Le criptovalute

19.05.2017

A cura di ***Andrea Poggi***
Analista finanziario indipendente.

Criptovalute: definizione e rischi connessi

Nell'attacco informatico di pochi giorni fa, che ha colpito oltre 100mila organizzazioni e 150 Paesi, si è assistito alla prima richiesta di riscatto in Bitcoin, una criptovaluta.
Ora cerchiamo di capire cos'è una criptovaluta.
È una moneta digitale e viene utilizzata come modalità di scambio attraverso la crittografia per rendere sicure le transazioni e controllare la creazione di nuova valuta.

Sfugge al controllo delle banche centrali e non ci sono intermediari a regolare le transazioni.

Vediamo come funziona il meccanismo che governa i database delle criptovalute.

Una criptovaluta come il Bitcoin consiste in una rete di nodi equivalenti (peers), cioè che possono fungere sia da cliente che da servente verso gli altri nodi terminali (host) della rete .
Ogni nodo equivalente ha un registro della storia completa di tutte le transazioni.

Una transazione è un file che dice: "Tizio dà X Bitcoin a Caio" e viene firmato dalla chiave privata di Tizio.

Dopo la firma, una transazione viene trasmessa in rete, inviata da un peer a ogni altro peer.

La transazione è conosciuta quasi immediatamente da tutta la rete. Ma solo dopo una certa quantità di tempo viene confermata.

Finché una transazione non è confermata, è in sospeso e può essere alterata.

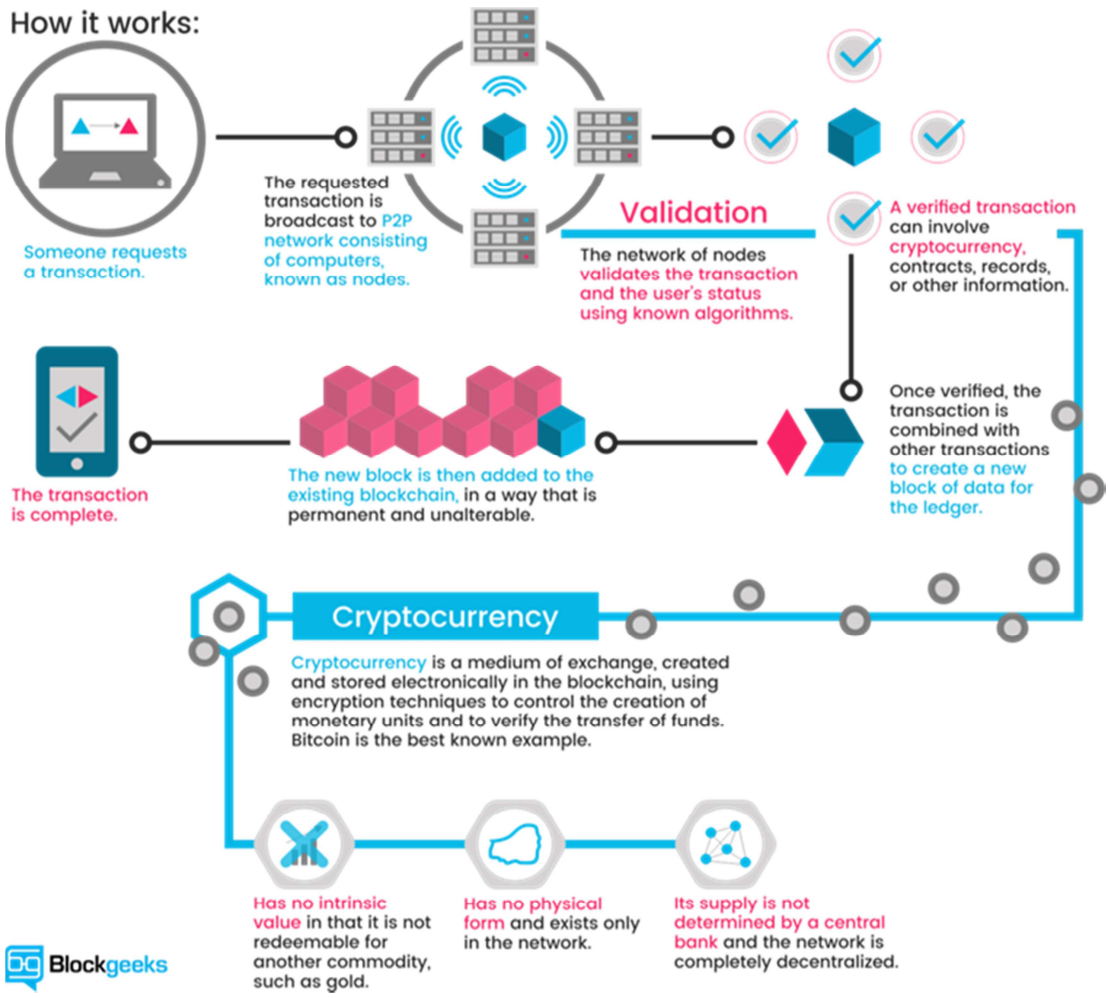
Quando una transazione è confermata, viene scritta nella pietra, cioè non è più alterabile, fa parte di un registro immodificabile di transazioni storiche della cosiddetta blockchain.

Solo i minatori possono confermare le transazioni.

I minatori accettano le transazioni, le "timbrano" come autentiche e le diffondono nella rete. Dopo che una transazione è confermata da un minatore, ogni nodo deve aggiungerla al suo database, così da diventare parte della blockchain.

Per il loro lavoro, i minatori vengono ricompensati con un token della criptomoneta.

Di seguito un'infografica molto ben fatta che spiega tutto il processo



Vediamo adesso la capitalizzazione del mercato delle criptovalute grazie al sito coinmarketcap.com

722 Currencies / 111 Assets / 3793 Markets Market Cap: $61.959.292.650 / 24h Vol: $2.267.250.796 / BTC Dominance: 47.2%

CryptoCurrency Market Capitalizations

Market Cap Trade Volume Trending Tools Search Currencies

All Currencies

All Currencies Assets USD ← Back to Top 100

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$29,226,008,393	$1789.18	16,334,862	$1,036,900,000	-0.64%	4.35%	3.16%
2	Ripple	XRP	$16,229,509,251	$0.423682	38,305,873,865 *	$502,197,000	2.92%	41.55%	129.59%
3	Ethereum	ETH	$8,228,966,361	$89.76	91,678,454	$191,938,000	0.13%	-2.97%	0.27%
4	Litecoin	LTC	$1,183,961,211	$23.15	51,141,707	$124,095,000	0.12%	-1.11%	-32.82%
5	NEM	XEM	$1,013,508,000	$0.112612	8,999,999,999 *	$16,399,800	-5.14%	-1.89%	-1.93%
6	Dash	DASH	$601,606,842	$82.40	7,301,018	$17,033,400	-1.22%	-4.59%	-12.91%
7	Ethereum Classic	ETC	$541,506,330	$5.91	91,700,690	$30,933,500	-0.71%	-6.33%	-8.30%
8	Stellar Lumens	XLM	$470,673,309	$0.049247	9,557,381,231 *	$77,051,800	-0.04%	6.14%	44.34%
9	Monero	XMR	$376,325,174	$26.00	14,474,156	$10,249,500	-1.17%	-4.36%	-11.69%
10	Steem	STEEM	$205,571,342	$0.880037	233,593,976	$7,550,540	12.71%	-0.45%	-3.24%
11	Golem	GNT	$164,233,701	$0.200121	820,672,000 *	$4,612,760	-0.77%	-3.91%	-12.34%

Cosa possiamo notare?

Innanzitutto ci troviamo di fronte ad un mercato in fase embrionale con una capitalizzazione totale di soli 62 miliardi, di cui quasi il 50% è in mano al Bitcoin e circa il 90% del totale viene conteso da sole 5 criptovalute sulle oltre 700 esistenti.

Come potete ben capire questo mercato è molto simile ad una start up che si quota in borsa, ovvero caratterizzata da alta volatilità, che si traduce in elevati guadagni o elevate perdite. A questa caratteristica aggiungeteci il fatto che siamo di fronte ad un mercato non regolamentato, che le truffe sono all'ordine del giorno, come nel caso OneCoin e che quasi ogni giorno nascono e "muoiono" molte criptovalute.

Ultimamente nel web si è venuta a creare una nuova categoria di venditori che chiameremo "I Profeti delle criptovalute". Questi personaggi, utilizzando un marketing di tipo aggressivo, promettono guadagni elevatissimi e incitano tutti ad investire in questo mercato, indipendentemente dalle loro conoscenze in ambito economico/tecnologico e della loro propensione al rischio, e denigrano coloro che ne vogliono star fuori.

Purtroppo, ci sono alcuni punti che i nostri Profeti delle criptovalute si scordano di evidenziare:

1) Quanto sta REALMENTE investendo in questa grande e sicura miniera d'oro/rivoluzione epocale il nostro Profeta?
Scoprirete che non vi metterà più di mille o duemila euro. Nei casi più assurdi non ci investe proprio niente.

2) Il rischio, inteso come volatilità e liquidità di questo mercato come detto sopra

3) Come proteggere il proprio portafoglio di criptovalute. Questa è la parte più importante di tutte, perché molti sistemi di scambio online hanno subito grandi violazioni e non assicurano ancora una sicurezza elevata come quella del sistema banca.
Qualche esempio: Agosto 2016 l'exchange Bitfinex subisce un furto per un valore di 65 milioni di dollari. La piattaforma decise di socializzare le perdite ed i suoi utenti hanno visto ridursi di circa il 36% il loro account.
Anche alcuni account negli Exchange Poloniex e Kraken hanno subito furti nel corso degli anni. Navigando sulla rete potete trovare molte discussioni in cui gli utenti affermano di essere stati ripuliti del loro account sulle sopracitate piattaforme.

Allora quale può essere un metodo per salvaguardare le proprie criptovalute?

- Fare un backup del portafoglio per proteggersi da guasti del pc o errori umani

- Criptare il portafoglio, cioè impostare una password per il ritiro dei fondi. Ci aiuta contro i ladri, ma non contro il keylogger hardware e software

- Il cold storage, ovvero tenere le criptovalute offline al di fuori della rete internet. Esempi: penna USB, Pc scollegato alla rete, CD/DVD, floppy disk o scritto su un pezzo di carta.

Con questo articolo non si vuole demonizzare completamente il mondo delle criptovalute, soprattutto il meccanismo della blockchain, ma semplicemente si vuole cercare di far capire all'utente medio che questo è un mercato nuovo e come tale va studiato molto attentamente sia da un punto di vista economico, tecnologico e soprattutto di sicurezza.

Glossario

http://www.moneyriskanalysis.com/it/glossario.php

General Disclaimer

Le informazioni contenute nel presente documento internet sono frutto di una accurata selezione di fonti da noi considerate attendibili. Non se ne garantisce l'accuratezza o la completezza e nulla, in questo documento, e' stato realizzato per fornire questa garanzia.

MoneyRiskAnalysis non si assume alcuna responsabilita' per i danni derivanti dall'uso d'informazioni contenute in questo documento.

Ne' questo documento, ne' il suo contenuto, ne' una sua copia possono essere modificati in qualsiasi modo, trasmessi o distribuiti senza citare la fonte ovvero MoneyRiskAnalysis.

I componenti del team di MoneyRiskAnalysis possono avere in corso acquisti, vendite o possono detenere posizioni di lungo o breve periodo sul mercato e/o avere interessi collegati ai valori mobiliari menzionati. Quanto espresso circa tali valori mobiliari riveste esclusivamente carattere informativo e non ha carattere di offerta, invito ad offrire o di messaggio promozionale finalizzato all'acquisto, alla vendita o alla sottoscrizione dei predetti valori mobiliari.

MoneyRiskAnalysis non si assume alcun tipo di responsabilita' in relazione alle informazioni fornite da altre fonti alle quali ci si possa collegare attraverso il presente documento. Qualsiasi raccomandazione o opinione espressa su tali altre fonti sono di esclusiva responsabilita' dei titolari di tali fonti e non costituiscono nella maniera piu' assoluta raccomandazioni o opinioni di MoneyRiskAnalsysis. L'eventuale possibilita' di collegarsi ad altre fonti non rappresenta pertanto una raccomandazione o un'approvazione da parte di MoneyRiskAnalysis a quanto contenuto in tali fonti.

L'analisi dei dati e le informazioni contenute in questo documentosono preparate a solo scopo informativo, e non rappresentano un'offerta o sollecitazione di un'offerta a comprare o vendere quote di Fondi di Investimento o di qualsiasi altro strumento finanziario, o a sottoscrivere Contratti di Gestione di qualunque societa'. Questo documento non fornisce nessuna indicazione o consulenza o necessaria a prendere alcuna decisione di investimento.

La performance del passato non e' indicativa di uguali rendimenti nel futuro.

Copyright Money Risk Analysis © Riproduzione riservata