Blockchain e Tecnologia "Distributed Ledger" - Trasformare il Mondo Finanziario

Spesso nelle notizie, Blockchain è destinato a trasformare il modo in cui operano i mercati finanziari, rivoluzionando l'industria in ogni settore.

Elementum Metals: 25/02/2021

25/02/2021

Per accompagnare il nostro webinar sull'emergente settore Blockchain, abbiamo risposto ad alcune delle domande del nostro pubblico, che comprendono domande tecniche, confronti e contrasti, e anche l'influenza dei memi di Internet.
Hai un'altra domanda per il nostro team? Usa la nostra pagina dei contatti per metterti in contatto.

Quali sono le differenze tra Blockchain pubbliche, private e autorizzate?

Blockchain pubblica: È una Blockchain dove chiunque può unirsi e partecipare alle attività della rete Blockchain. Queste blockchain sono decentralizzate, cioè nessuna singola entità ha il controllo sulla rete. Esempi popolari includono Bitcoin ed Ethereum.
Blockchain privata: Una Blockchain che permette solo ai membri autorizzati di unirsi alla rete. L'operatore ha i diritti di sovrascrivere, modificare o cancellare le voci necessarie sulla Blockchain. Qui c'è una centralizzazione. Gli esempi includono Ripple e Hyperledger.
Permissioned/Hybrid Blockchain: Ha proprietà di entrambe le Blockchain private e pubbliche. Stanno diventando sempre più popolari grazie alla loro capacità di assegnare permessi specifici ai vari utenti della rete. Questo varia da piattaforma a piattaforma, e molte sono molto più piccole dei nomi più affermati.

La tesi di investimento dietro la finanza decentralizzata è molto solida - la stampa di denaro senza precedenti da parte delle banche centrali porterà probabilmente allo svilimento, e una riserva di valore non-fat è un ottimo modo per proteggersi da questo. La mia domanda è: perché Blockchain? Quali vantaggi ha contro altre reti di pagamento sicure? Nel caso di Bitcoin, sembra goffo - ad alta intensità di energia, storia ostinata (mercato nero),

ed il fatto che ogni transazione deve essere verificata da tutti nel mondo sembra inefficiente?

Una grande domanda, con un paio di componenti a cui rispondere. Innanzitutto, perché usare Blockchain per i pagamenti? Blockchain è immutabile, democratica, decentralizzata e scritta in un codice che non può essere alterato. Questo le dà un vantaggio inattaccabile rispetto alle altre reti di pagamento sicure (Stripe, Apple Pay ecc.), che sono fondamentalmente centralizzate. Se faccio un pagamento usando una di queste società, quella transazione è verificata, approvata e gestita da quella singola società centralizzata. Questo può essere associato a rischi per la sicurezza (un unico obiettivo centralizzato per gli hacker), a costi più elevati (un unico ente centralizzato può applicare commissioni sulle transazioni) e antidemocratico (un'unica società centralizzata può stabilire i propri termini e condizioni).
Blockchain, d'altra parte, permette di costruire l'infrastruttura da zero. Questo significa che si progetta e si definisce l'economia e l'offerta monetaria una volta sola all'inizio, e nessuno può "stampare" denaro aggiuntivo in una fase successiva - questo aiuta con il vantaggio della "riserva di valore" che menzioni. Bitcoin ha cercato di fare questo (ha una fornitura limitata di 21 milioni di bitcoin che possono essere estratti), ma come dici tu, è associato a molte inefficienze, non ultimo l'uso intensivo di energia richiesto per estrarre le monete (vedi domanda 4, sotto, per saperne di più). Ogni transazione che ha bisogno di essere verificata da altri utenti non dovrebbe essere considerata una di queste inefficienze, tuttavia, ma piuttosto come una forza del sistema - evita la necessità di una piattaforma centralizzata (e quindi vulnerabile e potenzialmente costosa) inerente ad altri sistemi di pagamento sicuri.
Mentre avete il diritto di segnalare la storia del mercato nero di Bitcoin, questo è più un riflesso delle attività dei primi adottanti, piuttosto che un segno di qualche debolezza - pochi potrebbero sostenere che la valuta fisica dovrebbe essere totalmente scontata a causa del fatto che è stata usata per ragioni nefaste in passato.
Cos'altro potrebbe esserci là fuori? Nuovi concetti di pagamento basati su Blockchain stanno emergendo, sia per i pagamenti all'ingrosso che al dettaglio, alcuni sono decentralizzati, altri più centralizzati. Esempi di questi includono:

- Ripple: utilizzato per i pagamenti decentralizzati interbancari e transfrontalieri, regolando le transazioni in 3 -5 secondi in tutto il mondo e gestendo 1.500 transazioni al secondo utilizzando XRP.
- Diem (ex-Libra per la vendita al dettaglio): Un sistema di pagamento Blockchain autorizzato proposto da Facebook.
- CBDCs (Central Bank Digital Currencies): Queste stanno emergendo in tutto il mondo con la Cina che ha lanciato la prima valuta digitale della banca centrale del mondo conosciuta come DCEP, che è una versione digitale dello Yuan, sostenuta dai depositi di Yuan nella Banca centrale cinese.

Quindi, in conclusione, hai ragione nel dire che Bitcoin è un sistema goffo con alcuni inconvenienti evidenti e sempre più pubblicizzati (resta da vedere se possono essere rimossi). Tuttavia, la tecnologia che sta alla base di Bitcoin, cioè Blockchain, permette un'efficienza molto maggiore rispetto ad altri sistemi di pagamento più familiari che sono stati sviluppati negli ultimi due decenni circa.

Qual è la distinzione tra "proof of stake consensus" usato apparentemente nelle nuove blockchain/criptovalute e quello usato per bitcoin ("proof of work")?

Il meccanismo Proof of Work (PoW) è usato per rendere sicura la Blockchain di Bitcoin e per creare il consenso. Funziona facendo in modo che tutti i nodi (partecipanti/dispositivi) della rete risolvano algoritmi matematici (per verificare la legittimità delle transazioni), e il primo nodo che trova una soluzione viene premiato (la ricompensa del minatore è un certo numero di Bitcoin). PoW fornisce ulteriori benefici di sicurezza alla Blockchain, in quanto rallenta la creazione di un nuovo blocco a circa 10 minuti, il che significa che se un hacker vuole manomettere un blocco, deve rifare il PoW di ogni blocco nel sistema, che è quasi impossibile da fare a causa delle scale coinvolte.
Gli aspetti negativi associati al PoW tuttavia sono i seguenti:
i. A causa delle ricompense per l'industria mineraria, vengono create imprese d'industria mineraria sempre più grandi, consumando grandi quantità di elettricità (è stato recentemente riportato che l'industria mineraria di Bitcoin consuma tanta energia quanto l'intera Argentina).
ii. Per aumentare le possibilità di successo delle miniere, i minatori si raggruppano in "pool di minatori" che in realtà rendono la Blockchain più centralizzata, minando così l'ethos decentralizzante dell'impresa.
Nei forum online nel 2011, è stato proposto un nuovo algoritmo chiamato Proof of Stake (PoS), dove invece viene utilizzato un processo di elezione in cui un nodo viene scelto casualmente per convalidare il blocco successivo. Invece dei minatori, utilizza validatori che coniano/forgiano nuovi blocchi. Per diventare un validatore, il nodo deve depositare un certo numero di monete come puntata (pensa a questo come a un deposito di sicurezza). Più "depositi", più alta è la possibilità che tu sia un validatore. Questo è più equo di PoW, in quanto PoW favorisce coloro che hanno economie di scala in termini di capitale minerario/energia, mentre le barriere all'ingresso con PoS sono relativamente più basse.

Per assicurare che si verifichino convalide corrette, i validatori perderanno una parte della loro quota se approveranno transazioni fraudolente. Finché questa perdita è maggiore della loro ricompensa, il consenso regge attraverso la motivazione del prezzo. Infine, PoS è più decentralizzato in quanto blocca i pool di minatori ed è più economico creare un nodo all'interno della blockchain PoS.
Gli aspetti negativi associati a PoS tuttavia sono i seguenti:
i. Attacchi del 51%: A differenza di PoW dove si deve acquisire il 51% della rete, per PoS si deve acquisire il 51% del market cap della valuta, che per le piccole criptovalute market cap potrebbe essere relativamente facile.
ii. Gli algoritmi PoS non sono completamente casuali in quanto dipendono dalla partecipazione dei validatori (che possono favorire gli individui più ricchi).
Al momento, PoS non è comune, anche se si prevede che il sistema sarà utilizzato in Ethereum 2.0, che sarà rilasciato nel 2021.

Qualche commento su Tesla e la loro decisione di comprare Bitcoin piuttosto che un'altra forma di asset digitale? È pura speculazione?

Da una prospettiva aziendale Tesla, potrebbe essere una conseguenza dei tassi di interesse negativi e della gestione della tesoreria che cerca modi per diversificare l'allocazione degli asset. Dal punto di vista di Musk è difficile dire quale sia stata la sua motivazione più profonda. Ha investito sia in Bitcoin che in Dogecoin, causando aumenti di prezzo in entrambe le criptovalute dopo il suo annuncio degli acquisti su Twitter.
Musk è seduto in un posto speciale, può sperimentare tecnologie e concetti con conseguente risposta positiva del mercato, indipendentemente da qualsiasi ragione economica o commerciale. Gli analisti di Wedbush Securities hanno stimato che Tesla ha già fatto 1 miliardo di dollari di profitto dal suo investimento in Bitcoin. L'azienda è sulla traiettoria di fare più dai suoi investimenti in Bitcoin che i profitti dalla vendita di veicoli elettrici nel 2020.
Per quanto riguarda la scelta di Bitcoin e Dogecoin rispetto ad altre criptovalute, le cose sono meno chiare. Bitcoin è di gran lunga la scelta più grande e più ovvia, forse quindi percepita come meno rischiosa, mentre Musk stesso ha spesso coltivato un'immagine di essere inserito nella cultura online - Dogecoin, essendo nato inizialmente da memi di internet (oltre ad avere una capitalizzazione di mercato ben dentro i miliardi) potrebbe essere interpretato come parte di questo. Vale la pena notare, tuttavia, che lui non è l'unica figura di alto profilo a sostenere pubblicamente la criptovaluta: voci rivendicate dai musicisti Gene Simmons e Snoop Dogg hanno anche contribuito a guidare l'interesse.

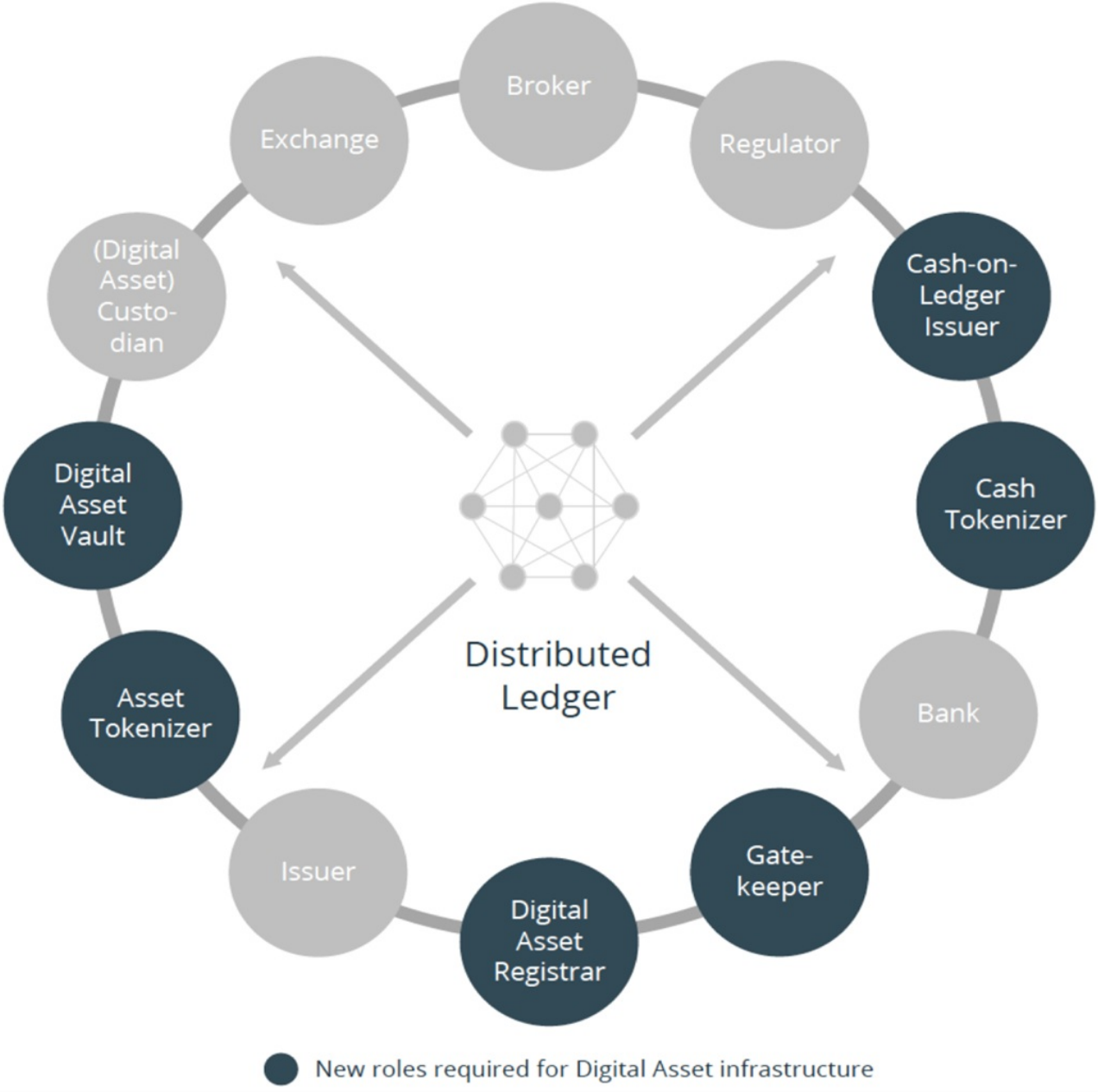
Qual è la capitalizzazione di mercato dei protocolli di finanza decentralizzata?

A Febbraio 2021, la capitalizzazione di mercato è di 45 miliardi di dollari.

In che modo il ruolo della Tecnologia "Distributed Ledger" (DLT) nei mercati dei capitali differisce dalle borse tradizionali?

Le borse tradizionali presentano un modo bilaterale e sequenziale di comunicazione e scambio di informazioni. La DLT ha già iniziato a ristrutturare le catene di valore dei mercati dei capitali cambiando i presupposti tradizionali e creando fiducia senza operazioni umane.
La DLT può aggiungere valore ai mercati dei capitali attraverso:

La DLT può aggiungere valore ai mercati dei capitali attraverso:
i) Informazioni condivise tra tutti i partecipanti - riducendo i costi di riconciliazione
ii) Contratti intelligenti - eliminando il rischio di controparte
iii) Traccia di controllo immutabile - miglioramento della regolamentazione
iv) Processi digitalizzati - Consentendo l'automazione pura
La maggior parte dei ruoli tradizionali nei mercati dei capitali come i broker, gli scambi e i depositari continueranno ad esistere in un mercato dei capitali DLT. Tuttavia, nuovi ruoli saranno richiesti insieme a quelli tradizionali. Il diagramma qui sotto illustra questo:



Fonte: Tokentrust AG
Le caratteristiche, le proprietà e le entità modificate includono:

- Custodi che hanno cassaforti di beni digitali dove salvaguardano le chiavi private necessarie per accedere ai portafogli di criptovalute e quindi ai beni.
- **Digital Asset Vault**, il software acquistato dai depositari per fornire la conservazione delle chiavi private.
- **Asset Tokenizer**, che consente processi legalmente conformi fornendo contratti intelligenti al fine di tokenizzare gli strumenti finanziari per conto dell'emittente.
- **Digital Asset Registrar,** che facilita il consenso tra le diverse parti interessate e governa il Digital Asset Registry attraverso la convalida di tutte le transazioni sulla piattaforma.

- **Gatekeeper**, che concede/limita l'accesso alla piattaforma tramite controlli KYC/AML.
- **Cash on Ledger Issuer**, che gestisce gli smart contracts e avvia le transazioni fiat attraverso la banca e convalida le transazioni cash on ledger.
- **Cash Tokenizer**, che fornisce l'infrastruttura per emettere il 100% di cash on ledger collateralizzato per il regolamento della catena (consegna rispetto al regolamento del pagamento).

Un esempio del mondo reale è quello della Borsa della Thailandia che sta creando una piattaforma di tokenizzazione e scambio di asset gestita da DLT. Informazioni adattate da qui.

Che ruolo hanno le valute digitali emesse dalle banche centrali (CBDC) per la "tokenizzazione" dei mercati dei capitali?

La "tokenizzazione" risponde alla necessità di un nuovo formato dominante per rappresentare beni e diritti, portando una maggiore flessibilità e liquidità. Dato che la moneta della banca centrale rimane preferita per le grandi transazioni, le CBDC rimangono un mezzo promettente per lo scambio basato sui token. Operano in modo simile alle valute forti ma con opportunità digitali. I CBDC possono integrare la valuta in circolazione e servire come alternativa ai pagamenti con carta. Inoltre, possono facilitare formati di pagamento diversificati e consentire lo scambio di token in moneta di banca centrale, creando ulteriore fiducia nella "tokenizzazione". Infine i CBDC facilitano le relazioni di pagamento diretto, riducendo la necessità di intermediari e quindi riducendo significativamente gli alti costi di transazione che tradizionalmente vediamo nei mercati dei capitali.

Compilato da Jay Kumar, NTree International, per Metal.Digital.