UNIVERSITÁ LIUC – CARLO CATTANEO

Blockchain:
cos’è, come funziona e come cambierà il business

La definizione di blockchain

Si tratta di un **data base distribuito** (*una sorta di registro delle transazioni dove i dati non sono memorizzati su un solo computer, ma su più macchine collegate tra loro via Internet, attraverso un'applicazione dedicata che permette di interfacciarsi con la "catena")* fatto di **blocchi di dati che memorizzano transazion**i; per essere consolidato all'interno di un blocco, ogni dato, e successivamente ogni blocco prima di essere inserito nella "catena", **viene sottoposto a un processo di validazione.**

Come funziona la Blockchain?

1

LA TRANSAZIONE

Viene creata una transazione con tutte le informazioni necessarie

2

IL BLOCCO

Sulla Blockchain viene creato un nuovo "blocco" con i dati della transazione

3

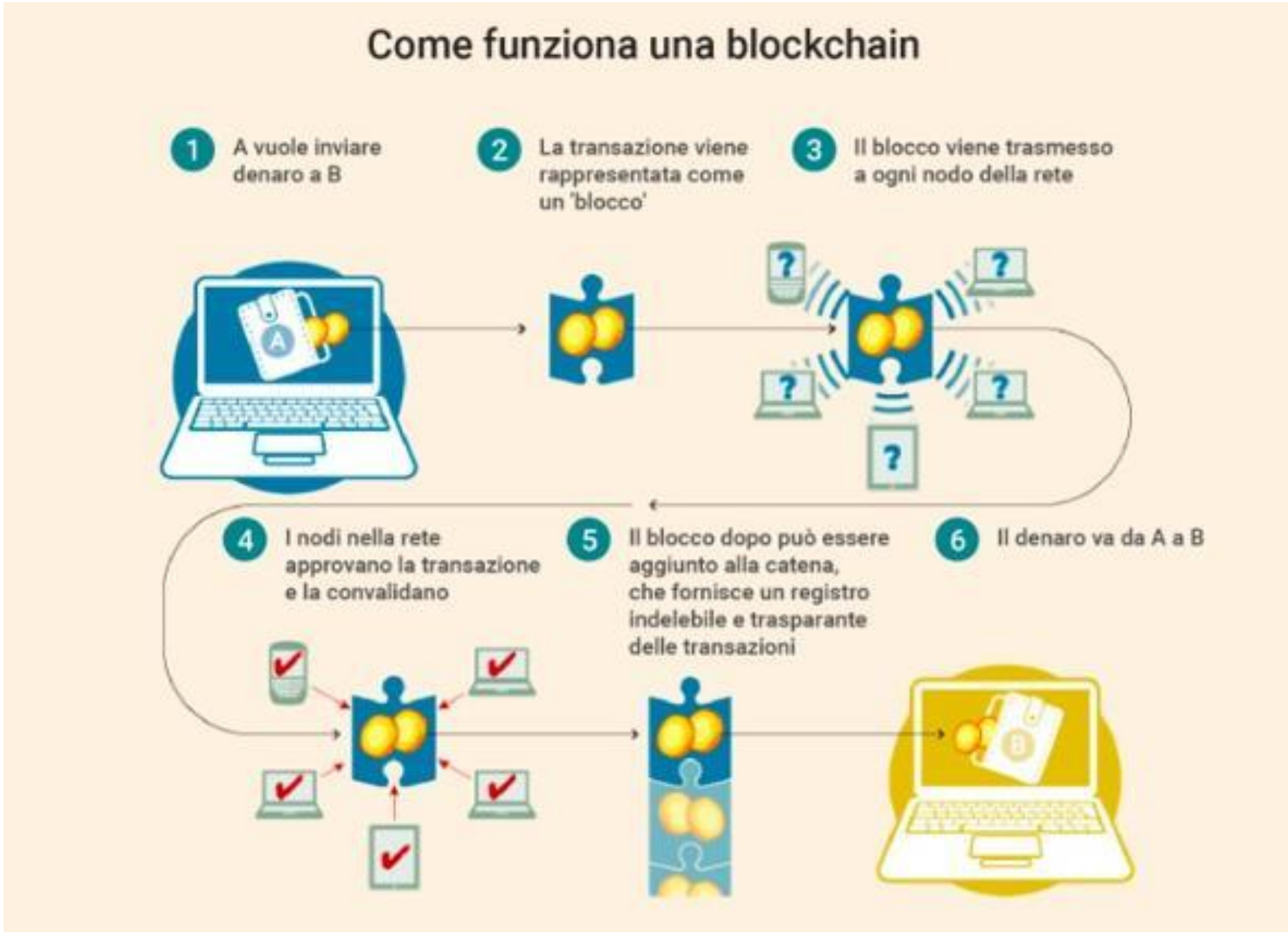
LA VERIFICA

Il blocco si aggiunge alla catena e tutti i partecipanti vi possono accedere

4

SUCCESSO!

Se le informazioni sono corrette e verificate, la transazione viene effettuata


Come funziona una blockchain
1 A vuole inviare denaro a B
2 La transazione viene rappresentata come un 'blocco'
3 Il blocco viene trasmesso a ogni nodo della rete
4 I nodi nella rete approvano la transazione e la convalidano
5 Il blocco dopo può essere aggiunto alla catena, che fornisce un registro indelebile e trasparante delle transazioni
6 Il denaro va da A a B

https://www.youtube.com/watch?v=vqLiAb7a3sU

https://www.youtube.com/watch?v=fiCWHrMMHr4

L’origine

La parola Bitcoin e criptovaluta **Bitcoin** è emersa per la prima volta nell'autunno del **2008** e la **rete Bitcoin è arrivata all’inizio del 2009**. Bitcoin é stata la prima decentrlizzazione della valuta digitale, il che significa che è un **sistema "cash" digitale che consente alle persone di scambiare denaro istantaneamente**, senza dover andare attraverso intermediari come le banche. Anche se piattaforme di pagamento digitali come **PayPal e Venmo instradano ancora trasferimenti di denaro attraverso banche, incorrendo commissioni e ritardi.**

Bitcoin è stata la prima **criptovaluta**, ma la sua creazione ha portato la creazione di **1.500 criptovalute che vengono acquistate e scambiate a livello globale**: Ether (da Ethereum), XRP (da Ripple) e Litecoin sono solo a alcuni esempi. La "criptovaluta" nella criptovaluta deriva **dall'uso di crittografia, che viene utilizzato per risolvere diversi problemi di base in trasferire denaro su Internet, eliminando i non autorizzati dalla creazione di nuovo denaro e donazione agli utenti un modo sicuro per dimostrare la propria identità e negoziare con ciascuno di essi altro senza la necessità di un ulteriore intermediario.**

Separiamo il concetto di Blockchain e criptocurrency

È importante **separare le criptovalute dalla blockchain**, che è la tecnologia di base che rende possibili le criptovalute.
Una blockchain è un registro delle **transazioni digitale, sicuro e pubblico (un libro mastro)**. "Blocco" descrive il modo in cui questo libro mastro organizza le transazioni in blocchi di dati, che vengono poi organizzati in una **"catena" che**
collegamenti ad altri blocchi di dati. I collegamenti rendono **facile vedere se qualcuno ha modificato qualsiasi parte della catena,** il che aiuta il sistema a proteggere contro transazioni illegali.

Concetti fondamentali: nodi della blockchain e miner

I **nodi sono i computer della rete che hanno scaricato la blockchain nella loro memoria;** chiunque può diventare un nodo, tramite **l'apposito programma (Bitcoin Core per esempio per Blockchain Bitcoin).**

I miner sono coloro che effettuano il controllo delle transazioni, grazie a computer molto potenti e attraverso un protocollo di validazione piuttosto complesso, e **il cui lavoro viene ripagato con un premio** (il termine ormai condiviso per questa operazione è "minare", italianizzando il termine inglese to mine ossia estrarre).

Il mining e il minatore

- Ogni blocco di transazione, ossia l'insieme di tutte le transazioni avvenute nell'arco di 10 minuti, è affidato ad un singolo Miner.
  Il compito del Minatore è quello di istallare nelle sue macchine il Cryptographic hash software, questo software è in grado di calcolare i dati delle transazioni BTC (bitcoin), alle quali viene aggiunto un valore casuale o pseudo casuale detto Nonce.
- L'insieme di questo valore con i dati del blocco delle transazioni, genera una stringa alfanumerica chiamata Hash. Per calcolare il contenuto di una stringa hash il minatore necessita di un grande numero di tentativi e calcoli, dunque un vasto numero di nonce.

Nel processo di calcolo viene aggiunto anche l'hash del blocco precedente che insieme ai dati del blocco di transazioni e al nonce, genera l'hash del blocco attuale.
La caratteristica che rende questo calcolo complesso ma essenziale per essere reputato corretto da sistema Bitcoin, è dovuta dal fatto che l'hash deve incominciare con un numero fisso di zeri. Quando la stringa viene validata, il blocco di transazioni viene reso a sua volta valido.
L'operazione si conclude con "l'estrazione" di BTC da parte del miner e l'aggiornamento del registro Blockchain, libro mastro dei blocchi di transazioni.
L'intero processo permette al sistema BTC di essere estremamente sicuro, poiché i blocchi di transazioni sono legati tra loro attraverso la condivisione dell'hash; questo permette ad un ipotetico malintenzionato di rinunciare all'alterazione delle transazioni in quanto andrebbe a modificare inevitabilmente anche i suo hash.

Il protocollo di validazione

Esso **definisce gli algoritmi validanti e chi può essere un miner**, e rappresenta dunque **l'elemento vitale principale della blockchain perché è proprio da questo che dipendono sostanzialmente la velocità della catena e la sua sicurezza** (gli algoritmi che governano questo processo non solo validano che ogni nuova immissione risponda a determinati criteri, ma impediscono anche che possano essere manomessi i dati già presenti nella catena). È dunque in questo ambito che **si vedono le principali evoluzioni e che si differenziano, dal punto di vista tecnologico, le diverse blockchain.** È comunque importante sottolineare che **non necessariamente un protocollo è migliore di un altro: l'utilizzo dell'uno o dell'altro dipende anche dal tipo di applicazione per la quale viene utilizzata la blockchain.**

I vari protocolli

Proof of Work – È il protocollo di **validazione primigenio, sul quale si è basata la prima blockchain, Bitcoin, e a tutt'oggi ancora il più diffuso**. Ogni **10 minuti un nuovo blocco, contenente migliaia di transazioni, viene immesso nella blockchain**. La criticità di questo meccanismo risiede nella **velocità per minare un blocco perché è un protocollo che, al crescere della blockchain, richiede sempre maggiore potenza elaborativa nei computer dei miner. Il tempo di validazione di una transazione (10 minuti) è uno dei motivi dal quale derivano le maggiori criticità in termini di scalabilità della tecnologia.**

Proof of Stake – Nasce per far fronte al **problema della scalabilità del precedente protocollo**, **semplificando** il processo di mining. Il protocollo prevede inoltre che **quando viene aggiunto un nuovo blocco venga automaticamente scelto il creatore del blocco successivo**; per effettuare questa operazione di selezione vengono oggi **utilizzati metodi diversi.**

Federated Byzantine Agreement (FBA) – Se quelli descritti sono i due protocolli principali, ne **sono stati poi creati altri,** in parte derivazione di questi, in parte con elementi totalmente nuovi. Tra i più interessanti segnaliamo **Federated Byzantine Agreement (FBA), sviluppato da Stellar Development Foundation (e utilizzato dalla seconda metà del 2015 dalla blockchain Stellar) basato su unità di fiducia (quorum slices) decise dai singoli server che insieme stabiliscono il livello di consenso del sistema**

Le tipologie di Blockchain

Blockchain pubbliche: tutti vi possono accedere e operare transazioni al suo interno o partecipare al processo di validazione. Bitcoin ed Ethereum sono i più famosi esempi di blockchain pubbliche

blockchain private: controllate da un'unica organizzazione che stabilisce chi può aderirvi, chi può operare transazioni al suo interno e partecipare al processo di consenso/validazione

consorzi blockchain: il processo di autorizzazione viene delegato a un gruppo preselezionato (tra i principali consorzi c'è per esempio R3 che raggruppa le più grandi banche del mondo). La possibilità di aderire alla blockchain e di operare transazioni al suo interno può essere pubblica o limitata ai soli partecipanti. **Questa tipologia di blockchain permissioned è particolarmente indicata per l'utilizzo nel mondo business**.

1

Le categorie di Blockchain

La **categoria Blockchain 1.0 riguarda tutte le applicazioni di carattere finanziario per la gestione di criptovalute (indipendentemente dal protocollo di validazione utilizzato**) a partire dalla storica (e che attualmente detiene ancora la leadership delle criptovalute) **Bitcoin**. In pratica, i bitcoin sono file che possono essere salvati nel wallet digitale di ogni utente. Ogni indirizzo bitcoin presente nel **wallet può essere associato a un numero variabile di bitcoin. E a ogni indirizzo (chiave pubblica), viene associata una firma digitale (chiave privata), per assicurarsi che solo il proprietario di un certo indirizzo possa avviare una transazione a esso legata.**

2

La categoria Blockchain 2.0

Estende la blockchain a settori diversi dal finanziario grazie all'implementazione degli smart contract

Il passo successivo sarà quello della *Blockchain 3.0 con la diffusione delle Dapp (decentralized applications): un futuro in cui tutti noi utilizzeremo le tecnologie blockchain, probabilmente senza neanche rendercene conto*, perché incapsulate nelle "cose" connesse tra loro, senza intervento umano, con applicazioni che si autocompileranno.

Che cosa sono gli smart contract e come funzionano

Uno **smart contract è un contratto sotto forma di codice che rimanda l'esecuzione di alcune o tutte le sue clausole a un software**. Il concetto di smart contract si compone di tre parti:

il codice di un programma che diventa l'espressione di una logica contrattuale (l'auto funziona se ne vengono pagate le rate);
messaggi inviati al programma stesso che rappresentano gli eventi che devono far attivare il contratto (il mancato pagamento della rata);
un meccanismo che ponga in essere gli effetti previsti dalla logica (all'auto viene inibita la messa in moto).
Perché uno smart contract funzioni, è indispensabile:

1) il **consenso tra le parti e, quindi, la presenza di un intermediario che ne garantisca l'affidabilità e impedisca manomissioni**

2) **oppure di un meccanismo che, in modo automatico e via software, si sostituisca a questo intermediario.**

Un esempio del primo caso è quello di eBay che incorpora degli smart contract, sotto forma di procedure automatizzate che eseguono le clausole del contratto che i contraenti sottoscrivono quando si affidano a eBay; questi smart contract vengono eseguiti sui server della società di aste e vendite online.

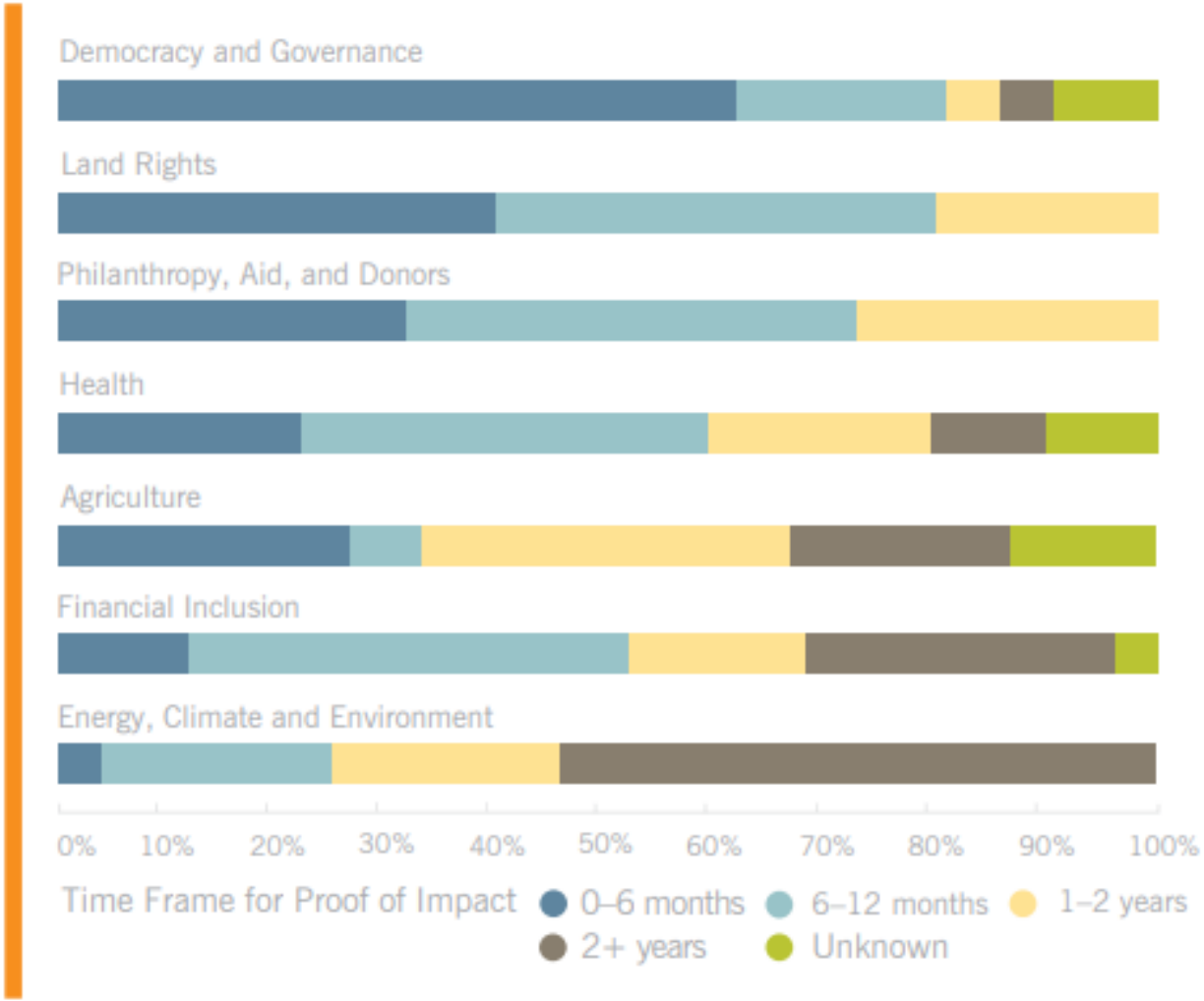
Le caratteristiche della Blockchain

Digitale. Valuta, contratti, documenti… nella blockchain tutto diventa digitale e le transazioni inserite nella catena possono riguardare qualsiasi asset, qualsiasi diritto o contenitore di valore e informazione.
Sicura. Grazie al processo di crittografia che la caratterizza, non è possibile variare o apportare delle modifiche ai blocchi già inseriti nella catena; i dati in essa salvati sono quindi sicuri, certi e non manipolabili.
Attendibile. Essendo organizzata cronologicamente (i blocchi vengono aggiunti alla catena secondo un preciso ordine cronologico immodificabile) impedisce l'insorgere di contestazioni in merito all'esecuzione, per esempio, delle diverse fasi di un contratto.
Affidabile. Le sue caratteristiche tecniche impediscono qualsiasi perdita di dati o danneggiamento: se anche uno dei nodi nei quali è salvata la catena venisse danneggiato, gli altri seguiterebbero a funzionare tenendo stabile la catena, senza alcuna perdita di dati.
Veloce. Non richiede un'entità centrale che ne verifichi la congruità e validità, questa avviene per consenso del network, ed essendo una soluzione completamente digitale elimina tempi di esecuzione, controlli, carta, back-office e rischi operativi.

L’impatto reale della blockchain

Fifty-five percent are estimated to have an end impact on their beneficiaries by early 2019.

Figure 2:Time Frame for Proof of Impact



L’halo effect della sicurezza: il caso charity/ donazioni

Trasparenza: chiunque abbia accesso alla rete può visualizzare a storia delle transazioni in tempo reale.

Impatto potenziale: i soldi la pista può essere seguita e monitorata con maggiore precisione in aree come distribuzione degli aiuti.

Immutabilità: le blockchain proteggono i dati da manomissioni; nessuno l'entità è in grado di modificare i dati passati senza avvisare la rete.

Impatto potenziale: l'immutabilità protegge aree come l'autenticazione degli elettori e registrazioni del titolo fondiario.

I settori della blockchain

Il settore delle banche e dei pagamenti non è, lo sappiamo bene, l'unico interessato dalla ventata di novità e benefici legati all'adozione delle blockchain. Anche **la sicurezza, i trasporti urbani, così come anche il comparto della beneficienza e del fund rasing potrebbero essere trasformati dal più vasto impiego dei registri distribuiti.**

L'esistenza di **Bitcoin come moneta digitale decentralizzata è resa possibile da ciò che è noto come la tecnologia blockchain: in buona sostanza, si tratta di un registro pubblico che automaticamente (e in modo sicuro) verifica e registra un elevato volume di transazioni in digitale.**

Banking e Finance

Le banche e le istituzioni finanziarie servono essenzialmente come depositi e come centri sicuri per il trasferimento di valuta e la blockchain – come registro digitalizzato, sicuro e a prova di manomissione – può assicurare la stessa funzione. In effetti, la svizzera UBS e la britannica Barclays la stanno già sperimentando come un modo per accelerare le funzioni di backoffice e di gestione. Alcuni operatori professionali de settore bancario affermano che si potrebbero ottenere risparmi, a livello globale, per il comparto, che arrivano fino a 20 miliardi di dollari l'anno in spese amministrative. Non a caso, le banche mondiali sono tra i principali investitori nelle startup che operano nel comparto delle tecnologie blockchain. La società R3 CEV, ha già ottenuto l'adesione di una cinquantina di banche ai suoi consorzi, nati per sviluppare soluzioni personalizzate abilitate dalle catene di blocchi per il settore finanziario.

Un gruppo chiamato Thought Machine ha sviluppato il sistema operativo Vault OS, che impiega una tecnologia di blockchain privata in abbinamento ad alcuni registri di crittografia distribuiti per consentire a qualsiasi banca di fornire sistemi finanziari sicuri end-to-end.

Pagamenti e trasferimenti di denaro

In un recente report (pubblicato sulla rivista Forbes) il World Economic Forum ha sostenuto che le tecnologie di pagamento decentrate – come Bitcoin stessa – potrebbero trasformare la "architettura di business" delle aziende che operano nel comparto dei trasferimenti di denaro, un settore rimasto statico negli ultimi 100 anni. Blockchain rende possibile **aggirare i vetusti sistemi di collegamento e creare un flusso di pagamento più diretto tra chi versa le somme e i beneficiari – dentro e oltre i confini della propria nazione – senza intermediari, a tariffe ultra-economiche e a velocità quasi istantanea.** Abra per esempio è una startup che promuove la tecnologia dei Bitcoin per realizzare un servizio trans-nazionale di money transfer altamente sicuro proprio perché basato sui principi dei database distribuiti.

Scuola e mondo accademico

La Holbertson School of Software Engineering, con sede a San Francisco, in California, ha annunciato di voler **utilizzare la tecnologia blockchain per autenticare i titoli e i certificati accademici**. Questo farà sì che gli studenti che sostengono di aver superato i corsi del suo programma di studi non siano in grado di **vantare crediti che non abbiano legittimamente guadagnato**. Anche altre università hanno iniziato a implementare strumenti basati sulla tecnologia dei registri distribuiti per assicurare una maggior trasparenza della gestione dei certificati accademici e nella trascrizioni di lauree e diplomi. Ecco perché le frodi afferenti questo tipo di applicazioni potrebbero essere più facilmente combattute, senza contare il risparmio a livello di tempo e costi legato alla possibilità di poter evitare controlli manuali di migliaia di documenti cartacei ogni anno.

Legittimazione del voto elettorale: e-voting

Le elezioni richiedono l'autenticazione dell'identità degli elettori, la conservazione in sicurezza dei registri (utile per tenere traccia dei voti) e un'attività di spoglio e conteggio assolutamente trasparente per determinare il vincitore. Le blockchain possono servire come strumento utile per la **selezione, il monitoraggio e il conteggio dei voti in modo specchiato, sgomberando** il campo da qualsiasi probabile tentativo di frode elettorale, trucchetti o perdita di dati e voti. Integrando la **selezione dei voti manifestati come operazioni all'interno delle blockchain, gli elettori possono essere rassicurati in merito alla correttezza e trasparenza del conteggio finale delle operazioni di voto,** perché sono in grado di contare direttamente i voti stessi e, grazie alla tracciabilità garantita dai database distribuiti delle blockchain, possono anche rassicurati in merito al fatto che i voti non siano stati modificati e che nessun voto legittimamente espresso sia stato aggiunto o, al contrario, cancellato. **Follow My Vote è stato già utilizzato in fase di test durante le ultime elezioni presidenziali americane come sistema end-to-end di voto online verificabile.**

Leasing e compravendita di automobili

Visa e DocuSign hanno presentato **una relazione che documenta un esperimento condotto nel comparto del leasing delle vetture**. Le due hanno **utilizzato i registri distribuiti per costruire un sistema proof-of-concept per la realizzazione di un processo che culmina con la concessione in leasing di un'auto in modo completamente autonomo e slegato dall'intervento di un operatore**. In pratica, la procedura di erogazione del leasing viene **trasformata in un processo "premi, firma e guida".** Il potenziale cliente sceglie l'auto che vuole ottenere in leasing e la transazione viene immessa sul registro pubblico delle blockchain. **Una volta sedutosi al posto di guida, il cliente firma un contratto di locazione e una polizza assicurativa e il distribuited ledger viene aggiornato con le informazioni relative**. Non è un'esagerazione immaginare che un processo di questo tipo potrebbe essere applicato alle procedure di vendite delle auto, come pure per la registrazione delle auto presso i pubblici registri come il PRA.

Musica Online

Molti artisti musicali si rivolgono alle tecnologie dei registri decentralizzati come a uno strumento per riuscire a condividere musica online in modo più equo. **Billboard riporta che tre aziende stanno cercando di risolvere questo ed altri problemi legati alla gestione e alla liquidazione dei diritti d'autore, promuovendo i pagamenti diretti agli artisti e l'utilizzo di smart contract per gestire e risolvere automaticamente i problemi di licenza**, **PeerTracks ha un progetto, ancora in fase di sviluppo, che si propone di offrire una piattaforma di streaming musicale "autogestita", che permette agli utenti di ascoltare musica e utilizzare i registri distribuiti per pagare direttamente gli artisti, senza ricorrere ad alcun tipo di intermediario**. La piattaforma spera anche di creare più interazione diretta tra artisti e clienti, in modo da stimolare una nuova era musicale più "customer-driven". **Mycelia, fondata dall'artista vincitore di un Grammy award, Imogen Heap, sviluppa canzoni "intelligenti" con contratti smart integrati. I contratti abilitati dalle blockchain consentono agli artisti di vendere direttamente ai fan i propri pezzi senza passare attraverso la lobby delle etichette discografiche.**

Ujo Music, guidato dall'imprenditore Phil Barry, sostiene che sta ricostruendo l'industria musicale sulla tecnologia delle blockchain. Al di là dello streaming, Ujo è visto come un modo per migliorare la catalogazione di autori, artisti e compositori che stanno dietro a un testo o alla musica di una canzone, anche utilizzando i contratti intelligenti (smart contract).

Sanitá

Le istituzioni **sanitarie soffrono dell'incapacità cronica di condividere in modo sicuro i dati tra le diverse piattaforme e istituzioni.** Una miglior collaborazione tra i fornitori di dati significa, in buona sostanza, **una maggior probabilità di stilare diagnosi accurate, una maggior probabilità di optare per trattamenti efficaci e, più in generale, un aumento della capacità complessiva dei sistemi sanitari di fornire una buona assistenza.** Le blockchain applicate al settore della sanità permettono a ospedali, contribuenti e altre strutture sanitarie di condividere l'accesso ai loro network senza compromettere la sicurezza e l'integrità dei dati. La startup **Gem ha lanciato Gem Health Network, una piattaforma basata sui registri distribuiti (e sul progetto peer-to-peer opensource Ethereum, in particolare) in abbinamento alla tecnologia di autenticazione multi-firma e multi-fattore per creare un'infrastruttura dati universale altamente sicura**. Tierion è un'altra startup che ha sviluppato una piattaforma per l'archiviazione e la verifica dei dati nel settore sanitario. Gem e Tierion hanno entrambe stretto una partnership con Philips Healthcare e Tierion poche settimane fa anche con Microsoft.

Monitoraggio della compravendita di armi

Un registro distribuito gestito tramite **tecnologie basate sulle blockchain offre diverse opportunità per rendere più sicuro il mercato della compravendita di armi**. Registri pubblici collegati tramite blockchain sarebbero **più difficili da manomettere e potrebbero impedire ai candidati ritenuti non idonei di acquistare armi o ottenere un porto d'armi**. Inoltre, collegando le cartelle cliniche con i registri dei nomi dei proprietari di armi, sarebbe possibile **avvisare le forze dell'ordine del fatto che, per esempio, un soggetto che detiene (lecitamente) un'arma ha subìto un evento (per esempio un ricovero coatto) che potrebbe portare a una maggior inclinazione a compiere atti violenti**. La startup Blocksafe si sta concentrando sulla creazione di un sistema blockchain-based che permetterebbe agli utenti di tenere traccia della posizione delle loro pistole nel mondo, allertandoli nel caso in cui risulti che quell'arma ha sparato di recente.

Vendita al dettaglio, mondo retail

Attualmente, *la fiducia nel sistema di vendita al dettaglio è legata soprattutto alla fiducia riposta nel marketplace in cui è stato compiuto un acquisto – ed ecco spiegato perché Amazon è, di fatto, la prima scelta di un utente che si appresta a fare shopping online*. Startup come OpenBazaar stanno sviluppando **utility basate sui registri distribuiti progettate per collegare acquirenti e venditori senza l'intervento di un intermediario super partes** e, ovviamente, senza i costi di intermediazione associati. In questi casi, la fiducia nel sistema sarebbe assicurata dal sistema stesso delle catene di blocchi e dall'ampio utilizzo di smart contract, come ha ben compreso la startup OB 1 che, per sviluppare

Charity e ONG

Per chi è coinvolto in **attività benefiche, fund raising e donazioni, una caratteristica particolarmente apprezzata delle blockchain è la sua capacità di monitorare con precisione dove finiscono i singoli centesimi donati da privati o aziende**. Una lamentela piuttosto comune per chi ha **poca fiducia nelle ONG (Organizzazioni Non Governative)** è l'inefficienza nella gestione dei fondi, unita alla massiccia e diffusa corruzione, che spesso impedisce che i soldi versati arrivino veramente ai bisognosi.

Enti benefici che utilizzano la tecnologia dei Bitcoin, come la fondazione BitGive, offrono la garanzia di una gestione più sicura e trasparente delle donazioni ottenute e hanno visto incrementare sensibilmente l'ammontare dei fondi rastrellati proprio in virtù della possibilità offerta ai donatori di tracciare in modo facile il percorso dei soldi incamerati e spesi.