro posseduto dalla banca centrale e quindi in ogni momento sarebbe stato possibile chiedere di convertire le proprie monete in oro) è stato superato (purtroppo, aggiungo io, dal 1971) ed ora la valuta è gestita da organi centrali (banche, per lo più private) che la emettono con modalità

opinabili (ma questo argomento è troppo complesso e non mi ci impelago).
Le monete legali quindi non hanno (più) un vero valore intrinseco (controvalore in oro) ma sono degli strumenti che consentono gli scambi di valore.

Diciamo che le valute legali (fiat) sono degli “atti di fiducia” verso un governo centrale che gestisce tutte le transazioni e si impegna a garantire il valore di quei “pagherò” che abbiamo nel portafogli e nel conto in banca.

Veniamo allora alla valuta digitale.

Anch'essa è uno strumento per effettuare transazioni di valore tra 2 soggetti.

Differenze rispetto alle valute fiat

ok ma allora quali sono le differenze rispetto alle valute fiat?

Una prima differenza è che la valuta digitale è appunto solo digitale, elettronica, non necessita di "oggetti simbolici" come la moneta metallica o la banconota e per questo per essere utilizzata ha necessariamente bisogno di dispositivi informatici (smartphone, PC, ma sono in fase di adozione anche carte tipo bancomant da usare con i sistemi POS – Point of Sale) e di

connessione ad internet.

Una delle principali differenze rispetto alle valute fiat è che le valute digitali non sono gestite/controllate/intermediate da organismi centralizzati (le Banche) ma grazie alla tecnologia sottostante , la blockchain di cui parleremo dopo, sono per loro natura **gestite in modo decentralizzato**, distribuito (e quindi non assoggettate ad un "ente controllore" …. o almeno così speriamo …).

La decentralizzione unita alla

tecnologia consente di avere:

- **Commissioni** di transazione **ridottissime** (< 0.5% contro l'oltre 4% di carte di credito, bonifici esteri, paypal e simili, …);
- **Tempi di transazione** ridottissimi (anche pochi secondi contro i gg che le banche prendono con i bonifici esteri);
- La valuta digitale sfrutta i meccanismi della crittografia e della distribuzione propri della blockchain per offrire uno strumento **solido e sicuro** .

Altri vantaggi della valuta digitale derivano dal fatto che è uno strumento **mondiale** che ha l'estensione di internet scorrelato quindi (e speriamo resti cosi) dagli stati , dai governi , dalla politica.

Per poter utilizzare valuta digitale non serve avere un conto in banca (cosa non facile per tutti, si pensi soprattutto ai paesi in via di sviluppo, ma anche a chi non rientra esattamente nei canoni della "società civile" e magari non ha una precisa residenza, non ha utenze intestate, uno stipendio regolare,….) ma basta un e-wallet (un portafoglio

elettronico servizio ampiamente disponibile on line) ed una connessione ad internet (nemmeno troppo performante).

Il fatto che la valuta digitale necessiti di un dispositivo (PC , Smartphone) e di connessione ad internet NON significa che ci potrò fare solo “acquisti on line” (alla Amazon , per capirci) ma non ci potrò mai comprare il latte nel bar sotto casa.


LA PAGO IN BITCOIN
BENE, CON QUESTA APP PUÒ SCARICARSI LA BISTECCA

e no! la bistecca la voglio vera! (vignetta di Stefano Rolli, per Il Secolo XIX)

E' solo una questione di diffusione di adozione: esistono già soluzioni di carte di pagamento e/o POS basate sulle valute digitali ma anche in assenza di questo se compratore e venditore sono abbastanza "smart" la transazione si può realizzare tra i loro 2 smartphone (ad esempio , uno genera un QR code e l'altro lo legge , oppure, senza necessariamente incontrarsi, si scambiano gli indirizzi dei rispettivi portafogli elettronici) in tempo reale e (quasi) senza commissioni.


bitcoin
accepted here

Pro e Contro

Ricapitoliamo quindi alcuni dei **vantaggi** suddetti a favore delle valute digitali.

Globali : valgono in ogni angolo del pianeta raggiunto da internet ;
Decentralizzate: non soggette al controllo di una struttura centrale;
Non necessitano di un conto in banca “tradizionale” ;
Veloci e con basse commissioni: proprio perché digitali e decentralizzate;
Sicure: grazie alla Blockchain di cui parleremo più avanti;

Anonime: nel senso che una transazione è , per ora, “poco” tracciabile rendendole simili all’utilizzo del denaro cash ma con il vantaggio di poter essere usate a distanza; (credo che) questo punto sarà sempre meno vero in futuro.

E i contro ?

Ancora “**immature**” : ce ne sono troppe e non tutte sopravviveranno;
Forte volatilità: ancora soggette, proprio perché immature, a forti oscillazioni di mercato (vedremo più avanti questo punto) per cui se possedete delle AltCoin il loro

controvalore in valuta fiat (es. euro) può variare anche del 30% e più in un giorno!

Regolamentazione incerta: per ora sono ancora molto poco (se non per nulla) regolamentate ma c'è da aspettarsi che non rimarrà a lungo così (anche perché il "sistema delle valute Fiat" cercherà di ostacolarne la diffusione);

ancora **scarsa diffusione** di esercizi che accettano criptovalute come forma di pagamento.

A proposito del tema della regolamentazione incerta si sente dire ogni tanto che qualche paese (la

Cina in particolare) vuole mettere al bando le criptovalute (questo perchè temono di perdere il controllo sui movimenti di denaro e la relativa tassazione) ma d'altra parte recentemente c'è stato un importante riconoscimento ufficiale del mondo bancario in particolare rispetto al BITCOIN : ad inizio Dicembre 2017 la Borsa di Chicago ha iniziato a rendere disponibile ai normali consumatori uno strumento (un **future** , non scendo nel dettaglio di cosa sia , non è troppo rilevante; a questo indirizzo potete controllare le quotazioni di questi futures : http://www.cmegroup.com/trading/ec

index/us-index/bitcoin.html) basato appunto sul BITCON.
Da una parte questa può essere considerata una notizia positiva: il BITCOIN non è più solo roba da “hackers” ma può essere in qualche modo comprata da chiunque possa accedere in Borsa (anche se possedere un Future basato sul Bitcoin non è la stessa cosa che possedere direttamente il Bitcoin).
Dall’altra però a mio avviso questa operazione potrebbe anche frenare lo sviluppo del Bitcoin come vero strumento di scambio relegandolo ad uno strumento speculativo che le grandi banche , ora che è entrato nel

circuito borsistico, cercheranno di controllare.
Staremo a vedere….

Comunque non c'è solo il BitCoin ; di valute digitali ne esistono tantissime con i nomi più disparati (vedremo più avanti) . D'ora in poi useremo il termine **AltCoin** (moneta alternativa) per indicare la generica criptovaluta alternativa al BitCoin.

Due parola di storia e di panoramica attuale

La prima valuta digitale ad avere un interessante grado di diffusione mondiale è stata appunto il **BitCoin (BTC)** nato nel 2009 da un progetto d i **Satoshi Nakamoto** (almeno questo è lo pseudonimo usato dalla/e persone che hanno dato vita al progetto; a questo indirizzo potete trovare il paper da cui tutto ha avuto inizio: https://bitcoin.org/bitcoin.pdf). In onore al fondatore la più piccola parte di un BitCoin pari a

0,00000001 BTC è detta **Satoshi**.

Il BitCoin è diventato popolare negli ultimi 5 anni per 2 motivi principali:

- silk road/ deep internet;
- rivalutazione oltre 1000%

Deep Web

Non mi metto qui a dilungarmi sul Deep Web ma probabilmente saprai che i siti che riusciamo a trovare con Google (giusto per dire il più famoso motore di ricerca) sono solo una parte dei siti (o più in generale dei "servizi" internet) esistenti. Esiste tutto un mondo sommerso di siti non indicizzati (nel senso di non trovabili con google e che magari non hanno nemmeno un url - tipo www.ilmiosito.it - ma si possono raggiungere solo conoscendone l'indirizzo IP: es. http://188.217.115.32) noto come **Deep Web** , dark internet e altri

nomi ancora.

Ora il fatto che un sito non sia indicizzato (trovabile quindi usando un motore di ricerca e delle parole chiave) non significa necessariamente che tratti “affari loschi” (tanti siti , ad esempio reti di ricerca universitarie, non hanno bisogno di essere trovate su google essendo solo per addetti ai lavori) ma diciamo che se vuoi fare affari loschi è meglio che non lo pubblicizzi ai 4 venti.

Insomma nella Dark Internet proliferano anche traffici illeciti

(vendita di droga, armi, servizi di hacking,….) che si svolgono in market tipo “ebay”. Uno di questi market, venuto agli altari della cronaca perché (forse) uno dei più grandi, dei primi e dei meglio organizzati si chiamava appunto “**silk Road**” (molto interessante la storia del fondatore ,**Ross Ulbricht**, un insospettabile giovane “nerd” americano – vedi https://it.wikipedia.org/wiki/Silk_Roac)

Welcome! | Silk Road

Welcome! | Silk Road

silkroad[illegible].onion/index.php

Startpage

Silk Road

anonymous market

messages 0 | orders 0 | account ฿0.0000

a few

the Dread Pira

Search

Go

Hi,

Shop by Category

- Drugs 12,072
  - Cannabis 2,821
  - Dissociatives 200
  - Ecstasy 1,290
  - Intoxicants 63
  - Opioids 362
  - Other 31
  - Precursors 86
  - Prescription 3,674
  - Psychedelics 1,303
  - Stimulants 1,425
  - Tobacco 316
- Apparel 530
- Art 14
- Biotic materials 2
- Books 1,161
- Collectibles 21
- Computer equipment 106
- Custom Orders 80
- Digital goods 852
- Drug paraphernalia 440
- Electronics 165

Valium (Apaurine) 10mg x 100.

฿1.6865

Oxycontin 30 mg "Roxys" Pharmacy Fresh Free Ship!

฿0.4260

10 Grams Pure Crystal Meth Methamphetamine

฿6.1324

From the fo

- New disp
- Try Tails secure C
- Who's yo
- Acknowl

1.5 GRAMS DUTCH WEED GROWN IN ITALY!!!

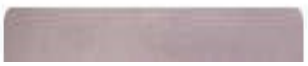
฿0.1678

Prima Lux Slims 6 (10 packs x 20 cigarettes)

฿0.3166

[HGH] Human Growth Hormone 200iu Set (8iu x

฿7.5712



una schermata di SilkRoad dove i prezzi sono espressi in BitCoin

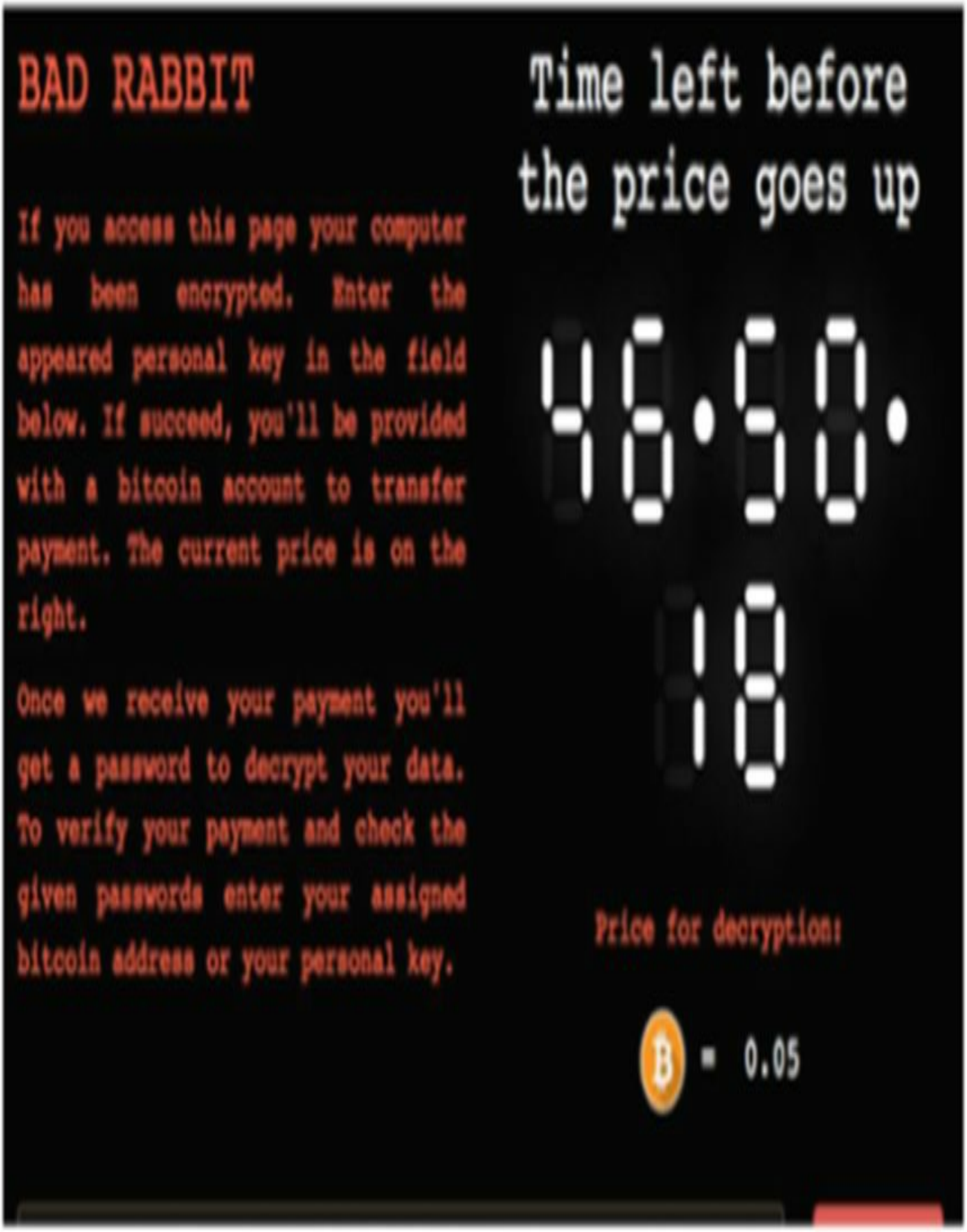
Per poter svolgere commerci illegali è fondamentale non essere tracciabili ma poter comunque scambiare valore per comprare/vendere.

Per quanto riguarda la non tracciabilità della navigazione esistono soluzioni che garantiscono l'anonimato (la più popolare è il browser **TOR** ma ce ne sono anche altre) ma poi serve una valuta di nuovo non tracciabile, da usare come fosse denaro cash, e questo aspetto è stato coperto appunto dal

BitCoin.

Tanto per rincarare la dose e evidenziare il collegamento tra BitCoin e “malavita” (ma ribadisco questo è solo uno dei possibili utilizzi che non devono per questo caratterizzare le criptovalute) avrai forse sentito parlare del fenomeno dei **ransomware** virus : con un virus entrano nel tuo PC e ti cifrano tutti i dati del HD rendendoli inaccessibili. Poco dopo verrai contattato (via mail o anche pop up sul tuo PC – vedi immagini di seguito) chiedendoti il riscatto per i tuoi dati. Se pagherai il riscatto , ovviamente in BitCoin per

non poter tracciare il malvivente, forse i tuoi dati verranno sbloccati (“Bad Rabbit” e WannaCry” sono due esempi di questa tipologia di ransomware virus) .


BAD RABBIT
If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.
Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.
Time left before the price goes up
46:58:18
Price for decryption:
= 0.05


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

*Augurati di non vederla mai sul tuo PC e soprattutto **fai sempre il backup!!***

Qualcuno ha fatto delle indagini e pare che oltre a tanti utenti privati anche qualche grande azienda e/o banca sia caduta in questa trappola ed abbia pagato senza divulgare la notizia.

A quanto sopra si deve la fama "negativa" del Bitcoin ma in realtà questa è solo un'applicazione di uno strumento/progetto che va ben oltre (come dire che la scoperta della fissione nucleare è stata nefasta perché ha consentito l'invenzione

della bomba atomica).

Rivalutazione a 3 cifre ed oltre

L'altro grande motivo che ha reso popolare il Bitcoin è il fatto che dal 2013 ad oggi (fine 2017) il suo controvalore ha registrato un **X 13000** (cioè 100 € nel 2013 sono diventati 1.3 Mln € a fine 2017; in realtà c'è chi ha investito anche prima del 2013 registrando un fattore moltiplicativo astronomico !!)

crescita del BitCoin dal 2013 a fine 2017

Ma anche guardando solo l'ultimo anno , il 2017 , il suo controvalore in Euro è aumentato del 1500% (cioè in un anno **X 20** ca.: 100€ ad inizio anno sono diventati 2000€ per Natale).

crescita del BitCoin nel solo 2017

Questa storia della rivalutazione a 3 cifre secondo me è la peggior palla al piede nello sviluppo delle valute digitali come vero strumento per il commercio: ha infatti instillato nell'opinione pubblica l'associazione di idee **criptovaluta = speculazione** dove per speculazione intendo il cercare di guadagnare cavalcando le variazioni di valore e soprattutto ha instillato nell'opinione pubblica l'associazione **criptovaluta = inaffidabilità** (per via appunto delle forti variazioni di valore non solo in positivo).

Come detto l'utilizzo nel deep web e la forte rivalutazione sono i principali motivi che hanno reso popolare il BitCoin ma a mio avviso bisogna anche riconoscere che un buon motivo di tanta popolarità è dovuto al fatto di essere stati i primi e soprattutto aver mantenuto vivo il progetto, irrobustendolo e cercando di spingerlo come mezzo di pagamento anche oltre il mondo del dark web.

Quante cryptovalute ci sono in circolazione?

Attratti dalla possibilità di realizzare grandi guadagni, sperando nel ripetersi di rivalutazioni a tre cifre, negli ultimi anni sono nate e continuano a nascere con un ritmo crescente nuovi progetti di Criptovalute alternative al BitCoin (AltCoin).

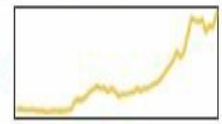
Di valute digitali ne esistono oggi oltre 600 (vedi qui http://coinmarketcap.com/) di cui BitCoin essendo stata la prima è ora la più diffusa e popolare seguita da

Ethereum (ETH) e **Litecoin** (LTC) (ma incalzate da **Ripple**, **Iota**, **Dash**,…).

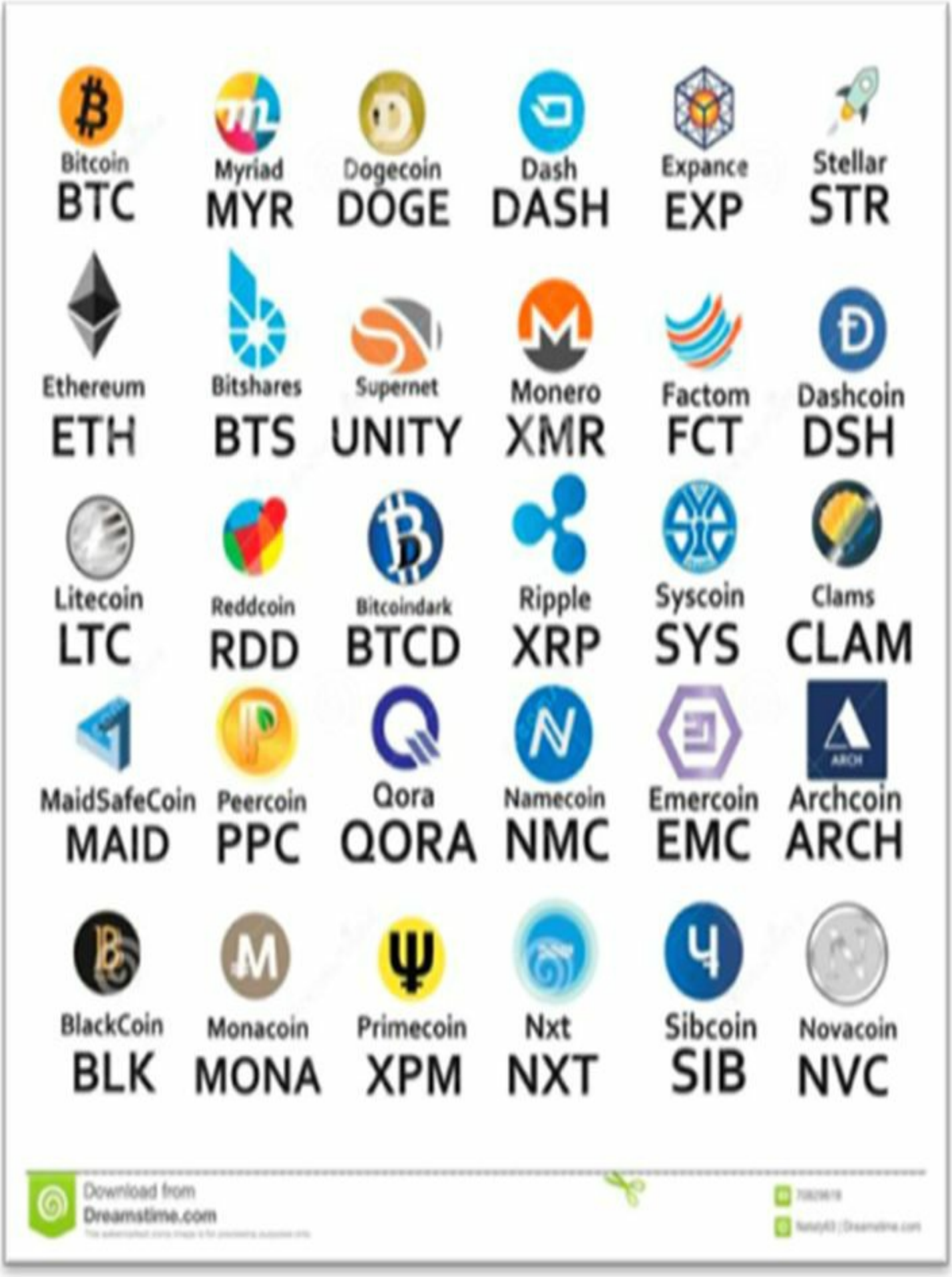
Cryptocurrency Market Capitalizations

Market Cap ▾ Trade Volume ▾ Trending ▾ Tools ▾ Search Currencies

All ▾ Coins ▾ Tokens ▾ USD ▾ Next 100 → View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$288.678.815.600	$17.246.50	$14.566.100.000	16.738.400 BTC	0.22%	
2	Ethereum	$66.004.351.166	$685.31	$5.064.210.000	96.313.552 ETH	20.63%	
3	Bitcoin Cash	$27.062.058.086	$1.605.74	$1.218.770.000	16.853.325 BCH	3.16%	
4	Litecoin	$18.481.455.678	$340.46	$5.442.280.000	54.284.258 LTC	10.24%	
5	Ripple	$18.104.661.866	$0.467348	$3.326.360.000	38.739.144.847 XRP *	69.10%	
6	IOTA	$12.059.409.062	$4.34	$480.634.000	2.779.530.283 MIOTA *	-7.80%	
7	Dash	$7.019.704.823	$905.70	$387.208.000	7.750.611 DASH	12.33%	
8	Monero	$5.013.600.184	$324.52	$282.918.000	15.449.232 XMR	10.86%	
9	NEM	$4.882.112.999	$0.542457	$78.339.500	8.999.999.999 XEM *	0.41%	
10	Bitcoin Gold	$4.625.604.473	$276.92	$267.454.000	16.703.999 BTG	5.46%	

Oltre a queste più di 600 crittovalute già attive ce ne sono tantissime in fase di lancio , quasi tutte come iniziative di privati ma c'è da segnalare che anche istituti bancari e governi (Cina, India, Finlandia, …) stanno lavorando per rilasciare proprie nuove valute digitali (ad esempio in India stanno puntando sul Laxmicoin: vedi qui: https://yourstory.com/2017/11/what-is-laxmicoin-indian-cryptocurrency/).



i logo e le rispettive sigle di alcune delle criptovalute più note

Altcoin e schema Ponzi

Come appena detto l'argomento criptovalute è molto attuale anche perché il lancio di nuovi progetti di valuta digitale è all'ordine del giorno ed è spesso accompagnato da soluzioni di marketing piramidale (o **multilevel marketing**).
Quando la nascente AltCoin non è ancora in produzione ma è solo un progetto serve reclutare un gran numero di "sostenitori" che credono al progetto e in qualche modo lo finanziano . Un modo per fare questo è il classico multilevel marketing : se tu ti associ , pagando una quota di

iscrizione , ti garantisci un certo numero di AltCoin per quando (forse) andranno sul mercato. In aggiunta a questo se porti degli amici che aderiranno al progetto tu guadagnerai qualcosa per la loro iscrizione e per quelle che loro porteranno….

A volte queste sono vere e proprie truffe nel senso che dietro non c'è nessun reale progetto e quando si è raggiunto un certo numero di adesioni il vertice della piramide scappa con il malloppo (è il caso del cosiddetto **schema Ponzi**, dal nome di Charles Ponzi, un immigrato

italiano negli Stati Uniti che divenne famigerato per avere applicato una simile truffa su larga scala).

Però sottolineo che questo marketing piramidale non c'entra niente con le Criptovalute. Il multilevel marketing si può applicare ad ogni cosa non solo alle pentole ed agli aspirapolvere.

La BlockChain

OK dopo tante chiacchiere parliamo un po' della tecnologia sottostante che ha reso possibile la nascita delle criptovalute.

il cuore delle criptovalute è la **blockchain**.

Provate a pensare di voler istituire tra i vostri amici/conoscenti una nuova valuta che valga per gli scambi a distanza tra di voi. volete che sia sicura e anche se siete amici non vi fidate troppo e volete essere cautelati rispetto a furti. Cosa vi

serve per farla funzionare?
Serve un “**libro mastro” pubblico** in cui vengano registrate tutte le transazioni dalla “notte dei tempi” e che quindi possa essere consultato in ogni momento per sapere chi ha quanto.

La blockchain è il “libro mastro” (in inglese “**ledger**”).

Pensate di avere un “libro mastro” in cui vengono registrate tutte le transazioni di valute digitale. Poiché si assume , correttamente, che all’istante 0 tutti avevano 0, a partire dal “log” aggiornato di tutte le

transazioni è possibile ricostruire quanto c'è ora nel portafogli elettronico di ognuno.

Può sembrare un po' complesso (ma ormai la potenza di calcolo è facilmente disponibile) ma d'altro canto è un sistema sicuro.

Quindi l'idea di archiviare tutte le transazioni dall'inizio dei tempi è buona; come si può renderla più "robusta"?

Con almeno 2 meccanismi principali:

- la crittografia;
- la distribuzione dello stesso

libro mastro su una rete P2P.

Ogni insieme di transazioni , quelle avvenute in un certo periodo di tempo, viene “sigillata” creando un “block” tramite un protocollo di cifratura (o hashing tipo SHA-256) che genera una **firma digitale** (“**digest**” o **Hash**) di quel blocco;

Block:	#	1				
Nonce:	139358					
Tx:	$	25.00	From:	Darcy	->	Bingley
	$	4.27	From:	Elizabe	->	Jane
	$	19.22	From:	Wickham	->	Lydia
	$	106.44	From:	Lady Ca	->	Collins
	$	6.42	From:	Charlot	->	Elizabe
Prev:	0000000000000000000000000000000000000000000000000					
Hash:	00000c52990ee86de55ec4b9b32beefd745d71675dc					

Mine

esempio di Block con alcune transazioni e il relativo digest calcolato (hash)

la firma digitale del blocco n-esimo viene **inglobata nel blocco successivo** (n+1) che viene anche lui firmato digitalmente creando una catena di blocchi (blockchain) che non può essere facilmente manomessa.


Block: # 1
Nonce: 139358
Tx:
$ 25.00 From: Darcy -> Bingley
$ 4.27 From: Elizabe -> Jane
$ 19.22 From: Wickham -> Lydia
$ 106.44 From: Lady Ca -> Collins
$ 6.42 From: Charlot -> Elizabe
Prev: 0000000000000000000000000000000000000000000000000
Hash: 00000c52990ee866e55ec4b9b32beefd745d71675dc
Mine
Block: # 2
Nonce: 39207
Tx:
$ 97.67 From: Ripley -> Lambert
$ 48.61 From: Kane -> Ash
$ 6.15 From: Parker -> Dallas
$ 10.44 From: Hicks -> Newt
$ 88.32 From: Bishop -> Burke
$ 45.00 From: Hudson -> Gorman
$ 92.00 From: Vasquez -> Apone
Prev: 00000c52990ee866e55ec4b9b32beefd745d71675dc
Hash: 000078be183417844c14a9251ca246fb15df1074019
Mine
Block: # 3
Nonce: 13884
Tx:
$ 10.00 From: Emily -> Jackson
$ 5.00 From: Madison -> Jackson
$ 20.00 From: Lucas -> Grace
Prev: 000078be183417844c14a9251ca246fb15df1074019
Hash: 0000c2c95f54a49b4f2bee7056a7dc3b7c1a488706c
Mine
Block: # 4
Nonce: 20688
Tx:
$ 62.19 From: Rick -> Ilsa
$ 867.96 From: Captain -> Strasser
$ 276.15 From: Victor -> Ilsa
$ 97.13 From: Rick -> Sam
$ 119.63 From: Captain -> Jan Bru
Prev: 0000c2c95f54a49b4f2bee7056a7dc3b7c1a488706c
Hash: 0000c03019ed59586405750968888fb65256e824924
Mine

BlockChain = concatenazione di blocchi (queste immagini sono tratte dal sito https://anders.com/blockchain/ che Ti consiglio vivamente di consultare per toccare con mano i concetti di hashing e blockchain)

Infatti se volessi modificare la registrazione di una transazione avvenuta nel passato (ad esempio Caio volesse modificare la transazione “tizio versa a caio 1 coin” in “tizio versa a Caio 100 coin”) dovrei andare a ritrovare quel blocco nella catena , modificarlo e “cifrarlo” di nuovo generando un nuovo digest , ma soprattutto dovrei andare a modificare tutti i blocchi successivi operazione che richiede

una potenza di calcolo enorme.

Ok , così è robusto ma si può fare di più?

Si , si può fare di più facendo in modo che di “libro mastro” non ce ne sia solo una copia (residente su un unico server fisico potenzialmente vulnerabile) ma che ne esistano N copie tutte uguali distribuite su una rete di computer indipendenti disseminati su internet (cosiddetta rete **Peer to Peer** – da pari a pari , **P2P** in gergo).

A questo punto se volessi modificare

il contenuto di una transazione dovrei farlo su tutte le copie disseminate su internet : operazione praticamente impossibile (tanto più complessa quanto più la rete è ricca di Nodi che collaborano ma che sono al contempo **indipendenti**).

quindi fare frodi intese nel senso di alterare il libro mastro delle transazioni è pressoché impossibile (o almeno moooooooooooolto complesso).

Il modello della Blockchain NON è

strettamente legato alla valuta digitale. Diciamo che la blockchain può essere applicata **anche** per far funzionare una valuta digitale ma non solo.

Il modello della blockchain può essere adottato in ogni circostanza in cui voglio essere sicuro della registrazione di una transazione ad esempio per gli atti notarili, per il catasto immobiliare , per il Registro delle Autovetture,…: le possibili applicazioni sono molteplici.

Piccolo approfondimento

sulla Crittografia

Di seguito due parole in più sulla crittografia che volendo potete anche saltare:
Cifrare un testo, nel nostro caso la lista descrittiva di un certo numero di transazioni di crittovaluta, significa applicare ad esso una funzione di compressione, **Hashing**, tale da generare una stringa , il già citato **digest**, strettamente collegato al testo oggetto di cifratura.

SHA sta per **Secure Hash Algorithm** ed è uno degli algoritmi di compressione più noti (insieme a MD5) :dato un testo di lunghezza

max 2^64 -1 di lunghezza variabile viene generato un digest di lunghezza fissa.

Per costruire una funzione di hash è necessaria una buona funzione di compressione; questa deve essere costruita in modo che ogni bit di input influenzi il maggior numero possibile di bit di output (il digest).
Di seguito un esempio di digest generato dal SHA-1:
SHA1("Cantami o diva del pelide Achille l'ira funesta") = **1f8a690b7366a2323e2d5b045120d**
In una buona funzione di hashing anche una minima variazione nel

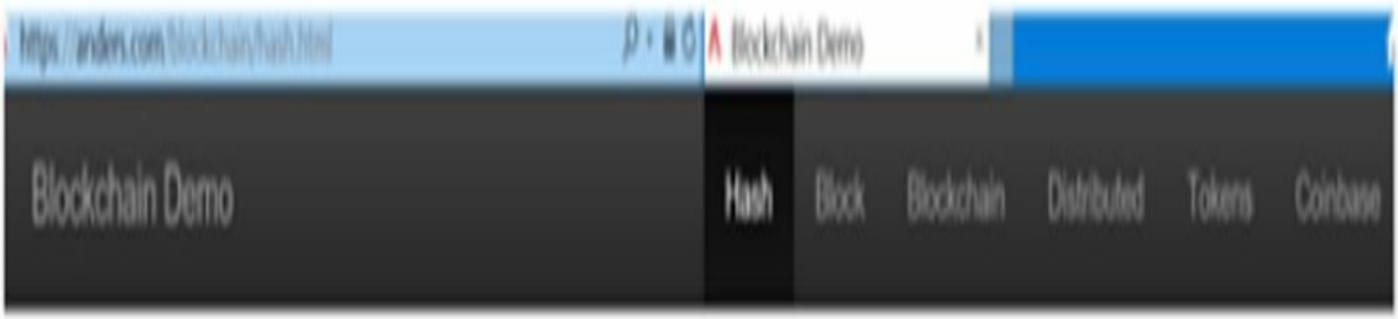
messaggio deve generare, un hash completamente differente. Ad esempio, sostituendo “Cantami” con “C**o**ntami” otteniamo:
SHA1("Contami o diva del pelide Achille l'ira funesta") = **e5f08d98bf18385e2f26b904cad23c**
(fortemente diverso dal precedente digest)

Le funzioni di hashing sono **unidirezionali**, cioè conoscendo il digest deve essere computazionalmente impossibile risalire al messaggio originale ; in altre parole dato y, è computazionalmente impossibile

trovare un m tale che h(m) = y.

Deve essere anche computazionalmente impossibile trovare due messaggi m1 e m2, con m1≠m2, tali che h(m1)=h(m2). In questo caso la funzione h è detta fortemente resistente alle collisioni (dove per collisione si intende il fatto che due messaggi diversi producono il medesimo digest).
Questo non significa che non esistano due messaggi diversi che producono lo stesso digest (d'altronde è pur sempre una funzione di compressione) ma solo (si fa per dire) che è

computazionalmente molto complesso trovarli.
SHA256 è uno algoritmo di cifratura usato da diverse criptovalute, tra cui proprio il BitCoin, ma non è l'unico (ad esempio il Litecoin usa l'algoritmo **Scrypt** che vanta a suo favore una maggiore velocità).
Se volete giocare con la funzione di hashing SHA256 e sperimentare quanto appena detto vi ripeto il consiglio di consultare il sito https://anders.com/blockchain/



SHA256 Hash

Data: Cantami o diva del pelide achille l'ira funesta

Hash: 00638c6d8a97b6c8f1bb2de0af0f5971ba41946033d4597c9017149c4852a14b

Come si forma il prezzo di una valuta digitale?

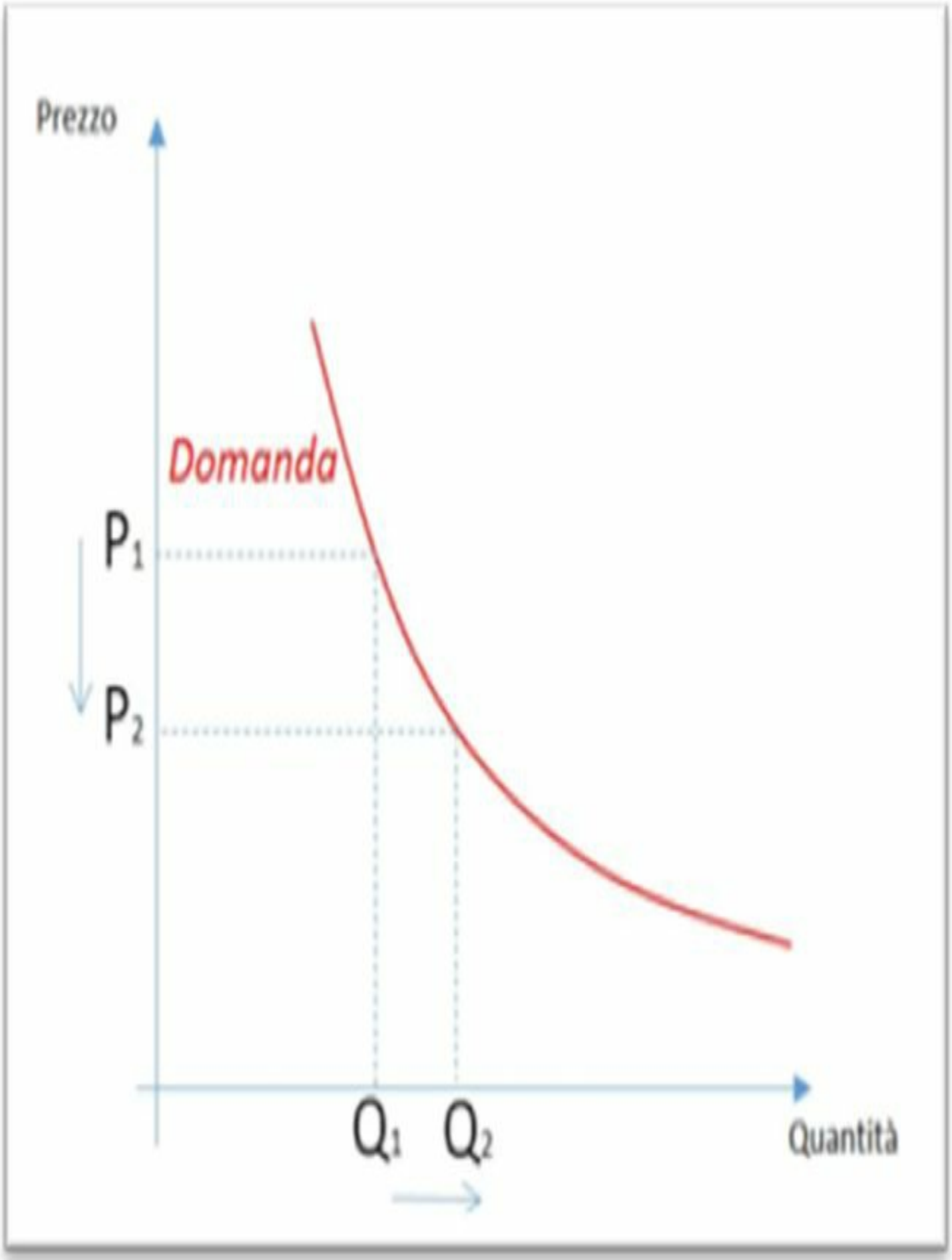
Come si stabilisce il prezzo di una valuta digitale?

Il meccanismo è più o meno quello che regola il prezzo di ogni bene di consumo "limitato" (nel senso che non è infinito) : la **legge della domanda e dell'offerta**.

Ripassiamo questo concetto: Come varia la domanda di un bene al variare del prezzo?

In generale Prezzo e Quantità scambiata (acquistata/venduta) dal

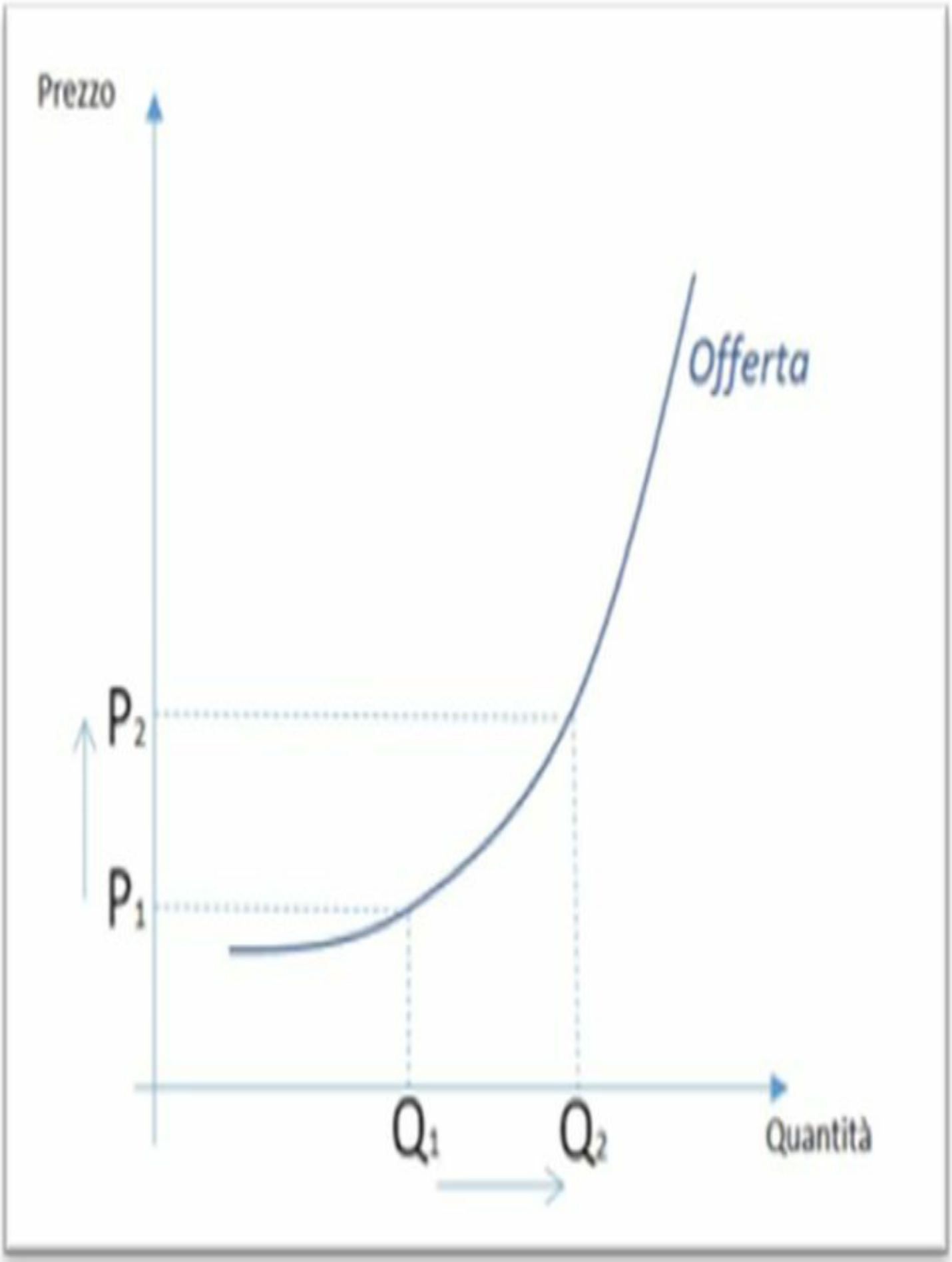
punto di vista dell'acquirente (la **domanda**) sono inversamente proporzionali: più il prezzo diminuisce e maggiore è la propensione del "mercato" , inteso come l'insieme dei tanti piccoli e grandi potenziali acquirenti, a comprarne crescenti quantità.


Prezzo
Domanda
P1
P2
Q1
Q2
Quantità

più il prezzo scende maggiore è la quantità che sono disposto a comprare

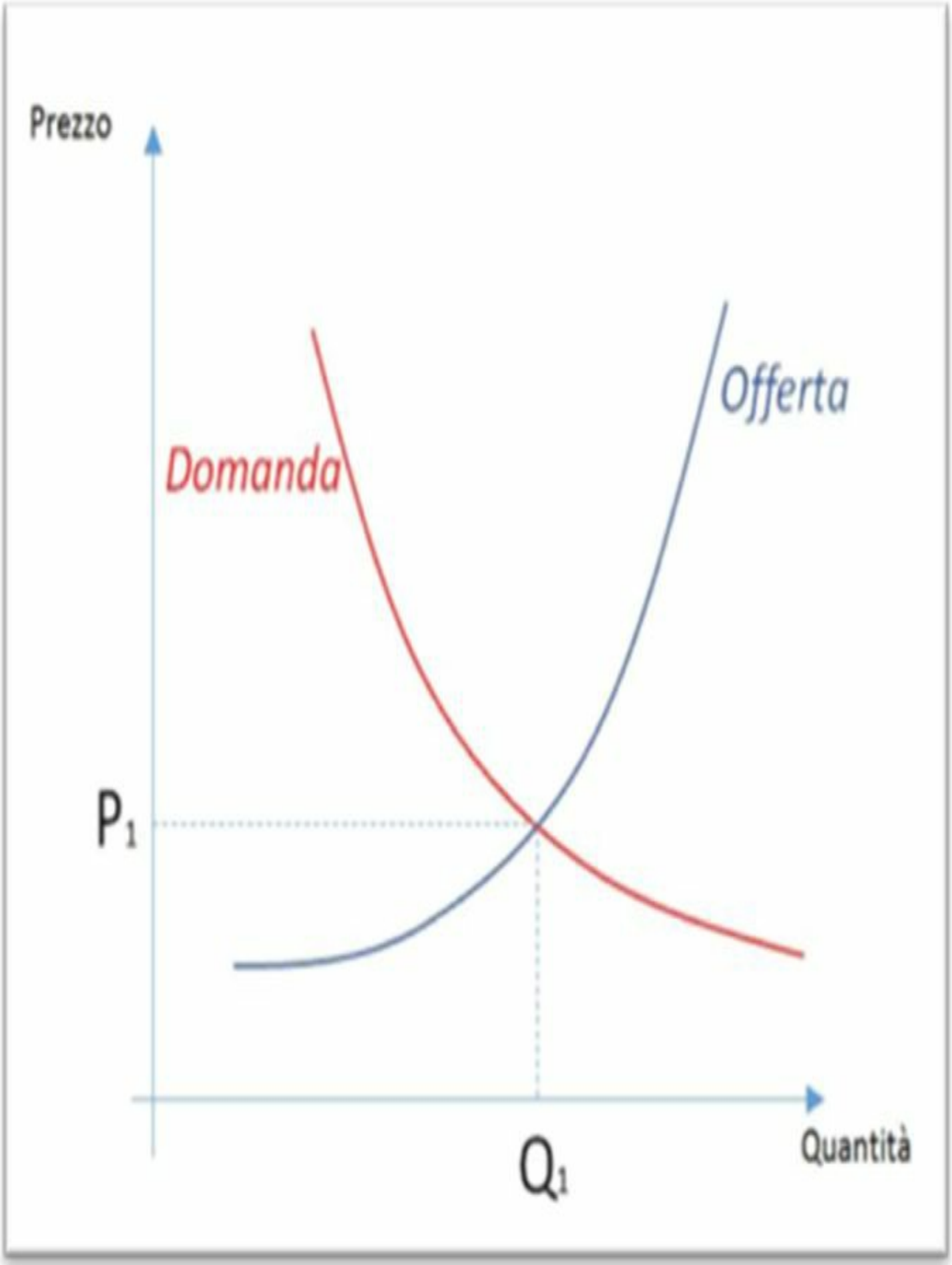
Dal punto di vista del produttore/possessore (**l'offerta**) invece le cose vanno al contrario: il produttore/possessore è orientato a massimizzare il profitto (profitto unitario X num. di pezzi venduti ; profitto=ricavi-costi) quindi se il produttore capisce che il prezzo unitario può salire si farà in quattro per aumentare la produzione (magari anche facendo investimenti in nuove risorse produttive sfruttando delle economie di scala che gli consentono di ridurre i costi di produzione e quindi aumentare i

ricavi unitari). Detto in un altro modo se la domanda cresce il produttore può permettersi di alzare il prezzo .


Prezzo
Offerta
P2
P1
Q1
Q2
Quantità

più il prezzo sale maggiore è la quantità che sono disposto a produrre

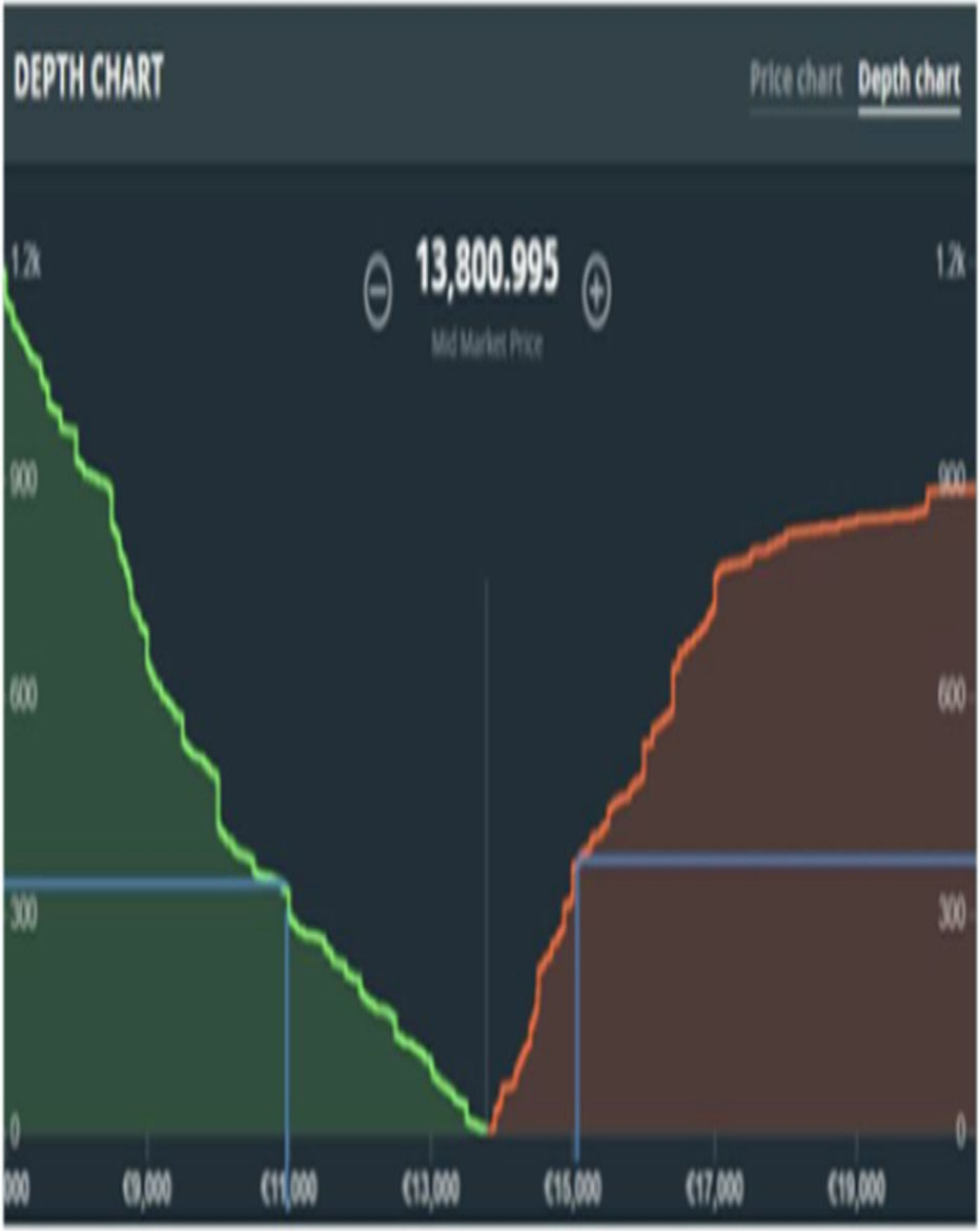
E allora qual è il prezzo giusto? Quello in cui le due curve si incrociano cioè dove domanda e offerta si incontrano.


Prezzo
Offerta
Domanda
P1
Q1
Quantità

Se c’è tanta domanda di un certo bene limitato il prezzo sale perché io che lo possiedo e che so che tu lo vuoi comprare , alzo il prezzo confidando che tu mi vieni dietro. Ma io venditore non posso “tirare troppo la corda” (cioè alzare troppo il prezzo) perché l’acquirente è sì interessato ma non pazzo e oltre un certo prezzo molla (come nei rialzi alle aste) . Allo stesso modo quando la domanda è bassa io venditore devo abbassare il prezzo per allettare chi al prezzo attuale non è interessato a comprare.

Questo discorso vale in linea di massima per tutti i beni commerciabili e quindi anche per il prezzo delle valute digitali che sono tipicamente beni limitati (ad esempio l'algoritmo del Bitcoin prevede un massimo numero di "monete" digitali emettibili).

Alcune piattaforme di trading di cryptovalute, come ad esempio GDAX (un **exchange** di cui parleremo più avanti), rendono molto bene in modo grafico come il prezzo sia un **equilibrio dinamico** tra due spinte: chi vuole comprare e chi vuole vendere.


DEPTH CHART
Price chart
Depth chart
13,800.995
Mid Market Price
1.2k
900
600
300
0
€9,000
€11,000
€13,000
€15,000
€17,000
€19,000

Questo è il **Depht chart** (di GDAX) , vediamo come si legge. In questo momento il prezzo del BTC è 13800€ (controvalore del Bitcoin il 24/12/17 in un certo preciso istante) La parte sinistra del grafico rappresenta i potenziali compratori, la parte destra i potenziali venditori. Ad esempio il grafico ci dice che se il prezzo scendesse a 11000€ ci sarebbero acquirenti disposti a comprare oltre 300 Bitcoin (cumulativamente tra i Clienti di GDAX); d'altro lato se il prezzo salisse a 15000€ ci sarebbero possessori di Bitcoin disposti a

venderne più di 300 complessivamente; 13800€ è in questo momento il **punto di equilibrio**. (Ma come fa GDAX a sapere quanti comprerebbero e quanti venderebbero? Perché può vedere gli Stop loss ed i Take Profit impostati , ma per capire questo dovete procedere con la lettura :-).

Questo meccanismo della domanda e dell'offerta è ben noto alle "**mani forti**" a chi cioè possiede grandi quantità di un certo bene o in alternativa di "potere d'acquisto" e che grazie a questo meccanismo riesce a indirizzare il mercato in

modo a loro conveniente.

Ad esempio se io possiedo una grossa quantità di BitCoin (diciamo 1000) potrei metterli in vendita tutti insieme; probabilmente in quel momento la domanda del “mercato non è in grado di assorbire tutte le mie vendite e quindi dovrò abbassare un po’ il prezzo ma alla fine le venderò tutte. Diciamo che prima di vendere i miei 1000 pezzi il Bitcoin valeva 100 (inteso come controvalore in una qualche moneta fiat di riferimento) e che per piazzare tutto il mio stock le ho dovute vendere ad un prezzo medio di 90.

A questo punto ho prodotto una variazione del prezzo che ha cominciato a scendere (100->90) nel senso che anche l'insieme di tutti gli altri venditori , e quindi tutto il mercato, ha dovuto adeguare il prezzo di vendita a quello che stavo facendo io (" ehi non puoi più venderlo a 100 ! c'è tizio che lo vende a 90!") .

Per la legge della domanda se il prezzo scende c'è chi è disposto a comprare .

Gli altri possessori di Bitcoin vedendo questa quantità di vendite

che eccede la domanda e vedendo scendere il prezzo si spaventa e comincia a pensare: “se le ha vendute lui che ne possedeva tante forse sa qualcosa che io non so, mi conviene seguirlo” e inizia un **effetto domino** di vendite per cui il prezzo scende ulteriormente , diciamo da 90 a 70 (e si vendono perché, sempre per la legge della domanda e dell’offerta, se il prezzo scende la quantità acquistata aumenta). A questo punto io , grande investitore, potrei decidere di riacquistare gli stessi 1000 Bitcoin che ho venduto prima e che ora posso comprare a 70. Diciamo che appena comincio a

comprare il prezzo risale un po' e per ricomprarle tutte devo pagarle un prezzo medio di 75 . Nel frattempo gli altri acquirenti faranno di nuovo il ragionamento "gregge": se compra lui che ha tanti soldi (e quindi se ne intende) forse sa qualcosa che io non so : mi conviene seguirlo e comprare" . Insomma nel giro di poco tempo il prezzo risale e diciamo che si riporta intorno ai 90. Alla fine a me, grande investitore, questa operazione è convenuta: ho sempre gli stessi 1000 bitcoin che prima valevano 100 ed ora valgono 90 , li ho venduti a 90 ma ricomprati a 75, quindi ci ho guadagnato circa il

5% dal nulla , cavalcando un’onda che ho creato io stesso !

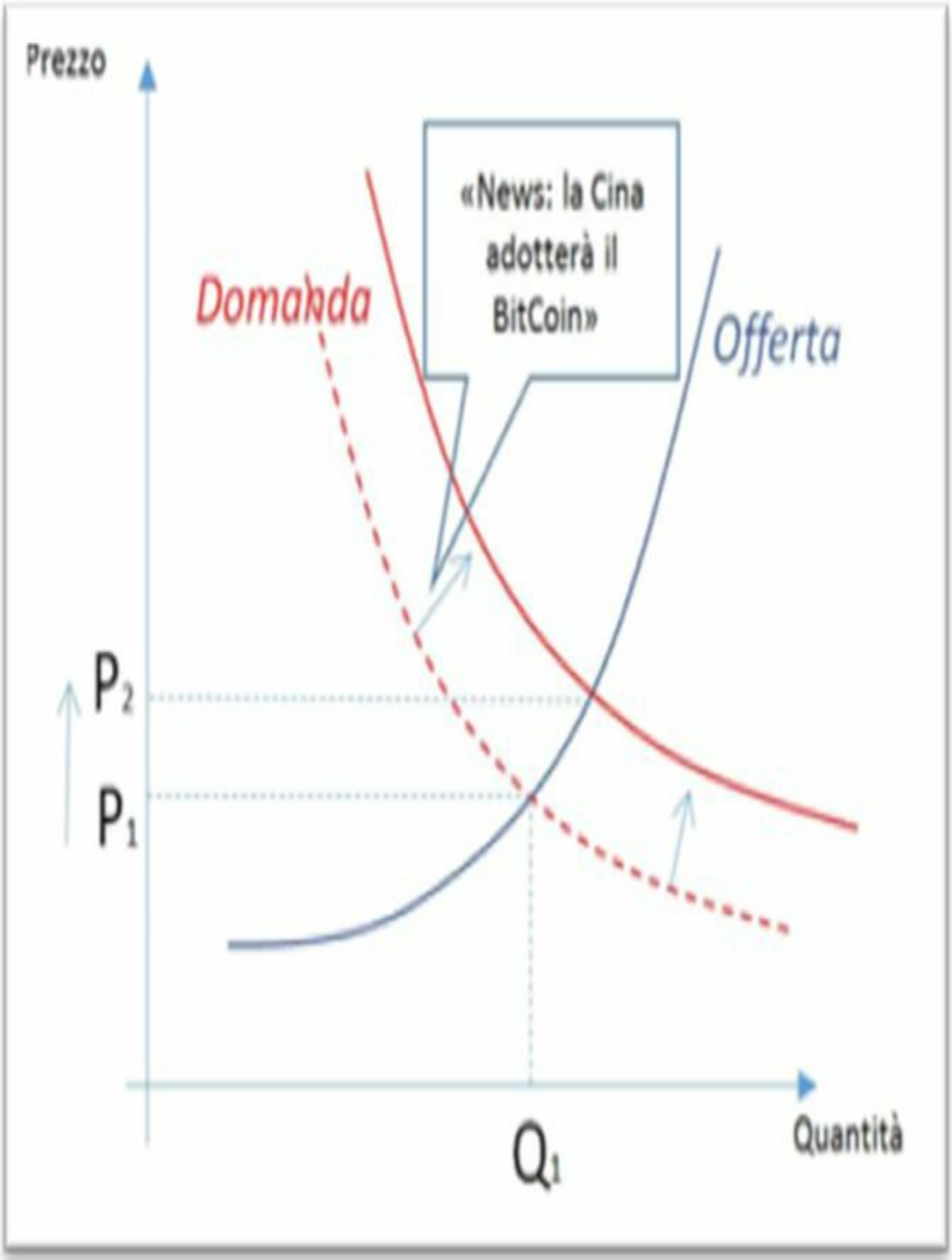

JUST A NORMAL DAY AT THE NATION'S MOST IMPORTANT FINANCIAL INSTITUTION...
I'VE GOT A STOCK HERE THAT COULD REALLY EXCEL
REALLY EXCEL?
EXCEL?
SELL?
SELL?
SELL
SE
SELL!
SELL!
SELL!
SELL!
SELL!
ELL!
SELL!
GOOD BYE?
BYE?
Buy?
BUY!
Buy!
BUY!!
Buy!
Buy!
THIS IS MADNESS! I CAN'T TAKE ANYMORE
GOOD BYE!
I'VE GOT A STOCK HERE...

A volte le cose vanno anche così....

La stessa operazione si può fare al contrario con il cosiddetto **Pumping**: un grande investitore o un gruppo coordinato di piccoli investitori decide di comprare ad un certo istante una significativa quantità di una certa Altcoin : il mercato vedendo crescere la domanda fa salire il prezzo (anche per "l'effetto gregge"); ad un certo punto salito il prezzo di un valore prefissato il grande investitore rivende, ad un prezzo più alto di quello d'acquisto, tutte le Altcoin precedentemente acquistate . E' come creare l'onda è

poi surfarci sopra!!

Quindi la legge della domanda e dell'offerta è una regola che vale anche per determinare il prezzo delle criptovalute, ma non c'è solo questo. Il valore di un bene può salire anche perchè il mercato gli riconosce una potenzialità ancora non pienamente espressa ma che si pensa possa concretizzarsi nel prossimo futuro.


Prezzo
«News: la Cina adotterà il BitCoin»
Domanda
Offerta
P2
P1
Q1
Quantità

all'uscita di una notizia favorevole la propensione all'acquisto aumenta improvvisamente il che graficamente si traduce in una traslazione verso dx della curva della domanda e quindi un aumento del prezzo

Nel caso del BitCoin, ma lo stesso vale per le principali AltCoin, il prezzo sta crescendo anche perché il mercato ne riconosce il valore (mi consente di fare transazioni veloci , con basse commissioni, con una buona sicurezza,…) e sa che il bene è limitato quindi quando tutti gli AltCoin di quella specifica valuta digitale saranno stati messi sul mercato non ce ne saranno più e

siccome è una valuta che “funziona” (per i motivi di cui sopra) mi conviene acquisirne prima che finiscano.

Ovviamente è impossibile che il prezzo salga sempre per tutti ; non tutte le valute digitali avranno successo: la maggior parte , delle oltre 600 già sul mercato, saranno dei flop , perché poco adottate, e il prezzo/valore crollerà.
Inoltre , come già successo in passato, si verificheranno episodi (veri o creati ad hoc) che potranno momentaneamente far perdere di fiducia in una specifica AltCoin

(come già accaduto al verificarsi ad esempio di una falla di sicurezza o alla dichiarazione di uno stato di tassare o di rendere illegale l'uso delle criptovalute) e quindi innescare una forte correzione dei prezzi .

Sicuramente finchè le valute digitali non diventeranno uno strumento utilizzato veramente per fare delle compra/vendite e non solo per speculazione dovremo assistere a queste forti fluttuazioni.


BITCOIN
NOT
ACCEPTED

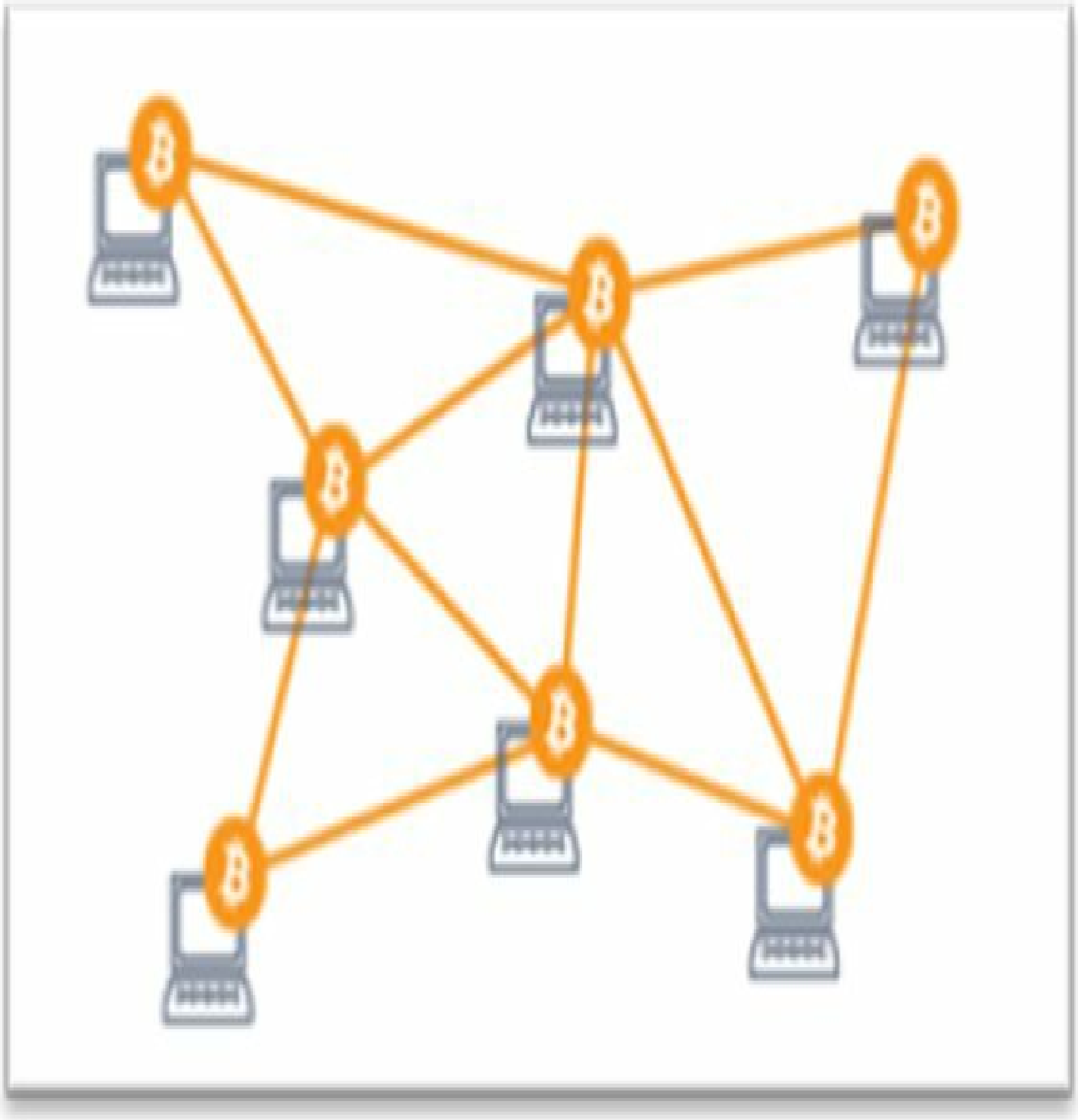
Riguardo alla **volatilità** c'è da segnalare un altro motivo per cui le oscillazioni sulle valute digitali possono essere così violente: perché seguono la pura legge di mercato senza un ente centrale che ne controlla il prezzo. Sul mercato azionario "tradizionale" quando un azione comincia a salire o scendere troppo il titolo viene sospeso (non può più essere scambiato) finchè le "acque non si calmano". Questo è uno degli effetti (non so dire se un bene o un male) dell'avere un mercato controllato in modo centralizzato. Con gli AltCoin invece quando il mare è mosso non c'è

nessuno che lo calmi per cui si possono verificare forti oscillazioni (anche un + o - 100% in un giorno)

La blockchain e i minatori

Ok ma in pratica come funziona la blockchain?
Abbiamo detto che ogni blocco, cioè un insieme di transazioni da registrare sul libro mastro, viene cifrato. Per cifrare dei dati serve della **potenza di calcolo** , dei computer con la CPU potente.
Ecco allora come funziona la blockchain legata ad una specifica criptovaluta:
chi vuole partecipare al progetto mette a disposizione un computer

collegato ad internet su cui fa girare il software che contiene l'algoritmo della specifica criptovaluta.
Tutti i computer che partecipano al progetto instaurano delle connessioni tra di loro formando così una rete magliata in cui ogni computer parla con ogni altro (rete P2P).



Cosa fa questa rete di computer?
essenzialmente 2 cose:

- mantiene aggiornato il libro

mastro;

- certifica le transazioni.

Focalizziamoci su questa funzione di **certificazione** .
Abbiamo detto che ogni tot transazioni (scambi di altcoin) che si verificano in un certo limitato lasso di tempo (secondo l'algoritmo che regola quella AltCoin) viene creato un blocco che deve essere cifrato e trascritto nel libro mastro. Questa operazione di cifratura necessita di potenza di calcolo , nasce allora una specie di gara a chi per primo riesce a certificare quel blocco di transazioni; chi ci riesce viene

“premiato” dal algoritmo stesso con un certo numero di Altcoin (o meglio con frazioni di essa). Questa attività è detta **mining** (minatura) evocando l’immagine dei **minatori** che scavano nella roccia per estrarre valore.

Una volta che le transazioni sono state certificate ed inserite nel blocco vengono “**riscontrate**” da tutti gli altri (o almeno da un buon numero) nodi della rete che confermano la validità della transazione.

Questo meccanismo di convalida multipla (sebbene questa descrizione sia molto sommaria) è quella che ha consentito di risolvere uno dei

principali problemi iniziali delle criptovalute: il **double spending**. In teoria il possessore di un certo ammontare di criptovaluta, diciamo 100 AltCoin, potrebbe lanciare più o meno contemporaneamente due (o più) transazioni di acquisto entrambe da 100 Altcoin in pratica spendendo i suoi soldi 2 o più volte (ricevendo quindi in cambio merci o servizi per 2/300 Altcoin pur avendone solo 100). Il fatto che le transazioni debbano essere confermate da tutta la rete (o almeno da un alto numero di nodi attivi) serve anche a scongiurare questo tipo di frode.

A questo riguardo c'è da segnalare che la potenza di calcolo necessaria per certificare un blocco e/o validare una transazione cresce nel tempo (anche perchè crescono le dimensioni del libro mastro); ecco perchè mentre all'inizio , per esempio dei bitcoin, questa attività di mining poteva essere svolta con normali PC (in particolare con schede grafiche performanti) e quindi poteva essere fatta da chiunque, ora invece , considerando che i blocchi sono sempre più complessi da certificare e che "il premio" è sempre più allettante

(perchè il valore del AltCoin è salito) non è più un'attività che può essere svolta dal singolo utente comune ma si sono sviluppate delle "**mining server farm**" , delle centrali di calcolo con batterie di computer performanti e ottimizzati per questa attività gestite da società private.

A questo riguardo segnalo 2 temi rilevanti:

- HW specializzato per il mining;
- **Centralizzazione** del potere di calcolo.

Per dei motivi tecnici che non sto qui ad illustrare le schede grafiche dei

PC (le cosiddette **GPU,** Graphics Processing Unit - parlo di PC particolarmente orientati alla grafica ad esempio per il gaming o il CAD) sono particolarmente adatte a svolgere i calcoli necessari per far funzionare la blockchain. Questa caratteristica ha fatto si che sia nata nel giro di poco tempo una fortissima domanda di schede grafiche (nate per la videografica ma invece usate per il mining) tanto da mettere in difficoltà i produttori (tipo NVIDIA, Matrox,…) che bene contenti ne hanno alzato il prezzo (vedi https://hardware.hdblog.it/2017/06/27/bitcoin-ethereum-prezzi-gpu/) .

Quanto sopra per rappresentare come il mondo delle criptovalute abbia innescato, tra le altre cose, un indotto di produttori di **HW pensato esplicitamente per il mining** (alta potenza di calcolo e bassi consumi): un mercato che prima non esisteva.
A titolo di esempio guardate questo link - https://asicshop.eu/antminer-s9-jan25 - dove si vendono questi computer specializzati per il mining la cui bontà è caratterizzata dal massimo **Hash Rate** (misurato in TH/sec , Tera Hash al secondo) vale a dire dal numero di operazioni di calcolo al secondo ma soprattutto

dal rapporto tra il max Hash Rate e la potenza assorbita valore questo espresso in (TH/s)/Watt : non dobbiamo infatti dimenticare che oltre ad una potenza di calcolo elevata queste macchine , pensate per essere accese sempre (h24 per tutti i gg dell'anno) devono consumare poca energia altrimenti i soldi che si guadagnano dal mining se ne vanno in bolletta elettrica.

computer ottimizzato per il mining

La seconda cosa da segnalare è che , come dicevo prima, ormai il mining è una cosa da professionisti che mettono su importanti server farm: questo fatto è un potenziale pericolo per il funzionamento "**libero e democratico**" della blockchain che invece si basa su una potenza di calcolo distribuita e indipendente. Si dice che un'importante % di tutta la potenza di calcolo che fa funzionare il BitCoin sia in realtà centralizzata in poche server farm (che quindi potrebbero in qualche modo esercitare un potere di controllo);

questo significherebbe tornare ad un modello centralizzato che è l'esatto opposto di uno dei pilastri delle criptovalute.

Per rimanere sul tema di quanto sia importante la potenza di calcolo per minare criptovalute segnalo tre "soluzioni" per fare mining:

- prendere in **affitto** potenza di calcolo;
- **affiliarsi** ad un **pool** di mining;
- svluppare **virus** (!)

L'alternativa a comprare HW specializzato è noleggiarlo: questo è un altro business indotto dalle

criptovalute . Così come ci sono server farm (o Data center che dir si voglia) messi in piedi da società private per minare per proprio conto allo stesso modo esistono società (spesso sono le stesse) che avendo grosse batterie di server specializzati vi consentono di noleggiare una certa quantità di potenza di calcolo: voi dovete solo decidere il taglio di potenza di calcolo (in TH/sec), pagare il canone mensile e incassare i frutti del mining, alla gestione del HW (acquisto, manutenzione, spazi , corrente, condizionamento,…) ci pensano loro . A titolo di esempio Vi

segnalo una di queste iniziative: https://www.cryptocompare.com/mining/bitcoin-platinum-mining-contract-lifetime-medium/

Affiliarsi ad un mining pool: sebbene personalmente penso che ormai l'affare sia diventato troppo grosso per i "pesci piccoli" c'è ancora la possibilità di comprarsi del HW specializzato attivarlo in casa usando la vostra corrente e la vostra connessione ad internet e aggregarsi ad un pool di altre persone come Voi che condividono la propria potenza di calcolo per realizzarne una complessiva di tutto

rispetto in grado di competere con i big. Non dovete far altro che accendere la vostra “scavatrice” (il vostro PC) affiliarvi ad un pool che vi darà il SW da installare e partire facendo lavorare la Vs macchina il più a lungo possibile (a titolo di esempio segnalo un sito che offre questo tipo di servizio: https://slushpool.com/home/)

Oltre ai succitati virus (ransomware) che vi sequestrano il PC e vi richiedono il riscatto in BitCoin ce ne sono altri , cosiddetti **CPU Miner**, meno invasivi ma altrettanto efficaci: si installano sul vostro pc e lanciano

un programma di mining in background (di cui non siete neanche consapevoli a meno che non vi mettiate a spulciare tutti i processi attivi con Task manager) che “ruba” un po’ della vostra CPU e della Vs connessione ad internet per collegarsi ad altri PC ugualmente “infettati” e formare un mining pool a vostra insaputa (al massimo Vi accorgete di un po’ di rallentamento del Vs PC) ed i cui proventi non andranno certo a Voi!. Anche questo è un modo , illecito, per minare criptovalute.

Come comprare e gestire le criptovalute

A parte soluzioni “dimostrative” come qualche “**bancomat (ATM) del BitCoin**” visto in giro (dove potete inserire la vostra carta di credito decidere quanti Bitcoin comprare e questi vi verranno trasferiti istantaneamente nel vostro e-wallet di cui con lo smartphone potete mostrare il QRcode),


QR
bitcoin
ATM

se volete comprare delle criptovalute ci sono gli **exchange**, delle piattaforme dove è possibile acquistare BitCoin e AltCoin pagandoli con valuta fiat.
Esistono tanti exchange a titolo di esempio ve ne segnalo 4 (a mio avviso i più importanti):

https://www.**kraken**.com/,
https://www.**gdax**.com/ ,
https://**poloniex**.com/ ,
https://www.**bitfinex**.com/ .

Da segnalare che diversamente dalle commissioni per fare

transazioni con criptovalute , qui le commissioni per convertire valuta fiat in Bit/AltCoin non sono trascurabili , intorno al 4%.

Gestire un Exchange è un altro gran modo per fare soldi che fino a pochi anni fa non esisteva!

In realtà di exchange ne esistono tanti e spesso hanno una connotazione geografica (chi lavora più in Cina , chi in USA, in India…); una cosa interessante da notare è che il valore della stessa AltCoin (o meglio il suo controvalore in dollari americani – USD) può variare da

exhange a exchange (in una qualche misura l'exchange può decidere il cambio).

Prima di comprare criptovaluta avete bisogno di un ***e-wallet*** dove tenerli.
Ci sono 2 possibilità :

- tenete il Vs portafogli sulla stessa piattaforma di exchange (esempio GDAX);
- oppure tenete il vostro e-wallet "in locale" residente cioè sul Vs smartphone o PC dove avrete preventivamente installato un apposito programma o App.

Per la cronaca da poco sono disponibili **e-wallet fisici** : non ho approfondito il funzionamento ma se vi interessa date un'occhiata a questo sito: https://www.ledgerwallet.com/produc

.

un e-wallet fisico

Io preferisco tenere i miei AltCoin sulla piattaforma di exchange perché posso gestirli meglio.
Con gestirli intendo controllarne l'andamento e fare anche delle operazioni (**trading**) tipo ritrasformarli in valuta fiat in uno dei seguenti 2 casi :

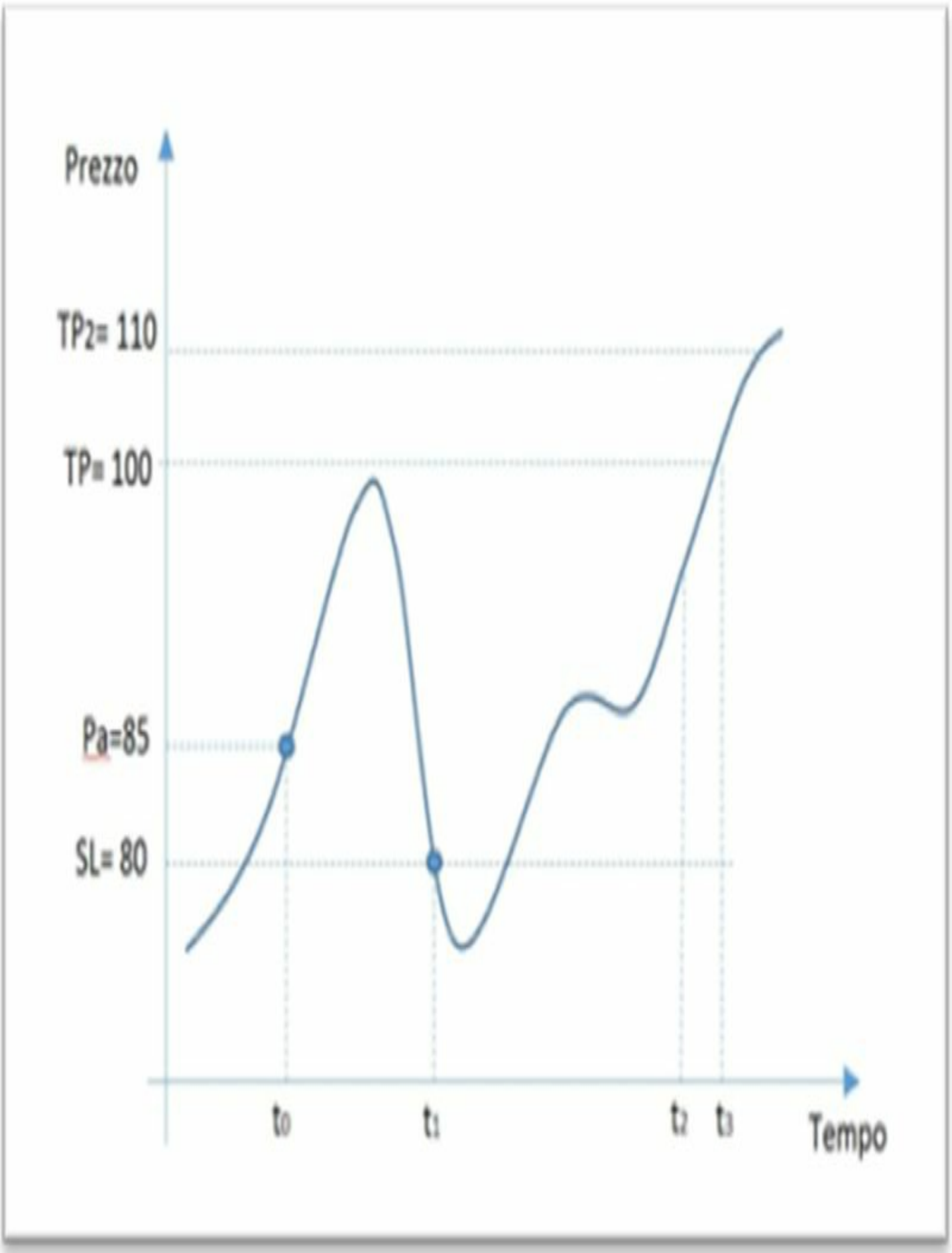
- se secondo me hanno raggiunto un controvalore particolarmente alto (che mi consentirebbe un guadagno perché vendo ad un prezzo maggiore di quello d'acquisto – questa operazione è chiamate banalmente **Take Profit - TP**)
- se secondo me hanno

raggiunto un valore troppo basso (sensibilmente inferiore a quello a cui le ho comprate) e voglio contenere le perdite (**Stop Loss - SL**).

Sulla piattaforma di Exchange posso impostare i valori che desidero di TP e/o SL per cui quando il prezzo raggiunge uno di questi valori la piattaforma **esegue automaticamente** l'operazione impostata (risparmiandomi di stare h24 davanti al monitor a controllare l'andamento del prezzo).

I valori di Take Profit e Stop Loss su valute che oscillano molto nel prezzo

sono molto “delicati” da gestire: poiché il prezzo oscilla molto dovete mettere dei margini , sia lo SL che il TP, abbastanza “larghi” distanti cioè dal prezzo corrente per evitare che un momentaneo repentino ribasso vi faccia scattare un ordine di vendita (SL) facendovi perdere un eventuale lunga risalita (ma al contempo , cosi facendo vi esponete al rischio di una perdita siginificativa).


Prezzo
TP2= 110
TP= 100
Pa=85
SL= 80
t0
t1
t2
t3
Tempo

esempio di impostazione di TP e SL

A titolo di esempio (faccio riferimento al grafico qui sopra) immaginate di comprare all'istante t_0 un certo quantitativo di AltCoin pagandole ad un controvalore in valuta fiat di 85. Un attimo dopo, come è bene fare, fissate le soglie di SL (a 80) e di TP (a 100). Immaginiamo ora un'evoluzione sfavorevole del controvalore del AltCoin: questa inizia a scendere e all'istante t_1 raggiunge il valore di SL e scatta in automatico la vendita : avete perso il 6% del Vs. capitale. Inizialmente siete anche contenti di

questa vendita in automatico perché il prezzo scende ancora e raggiunge un valore minimo di 76 (avreste perso ancora di più) ma poi inizia una risalita che Vi avrebbe portato a prendere il TP inizialmente ipotizzato o magari anche di più (vedendo salire il prezzo consistentemente all'istante t_3 avreste potuto decidere di alzare il TP).

"Ah, se avessi messo uno SL meno stretto , magari a 75 !!"

Questo è trading o se volete , speculazione, che non è una parolaccia, si possono fare dei soldi

(ma anche perderne molti) ma **NON** è il fine per cui sono state create le crittovalute.

Tanto per rimanere in tema di speculazione come detto prima può capitare che la stessa AltCoin abbia **controvalori diversi in diversi exchange**: avendo account su entrambi gli exchange potete anche speculare su queste differenze.

Conclusioni …?

Sicuramente l'idea della **BlockChain** ha un valore intrinseco importante e come abbiamo visto si presta ad essere applicata in vari campi e non solo alle criptovalute (es. Catasto urbano piuttosto che registro automobilistico ed altro ancora). Quindi sicuramente vedo un futuro nell'utilizzo di questa tecnologia.

Per quanto riguarda le criptovalute il futuro è più incerto. Indubbiamente l'idea di una (o più) valute mondiali, decentralizzate , svincolate dai governi , aperte a tutti è affascinante ma personalmente ho il timore che i

“poteri forti” mondiali , che poi sono le grandi banche e chi le controlla, cercheranno in tutti i modi di imbrigliare e piegare al loro vantaggio questa soluzione oppure di annientarla.


HOW WOULD YOU LIKE THIS WRAPPED?
ANTI-TERRORISM
PROTECT KIDS
CORPORATE MEDIA
U.S. GOV'T.
CONTROL OF BITCOIN
JANIK

*Questa vignetta di **Jonik** è terribilmente stupenda*

Sicuramente siamo ancora lontani dal vero utilizzo delle criptovalute come mezzo consolidato per regolare transazioni commerciali : si c'è qualche esempio di POS, qualche esercizio, che più per pubblicità che per altro, accetta pagamenti in BitCoin ma da qui a farla diventare una "normale" valuta c'è ancora di mezzo il mare.


Now Accepting
BITCOINS!

Quando arriveremo a questo?

Le brusche variazioni, la speculazione , l'eccessivo numero di progetti di AltCoin di sicuro non aiuta. Penso e spero che si convergerà presto verso un consolidamento di poche criptovalute molto robuste.
Sicuramente ci aspettano anni interessanti in cui seguire con attenzione l'evoluzione del mondo delle criptovalute.
Quello che posso consigliarvi nel frattempo è di non limitarvi a guardare ma di metterci le mani , aprire un piccolo conto su un qualche

exchange , e giocarci un po’ (piccole cifre, mi raccomando , solo per giocare ;-).

P.S. per suggerimenti , consigli (richiesti o forniti) potete scrivermi a **cloudkiter@gmail.com**

P.P.S. se sei appassionato di tecnologia e vuoi essere introdotto al mondo della **Virtualizzazione** applicata alle **Telecomunicazioni** ti consiglio questa mini guida sempre scritta da me:

https://www.amazon.it/Cenni-NFV-mini-guida-concetti-networking-ebook/dp/B01ABYVROC/ref=sr_1_1ie=UTF8&qid=1514060512&sr=8-1&keywords=cenni+di+nfv

Aloha!