

9 febbraio 2021 16:23

DiFi: l'abc della finanza distribuita

di [Alessandro Pedone](#)



Il 2020 è stato, fra le tante altre cose, l'anno nel quale si è compreso che la finanza distribuita è destinata a rivoluzionare definitivamente la finanza.

Anche fra i cosiddetti esperti di finanza, la quasi totalità non ha la più pallida idea di cosa sia la finanza distribuita. Con questo articolo, quindi, ci rivolgiamo a coloro che non sanno assolutamente nulla di blockchain, protocolli ed informatica in generale. A questa categoria di persone tenteremo di far comprendere cosa sia la finanza distribuita e perché sia così importante capirlo e muovere l'opinione pubblica affinché una tecnologia così potente sia utilizzata a vantaggio di tutta la società e non in modo distorto.

Fiducia

Da sempre, in ogni negoziazione, la domanda chiave è: *mi posso fidare?*

La fiducia è l'olio negli ingranaggi di ogni rapporto economico-finanziario.

Nella società attuale, il fondamento della fiducia che riponiamo in un soggetto totalmente sconosciuto è costituito dalle **istituzioni pubbliche**. Accetto come pagamento per il mio lavoro o per un bene che possiedo dei pezzi di carta (o un flusso di "bit" sul mio conto corrente) perché ho fiducia nelle istituzioni le quali, di fatto, mi "garantiscono" che in futuro potrò usare quelle cose per acquistare a mia volta beni o servizi.

Quando investo in un'obbligazione che promette un certo tasso d'interesse, lo faccio perché so che se l'emittente non assolve a quell'obbligo incorre in una serie di problemi giudiziari e ci penserò molto bene prima di cambiare idea.

Quando acquisto un immobile o un'auto da un perfetto sconosciuto, lo faccio perché mi fido del fatto che il bene è veramente suo grazie ai pubblici registri.

In altre parole, la fiducia si fonda sul fatto che esistono delle istituzioni alle quali appellarsi se le cose non vanno come dovrebbero andare.

Fino a poco tempo fa, considerata la potenza di elaborazione delle informazioni di cui disponeva l'umanità, questo era l'unico modo sensato di garantire il maggior grado di fiducia possibile fra gli attori economici.

Da alcuni anni, sta emergendo una modalità incredibilmente più efficiente di garantire la fiducia nelle transazioni.

Blockchain

La blockchain è un insieme di tecnologie informatiche che realizzano un *registro distribuito* con un elevatissimo livello di sicurezza e affidabilità circa le informazioni registrate. Il termine "distribuito" indica che non c'è nessun "ente centrale" in grado di controllare il registro. La blockchain è composta da una rete di computer proprio come internet. Se la rete è sufficientemente ampia è impossibile "spegnerla" o controllarla. Il termine "registro" indica in sostanza una base di dati che può rappresentare qualunque cosa, a partire da transazioni monetarie, portafogli elettronici, ma anche un catasto, il pubblico registro automobilistico, il database delle fatture elettroniche, ecc. Ogni database, potenzialmente, potrebbe essere trasferito su blockchain.

L'enorme sicurezza della blockchain è realizzata attraverso una geniale combinazione di abilità informatiche e teoria dei giochi. Ci porterebbe troppo oltre lo scopo di questo articolo descrivere nel dettaglio perché è sostanzialmente impossibile violare la sicurezza della blockchain, ci tengo a sottolineare però che non è soltanto

un fatto di tecnologia e potenza di calcolo, ma è anche e soprattutto il fatto che il design della blockchain rende conveniente tenere comportamenti utili a mantenere la sicurezza della rete e sconveniente tentare di fare il contrario.

Con la blockchain è stato introdotto il concetto, un po' fuorviante, di "trustless" che letteralmente significa "assenza di fiducia". Ma in realtà significa assenza di un ente centrale nel quale si debba riporre fiducia circa la correttezza dei dati riportati nel registro.

Ad esempio, se io voglio assicurarmi che un certo intermediario finanziario abbia tutti i requisiti per svolgere il proprio lavoro mi rivolgerò all'autorità di vigilanza e consulterò il pubblico registro degli intermediari finanziari. Così facendo, sto riponendo la mia fiducia sul fatto che l'Autorità Pubblica abbia svolto tutti i controlli del caso. Se vi fosse una blockchain che svolgesse lo stesso lavoro, sarebbe il processo stesso a garantire la correttezza di tutti i dati.

A questo punto, la maggior parte dei lettori probabilmente sarà in confusione perché è difficile immaginare come un processo possa sostituire la capacità di giudizio di un essere umano. Per una piccola parte di attività siamo ancora distanti dal poter sostituire un essere umano con una serie di calcoli, ma per una fetta enorme di attività non c'è affatto nessun bisogno di un essere umano che applichi il proprio discernimento.

La blockchain è iniziata con le transazioni di un bene digitale, ormai famosissimo, che si chiama Bitcoin. Chiaramente non c'è bisogno di nessun discernimento umano per certificare che un Bitcoin è passato da un portafoglio elettronico ad un altro. La Blockchain deve solo assicurarsi, ed è per quello che è nata, che lo "stesso" Bitcoin non venga trasferito contemporaneamente su più portafogli elettronici. Questo è il lavoro che fa egregiamente la blockchain di bitcoin.

Riassumendo, quindi, una blockchain è una tecnologia che serve a gestire un pubblico registro distribuito affinché le informazioni in esso contenute siano sicure ed affidabili senza la necessità di un ente centrale.

Smart Contract

Compreso il concetto di blockchain, per comprendere bene cosa sia la finanza decentralizzata e perché potrà essere così importante, dobbiamo focalizzare un solo altro concetto: gli smart contract.

Abbiamo compreso che la blockchain è un registro distribuito affidabile e sicuro che non richiede la presenza di un organo centrale. Ma come vengono cambiate le informazioni nel registro? Attraverso dei pezzi di software i quali rendono *automatica* l'applicazione di una serie di regole pubbliche. Questi pezzi di software vengono chiamati "smart contract" e funzionano sulla blockchain.

Ipotizziamo che io voglia prendere in prestito 10.000 dollari mettendo a garanzia il controvalore di oggi di 15.000 Bitcoin (magari perché non li voglio vendere) pagando un certo interesse e restituendo il capitale ad una certa data.

Un'operazione di questo tipo è svolta da diversi tipi di smart contract, forse il più famoso si chiama Compound, un software che gira sulla blockchain di Ethereum e che attualmente ha un controvalore di circa 8 miliardi di dollari di asset disponibili in prestito.

Il punto degli smart contract è che, chi si affida a questo sistema, sa che **l'esecuzione è certa**.

Non è possibile fermare uno smart contract. Ad esempio, se il valore dei Bitcoin messi in garanzia diminuisce sotto una certa soglia, lo smart contract chiederà di reintegrare le garanzie, se l'utente non lo fa, le garanzie vengono vendute ed il contratto è chiuso. Punto.

Gli smart contract funzionano 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno e funzionano in modo quasi istantaneo. Se vuoi prendere in prestito dollari, se hai gli asset in garanzia lo fai senza nessuna perdita di tempo.

Un esempio classico di smart contract è l'affitto di un bene, che potrebbe essere digitale o fisico. Fino a quando c'è il pagamento lo smart contract fornisce l'accesso al bene, quando chi ha preso in prestito il bene non paga più lo smart contract disabilita l'accesso (nel caso di un immobile potrebbe essere con una chiave elettronica).

Se il concetto di blockchain è potente, il concetto di smart contract è super potente, ma - per citare il "filosofo" Benjamin "Ben" Parker, zio dell'Uomo Ragno - *"da un grande potere deriva una grande responsabilità"*.

DeFi: decentralized finance

Negli ultimi tempi si è fatto un gran parlare di Fintech, ovvero l'applicazione di tecnologie informatiche alla finanza tradizionale. Tutte le tecnologie per facilitare i pagamenti attraverso app sui telefonini, i "robo advisor" per dare consigli d'investimento, ecc.

Tutte queste cose sono certamente interessanti, ma sono insignificanti rispetto alla dirompente rivoluzione che sta maturando con la finanza decentralizzata (abbreviata in DeFi).

Un tassello fondamentale della DeFi sono le cosiddette “stablecoin” ossia delle cryptovalute (cioè degli asset digitali come il Bitcoin) il cui valore è ancorato ad una moneta a corso legale, tipicamente il dollaro. Le valute a corso legale non “girano” sulla blockchain, quindi è stato necessario creare un surrogato.

Avendo la blockchain, gli smart contract e le stablecoin, è stato possibile costruire tutta una serie di strumenti per consentire agli utenti di fare sostanzialmente tutto ciò che si fa nella finanza tradizionale senza bisogno di nessun ente centrale che garantisca la correttezza dei comportamenti, perché ogni cosa è automatizzata sulla base di regole trasparenti.

Al momento il totale degli asset depositato all'interno di smart contract che sviluppano servizi di finanza decentralizzati è pari a circa 37 miliardi di dollari. Una cifra considerevole in assoluto ma che è ancora irrisoria rispetto alle cifre complessive della finanza mondiale che sono di due ordini di grandezza superiori.

Ciò nonostante, queste cifre ci dicono chiaramente che la finanza decentralizzata, la blockchain ed in particolare il bitcoin, hanno raggiunto la massa critica e una maturità tecnica per essere considerati ormai strumenti destinati a modificare per sempre il modo in cui gli esseri umani faranno la maggior parte delle transazioni economico-finanziarie nei prossimi decenni.

Vantaggi e problemi della DeFi

I vantaggi potenziali della DeFi sono semplicemente enormi. L'eliminazione della necessità di intermediari finanziari per avere accesso alle tipiche funzioni della finanza (essenzialmente prendere denaro - come debito o capitale- e investire denaro) apre la porta a tutta una serie di efficientamenti del sistema finanziario precedentemente inimmaginabili.

Nei giorni passati c'è stato, ad esempio, un evento che ha fatto molto clamore, il caso di GameStop, del quale si è molto parlato e certamente non vorrò farlo in questa sede. Mi limito a dire che in un sistema DeFi ben progettato questi casi non potrebbero esistere perché non sarebbe possibile vendere allo scoperto un numero maggiore di azioni rispetto a quelle disponibili.

La DeFi è un'opportunità enorme per riprogettare il sistema finanziario secondo regole più sensate rispetto a quelle che si sono stratificate nel tempo.

Il fatto che non ci siano gli intermediari finanziari non significa che non servano regolatori pubblici, come in genere pensano coloro che lavorano nel settore.

Bitcoin nasce all'interno di una cultura iper-liberista che vede qualsiasi istituzione centrale come nemica della libertà individuale.

Paradossalmente, invece, proprio la finanza decentralizzata rende ancora più importante il ruolo dei regolatori poiché tutta dal DeFi si fonda sull'applicazione automatica di regole. E' fondamentale che si facciano valutazioni molto approfondite sugli effetti sistemici di queste regole e ci si assumano ragionevoli garanzie di stabilità per tutto quel genere di cose che la blockchain non può verificare in modo automatico.

Ad esempio, la stablecoin più usata nella DeFi è Tether, una cryptovaluta che dovrebbe essere ancorata al dollaro e sulla quale vi sono una serie di dubbi per scarsa trasparenza.

Se Tether si dovesse rivelare una truffa, i danni sarebbero di proporzioni enormi. Probabilmente la DeFi, complessivamente, sopravviverebbe, ma la botta sarebbe enorme.

Più pericolosi ancora delle truffe vere e proprie, sono gli effetti potenzialmente imprevedibili degli intrecci fra i vari smart contract. E' fondamentale stabilire regole prudenziali per evitare che qualche cigno nero faccia scattare una serie di reazioni a catena.

E' possibile pensare ad un'applicazione di queste tecnologie in chiave “comunitaria” nel quale lo scambio non è solo di asset finanziari, ma anche di credibilità personale “garantita” dalla comunità, così come avviene nel baratto multilaterale.

Così, sarebbe possibile prendere in prestito in modo automatico una certa quantità di denaro anche senza mettere a garanzia degli altri asset.

Conclusioni

La DeFi è qui per restare. Siamo solo agli albori di una tecnologia che nei prossimi decenni avrà effetti dirompenti su tutto il sistema finanziario. I livelli di efficientamento che portano queste tecnologie sono incredibili, ma anche i rischi ed i problemi di tipo etico-politico sono ugualmente elevati. E' fondamentale che si avvii una discussione pubblica adesso che i numeri sono ancora abbastanza contenuti (in rapporto alla finanza mondiale) perché mano a mano che i numeri si moltiplicheranno, sarà impossibile evitare shock con effetti sistemici importanti.

CHI PAGA ADUC

l'associazione non **percepisce ed è contraria ai finanziamenti pubblici** (anche il 5 per mille)

[La sua forza sono iscrizioni e contributi donati da chi la ritiene utile](#)

DONA ORA (<http://www.aduc.it/info/sostienici.php>)