



Stefano Bortolato

dsb005

Informatica Blockchain

Cosa sono le Criptomete

2

Roma 21/6/2023





Criptomete



Se parliamo di criptomenete tutti pensano ai Bitcoin: ma cosa sono?

Le criptomete sono costruite su due principi: il mining e le blockchain.

Ma cosa sono?

Cosa sono le Criptomenete?





Criptomete: cosa sono

Il nome è ingannevole: non sono monete, ma valute alternative, un valore privato di scambio.

Le monete sono proprietà di uno stato, hanno un circuito bancario che le gestisce, hanno il valore facciale e sono valori al portatore immediatamente scambiabili per il valore che riportano.



Criptomete: cosa sono

- sono garantiti dalla nazione
- la nazione decide il valore
- la nazione li conia e distribuisce
- ogni nazione ha una sola moneta corrente.

Criptomete: cosa sono

Nel caso delle criptomonete vengono meno questi principi pertanto:

- sono garantite da un privato (per molte il *garante* è un algoritmo impersonale)
- non hanno un controvalore reale (pochi le cambiano e non è detto che vengano cambiate per il valore nominale)
- non sono circolanti (nella realtà fisica).



Criptomete: cosa sono

Funzionano perché un gruppo più o meno grande di privati le riconoscono, le scambiano e le *spendono*.

Purtroppo esistono molte e molte criptomonete con caratteristiche (e valori) molto diversi. Alcune legali, altre no. Alcune con livelli di sicurezza altissimi, altre no. Le differenze sono molte anche se tutte usano le stesse tecnologie di base: il mining, la blockchain e il funzionamento automatico (non hanno un controllo centrale, non necessitano dell'intervento umano').

Criptomete: cosa sono

Insomma possiamo dire, semplificando la realtà, che le criptomonete (o criptovalute) sono:

- una moneta virtuale
- esistono solo nella loro forma digitale
- vivono di una vita autonoma
- esistono pochissimi *luoghi reali* di scambio che le convertono in moneta corrente.

Come funzionano





Blockchain



Le criptomonete nascono da una rete più o meno ampia di blocchi (computer) reciprocamente interconnessi da una rete (solitamente internet).

Un algoritmo controlla la generazione delle monete in modo che il valore cresca nel tempo.

La rete di interconnessione garantisce il controllo costante della criptovaluta e la conoscenza del possessore in ogni istante.

La generazione delle monete è detta "mining".

L'interconnessione usa la blockchain.

Mining





Blockchain



In prima approssimazione il mining mutua la realtà fisica delle miniere:

- l'estrazione iniziale garantisce una disponibilità costante con un valore non troppo alto
- lo sfruttamento porta progressivamente all'esaurimento del filone causando la riduzione del materiale estratto ed il progressivo aumento del suo valore
- in fine avviene l'esaurimento e la chiusura della miniera
- in quest'ultima fase resta disponibile solo il materiale estratto in precedenza ed il suo valore tendenzialmente sale ed è stabilito dalla contrattazione di mercato.

Blockchain





Blockchain



Le abbiamo viste nella lezione precedente.

Questo tipo di interconnessione tra i blocchi della catena garantisce l'assoluta sicurezza, la totale riservatezza delle informazioni, l'impossibilità di interpolazione e manipolazione e la ridondanza dell'informazione tramite la duplicazione su ogni ogni luogo.

L'adozione delle blockchain offre svariati vantaggi, tra i quali l'altissima resilienza (se si staccano uno o più blocchi le informazioni restano, continuano a essere coerenti e consistenti), la possibilità di usare hardware già esistente (ad esempio il PC di casa o il proprio cellulare) e di avere la certezza comprovata del quando sono state generate le criptomonete, del quando sono avvenute le transazioni e di chi le possiede per tutto l'arco dell'esistenza della moneta.

Considerazioni, pro e contro





Blockchain



La connessione del mining e delle blockchain genera una soluzione *intrigante*.

A favore possiamo considerare:

- il buon funzionamento di tutta la tecnologia è comprovato da anni di funzionamento sul campo (il Bitcoin si fa risalire al 2008)
- la totale digitalizzazione azzerava lo sfruttamento di risorse del pianeta (pietre preziose, metalli di valore, ecc...)
- l'uso di elementi solamente digitali e inalterabili nelle informazioni di chi le possiede e di quando sono avvenute le transazioni rende impossibile il furto e la truffa
- l'automatismo del mining e la bontà dell'algoritmo generativo inibiscono azioni *scriteriate* da parte delle autorità centrali
- l'impiego di strumenti domestici (normali PC, cellulari, ecc...) e la presenza della rete ovunque rende la soluzione democratica e popolare con costo di produzione (apparentemente) nullo o, comunque, già pagato
- le tecnologie impiegate sono di pubblico dominio quindi nessuno ne è il proprietario esclusivo e si possono liberamente creare criptomonete con specifiche caratteristiche.



Blockchain



Vanno, però, anche aggiunte alcune considerazioni a detrimento di queste tecnologie. Alcuni aspetti sono squisitamente tecnici, ma cercheremo di esporli in modo facilmente comprensibile:

- in primo luogo si tratta di una soluzione estremamente energivora. Recenti calcoli, considerando i computer coinvolti, i CED necessari, l'impiego della rete internet mondiale ed un uso diffuso e comune quantificano il consumo totale fino al 30% di tutta la corrente elettrica prodotta al mondo
- l'inalterabilità del sistema significa l'impossibilità di intervento umano sui meccanismi controllati dagli algoritmi rendendo impossibile ogni tipo di *correzione*. Quindi in una congettura di grande inflazione, ad esempio, nessuna autorità potrebbe intervenire per correggere l'andamento spontaneo della svalutazione e dei costi del denaro

- l'uso esclusivo di elettronica e bit rendono questa soluzione:
 - poco *resistente*: se manca la corrente, se le batterie sono scariche non è possibile far nulla, né far vedere di quanto si dispone. Lo stessa riflessione va fatta per la connessione di rete
 - poco *diffusiva*: serve una capillare diffusione delle tecnologie e le singole nazioni devono essere in grado controllare le tecnologie delle criptomonete. Ciò significa che ingeneri e aziende devono essere in forza allo stato, che la corrente deve essere presente ovunque, a disposizione di tutti (e gratis?) e che la copertura di rete sia capillare
 - è *escludente*: coloro che non hanno i requisiti sopra sono automaticamente esclusi. Ma anche chi non può imparare queste tecnologie o non può disporre di quanto serve per costruire le parti è altresì escluso e/o condannato a restare fuori da queste vie

- prima di metterle in uso devono diventare *proprietà* dello stato come per la valuta di carta e di metallo
- l'elettronica è in diversi casi fragile:
 - le probabilità di guasto e o durata nel tempo non garantiscono lunghe durate
 - l'obsolescenza dell'elettronica possono rendere incompatibili le tecnologie più recenti con le più datate
 - non sempre i formati datati (anche di poco) sono usabili dalle tecnologie più recenti

- al momento non abbiamo ancora solide dimostrazioni del valore delle criptomonete a lungo termine
- ci sono problemi circa la scalabilità:
 - ampliare una criptomoneta su larga scala rende le blockchain lente e molto costose
 - il numero di transazioni per secondo sembra ancora troppo basso per essere adeguato alla *vita reale*
- più di qualcuno prevede un aumento molto grande di truffe con i meno esperti
- infine lo stato attuale delle tecnologie e dei quadri normativi rendono possibile l'adozione o la creazione di criptomonete per scopi illegali (cioè fare una criptomoneta per i delinquenti, come è avvenuto con alcuni cartelli del narcotraffico).



Blockchain



A ulteriore conferma della serietà di questi *limiti* va considerato che a oggi non ci sono stati che hanno adottato le criptomonete, né banche nazionali. A onor del vero ci sono un paio di soggetti che hanno fatto questo passo, ma sono rimasti casi isolati e non hanno mostrato dati positivi tali da essere convincenti.

Altri, come l'Unione Europea e il Fondo Monetario Internazionale, hanno mostrato un cauto interesse, ma dichiarano che faranno passi esecutivi e/o valutazioni per decidere solo tra anni.

Quante criptovalute esistono





Blockchain



Prima di fare una conclusione ci potremmo chiedere quante criptomenete esistono al momento.

È moto difficile dare una risposta. Una stima dice che nel 2020 erano 2.677, ma il conteggio è in difetto (ad esempio non rileva le criptomonete del dark web). Inoltre alcune hanno avuto un limitato tempo di vita. Altre sono scomparse per il crack finanziario di alcune *banche* o *piazze di scambio* che lavoravano con le criptovalute (una per tutte si ricordi il crack della FTX a novembre 2022).

Anche questi elementi non alimentano la fiducia verso le criptovalute.

Conclusione





Blockchain



Lo scenario ha preso forma e rappresenta un pool di tecnologie digitali veramente buone, ma che non vengono usate nella realtà per il loro scopo.

Un'attenta osservazione, infatti, mostra che ci sono alcuni aspetti delle criptovalute che non hanno ancora un'adeguata soluzione.

La comunità umana degli specialisti ne ha preso atto e assistiamo, di fatto, a una corale posizione di prudente distanza e non adozione e a una piccola minoranza che né è entusiasta e l'adotta.

Con la prossima lezione vediamo come alcune delle tecnologie impiegate nelle criptomonete sono in uso offrendo e offrono benefici apprezzati.

Domande?

Questions?

Stefano Bortolato

dsb005

Informatica Blockchain

Cosa sono le Criptomete

2

Roma 21/6/2023



