PROJECT WORK:

FINANZA DECENTRALIZZATA E MONETE DIGITALI

Jacopo Pezzi
Valerio Sagazio
Andrea Di Martino
Luca Marangione
Matteo Lozzi

introduzione:

THE CHANGING WORLD ORDER

Ray Dalio

Introduzione

Ray Dalio, con il documento pubblicato il 23/04/2020 annuncia l' arrivo di «un nuovo ordine mondiale»

L' oggetto chiamato in causa è il sistema finanziario per come lo conosciamo oggi.

COS'E' LA MONETA?

- STORIA

La moneta è una «tecnologia» che

nasce per liberarci dall' inefficienza del baratto: non sempre chi voleva vendere era interessato alla contropartita che il potenziale acquirente era disposto a cedere.

La moneta diventa uno «store of value» usato come mezzo di scambio per accedere ad altri beni.

- INTERPRETAZIONE

L’ uomo percepisce la moneta come ricchezza.

Infatti, tendenzialmente, si è soliti pensare al «ricco» come colui che possiede molto denaro.

Cosa potremo comprare con il denaro se nessuno dovesse essere disposto a venderci qualcosa?

La moneta è rappresentazione della ricchezza, un credito e altro ancora ma, di certo, non è ricchezza.

La vera ricchezza sono gli assets.

- LE CONSEGUENZE

La persona che possiede più denaro spenderà di più perché avrà la sensazione di essere più ricca e i governatori non resisteranno a far «arricchire» i propri elettori.

Tutto questo sarà sostenibile solo per un periodo di tempo circoscritto.

Come precisa Dalio, prevedere ciò che ci attende è assai difficile perché necessita competenze non solo economico-finanziarie ma anche storico-sociologiche.

Lui prova comunque a farlo…

DEBITI &CREDITI

- LE BASI

Sappiamo bene che la nostra economia è alimentata dal credito.

Infatti vi sono unità in surplus che finanziano unità in deficit: le prime otterranno «assets» e le seconde «liability».

Ciò scaturisce un circolo virtuoso se, e solo se, tutti i debitori sfruttino la leva per aumentare la produttività.

I principali problemi possono essere racchiusi in due punti:

1)la produttività ha un limite

2) alcuni di quelli che assumono debiti lo fanno per aumentare il consumo •

CICLO DEL DEBITO A BREVE
&
CICLO DEL DEBITO A LUNGO

Come accennavamo prima la politica non si sottrarrà al compito di rendere più «ricchi» i suoi elettori con misure di politica fiscale espansive.

Questo farà sentire le persone più ricche, invogliandole a spendere sempre più denaro. Spesso a questo si aggiunge il ricorso al debito finalizzato al consumo, soprattutto quando i tassi di interesse sono ridotti.

Si innescherà così un ciclo a rialzo che causerà sopravvalutazioni di valori mobiliari e immobiliari. Questo rappresenta il «ciclo del debito a lungo termine» perché dura , a detta di Ray Dalio, tra i 50 e i 100 anni, motivo per cui è spesso difficile individuarlo (perché spesso una persona non assiste a più cicli).

La richiesta di denaro da parte del privato genererà, di riflesso, un maggiore indebitamento dello Stato e una quantità di moneta stampata superiore.

Se la produzione non dovesse aumentare, questo processo genererebbe un processo inflattivo causando una perdita di potere di acquisto della moneta. Questo fenomeno, affiancato alla sopravvalutazione di molti assets, farà in modo che sempre più persone vorranno detenere assets e non denaro.

HARD MONEY & EASY MONEY

Nel frattempo, le istituzioni che stampano moneta si rendono conto che il sottostante della moneta, il vero «value», è terminato (nel nostro caso l' oro) ma, non potendo smettere di stampare valute, promettono che il denaro stampato avrà sempre un certo potere d' acquisto, mantendo sotto controllo l' inflazione attraverso il regolamento dei tassi.

Questo è un esempio di «easy money», moneta che può essere stampata all' infinito. Questo è la causa della distruzione. La moneta difficile da stampare invece viene definita «hard money».

CICLO DI DEBITO A BREVE TERMINE

Le banche centrali, per mantenere l' inflazione controllata, aumenteranno i tassi di interesse sui prestiti generando una contrazione della domanda.

Questo causerà non pochi problemi ai debitori che dovranno restituire le quote.

Molti tra privati, aziende e istituzioni non saranno in grado di saldare i debiti andando così a generare un effetto domino sul sistema creditizio che inevitabilmente si bloccherà, causando fallimenti e svalutazioni di vari assets.

Questo fenomeno dura circa 10 anni.

DECLINO

A questo punto molti prestatori di fondi pretenderanno il loro denaro che invece il debitore non avrà. Questo potrebbe avvenire anche tra correntisti e banche (run bank):

nel momento in cui le banche non potranno restituire le somme dovute le persone perderanno la fiducia nella moneta usata e bisognerà trovare una soluzione onde evitare rivolte e guerre.

CHI SOFRIRA' DI PIU' ?

I primi stati ad accusare il colpo saranno coloro che non hanno in mano la produzione di moneta e che non potranno restituire alle BC il ricevuto. Sono quindi tutti gli stati che adottano l'euro e il dollaro e che non appartengono ne all' Unione Europea ne all' America (le transazioni avvengono al 55% in dollari, al 25% in euro e il 10% in yen).

Dalio dice che in situazioni di questo tipo, la forza monetaria sarà più importante della forza armata.

RISOLUZIONE

A questo punto sarà necessario ricreare fiducia in una moneta, forse nuova, per far in modo che avvengano gli scambi nell' economia e che si generi un rapporto win - win.

Il ciclo ripartirà da un hard money, come ad esempio l' oro, che successivamente verrà trasformato in un sound money per questioni di praticità. Il problema nasce quando i sound money, a causa dell' eccessivo uso, torneranno easy money.

AD OGGI…

Secondo Dalio, oggi siamo al termine di un ciclo di breve termine iniziato nel 2008, che da recessione si sta trasformando in depressione, accelerata poi dal calo della produttività dovuta al corona-virus.

«I furbi investono in hard money»

CIT. RAY DALIO

…Quale sarà la prossima?

BLOCKCHAINS & CRIPTOVALUTE

Tutti i sistemi economici per potersi sviluppare, richiedono **fiducia**: ciò significa affidarsi a **istituzioni** che hanno la possibilità di monitorare gli attori coinvolti e di utilizzare l'esecuzione dei contratti per facilitare gli scambi tra le controparti.

In ogni caso, il coinvolgimento e l'affidamento ad una terza parte presenta alcuni potenziali **svantaggi**, come l'aumento del costo delle transazioni, il tempo più lungo per eseguire la transazione e il rischio di cybersicurezza.

Per migliorare questo particolare quadro di riferimento, nel 2008 è stata creata una tecnologia innovativa: la tecnologia **blockchain** è un modo per costruire un **libro mastro distribuito sano, sicuro e trasparente**.

Il **libro mastro** è una tecnologia di contabilità in grado di registrare le transazioni e la proprietà di specifici beni: il libro mastro **centralizzato** è stato digitalizzato a partire dalla fine del XX secolo.

La tecnologia blockchain è strutturata come un **libro mastro distribuito decentralizzato**, potenzialmente più efficiente in termini di costi e sicurezza.

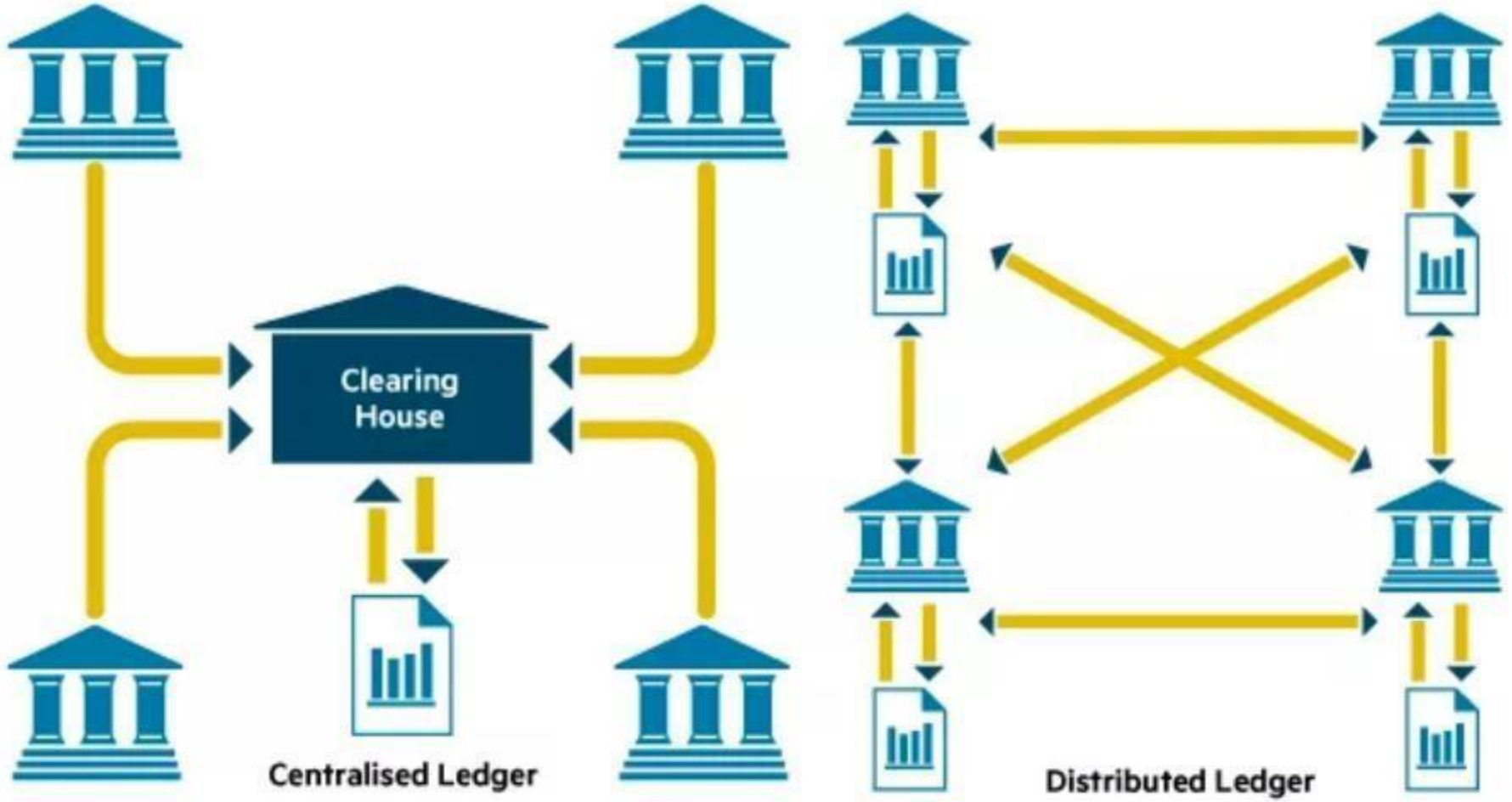
La blockchain è un **database di** informazioni **successive** concesse con metodi di prova crittografica, che offre un nuovo metodo per creare, scambiare e tracciare la proprietà dei beni su base peer **to peer.**

THE DEFINITION OF DISTRIBUTED LEDGER

Il libro mastro distribuito è un concetto che può essere interpretato come un'evoluzione dal libro mastro centralizzato passando per il libro mastro decentralizzato.

- Il **Ledger centralizzato** rappresenta il libro mastro tradizionale, quindi basato su un rapporto **uno-a-molti**, dove tutto deve essere gestito facendo riferimento ad una struttura o autorità centralizzata (la fiducia è nell'**autorità**).
- Il **Ledger decentralizzato** ripropone la logica della centralizzazione a livello locale con alcuni centri organizzati come satelliti sempre sotto forma di uno-a-molti: il singolo soggetto centrale viene sostituito da molti **soggetti locali** (Trust è in un soggetto locale).
- **Distributed Ledger** si basa su una logica distribuita, dove non ci sono più centri ma la governance e la fiducia si instaura e si costruisce attorno alla **fiducia tra soggetti**, che sono utenti ma che occupano anche un ruolo di governance: nessuno come possibilità di prevalere perché il processo decisionale passa rigorosamente attraverso il **consenso generale di** tutti gli utenti per le loro doppie funzioni.

All'interno della tecnologia delle catene di blocchi, i soggetti coinvolti sono chiamati **nodi** e svolgono un ruolo cruciale nel funzionamento della catena di


Clearing
House
Centralised Ledger
Distributed Ledger

Blockchain permette la creazione e il coordinamento di un **complesso database distribuito,** per la sincronizzazione delle transazioni condivisibili tra molti nodi di una rete.

E' strutturato in blocchi collegati tra loro in modo che ogni transazione avviata sulla rete sia validata dalla rete stessa o, meglio, dai **nodi** stessi:

- **vedi le transazioni** degli altri nodi
- **verificare** che tutte le transazioni siano coerenti
- **approvare** le operazioni di ciascuna operazione.

Tutto questo meccanismo crea una **rete** che permette la **tracciabilità** di tutte le transazioni: ogni blocco è anche un **archivio** per tutte le transazioni così come la storia di ogni transazione viene scaricata da ogni nodo.

Per essere approvata dalla rete e per essere presente su tutti i nodi della rete, la transazione deve essere assolutamente **immutabile** se non attraverso la ripetizione della stessa a tutta la rete e solo dopo aver ottenuto nuovamente l'approvazione: per questo motivo sono **immutabili**.

La blockchain costituisce un nuovo protocollo di comunicazione utile alla creazione e gestione di una tecnologia basata sulla logica del **database distribuito**.

La blockchain è organizzata in modo da **aggiornarsi automaticamente su ogni cliente** partecipante alla catena: ogni operazione effettuata deve essere **confermata** da tutti i singoli anelli della catena, esaminando un pacchetto dati per volta, definito da chiave privata, che viene utilizzato per firmare le transazioni garantendo l'identità di chi le ha autorizzate.

Il database è gestito da un **Database Management System** (DBMS) in cui le strutture dati non sono persistenti nella stessa macchina ma su più computer (nodi).

Quindi il database può essere localizzato su più computer che si trovano nello stesso luogo fisico o distribuiti in una **rete di computer,** collegati attraverso un sistema distribuito.

Qualunque sia la tecnica di divisione dei dati scelta (frammentazione verticale o orizzontale),
deve necessariamente garantire due condizioni:

- **Completezza**: ogni elemento della tabella deve essere presente in almeno un frammento.

THE PROOF-OF-WORK

Il consenso, nella struttura intrinseca della catena di blocchi, gioca un ruolo fondamentale in quanto l'intera catena di blocchi viene aggiornata solo dopo aver ottenuto il consenso da ogni nodo: solo dopo il consenso, i nodi vengono aggiornati uno per uno con la nuova versione.

Ma qual è il legame tra il concetto di soluzione di un problema e quello di **fiducia**, con il consenso?

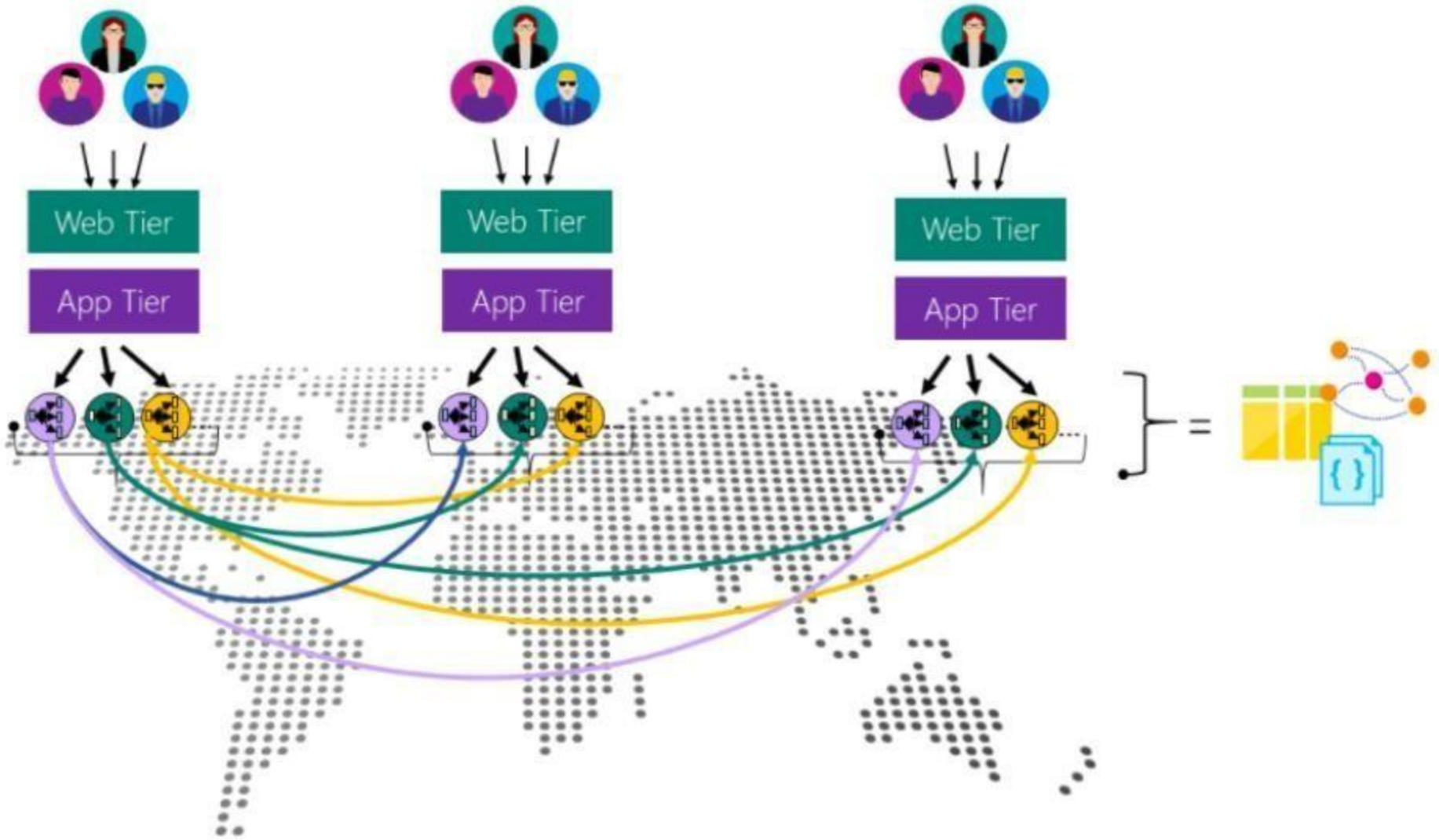
Quando si vuole **aggiungere una transazione** al blocco e chiuderlo, è necessario risolvere un problema matematico, un calcolo che si rivela complicato.

Questi calcoli, chiamati **prove di lavoro**, sono utilizzati per stabilire con certezza la l'**autenticità** della transazione e servono anche a costruire la fiducia nella comunità.

I partecipanti alla validazione non si conoscono quindi la prova del lavoro rappresenta un modo concreto per costruire un **rapporto di fiducia**.

Questa fiducia ha due significati:

- fiducia nel **sistema**
- fiducia nei **nodi**.


Web Tier
App Tier
Web Tier
App Tier
Web Tier
App Tier

FIDUCIA E BLOCKCHAINS

Quando c'è la necessità di una **nuova transazione** da approvare ed eventualmente registrare nel database distribuito, questa transazione viene **unita ad altre per creare un blocco**

È necessario, quindi, che ogni volta che si costituisce un nuovo blocco si compia contemporaneamente un **complesso calcolo crittografico**

Questa operazione si chiama **estrazione mineraria,** per far sì che questo meccanismo sia condiviso e realizzato dal maggior numero possibile di persone, **tutti possono essere minatori** (cioè pubblici block chain)

Il meccanismo che si crea tra i minatori è una vera e propria concorrenza: c'è un **incentivo** a sfruttare la loro potenza di calcolo

I partecipanti accettano un nuovo blocco quando si verifica che tutte le transazioni che lo compongono sono valide: se c'è un'**anomalia** in una di esse, l'intero **blocco** si ferma

PUBLIC AND PRIVATE BLOCKCHAINS

- **Blockchains pubblici**: detti anche **registri non autorizzati,** sono **aperti** a tutti coloro che non sono soggetti ad un'autorità o ad un sistema di riferimento e sono fatti apposta per non essere controllati da nessuna autorità centrale.
- **Private Blockchains**: chiamano anche i **libri contabili autorizzati**, hanno alcune specificità riguardanti il modo in cui gestiscono le informazioni sulle transazioni che consentono di essere gestite da un'**autorità** centrale.

In quest'ultimo caso, tuttavia, il concetto di **consenso condiviso** non è pienamente raggiunto ed è il punto focale di divergenza tra i due tipi di catene a blocchi.

GLI SMART CONTRACTS

Gli **Smart Contracts** sono un sistema di **trasferimento di diritti** in esecuzione di un algoritmo matematico

La **particolarità** è che si tratta di un **pezzo di codice** memorizzato in una catena di blocchi, attivato da transazioni effettuate su quella catena di blocchi e che legge e scrive i dati sulla catena di blocchi stessa.

I Smart Contracts formalizzano gli elementi di un accordo ed **eseguono automaticamente i termini** dello stesso quando le **condizioni** previste dall'accordo sono soddisfatte.

Una volta impostato e lanciato lo Smart Contract nella blockchain, quando si verificano le condizioni, la conseguenza sarà automaticamente eseguita: diventa quindi fondamentale la **verifica** della condizione (**trigger point**).

Se la **condizione** è un termine interno alla blockchain allora la sua verifica è certa e immediata ma la condizione dell'evento può derivare da **fonti pubbliche o istituzionali**: in questo caso il codice del contratto farà scattare l'esecuzione da questi controlli.

Quando una "**conferma estesa**" da una fonte al di fuori della catena di blocco è necessaria, è necessario per un internet Oracle.

- Cos'è l'Oracle ? **Oracle** è il punto di contatto tra la realtà (digitale) e la blockchain dove deve essere eseguita l'esecuzione di un Smart Contract

L'esecuzione di un Contratto Smart non dipende dalla volontà delle parti: la **forza vincolante** di tali contratti non deriva dalla legge ma infatti dal codice che li predispone.

L'attenzione deve essere spostata verso la sua **codifica**: lo **scopo ?** Quello di prevenire le violazioni delle parti e di eliminare qualsiasi controversia relativa all'esecuzione del contratto.

Gli Smart Contracts sono già **implementati** in diverse aree: oltre a Ethereum, gli Smart Contracts sono stati applicati per l'esecuzione di **derivati finanziari** o per la **vendita di beni** su internet (come Open Bazar).

BLOCKCHAINS E MERCATI DEI CAPITALI

L'obiettivo dei Blockchains è quello di creare un'**unica versione della verità**, utilizzata da tutti gli operatori del mercato

Potrebbe consentire **nuovi processi di settore**, basati sull'utilizzo di dati trasparenti in tempo reale, sul regolamento immediato delle transazioni e sull'espansione dei contratti intelligenti a esecuzione automatica, con una logica di business integrata nel libro mastro.

La **trasparenza dei dati in tempo reale** creerebbe importanti vantaggi operativi per gli utenti, eliminando la necessità di arricchire i dati

1) Potrebbe ridurre l'**esecuzione e il rischio di credito**
2) Mentre i **beni non tipicamente negoziati** potrebbero essere più facilmente considerati come fonti affidabili di valore

I clienti ne trarranno il massimo beneficio, grazie alla riduzione dei costi di negoziazione sui mercati dei capitali e di servizio titoli, mentre i **dealer saranno** più bravi a reperire liquidità o ad assumere rischi

GLI OSTACOLI ALL'ADOZIONE

- **Scalabilità della tecnologia**: sarà necessario gestire un set di dati molto più grande se si vuole sostituire una parte fondamentale del sistema del mercato dei capitali
- **Regolamentazione e legislazione**: le innovazioni nei mercati finanziari richiedono la benedizione esplicita delle autorità di regolamentazione con largo anticipo.
- Occorre quindi concordare un protocollo di consenso comune, che vada oltre i requisiti geografici territoriali attualmente esistenti in materia di conservazione fisica dei dati come fonte d'oro.
- **Standard e governance comuni**: sarà necessario l'allineamento dell'industria su alcuni punti, come l'adozione di un libro mastro aperto o autorizzato o di principi per interagire con il libro mastro, nonché un chiaro accordo su come gestire la catena di blocco.
- **Gestione dell'anonimato**: richiederà un'attenta gestione dei record delle chiavi, mantenuti separatamente per ogni partecipante, per decifrare e consultare i dati personali.

PRIMA E SECONDA OPERAZIONE DI REGISTRAZIONE

Type	Use case	Capital markets examples	Other industry examples	Rationale for adoption
First order adoption – works as standalone	• Tokenising assets not currently on a common ledger (new blockchains or tokens on Bitcoin)	• Pre-IPO equities • Syndicated loans • Depository receipts	• Physical objects e.g. diamonds, paintings	• Proof of ownership/ provenance • Settlement efficiency
	• New blockchains to share data between participants	• KYC data sharing • Collateral ledger to support efficient margining • Reference and market data	• Supply chain data invoicing • Trade finance	• Efficiency of information collection
	• New blockchains to process transactions	• Corporate finance bookrunning • Fund portfolio management	• Inter-bank blockchain to support cross-border banking payments • Intra-bank blockchain to support cross-bank accounting	• Disintermediation of actors • Simplified data and infrastructure
Second order adoption – reliant upon critical mass of assets on blockchains	• Monitoring of richer datasets	• Concentration monitoring • Market surveillance • Pricing data	• Trade flows, transit data	• Powerful understanding of data
	• Processing using blockchains	• Securities servicing • Regulatory reporting		• Efficient processing capabilities

BITCOIN:ORIGINE E DEFINIZIONE

Il 31 ottobre 2008, il creatore della prima criptovaluta, con lo pseudonimo di **Satoshi Nakamoto,** ha pubblicato il libro bianco «Bitcoin: A Peer-to-Peer Electronic Cash System».

Egli definisce il Bitcoin come «**un sistema di pagamento elettronico** basato sulla prova crittografica invece che sulla fiducia, che permette a due parti interessate di effettuare transazioni direttamente tra loro senza la necessità di una terza parte fidata».

Due mesi dopo, «il **blocco della genesi**», il blocco originario di ogni catena di blocchi, fu generato.

Il Bitcoin è la prima e più grande moneta digitale funzionante: un sistema monetario e di pagamento basato su internet che **non richiede intermediari**, come le banche, per l'elaborazione dei pagamenti, basando il tutto sulla tecnologia del blockchain.

Diverse migliaia di aziende attualmente accettano Bitcoin in pagamento, la stragrande maggioranza è legata ai prodotti web: i pagamenti possono essere effettuati in qualsiasi momento e tra due utenti qualsiasi in tutto il mondo.

Gli utenti, inoltre, possono ricevere bitcoin come ricompensa per la verifica di transazioni.

FUNZIONAMENTO E CARATTERISTICHE(1)

Un utente che desidera effettuare un pagamento emette un'istruzione di pagamento in un **distributed ledger**, in modo che altri utenti possano verificare la transazione, ad esempio che il pagatore possieda la valuta necessaria.

Utenti speciali, chiamati **minatori**, raccolgono blocchi di transazioni e competono tra loro per verificarli: i minatori che verificano con successo un nuovo blocco ricevono sia bitcoin di nuova creazione, sia l'eventuale commissione di transazione offerta dalle parti coinvolte.

Il bitcoin è creato dal "nulla", non c'è un'**istituzione che ne** controlli l'approvvigionamento e nessun **governo** che ne possa discrezionalmente beneficiare: la "distribuzione programmata dei bitcoin" è garantita da un **algoritmo**, che si basa sulla potenza computazionale del software offerta dagli utenti.

Le **caratteristiche** principali del Bitcoin sono:

- **Decentralizzazione**, in quanto progettata in modo che qualsiasi persona, azienda o macchina che sia coinvolta in una transazione diventi parte di una rete globale, permettendo, in caso di chiusura imprevista di alcuni nodi, di far fluire comunque il denaro.
- **Velocità**, in quanto una transazione, indipendentemente dalla posizione geografica delle parti, viene validata e trasmessa, in media, ogni 10 minuti.

ANONIMATO E TRASPARENZA

I fattori di **anonimato** per Bitcoin sono principalmente due: **primo**, a differenza di un conto bancario e di altri sistemi di pagamento, gli indirizzi Bitcoin non sono legati all'identità degli utenti; **secondo,** nemmeno le transazioni sono legate all'identità degli utenti.

Chiunque sia in possesso della **chiave privata** di un indirizzo specifico può utilizzarla per effettuare la transazione: gli indirizzi Bitcoin possono essere collegati a identità reali se queste sono usate in combinazione con gli indirizzi Bitcoin.

La **trasparenza** del Bitcoin è alla base della tecnologia blockchain e si traduce in piena trasparenza delle transazioni: tutte le operazioni sono memorizzate su di essa e possono essere controllate da chiunque.

Il Bitcoin non è una moneta a **corso legale**, quindi i commercianti non sono obbligati ad accettarlo come veicolo di pagamento, cosicché la sua probabilità di diffusione è interamente legata alla volontà dei commercianti di accettarlo.

La **risoluzione delle controversie** potrebbe, seppur di rado alla luce di quanto detto, costituire un problema: a causa della mancanza di un'autorità centrale, non vi è un'entità che possa garantire le transazioni o tutelare le parti in caso di errori o frodi.

OFFERTA DI BITCOIN E SCARSITA' DIGITALE

Nakamoto ha scritto: "La **circolazione totale sarà di 21.000.000 di monete**. Sarà distribuito ai nodi della rete quando faranno dei blocchi, con l'importo totale diviso ogni 4 anni".

Alla nascita di tale sistema, la **ricompensa dei blocchi era programmata** a 50 bitcoin per blocco: ogni quattro anni circa, o dopo l'emissione di 210.000 blocchi, la ricompensa dei blocchi si sarebbe dimezzata («halving»)

In base a questo programma, l'**offerta** continuerà ad aumentare ad un ritmo decrescente, avvicinandosi asintoticamente a 21 milioni di monete, presumibilmente intorno al 2140, e a quel punto non saranno più emessi bitcoin.

Poiché le nuove monete vengono prodotte solo con la soluzione dei problemi di prova (proof-of-work), c'è un **costo reale per l'emissione** di nuovi bitcoin.

Con l'aumento del prezzo di mercato del bitcoin, un numero maggiore di nodi entrerà in competizione per la risoluzione del PoW, il che aumenterà la difficoltà del problema e renderà più oneroso ottenere la **ricompensa**.

Con questo «design tecnologico», Nakamoto ha modellato un concetto di **assoluta scarsità digitale**: il bitcoin è il primo esempio bene digitale che è scarso e non può essere riprodotto all'infinito, con una quantità fissa prestabilita che non può essere aumentata.

IL BITCOIN COME MEZZO DI SCAMBIO

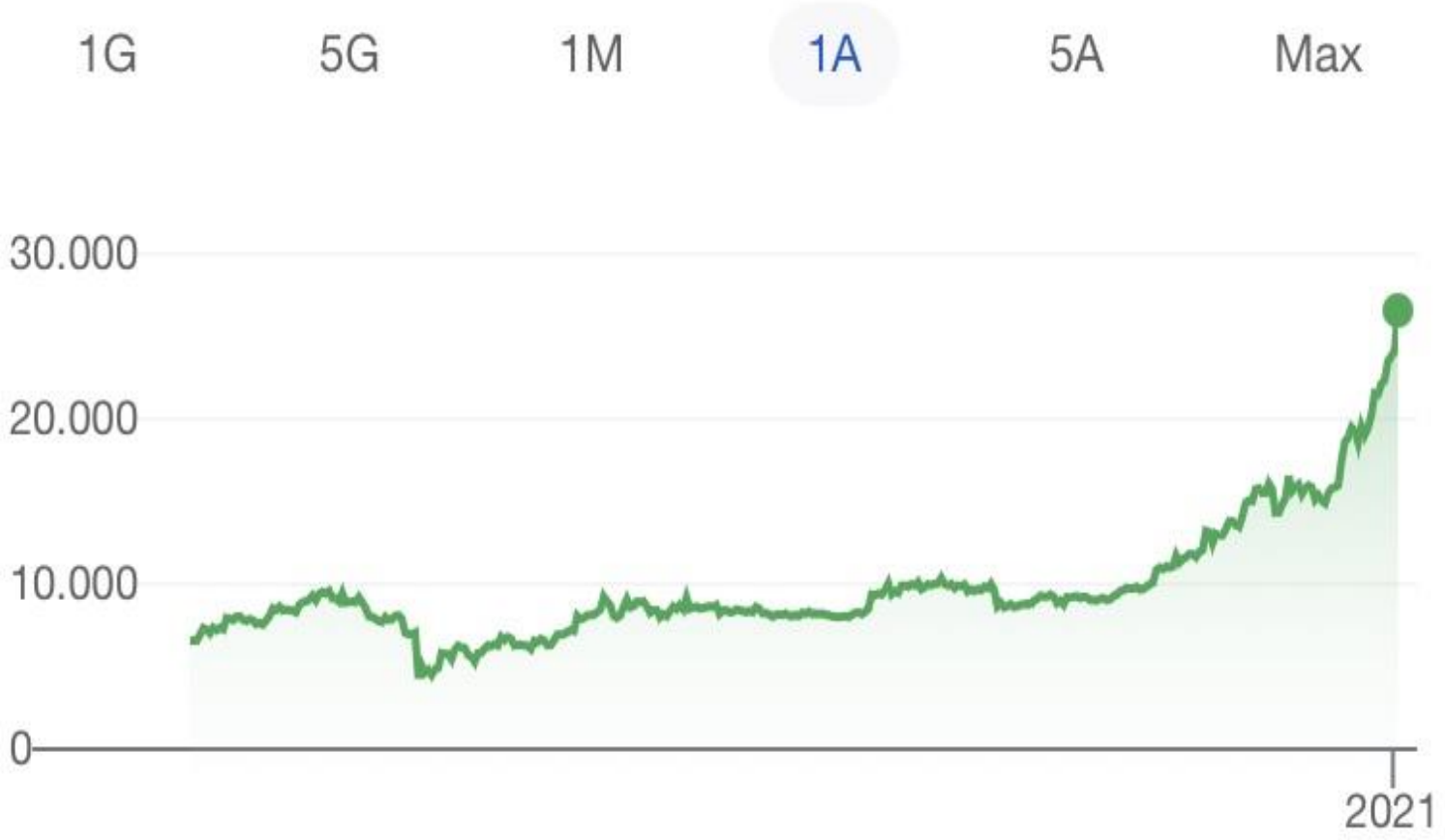
Rispetto alle valute tradizionali, il Bitcoin ha un evidente vantaggio comparativo nei **costi di transazione**, in quanto le commissioni coprono solo il costo di mantenimento del sistema dovuto ai minatori: non ci sono costi legati a terzi intermediari.

Le **commissioni medie di transazione** per transazione sono comprese tra lo 0% e l'1% utilizzando Bitcoin, mentre le commissioni dei sistemi di pagamento online tradizionali sono comprese tra il 2% e il 5% (e sarà necessaria fino a una settimana per la convalida, contro i 10 minuti del bitcoin).

Ma i rivenditori online che attualmente accettano Bitcoins rappresentano solo lo 0,006% dei più grandi: la maggior parte delle transazioni in bitcoin sono **investimenti o speculazioni**.

A partire da Ottobre 2020, complice una sempre più crescente propensione alla rinuncia all'oro come bene rifugio ed il consueto effetto halving, il Bitcoin ha visto notevolmente incrementare il proprio valore superando la soglia dei 30'000 dollari in questo Gennaio 2021.

ANDAMENTO DEL VALORE DEL BITCOIN



UNITA' DI CONTO E RISERVA DI VALORE

«Affinché una valuta funzioni come **unità di conto**, i consumatori devono trattarla come un numerario quando confrontano i prezzi di un bene alternativo al dettaglio» (Yarmack,2014).

Il problema principale di Bitcoin è l'**enorme volatilità** che mostra nel tempo: il valore totale dei bitcoin in circolazione e il numero di aziende che usano Bitcoin sono molto bassi rispetto a quanto potrebbero essere. Pertanto, piccoli eventi, scambi o attività speculative potrebbero variarne significativamente il prezzo. Questo costringe i commercianti ad aggiornare i prezzi ogni 10-15 minuti per evitare perdite inaspettate.

Per essere considerato una valida **riserva di valore,** il bitcoin richiede, come tutte le valute standard, due proprietà: **sicurezza** e **bassa volatilità**.

Mentre la volatilità è un dilemma sotto questo punto di vista, le transazioni sono assolutamente sicure: il problema sorge quando si tratta di **scambi online**, che permettono a utenti comuni di ottenere bitcoins vendendo denaro tradizionale.

VOLATILITA’ DEL BITCOIN

RAPPRESENTAZIONE GRAFICA DELLA VOLATILITA’ DEL BITCOIN

ALTCOINS

- Gli Altcoin rappresentano un'intera categoria di cripto valute: dividere la parola in due parti, "alt" rimane per "alternativa" e "moneta" si riferisce indirettamente a Bitcoin. Per questo motivo gli altcoin sono tutte quelle valute crittografiche che in qualche modo assomigliano a Bitcoin ma che offrono molteplici funzionalità avanzate e cercano di essere migliori del cripto mai inventato prima. Gli Altcoin rappresentano una quota che va dal 40% al 60%, a seconda del periodo e della variazione complessiva dei prezzi: alcuni di essi mirano a sostituire i Bitcoin, essendo più efficienti e stabilendo una sorta di monopolio, mentre altri sono progettati per risolvere problemi specifici e per soddisfare esigenze particolari. Possono essere divisi in due categorie principali: gli altcoin che sono costruiti utilizzando il protocollo originale open-source di Bitcoin, con modifiche che concepiscono una nuova moneta con caratteristiche diverse, e gli altcoin che hanno un proprio protocollo e un libro mastro distribuito. Tra il vasto universo delle crittocittà, ci concentreremo su due delle più grandi e peculiari implementazioni di blockchain e ledger distribuiti: Ethereum e Ripple.

ETHEREUM

- Ethereum è una piattaforma decentralizzata che gestisce contratti intelligenti: un'applicazione che funziona esattamente come programmato senza alcuna possibilità di fermo macchina, censura, frode o interferenza di terzi. La piattaforma Ethereum offre agli sviluppatori strumenti per sviluppare i propri progetti e le proprie applicazioni: i Dapps (Decentralized application) possono molto l'uno dall'altro, dal sistema token alle organizzazioni autonome decentralizzate (DAO). Ethereum è ora la piattaforma più efficiente su cui costruire Dapp e DAO, in quanto può contare sulla seconda valuta crittografica più popolare al mondo: l'Etere. L'etere è la forma di pagamento che i clienti della piattaforma effettuano alle macchine che eseguono le operazioni richieste: è la "moneta" che deve essere adottata quando si tratta di un progetto basato su Ethereum. Rappresenta la ricompensa per i minatori che approvano il contratto intelligente e non ha una dotazione di denaro fisso: per il momento è stato mantenuto un tetto massimo di 18 milioni di eteri per anno, ma alla fine potrebbero sorgere problemi di inflazione. Nel 2014 sono stati distribuiti 60 milioni di eteri attraverso una prevendita: 12 milioni sono andati in anticipo

RIPPLE

- Ripple è una piattaforma di pagamento digitale decentralizzata peer-to-peer e open-source che consente trasferimenti di valuta quasi istantanei indipendentemente dal fatto che si tratti di USD, Euro, Yen o Bitcoin. Lanciata nel 2012 da Ripple Labs Inc, una società con sede negli Stati Uniti, mira ad offrire il modo più efficiente, veloce ed economico per effettuare trasferimenti internazionali di denaro, concentrandosi sul sistema bancario. I clienti principali sono banche e fornitori di servizi di pagamento e tra i partner attuali troviamo Accenture, American Express, Deloitte, Royal Bank of Canada, Santander, UBS e Unicredit. Ripple ha rilasciato la sua criptovaluta, basata sulla sua stessa catena di blocco, che funge da ponte verso altre valute senza discriminare tra una fiat/criptovaluta ad un'altra, soprattutto per quelle meno popolari. L'ondulazione non può essere estratta da nessuno, le transazioni non sono convalidate attraverso la prova del lavoro ma con un protocollo di consenso specifico e si tratta di una criptovaluta parzialmente decentralizzata con solo 18 validatori. Ripple non ha raccolto fondi attraverso un'emissione di cripto-valuta, ma è stata finanziata privatamente.

ALTRE VALUTE CRIPTATE

- Bitcoin Cash è una copia di Bitcoin, rilasciata a supporto del progetto originale che affronta i temi dell'usabilità e dell'aumento della capacità di rete.
- Anche Litecoin si basa sull'algoritmo originale di Bitcoin con un unico e rilevante miglioramento, la velocità di transazione (un quarto dell'originale) e una massa monetaria quadruplicata, fino a 84 milioni di monete.
- Stellar è un'infrastruttura di pagamento distribuita e open source simile a quella dello Squartatore, ma si concentra sulle persone piuttosto che sulle grandi istituzioni finanziarie, fornendo un accesso più diretto al denaro: è pre-minata e utilizza un proprio protocollo.
- Tether è l'unico "stablecoin" di successo: il valore di un Tether è sostenuto dal valore di un USD. Mantiene il vantaggio di quasi tutte le crittovalute a catena di blocco, ma evitando la debolezza dell'oscillazione volatile dei prezzi. Ogni Tether emesso è coperto in un rapporto di 1 a 1 dall'unità monetaria fiat corrispondente detenuta in deposito da Tether Limited con sede a Hong Kong: ciò implica la presenza di una banca che custodisce "fisicamente" i fondi, esattamente come un'attività standard.

OFFERTA INIZIALE DI MONETA

- Al giorno d'oggi nel panorama delle crittocittà c'è molta concorrenza tra i progetti e la maggior parte di essi è orientata al business. Le offerte iniziali di monete (ICO) o la vendita di gettoni sono un meccanismo per raccogliere fondi esterni attraverso l'emissione di gettoni: dopo l'emissione il proprietario ha una chiave che permette di accedere alla catena di blocco ed eventualmente di riassegnare la proprietà del gettone. I gettoni di solito non trasmettono il diritto di voto, ma sono valute virtuali che possono essere utilizzato per pagare i servizi che il progetto di emissione fornisce. La prima fase, che precede l'ICO vera e propria, è il lancio di una campagna di marketing attraverso il sito web, la pubblicità sociale e le chat, con l'obiettivo di creare una community. Un po' di tempo prima dell'ICO, verrà lanciato un "white paper": presenta il progetto e potrebbe essere più o meno sofisticato, tecnico e preciso ma non soddisfa alcun requisito di alcun regolatore. Molti progetti vanno per un Pre-ICO, che è un primo round di distribuzione di gettoni in quantità limitata, di solito a prezzi molto scontati rispetto al prezzo di emissione ufficiale.

- Ci sono tre variabili economiche rilevanti nell'ICO: i ricavi target, la frazione dell'offerta totale di gettoni venduti e il meccanismo dei prezzi. Molte ICO cercano solo di ottenere dei proventi, altre vogliono finanziare un obiettivo specifico e mirano a raggiungere una somma di denaro prefissata. Una sorta di "tetto" al numero di gettoni disponibili è comunemente fissata, ma non si traduce necessariamente in un importo massimo di finanziamenti raccolti; una frazione dell'importo complessivo dei gettoni è tenuta a parte per i fondatori. Il più semplice e comune meccanismo di determinazione dei prezzi ICO vende un certo numero di gettoni in base al principio "primo arrivato, primo servito" a un prezzo fisso, mentre alcuni emittenti hanno organizzato cicli consecutivi in cui i prezzi dei gettoni aumentano ad ogni nuovo ciclo. Alla fine, se l'ICO si rivelerà un successo, i fondatori potranno decidere di candidarsi per la lista su una borsa online: se accettata, la quotazione garantisce la liquidità. Il mercato delle offerte iniziali di monete cresce rapidamente negli ultimi due anni (più di 20 miliardi di dollari secondo Coindesk), sfidando i tradizionali VC e il crowdfunding: sono il modo in cui le crittocittà servono le nuove imprese e le start- up basate su blockchain.

THANKS FOR YOUR ATTENTION!