Affidabile, Autorevole, Accessibile

3ACHAIN

"Un luogo sicuro, dove sviluppare, testare, implementare e applicare soluzioni basate su blockchain, in un contesto altamente professionale e supportato da un autorevole network di fiducia"

Indice **argomenti**

3Achain: **la proposta**

Di cosa si tratta?

Un'infrastruttura blockchain istituzionale, promossa dalla Città di Lugano in collaborazione con partner pubblici e privati, volta a favorire l'accesso a questa particolare tecnologia rivoluzionaria, per creare una cultura digitale e incentivare ricerca e sviluppo, favorire la crescita economica e l'efficienza delle aziende che intenderanno adottarla.
Un'operazione di promozione economica che punta su un settore tecnologico verticale come quello della blockchain per favorire la crescita e l'efficienza delle aziende che intenderanno adottarla, beneficiando delle sue caratteristiche principali quali la distribuzione della fiducia tra le parti e l'accelerazione dei processi di scambio del valore, senza la lentezza e l'onerosità di un intermediario.

Oggi il grande pubblico tende a relazionare la tecnologia blockchain alle valute digitali come Bitcoin e in generale al mondo della finanza. In realtà la stessa può essere utilizzata per un'ampia gamma di applicazioni, come la tracciabilità di un processo di produzione, la certificazione della proprietà, l'autenticità di una documentazione, di un prodotto o di un diritto acquisito arrivando sino al voto online sicuro e alla gestione dell'identità digitale. Se da un lato la comprensione della portata della tecnologia blockchain è ancora limitata, così come pure i casi concreti di utilizzo, sono sempre di più le voci che comparano il momento attuale agli albori del Web nella prima metà degli anni novanta.

La Città di Lugano, durante l'esperienza positiva del progetto MyLugano e la creazione dei LVGA Points, ha avuto modo di utilizzare concretamente la tecnologia blockchain quale infrastruttura principale dell'applicazione e per la gestione dei flussi economici. Si è deciso quindi di lanciarsi coraggiosamente in quest'ulteriore iniziativa ritenendo l'enorme potenziale che una tecnologia come quella della blockchain offre; potenziale ancora poco sfruttato e, al momento, poco conosciuto.

I limiti attuali delle blockchain pubbliche e totalmente decentralizzate (come ad esempio quella di Ethereum) sono quelli della scalabilità e del suo costo. Per distribuire fiducia tra le parti economicamente attive di una società, le istituzioni possono mettere a disposizione la propria autorità e trasparenza a favore di un'architettura più snella ed economica che favorisca l'interazione sociale.

Non si tratta di sostituirsi alle blockchain pubbliche (cosiddette permissionless), ma di affiancarle con delle architetture permissioned che garantiscono le parti coinvolte non tanto attraverso la bontà dell'algoritmo che si occupa di validare le transazioni mediante la potenza di calcolo, ma attraverso la convalidazione dei blocchi da una autorità super partes.

Per agevolare l'accesso a questa tecnologia l'idea è quindi quella di creare un'infrastruttura istituzionale, di facile accesso per stimolarne il più possibile l'adozione diminuendo nel contempo la burocrazia dei processi.

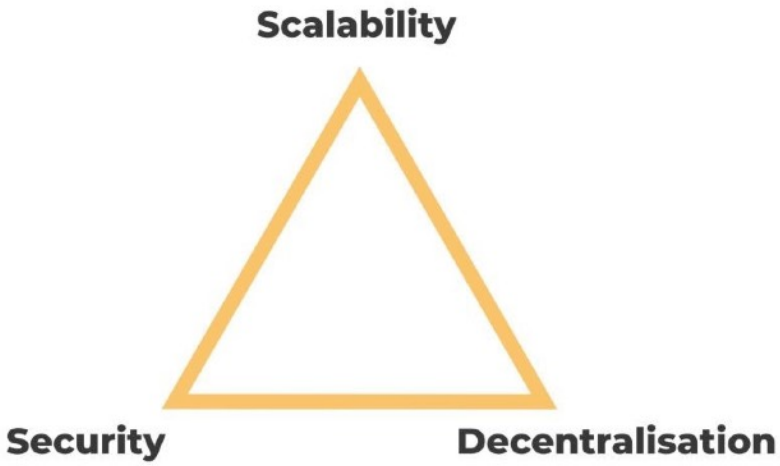
L'accesso all'infrastruttura 3Achain è suddiviso su più fasi e livelli. L'infrastruttura prevista potrà fungere infatti sia da piattaforma operativa che da "palestra" dove, con facilità, poter sperimentare, testare e provare la tecnologia (questo anche in un'ottica di LAB e nell'interesse della ricerca e dello sviluppo). Questo faciliterà l'accesso a un'infrastruttura altamente professionale con un investimento estremamente contenuto garantendo una soglia d'entrata abbordabile per tutti coloro che decideranno di affacciarsi a questa tecnologia. Quest'approccio permetterà di andare oltre agli ostacoli iniziali che si riscontrano quando ci si approccia a una nuova tecnologia estremamente specialistica, facilitandone l'adozione senza dover rinunciare a un servizio professionale e di qualità.
Inoltre, suddividendo su più livelli la possibilità di accesso, sarà possibile incentivare allo stesso tempo la ricerca e lo sviluppo, così come pure la creazione di nuove attività imprenditoriali che potranno sfruttare un aiuto iniziale concreto trovandosi a disposizione un'infrastruttura pronta all'uso e limitando i costi nelle fasi iniziali di progetti che spesso risultano cruciali per l'avvio di una nuova attività economica.
L'accesso a più livelli permetterà di beneficiare di servizi altamente performanti indipendentemente dal fatto che si faccia parte del network promotore dell'iniziativa, che se ne utilizzi unicamente l'infrastruttura o che si effettuino solo dei test.

Chiunque lo desideri potrà iniziare a muovere i primi passi nel mondo della blockchain facendo capo a un'infrastruttura pronta e già implementata, così come pure aziende che decideranno di supportare il network prendendosi a carico una parte dell'infrastruttura stessa (essendo la blockchain per natura decentralizzata); il tutto in una realtà altamente professionale.

Per supportare l'approccio su più livelli verranno create due blockchain: una in ambiente di test/sviluppo e una nell'ambiente di produzione effettivo per la registrazione delle transazioni in ambiente di produzione effettivo, ancorata alla blockchain di Ethereum.
La soluzione ipotizzata garantisce oggi il miglior compromesso in termini di flessibilità e decentralizzazione, permettendo agli utilizzatori di poter effettuare transazioni veloci e a zero commissioni, ma fornendo contemporaneamente la possibilità di correlare le proprie transazioni alla blockchain oggi più diffusa al mondo, quella del network Ethereum.

Il trilemma della blockchain: cos'è e come funziona

Il trilemma della blockchain è una condizione che riguarda i tre principi fondamentali della tecnologia ossia: sicurezza, scalabilità e decentralizzazione.



Inizialmente espresso da Vitalik Buterin, creatore della rete Ethereum, il trilemma afferma che tutte le blockchain possono risolvere solo due dei problemi appena citati.

L'esempio di Bitcoin è emblematico: fino al 2017 era una moneta decentralizzata e sicura ma estremamente lenta nel processare un elevato numero di transazioni. La poca scalabilità della blockchain di Bitcoin è dovuta all'architettura della stessa che, valorizzando sicurezza e decentralizzazione, permette di creare un muro per proteggere la criptovaluta. In particolare l'algoritmo di consenso della criptomoneta (Proof of Work) non gli permette di scalare in maniera esponenziale come altri (es. Proof of Stake), ma dalla sua ha sicuramente la sicurezza e la durevolezza che la rendono la più sicura da attacchi di qualsiasi tipo.

Per risolvere il trilemma, e quindi diventare a tutti gli effetti una blockchain ideale, il protocollo creato da Satoshi Nakamoto doveva necessariamente scalare.

Il trilemma della blockchain: la soluzione proposta

Se in questo momento la criptovaluta sta attirando gli occhi di investitori istituzionali e trader di tutto il mondo, quando diventerà mainstream farà la stesso con tutto il mondo retail.

Se la blockchain è il registro per l'oro 2.0 e ormai non sono più solamente i nerd a dirlo ma anche le banche e i canali di pagamento come Paypal, Visa e Mastercard, è necessario individuare soluzioni che permettano ad istituzioni, imprese e cittadini la possibilità di notarizzare le proprie registrazioni in modo semplice e intuitivo, garantendo un adeguato livello di sicurezza, scalabilità e nel contempo decentralizzazione.

La soluzione proposta dalla Città di Lugano tecnicamente è una Private Blockchain (permissioned blockchain) ancorata alla rete Ethereum, basata su un sistema di validazione definito PoA (Proof of Authority - di cui sono disponibili approfondimenti tecnici su richiesta). L'algoritmo di consenso PoA consente appunto di poter effettuare transazioni infinite, a zero costi di transazione, con un adeguato livello di sicurezza, basandosi non sulla risoluzione di complessi calcoli matematici come nel PoW ma sull'autorevolezza di quelli che sono i nodi validatori che fanno parte della rete. In sostanza, l'elevata complessità dei calcoli necessari per garantire la sicurezza in una blockchain pubblica in cui non si conosce l'identità dei nodi (Bitcoin, Ethereum, etc.) viene superata affidando la gestione delle transazioni esclusivamente a dei nodi scelti e verificati, di cui si ha piena fiducia, come appunto enti pubblici, università e società private che collaborano l'una con l'altra nel registrare e validare transazioni reciproche, senza averne nessun guadagno diretto e garantendo tutte insieme l'immutabilità delle transazioni.
Le transazioni sono registrate in ogni nodo, vale a dire presso ogni singola struttura o ente che aderirà al progetto, e verranno tutte riconciliate con la blockchain pubblica di Ethereum alle 24.00 di ogni giorno così da garantire un doppio livello di sicurezza a tutti quanti entreranno nel network promosso dalla Città di Lugano. Ogni registrazione avrà quindi un proprio hash sia nel network 3Achain che nel network di Ethereum.

Perché il progetto sia completo e scalabile, è necessario garantire anche un elevato livello di estensione del network stesso; è per questo motivo che la Città di Lugano apre ora ad altri partner istituzionali il progetto iniziato nel 2020, volto a essere la risposta Svizzera a diverse soluzioni che stanno fiorendo a livello globale, dalla vicina Austria, agli Stati Uniti sino alla Cina.

A oggi l’esempio più affermato di infrastruttura blockchain pubblica che offre a sviluppatori e PMI risorse per costruire servizi e applicazioni basate sulla blockchain a costi accessibili sembra essere la piattaforma cinese Blockchain-based service network (Bsn).

La città di Vienna invece sta testando una soluzione su blockchain per convalidare e proteggere i suoi Open Government Data (OGD), che includono dati come le tratte dei trasporti pubblici, gli orari dei treni, ecc.. Il progetto fa parte dell'iniziativa di digitalizzazione della città chiamata "DigitalCity.Wien". Vienna utilizza la blockchain per semplificare e automatizzare i processi amministrativi, in particolare per OGD come report energetici e registrazioni aziendali valide, che devono essere aggiornate frequentemente. Inoltre, le reti blockchain stanno contribuendo a migliorare la sicurezza dei dati di queste informazioni. Da quando la soluzione è stata lanciata circa 350 set di dati sono stati protetti sulle reti blockchain. Una delle prime ad essere lanciate in Europa, con lo scopo di proteggere i documenti ufficiali archiviando gli hash dei set di dati sulle blockchain pubbliche, consentendo ai dipendenti della città e ai cittadini di rivedere l'autenticità dei documenti, quando sono stati creati e quando e se i dati sono stati modificati.

È bene ricordare che non è importante definire in anticipo per quale finalità venga utilizzata una blockchain, essa infatti è una tecnologia agnostica, che non fa altro che validare dati e transazioni. Una volta implementata, potrà essere utilizzata per i registri del catasto, per emettere fatture, registrare i pagamenti delle imposte, per certificare degli elenchi di sussidi o, semplicemente, per annotare tutte le transazioni di una moneta locale, come i LVGA Points. In sostanza la Blockchain è un’infrastruttura abilitante per lo sviluppo di tutta una serie di nuove applicazioni che si appoggiano su di essa per funzionare.
Il registro sarà il medesimo, e potrà essere utilizzato anche da tutti gli operatori economici che volessero certificare alcuni processi di produzione interna, come la tracciabilità di un prodotto, l’autenticità e la sua proprietà. Tutti utilizzeranno la stessa blockchain e ognuno sarà un nodo del network che replicherà le informazioni e ne garantirà esso stesso la trasparenza e la sua immutabilità.

Saranno sviluppati e messi a disposizione di tutti i participanti del progetto anche dei tool e dei bridge che permetteranno la trasportabilità dei dati dalla blockchain 3Achain a quella pubblica di Ethereum. Questo permetterà di testare le proprie soluzioni sulla blockchain permissioned per poi passare, qualora ve ne fosse la necessità, a quella permissionless e totalmente decentralizzata senza disperdere tutto l’investimento e lo sviluppo sostenuto fino a quel momento.

Il Network 3Achain

È possibile aderire al progetto promosso dalla Città di Lugano in diverse forme.

La forma di partecipazione può essere quella di semplice utilizzatore della rete di TEST, oppure utilizzatore dell'infrastruttura MAIN, in diverse modalità di partecipazione, da utilizzatore, a detentore di una copia di tutto il registro (nodo), diventando partner dell'intera soluzione e contribuendo alla crescita ed allo sviluppo della stessa.

Per questo progetto la Città di Lugano ha fortemente voluto coinvolgere anche il mondo accademico locale: si ritiene infatti che le università, avendo libero accesso all'infrastruttura, potranno giocare un ruolo fondamentale nelle attività di ricerca e sviluppo.

È importante inoltre permettere a studenti e facoltà di poter accedere a nuove tecnologie in forma quanto più possibile gratuita, per consentire alle giovani menti che saranno il pilastro della nostra economia di domani, di approcciarsi a questi strumenti di innovazione tecnologica sin dai momenti di studio ancora prima che sui posti di lavoro.

La Città di Lugano sta elaborando al riguardo un modello di governance in collaborazione con dei consulenti esterni. Lo stesso verrà condiviso con tutti i partner che hanno dichiarato interesse all'iniziativa.

Condizioni particolari verranno riservate ai partner della prima ora che volessero contribuire allo sviluppo e all'implementazione dell'ecosistema promosso dalla Città di Lugano.

Per questo progetto è già stato attivato uno specifico team blockchain, in collaborazione con aziende locali che già fanno parte del network di Lugano Living Lab e che, in collaborazione con la Città di Lugano, hanno contribuito allo sviluppo del progetto MyLugano.
Questo team sta già lavorando in diversi settori come ad esempio nella certificazione di autenticità di prodotti e la tracciatura della loro filiera; ma le applicazioni sono molteplici e vanno dai prodotti farmaceutici, all'energia, ai servizi assicurativi, bancari e finanziari, sino alla gestione di diritti su contenuti e delle royalties.

Chi deciderà di aderire a quest'iniziativa potrà quindi trovare già attive nel progetto le necessarie competenze e far capo a queste aziende che sono state coinvolte sin dal principio alla creazione dell'infrastruttura; oppure potrà tranquillamente ricorrere a personale proprio o rivolgersi, se del caso, ad altre aziende di sua fiducia.

Questo progetto rende la Città di Lugano un pioniere nell'implementazione della blockchain nella pubblica amministrazione ed è un fattivo contributo per una città aperta e partecipativa con una burocrazia ridotta. Con la blockchain, i collaboratori degli enti pubblici e privati, i residenti o gli sviluppatori di app, potranno tracciare i cambiamenti dei dati, condividere conoscenza e far divenire Lugano un'eccellenza per la blockchain, nonché una delle città tecnologicamente più lungimiranti al mondo.

La soluzione tecnologica

La blockchain

La blockchain che verrà utilizzata per creare la 3Achain si basa sulla tecnologia di Quorum®.

Quorum è una piattaforma blockchain per applicazioni aziendali e industriali. Deriva da un fork del client Ethereum pubblico 'geth' con diversi miglioramenti a livello di protocollo per supportare le esigenze di maggiore scalabilità.

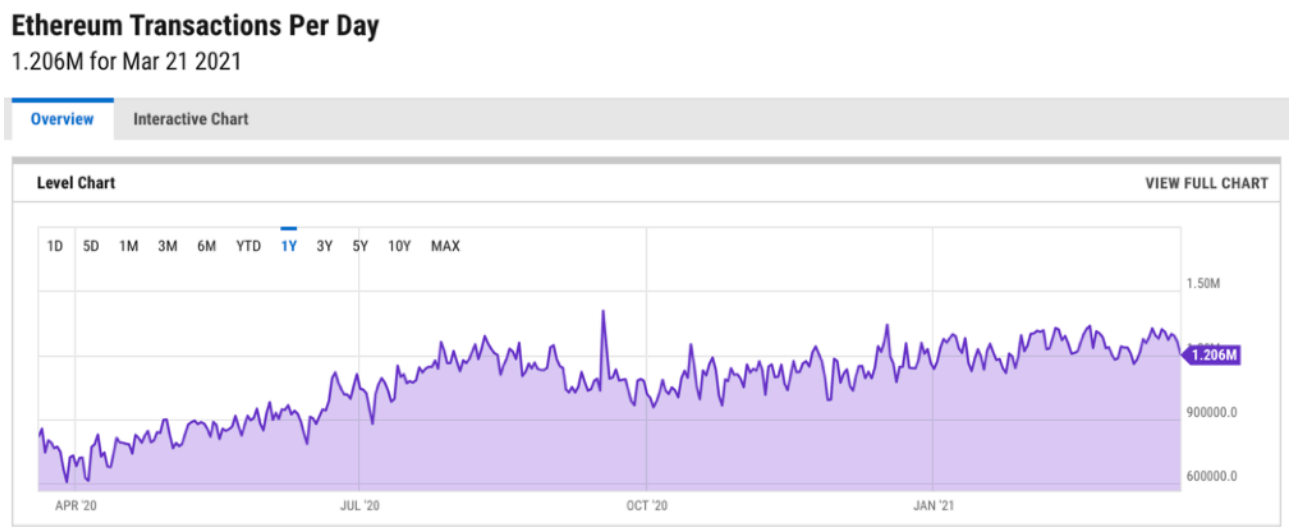
Poiché Quorum è un progetto open-source, il codice di base della piattaforma è aperto e verificabile da chiunque, il che promuove la trasparenza e di conseguenza la fiducia nella piattaforma. L'approccio open-source permette inoltre di attrarre sviluppatori di diversi settori a partecipare all'evoluzione di questa piattaforma.

È un codice già utilizzato da organizzazioni di provata fiducia quali:

Microsoft J.P.Morgan covantis South African Reserve Bank sia CHAIN komgo

Ci sono due vantaggi principali nell'utilizzare questa soluzione.

Il primo è che la tecnologia è testata da oltre 6 anni di attività della rete Ethereum che ad oggi sviluppa già oltre 1,2 MLN di transazioni al giorno senza che questo abbia mai comportato una sola perdita di un dato.



Inoltre applicando alla stessa tecnologia un algoritmo di validazione Proof of Authority (PoA), anziché una Proof of Work (PoW), la scalabilità è innalzata di n fattori, portando la potenza di registrazione a centinaia di transazioni al secondo.

Il secondo vantaggio è che questa tecnologia, con il suo linguaggio di programmazione Solidity, è in assoluto la più diffusa in ambito blockchain.
Vi sono infatti centinaia di team di sviluppo in tutto il mondo che apportano innovazione spesso in versione open-source, e quindi liberamente consultabile e utilizzabile, il che porta ad una sinergia mai vista prima in un ambiente di sviluppo. Ciò significa che tutte le innovazioni portate da Ethereum Foundation in primis, e dagli altri team di sviluppo, potranno essere implementate sulla 3Achain.

L'infrastruttura
(caratteristiche tecniche dei nodi validatori)

Come già descritto precedentemente, i componenti del Network 3Achain, oltre a creare un'importante alleanza strategica, saranno essi stessi a costituire la rete blockchain, diventando ognuno una componente dell'infrastruttura.

Questo significa che ogni membro del network ospiterà e gestirà uno dei nodi validatori che compongono la blockchain 3Achain.

In sostanza si tratta di ospitare (presso i propri datacenter o in cloud) un server che ospiterà il proprio nodo validatore. La manutenzione e gli aggiornamenti di tutti i nodi verranno coordinati centralmente; questo permetterà di limitare gli interventi da parte dei partner del network, in modo da non pesare eccessivamente chiedendo importanti sforzi e risorse, pur mantenendo e garantendo il principio sacrosanto alla base della blockchain: la decentralizzazione.

Il server che ospiterà il nodo validatore, dovrà avere le seguenti caratteristiche.

Requisiti hardware minimi	Requisiti hardware minimi
VPS running recent versions of Mac OS X or Linux	VPS running recent versions of Mac OS X or Linux
500 GB of free disk space, solid-state drive (SSD)	500 GB of free disk space, solid-state drive (SSD)
2 cores of CPU and 4 gigabytes of memory (RAM)	2 cores of CPU and 4 gigabytes of memory (RAM)
A broadband Internet connection with upload/ download speeds of at least 5 megabyte per second	A broadband Internet connection with upload/ download speeds of at least 5 megabyte per second

Stima effort per installazione di un nodo della 3Achain: 5/6 ore di un sistemista esperto per installazione + test (una tantum) e 48 ore/anno come per la manutenzione.

Approfondimenti: il caso MyLugano / LVGA Points e concetti relativi alla Blockchain

L'app MyLugano

MyLugano è il nuovo programma della Città di Lugano che intende promuovere la spesa locale in un periodo ricco di sfide inedite per tutti.

Il programma ha per obiettivo:

- offrire una tessera del tempo libero a favore dei cittadini di Lugano e di chi vive la città pur non essendo residente,
- rispondere alle nuove abitudini degli utenti, sempre più orientati verso l'offerta online di esercizi e istituzioni,
- sostenere il commercio del territorio, riconoscendone l'importante ruolo di aggregatore sociale,
- aiutare l'economia locale a beneficio dei cittadini e degli esercizi commerciali, sfruttando il circuito Lugano Card.

I LVGA Points e il sistema di cashback

La novità introdotta dalla Città è il programma fedeltà che coinvolge i partner di MyLugano.

I punti del circuito MyLugano si chiamano LVGA Points. I LVGA Points sono una vera e propria moneta complementare digitale. I punti vengono accreditati attraverso acquisti presso qualsiasi partner del circuito MyLugano, per un importo pari al 10% del valore dell'acquisto. Gli stessi sono cumulabili attraverso più acquisti presso diversi partner del circuito e spendibili in nuovi acquisti all'interno dello stesso. I LVGA Points sono pure acquistabili tramite l'app MyLugano.

I punti hanno un tasso di conversione CHF 1.- = 100 punti; hanno una scadenza di 24 mesi e un tetto massimo di accumulo annuo di 100'000 punti e di movimenti mensili pari a 500'000 punti.

Partecipare al programma fedeltà MyLugano è un modo concreto per sostenere l'economia locale e creare un network virtuoso all'interno del territorio.

La tecnologia utilizzata per l'app MyLugano: la blockchain

Una necessità fondamentale per aziende e istituzioni è quella di archiviare dati ed effettuare transazioni in modo celere, sicuro e condivisibile tra gli addetti ai lavori.
A questo scopo, una nuova tecnologia è venuta alla ribalta per garantire tutto questo in modo semplice, veloce e soprattutto decentralizzato.

La blockchain, tradotta in italiano "catena dei blocchi", nata nel mondo finanziario, sta trovando infatti numerose applicazioni anche nel mondo industriale, dove interviene a semplificare e garantire i processi aziendali, attraverso l'implementazione di un registro digitale che raggruppa i dati in blocchi ordinati, posti cronologicamente e crittografati.

La blockchain è nata come rete architettonica decentralizzata, in quanto non possiede un amministratore centrale, ma è amministrata e gestita autonomamente dai diversi utenti in ogni parte del mondo, i quali confermano la validazione delle transazioni in essa contenute.
Ogni blocco contiene caratteristiche uniche dovute al fatto che il suo contenuto non è più modificabile né eliminabile da esterni una volta scritto e, pertanto, costituisce una sicura alternativa alle banche dati e/o registri, gestiti, per esempio, dalle pubbliche amministrazioni, dagli intermediari di pagamento, da assicurazioni, banche, e si pone come tecnologia alternativa grazie alla sua affidabilità, sicurezza e trasparenza.

È evidente quindi che i campi di applicazione di tale innovativa tecnologia risultano essere innumerevoli.

Che cosa è la blockchain?

La Blockchain è un registro digitale aperto, un libro mastro elettronico pubblico, volto a memorizzare un numero infinito di dati (i.e.: transazioni) mediante la crittografia, la quale rappresenta senz'altro il principale elemento del suo successo, dato che svolge la conversione dei dati leggibili in dati codificati, i quali, pertanto, possono essere letti ed elaborati in modo pseudo-anonimo, tramite codici alfanumerici, e sono contrassegnati ognuno da una marca temporale, che li rende univoci, preservandone così la privacy. In buona sostanza, si immagini una immensa banca dati condivisa, alla quale si possono sistematicamente aggiungere nuovi blocchi di informazioni, che verranno crittografate, alla quale tutti possono accedere, ma che nessuno può modificare, riducendo al minimo la quantità di interazione umana necessaria per far funzionare l'intero sistema.

Tipologie di blockchain

Al mondo oggi esistono varie tipologie di Blockchain, che possono essere suddivise essenzialmente in due grandi categorie, di tipo pubblico o privato. Nel primo caso, le transazioni possono essere visionate, ricevute ed inviate da chiunque, spesso sono utilizzate per le applicazioni di carattere finanziario e per la gestione di criptovalute.

Le Blockchain private, invece, sono limitate a pochi partecipanti individuati in modo predeterminato, (si pensi al caso di un gruppo di impiegati di una data azienda o gruppo di aziende, oppure a quello di una rete di banche), e solamente essi sono autorizzati a scrivere sul libro mastro distribuito. Le Blockchain private sono controllate da un'unica organizzazione o da gruppi di organizzazioni riuniti in una "federazione", autorizzati ad indicare chi è legittimato ad aderirvi, ad operare transazioni, nonché chi può partecipare al processo di consenso e validazione.

È proprio questo secondo ambito a rappresentare la nuova sfida della "Blockchain 2.0", presente per lo più in ambito finanziario, attraverso l'implementazione di smart contract, o "contratti intelligenti", contratti scritti sotto forma di codice che rimandano l'esecuzione di alcune o tutte le loro clausole a un software, che le esegue in automatico al verificarsi di determinate condizioni. Tali contratti sono ad esempio già in uso presso diverse compagnie assicurative e stanno prendendo piede in svariate applicazioni.

Blockchain e diffusione del fenomeno

Il concetto di blockchain è strettamente collegato al nome di “bitcoin”, criptovaluta o valuta digitale per eccellenza, nata nel 2009 a seguito dell’ultima grande crisi finanziaria, e che permette di fare pagamenti, anche cross-border (o transfrontalieri), in ogni angolo del globo, in pochi minuti e con bassissimi costi per ogni transazione. Il bitcoin è stato definito dal suo fondatore, Satoshi Nakamoto, “una versione peer-to-peer di denaro elettronico che consente di inviare direttamente pagamenti online da un soggetto all’altro senza passare attraverso un istituto finanziario”.

L’idea rivoluzionaria di Nakamoto comprende un tipo di archiviazione dati in cui tutti possono vedere cosa c’è dentro e assicurarsi che sia reale. Non può essere modificato neanche un singolo bit, e una volta che qualcosa è sulla rete, rimane lì per sempre. La tecnologia, nata appunto nel mondo finanziario delle criptovalute e usata per verificare tutte le transazioni tra gli utenti per evitare le frodi si è velocemente allargata e sviluppata all’interno di molteplici settori economici.

Ad esempio la blockchain viene usata nel settore agroalimentare o logistico per verificare la provenienza di un prodotto o in quello legale per rendere sicuri i contratti (con i cosiddetti smart contract) o ancora in quello della pubblica amministrazione per la gestione di voti o dati sensibili online.
Da queste poche parole si può già intuire la portata rivoluzionaria di questa tecnologia. Il futuro è ancora da tutto da scrivere, ma sembra portare alla “Blockchain 3.0”, mediante la diffusione e lo sviluppo delle “Dapp” o decentralized applications, create per la maggior parte sulla blockchain di Ethereum, seconda catena di blocchi più famosa e sicuramente la più estesa al mondo al giorno d’oggi.

È abbastanza facile immaginare che presto chiunque utilizzi funzioni della blockchain lo farà senza nemmeno esserne edotto sulla tecnologia sottostante, come oggi avviene per impostare un indirizzo mail sul nostro smartphone, perché esse saranno presenti ovunque, inserite nelle applicazioni relative a prodotti e servizi.

Perché utilizzare la blockchain e quali sono i vantaggi?

La tecnica blockchain può essere applicata a tutti i processi di transazione che coinvolgono diversi partecipanti e i suoi applicativi sono potenzialmente infiniti. Tra i principali vantaggi di questa tecnologia citiamo:

- **Efficienza**: lo scambio di tali valori avviene in tempo reale.
- **Struttura decentrata e sicurezza**: i dati blockchain non vengono memorizzati su un solo computer ma all'interno di un network distribuito di nodi, per cui il sistema e i dati sono resistenti a errori tecnici e attacchi malevoli. Ciascun nodo è in grado di replicare e archiviare una copia dell'intero database sin dalla sua origine.
- **Incontestabilità**: la decisione di validare un'informazione non viene presa unilateralmente ma attraverso un meccanismo di raccolta del consenso all'interno della rete, rendendo particolarmente difficile metterne in discussione l'esito.
- **Costo di transazione ridotto**: perché è una rete peer-to-peer senza intermediari che andrebbero remunerati.
- **Immutabilità**: le transazioni e i dati che vengono registrate all'interno dei blocchi sono immutabili.
- **Tracciabilità**: riguardante i dati e i trasferimenti.
- **Trasparenza**: rafforza le relazioni di fiducia perché ogni soggetto autorizzato all'interno della rete può visualizzare in qualunque momento importo, mittente e destinatario di una qualsiasi transazione.
- **Sistema trustless**: a differenza dei sistemi di pagamento tradizionali, le transazioni non necessitano di alcun intermediario finanziario.
- **Programmabilità**: all'interno dei blocchi possono essere incluse istruzioni che facciano scatenare specifiche azioni al verificarsi di determinate condizioni.
- **Flessibilità**: può essere utilizzata sia per scopi commerciali che privati.

Cosa è un token?

Nel mondo della blockchain, un token è un gettone virtuale, il cui valore è emesso da un'organizzazione ed eventualmente accettato da una comunità. Pertanto, il valore di un token è quello che il suo creatore decide di attribuirgli garantendone una convertibilità, oppure sarà quello che gli assegnerà il mercato.

Esistono diverse forme e funzioni di token: gli utility token permettono di accedere ad un servizio, gli asset token certificano la proprietà di un determinato bene, i payment token sono un succedaneo del denaro corrente.

I token non sono da confondere con le coins native di una blockchain, in quanto a differenza di queste ultime si basano su una blockchain terza all'interno della quale vengono creati. La più utilizzata è quella di Ethereum in cui vengono eseguiti anche degli smart contracts che definiscono funzioni e operatività dei token.

Cosa è un wallet?

Essendo i token dei gettoni digitali, per poterli utilizzare, possedere e scambiare occorre creare un portafoglio digitale chiamato appunto "wallet", parola inglese che significa appunto "portafoglio". Un wallet è quindi un portafoglio digitale sicuro (perché protetto da crittografia) usato per ricevere e trasferire token (gettoni digitali). Proprio come avviene con i numeri IBAN ogni portafoglio elettronico ha un suo indirizzo univoco composto da lettere e numeri usato per ricevere e trasmettere i token.

Gli scambi avvengono in modo semplice ed immediato, tramite visualizzazione di QR Code indicanti l'indirizzo alfanumerico del ricevente, ed in pochi semplici click è possibile effettuare un trasferimento "peer to peer", vale a dire da punto a punto o da persona a persona, tra due soggetti, emittente e ricevente, senza intermediario.

Cosa è uno smart contract?

Gli smart contract sono un insieme di righe di codice informatico che operano su una blockchain, che al pari di un contratto tradizionale definiscono i termini di un accordo tra due o più parti. La differenza principale sta nella presenza all'interno del software della funzione if/then (se/allora), le quali rendono automatica un'azione (come ad esempio un pagamento) al verificarsi di una determinata condizione.

Questi codici consentono quindi un automazione decentralizzata, facilitando, verificando e facendo rispettare le condizioni di un accordo predefinito.

Gli smart contract consentono di scambiare qualsiasi cosa di valore, compreso denaro, azioni e proprietà ecc.. in modo sicuro e trasparente e senza ricorrere ad intermediari.

Ethereum è la piattaforma blockchain più popolare per la creazione di smart contract e per questa ragione i due termini vengono spesso associati.

È vero che la blockchain non è sostenibile e che consuma molta energia?

Va innanzitutto precisato che ogni soluzione tecnologica e digitale, necessita di energia (elettricità) e quindi crea conseguentemente dei consumi e, a dipendenza degli stessi, può avere un impatto più o meno importante sull'ambiente.

Quando si parla di blockchain, spesso e volentieri, la mente corre al Bitcoin. Effettivamente soluzioni estese, importanti e complesse, come quelle che sono alla base di questa criptovaluta necessitano di un'infrastruttura articolata e un consumo energetico importante.
Nel caso di Bitcoin, l'energia richiesta per il mantenimento della rete è dato dal fatto che per validare le transazioni è necessario risolvere algoritmi complessi, che richiedono potenti computer, questo meccanismo, denominato "proof of work" o "prova di lavoro" è stato rivisto nel corso degli anni, e Bitcoin stesso sta evolvendo verso nuove forme di consenso meno "energivore".

Soluzioni successive, come ad esempio quelle adottate dalla rete Ethereum, prima al mondo per dimensione e utilizzo, dalla quale è mutuata anche l'Applicazione My Lugano, stanno sviluppato forme di consenso più veloci e meno impattive, in linea con le principali applicazioni informatiche in altri settori.

In un orizzonte temporale di pochi anni, l'energia richiesta per validare le transazioni sarà molto ridotta, sia grazie a soluzioni di validazioni PoS (Proof of Stake), sia all'utilizzo di second layer per minimizzare le registrazioni sull'archivio principale.

Come detto in entrata, qualsiasi soluzione digitale, causa dei consumi; si pensi ad esempio anche solo un semplice sito web che deve essere ospitato su un server e quest'ultimo deve essere attivo 24 ore su 24 collegato alla rete elettrica.

Nel caso specifico, l'infrastruttura a capo della blockchain che gestisce la soluzione MyLugano, è una soluzione relativamente semplice e con un perimetro circoscritto e limitato; questo fa sì che i consumi siano già oggi contenuti e quindi con un impatto ambientale minimo, pari a qualsiasi piattaforma web.

Pensiamo inoltre che l'obiettivo dell'iniziativa (incentivare il commercio locale) ha delle ripercussioni estremamente positive anche dal punto di vista della sostenibilità ambientale, oltre che sociale ed economica.

Glossario

Address: è la chiave pubblica di un portafoglio in criptovaluta ed è formata da una stringa di caratteri alfanumerici utilizzata per ricevere o inviare le transazioni. E' la sola informazione che va fornita per ricevere unità di una valuta digitale.

Bitcoin: è un sistema di pagamento peer-to-peer e una valuta digitale, decentralizzata, open source, alimentata dai suoi utenti e senza nessuna autorità centrale o intermediari. Per convenzione si utilizza la parola “Bitcoin”, scritta in maiuscolo per riferirsi alla tecnologia di pagamento e registrazione crittografia di informazioni, mentre la parola “bitcoin”, scritta in minuscolo, si riferisce alla valuta digitale.

Blocco: è l’unità che compone la Blockchain e contiene tutte le transazioni confermate durante il periodo di generazione del blocco stesso. In media ogni 10 minuti un nuovo blocco, che include delle transazioni, viene generato e aggiunto alla Blockchain attraverso il processo di mining.

Blockchain: è un registro pubblico o “libro mastro" di tutte le transazioni in una valuta digitale. In termini informatici si può definire come un database distribuito su ogni nodo che fa parte del network e che sfrutta la tecnologia peer-to-peer.
È quindi un canale di comunicazione distribuito (una catena di blocchi di informazioni) che permette di trasferire un valore o una proprietà digitale con la garanzia che nessun terzo possa danneggiare o modificare le transazioni per trarne vantaggio.
La blockchain è fatta di blocchi che memorizzano gruppi di transazioni valide, correlate da un marcatore temporale (timestamp). Ogni blocco include l'hash del blocco precedente, collegando i blocchi insieme. I blocchi collegati formano una catena, con ogni blocco addizionale che rinforza quelli precedenti. La definizione originale fu scritta da Satoshi Nakamoto e trovata nel codice sorgente di bitcoin.

BTC: è un'unità comune utilizzata per designare un bitcoin.

Chiave privata: è una parte di dati segreti (un codice alfanumerico) che provano che sei tu ad utilizzare bitcoin o altra criptovaluta da un determinato portafoglio (wallet) attraverso una firma crittografata. La chiave privata (o chiavi private) è conservata nel tuo computer se utilizzi un portafoglio software; è invece conservata in un server remoto se utilizzi un portafoglio web. La chiave privata deve essere custodita con la massima cura, non deve essere rivelata ad altri in quanto ti permette di accedere ai fondi dal tuo wallet.

Chiave pubblica: è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica che nell'ambito delle criptovalute è rappresentata dall'address. La chiave pubblica può essere scambiata per effettuare le transazioni.

Conferma (o consenso): una transazione in Bitcoin (o di altra criptovaluta) é valida solo quando viene confermata dal network attraverso l'attività di mining. La conferma indica che una transazione è stata processata dalla rete, ed è altamente improbabile che sia respinta. Le transazioni ricevono una conferma quando sono incluse in un blocco, e per ogni blocco successivo. Ogni conferma, esponenzialmente, diminuisce il rischio di una transazione respinta.

Crittografia: è quella branca della matematica che ci consente di creare prove matematiche che forniscono elevati livelli di sicurezza, dando così la possibilità di trasmettere un messaggio mantenendolo segreto a tutti, tranne alle persone che possiedono le chiavi per decifrarlo. Si definisce crittografia simmetrica quando si utilizza la medesima chiave per cifrare e decifrare un messaggio, e crittografia asimmetrica quando si utilizzano chiavi diverse (come nel caso del sistema Bitcoin).

Cryptocurrency (o criptovaluta): è una valuta o mezzo di scambio, che utilizza la crittografia per proteggere le transazioni e controllare la creazione di nuove unità.

Dapp (Decentralized Application): applicazione decentralizzata, basata su reti distribuite, con software open source, il cui funzionamento è abilitato da token crittografici che servono come misura di valore ed eventuale filtro di accesso.

DAO (Decentralized Autonomous Organizations) o DAC (Decentralized Autonomous Corporations): organizzazioni autonome decentralizzate che si finanziano emettendo una propria criptovaluta. Gli investitori e finanziatori conferiscono nell'impresa valuta fiat e ottengono in cambio la criptovaluta che funge da titolo di partecipazione alla distribuzione dei dividendi dell'impresa e al contempo da mezzo di scambio spendibile sul mercato.

Distributed ledger: altro termine per indicare la blockchain.

Ethereum: piattaforma per la costruzione di applicazioni decentralizzate, protette a livello crittografico.

Ether: criptomoneta che serve per richiedere risorse computazionali al sistema Ethereum.

Fiat currency: è la moneta tradizionale che deriva il suo valore essenzialmente da un'autorità e dalla fiducia della gente. Può essere considerato un valore fiduciario, cioè non determinato dal valore intrinseco di un materiale, quale per esempio l'oro e l'argento. Tutte le attuali monete ufficiali sono di fatto fiat currency.

Firma Crittografica: è un meccanismo matematico che consente di provare la proprietà. Nel caso di Bitcoin, un portafoglio Bitcoin e la sua chiave privata(e) sono collegati per mezzo di un vincolo matematico. Quando il tuo software Bitcoin segna una transazione con la chiave privata appropriata, l'intera rete può vedere che la firma combacia con i bitcoin spesi. Tuttavia, non c'è alcun modo per gli altri di scoprire la tua chiave privata, per derubarti dei tuoi bitcoin, ottenuti col sudore della fronte.

Fork: Si divide in hard fork e soft fork. Un soft fork è quando una nuova versione del protocollo è introdotta, ma i vecchi client riescono comunque a processare le transazioni generate dai clienti aggiornati. Un hard fork è quando invece questo non avviene, e i vecchi client non riescono più a processare i blocchi dei nuovi.

Funzione Hash: è una funzione che trasforma un messaggio di lunghezza arbitraria in un codice alfanumerico di lunghezza prefissata, che prende il nome di Hash, Digest o impronta del messaggio. La funzione Hash utilizzata nel sistema Bitcoin è l'algoritmo SHA-256.

Incentivi: è il "rimborso" per il lavoro svolto e riconosciuto ai minatori. Si compone di nuovi bitcoin e commissioni di transazione incluse in ogni blocco. Vengono assegnati 50 bitcoin per ogni blocco risolto, ma questo valore si dimezza ogni 210.000 blocchi.

Indirizzo (o Address): vedi Address.

Input: è quella parte di una transazione in bitcoin che identifica l'origine della transazione stessa. Tipicamente si tratta di un address, salvo il caso in cui si tratti di bitcoin di nuova generazione.

Mining: è il processo con cui si verificano e registrano tutte le transazioni in bitcoin, ma è anche l'attività che permette di coniare nuovi bitcoin. Tale processo fa eseguire all'hardware del computer calcoli matematici al fine di confermare le transazioni ed aumentare la sicurezza della rete Bitcoin. Come ricompensa per il loro servizio, i miner (minatori) di Bitcoin possono incassare delle commissioni sulle transazioni che confermano insieme ai nuovi bitcoin appena creati. Il numero massimo a disposizione è pari a 21 milioni e tale offerta verrà completata entro il 2140.

Network: il sistema Blockchain è organizzato in nodi secondo una rete distribuita, decentralizzata e paritaria. Questo tipo di rete è detto P2P (peer-to-peer).

Output: è quella parte di transazione in bitcoin che identifica l'address di destinazione della transazione stessa.

Peer-to-peer (P2P): generalmente inteso come sistema di trasmissione di transazioni direttamente tra due individui senza intermediari.
In informatica, è un'espressione che indica un modello di architettura logica di rete informatica in cui i nodi non sono gerarchizzati unicamente sotto forma di client o server fissi (clienti e serventi), ma sotto forma di nodi equivalenti o paritari (in inglese peer) che possono cioè fungere sia da cliente che da servente verso gli altri nodi terminali (host) della rete. Essa dunque è un caso particolare dell'architettura logica di rete client-server.

Portafoglio: vedi Wallet

Proof-of-work: è una misura economica per scoraggiare attacchi denial of service (diniego di servizio) e altri abusi di servizio, come spam sulla rete, imponendo alcuni lavori dal richiedente del servizio, di solito intendendo tempo di elaborazione di un computer. Una caratteristica chiave di questi schemi è la loro asimmetria: il lavoro deve essere moderatamente complesso (ma fattibile) dal lato richiedente, ma facile da controllare per il fornitore del servizio (service provider).

Proof-of-burn: sistema con cui un numero di bitcoin sono inviati ad un indirizzo che li elimina in modo permanente dalla circolazione.

Proof-of-stake: vagamente traducibile in Italiano come, "prova che si ha una posta in gioco" è il nome di un metodo per la messa in sicurezza di una rete di criptovaluta e per il conseguimento di un consenso distribuito. È basato sul principio che ad ogni utente venga richiesto di dimostrare il possesso di un certo ammontare di criptovaluta. Si differenza dai sistemi proof-of-work che sono basati su algoritmi di hash che validano le transazioni elettroniche. Peercoin è stata la prima criptovaluta ad utilizzare sin dal lancio il sistema Proof-of-Stake.

Satoshi Nakamoto: è uno pseudonimo dietro al quale si è celato il creatore del sistema Bitcoin e della moneta bitcoin. Ad oggi non c'è ancora certezza circa la sua identità.

Smart contract: contratti tra parti che hanno la possibilità di auto-verifica e auto-enforcing in assenza di terze parti. Sono accordi fra parti, fissati a livello algoritmico e con caratteristiche di auto-eseguibilità e controllo, indipendenti dall'intervento di terze parti e dall'adesione a un sistema giuridico e normativo esistente.

Software Open source: in informatica, il termine inglese open source (che significa sorgente aperta) indica un software di cui gli autori (più precisamente, i detentori dei diritti) rendono pubblico il codice sorgente, favorendone il libero studio e permettendo a programmatori indipendenti di apportarvi modifiche ed estensioni. Questa possibilità è regolata tramite l'applicazione di apposite licenze d'uso. Il fenomeno ha tratto grande beneficio da Internet, perché esso permette a programmatori distanti di coordinarsi e lavorare allo stesso progetto.

XTB: altra sigla che può indicare il bitcoin.

Wallet (o Portafoglio): è un portafoglio elettronico che memorizza tutte le credenziali digitali per accedere, spendere e trasferire i bitcoin o le altre altcoin. Esistono tre tipi di wallet: desktop, smartphone e web wallet. Il wallet gestisce le chiavi private che permettono di firmare le transazioni. Ogni portafoglio Bitcoin può mostrarti il bilancio totale di tutti i bitcoin che controlla e ti permette di pagare cifre precise ad una persona specifica, come un vero portafoglio.