Universitas Mercatorum

LA BLOCKCHAIN

Carlo De Matteo

Indice

1. DEFINIZIONI

La blockchain è una tecnologia informatica che consente di registrare, su un database condiviso da una rete di computer, qualsiasi tipo di dato in modo sicuro e tracciabile. Il suo fulcro è quello del consenso tra i partecipanti, che collaborano al mantenimento e alla "messa in sicurezza" della piattaforma.

Si configura come un registro (Ledger) pubblico, sicuro e condiviso da tutte le parti che operano all'interno di una data rete distribuita di computer. Registra e archivia tutte le transazioni che avvengono all'interno della rete e si aggiorna automaticamente su ciascuno dei computer che partecipano al network, eliminando in definitiva la necessità di terze parti che certificano le transazioni.

Il nome deriva dalla sua natura distribuita: ogni nodo del network svolge un ruolo nella verifica delle informazioni, inviandole al nodo successivo in una catena composta da blocchi, blockchain appunto.

Tutte le operazioni effettuate sono confermate dai singoli nodi attraverso software di crittografia, che verificano un pacchetto di dati definiti a chiave privata o semi, che viene utilizzato per firmare le transazioni. Garantendo l'identità digitale di chi le ha autorizzate. La marca temporale impedisce anche che l'operazione, una volta eseguita, venga alterata o annullata. La caratteristica principale del modello, dunque, è che il funzionamento non è garantito da un ente

centrale, ma ogni singola transazione è validata dall'interazione di tutti i nodi.

2. STORIA E ORIGINI

Nel 1994 Nick Szabo, informatico statunitense, delinea il concetto di Smart Contract, ovvero un tipo di software che automatizza, in maniera efficiente e trasparente, taluni compiti preassegnati da una o più parti. Il primo modello essenziale di Smart Contract teorizzato è quello della vending machine, dove il software e l'hardware della macchina distributrice gestiscono la vendita di un certo bene, ad esempio un caffè, verificando che quando sia depositata dall'acquirente una cifra predeterminata, sia consegnato il prodotto desiderato. Ciononostante nel 1994 mancava la tecnologia e la vera necessità affinché gli Smart Contract potessero svilupparsi e diventare di uso quotidiano.

Nel 2009 venne introdotto Il Bitcoin basato sulla tecnologia blockchain, che qualche anno dopo avrebbe spalancato le porte all'avvento dell'era degli Smart Contract.

Il punto di svolta della tecnologia blockchain, fino ad allora relegata quasi esclusivamente al settore della monetica, avviene quando l'allora diciannovenne Vitalik Buterin pubblica il White Paper di Ethereum nel 2014 delineando le caratteristiche di quella che sarebbe diventata successivamente la piattaforma di riferimento per lo sviluppo e l'esecuzione degli Smart Contract sulla blockchain.

Pur esistendo modelli teorici di Smart Contract, come l'acquisto presso di un caffè presso una macchina distributrice di generi alimentari, questi non disponevano fino ad allora di una tecnologia,

appunto la blockchain e di una piattaforma, Ethereum, che offrissero la possibilità di cristallizzare la volontà di una o più parti in modo indelebile ed immutabile, garantendo che ad una certa/e premessa/e corrispondesse un risultato certo al verificarsi di determinate condizioni.

3. FUNZIONAMENTO E TIPOLOGIE

L'approccio di blockchain è detto a ledger distribuiti perché prevede che tutti i partecipanti a una rete blockchain conservino una copia identica di un ledger (letteralmente un libro contabile) che a sua volta contiene le transazioni collegate a quella specifica implementazione di blockchain.

Come indica la denominazione, blockchain dal punto di vista del funzionamento è una catena (chain) di blocchi (block). Ogni blocco contiene una certa quantità di informazioni (per semplicità supponiamo una sola transazione, ma possono essercene diverse), è firmato digitalmente, è "condensato" in un hash numerico e punta, per realizzare una catena, al blocco successivo e a quello precedente.

La Blockchain quindi è una base di dati fatta di blocchi che memorizzano blocchi di transazioni valide correlate da un marcatore temporale (timestamp). Ogni blocco include l'hash (una funzione algoritmica informatica non invertibile che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita) del blocco precedente, collegando i blocchi insieme. I blocchi collegati formano una catena, con ogni blocco addizionale che rinforza quelli precedenti.

Quando una transazione (più in generale un blocco) si aggiunge a una blockchain, viene replicata in tutti i ledger del sistema. Il punto chiave di questo approccio è che è impossibile modificare una transazione senza che il resto del sistema lo ignori. Modificando una

transazione infatti si modifica un blocco, che quindi varia il suo codice hash.

È facile verificare che un hash di un blocco è diverso da quello delle altre copie dei ledger ed è anche facile capire quale sia il valore giusto: è quello che è presente nella maggioranza dei ledger. Il sistema blockchain raggiunge cioè un "consenso" sul valore corretto. In realtà il sistema è anche più rigido di così: variando un blocco si invalidano tutti quelli seguenti, il che significa che variando una transazione si invalidano tutte quelle successive. Impossibile non accorgersene.

Tutte le operazioni sono confermate dalla rete entro un tempo predeterminato. In pratica la correttezza del blocco di operazioni immesse nella rete viene verificata dai computer dei partecipanti al network confrontandolo con la versione più aggiornata della blockchain. Il primo nodo che ottiene semaforo verde lo comunica a tutti gli altri, che provvedono a convalidare il blocco aggiornando la blockchain. In questo modo si preservano al tempo stesso l'ordine cronologico delle operazioni e la neutralità della rete.

Il ledger è il “Libro Mastro“, ovvero la base fondamentale della contabilità. I ledger fanno poi riferimento a degli archivi, ovvero a una serie di dati che permettono di definire delle regole di analisi, di controllo, di verifica ad esempio delle transazioni commerciali di una azienda o degli atti di una Pubblica Amministrazione. Sino all’avvento dell’informatizzazione i ledger sono stati interpretati con la logica centralizzata che caratterizzava la carta. C’era qualcuno che

si occupava della data entry di dati che nascevano come analogici, c'era qualcuno che gestiva i sistemi e c'era qualcuno che, centralmente, gestiva le estrazioni dei dati o la loro elaborazione.

Con l'avvento della blockchain i primi digital ledger vedono un'accelerazione grazie alla contemporanea disponibilità di due fattori abilitanti: la criptografia e lo sviluppo di algoritmi di controllo e verifica dei dati che aprono le porte a quelli che diventano i distributed ledgers, con i quali si entra nell'ambito dei database distribuiti, ovvero di che possono essere aggiornati, gestiti, controllati e coordinati non più solo a livello centrale, ma in modo distribuito, da parte di tutti gli attori.

Gli aggiornamenti o records infatti non sono più gestiti, come accadeva tradizionalmente, sotto il controllo rigoroso di una autorità centrale, ma sono invece creati e caricati da ciascun nodo in modo appunto indipendente. In questo modo ogni partecipante è in grado di processare e controllare ogni transazione ma nello stesso tempo ogni singola transazione, ancorché gestita in autonomia, deve essere verificata, votata e approvata dalla maggioranza dei partecipanti alla rete.

E qui arriviamo alla base del concetto di distributed ledgers ovvero al concetto di "consenso". L'autonomia di ciascun nodo è subordinata al raggiungimento di un consenso sulle operazioni che vengono svolte e solo con questo consenso sono poi autorizzate e attivate. I distributed ledgers vengono aggiornati solo dopo aver ottenuto il consenso e ogni nodo viene aggiornato con l'ultima versione

di ogni singola operazione di ciascun partecipante. Ogni operazione rimane poi in modo indelebile e immutabile su ogni singolo nodo.

Il modello si basa sulla combinazione tra firma digitale e marca temporale (timestamp): la prima garantisce che mittente e destinatario di un qualsiasi tipo di messaggio (ad esempio la transazione nel mondo dei pagamenti) siano identificati in modo certo, il secondo permette che un insieme di messaggi, validato con la marca temporale da parte di un nodo scelto casualmente da un robusto modello matematico, venga comunicato e scritto nel registro di tutti gli altri nodi della rete e reso irreversibile.

Tutte le operazioni sono confermate attraverso il processo di consenso distribuito detto "mining". In pratica la correttezza del blocco di operazioni immesse nella rete viene verificata dai computer dei partecipanti al network confrontandolo con la versione più aggiornata della blockchain.

Perché un nuovo blocco di transazioni sia aggiunto alla Blockchain è necessario appunto che sia controllato, validato e crittografato. Solo con questo passaggio può poi diventare attivo ed essere aggiunto alla Blockchain. Per effettuare questo passaggio è necessario che ogni volta che viene composto un blocco venga risolto un complesso problema matematico che richiede un cospicuo impegno anche in termini di potenza e di capacità elaborativa. Questa operazione viene definita come "mining" ed è svolta dai "miners".

Il lavoro del "miners" è assolutamente fondamentale nell'economia della gestione delle Blockchain. Chiunque può diventare un "miner" e può competere per essere il primo a risolvere il complesso problema matematico legato alla creazione di ogni nuovo blocco di transazioni in modo valido e crittografato che possa essere aggiunto alla Blockchain.

Trattandosi di un impegno importante, come detto con importante dispendio di energie, è un impegno che necessità di essere remunerato e incentivato. Nelle Blockchian "private" o Permissioned questo ruolo è svolto, in funzione della goveranance, dall'autorità che attiva la Blockchain stessa.

Nelle Blockchain pubbliche o Permissionless questo ruolo può essere svolto da qualsiasi partecipante alla Blockchain e il miners viene incentivato con delle forme di remunerazione che dipendono dal tipo di regole o governance definite da ciascuna Blockchain.

Nella maggior parte dei casi il primo miner che crea un blocco valido e lo aggiunge alla catena viene ricompensato con la somma delle commissioni per le sue transazioni. Le commissioni fanno riferimento a valori unitari per ogni singola transazione, ma i blocchi vengono aggiunti regolarmente e possono contenere migliaia di transazioni dunque il valore del miner può essere anche molto significativo. I miner possono inoltre ricevere nuove valute create e messe in circolazione come meccanismo di inflazione, come ad esempio nel caso della Blockchain Bitcoin.

Un elemento accessorio ma importante della tecnologia blockchain sono gli smart contract. Anche in questo caso la denominazione è molto chiara, si tratta di contratti indicati come smart perché si possono attivare da soli: quando si verificano determinate condizioni nella catena delle transazioni, il sistema interviene. Ad esempio genera una transazione automatica se il conto di un determinato utente scende sotto una certa soglia. Di nuovo c'è che dal punto di vista dei sistemi blockchain questi contratti sono veri contratti: hanno cioè un valore legale tra le entità contraenti anche se esistono solo digitalmente.

4. CARATTERISTICHE E TIPOLOGIE

La blockchain ha delle caratteristiche che la contraddistinguono rispetto a qualsiasi altro sistema di comunicazione a rete.

- Decentralizzazione: La blockchain è il libro mastro di tutte le transazioni. È la prova di ogni scambio avvenuto nel network. un sistema completamente decentralizzato e aperto.
- Trasparenza: Tutte le transazioni effettuate attraverso la blockchain sono visibili a tutti i partecipanti, garantendo così trasparenza nelle operazioni.
- Affidabilità: La blockchain è affidabile. Non essendo governata dal centro, ma dando a tutti i partecipanti diretti una parte di controllo dell'intera catena, la blockchain diventa un sistema meno centralizzato, meno governabile, ed allo stesso tempo molto più sicuro e affidabile, ad esempio da attacchi di malintenzionati. Se infatti soltanto uno dei nodi della catena subisce un attacco e si danneggia, tutti gli altri nodi del database distribuito continueranno comunque ad essere attivi ed operativi, saldando la catena e non perdendo in questo modo informazioni importanti.
- Convenienza: Effettuare transazioni attraverso la blockchain è conveniente per tutti i partecipanti, in quanto vengono meno interlocutori di terze parti, necessari in tutte le transazioni convenzionali che avvengono tra due o più parti (ovvero le banche ed altri enti simili).

- Solidità: Le informazioni già inserite nella blockchain non possono essere modificate in alcun modo. In questo modo le informazioni contenute nella blockchain sono tutte più solide ed attendibili, proprio per il fatto che non si possono alterare e quindi restano così come sono state inserite la prima volta.
- Irrevocabilità: Con la blockchain è possibile effettuare transazioni irrevocabili, e allo stesso tempo più facilmente tracciabili. In questo modo si garantisce che le transazioni siano definitive, senza alcuna possibilità di essere modificate o annullate.

Un ulteriore differenziazione è data dai concetti di blockchain o ledger "permissionless" ovvero senza permessi, aperta a tutti e senza particolari criteri di certificazione dell'identità dell'utente della rete o "permissioned" (con permessi).

La blockchain permissionless più famosa è certamente il Bitcoin, che incorpora come sappiamo tra le proprie caratteristiche principali quella di mantenere anonima l'identità dei partecipanti, anche se si sono cominciati a sviluppare sistemi per consentire l'identificazione degli pseudonimi utilizzati nella blockchain, in qualche modo riconoscibili, sulla base dei loro pattern di utilizzo. Questa della irriconoscibilità è una delle primissime preoccupazioni del mondo finanziario sui Bitcoin, essendo la riconoscibilità degli attori delle transazioni registrate un forte requisito di tutta la normativa sull'antiriciclaggio e dell'identificazione della clientela.

Il modello di permissioned blockchain nasce quindi come possibile alternativa in quanto, mantenendo le altre caratteristiche del sistema blockchain permette la partecipazione di legal entities riconosciute per validare le transazioni e i dati contenuti dell'archivio distribuito, ed attraverso queste di procedere alle procedure di riconoscimento dei clienti finali (le cosiddette prodcedure KYC "Know Your Customer") e dei possessori degli asset registrati nei ledgers.

La blockchain può essere, a seconda dei processi stabiliti rispetto all'accesso, al consenso e al processo di mining:

Pubblica: come ad esempio il Bitcoin la cui visione è quello di avere un network nel quale le persone possono scambiarsi denaro attraverso una modalità p2p. Il database che rappresenta la lista di tutte le transazioni è pubblico, scaricabile sul computer per ognuno, in tutte le zone del mondo, che vuole diventare un nodo. Queste tipologie di Blockchain vengono definite "completamente decentralizzate". Anche la Blockchain di Ethereum è completamente pubblica, decentralizzata e distribuita. Qualunque utente può essere un miner.

Privata: In una blockhain privata, il consenso e il permesso di scrivere i blocchi nella catena è centralizzata da una unica organizzazione, quindi solo 1 nodo crea il consenso e può minare. La possibilità di scaricare la blokchain è solitamente ristretta a pochi. In realtà, una piattaforma privata è essenzialmente un tradizionale database centralizzata con l'aggiunta della crittografia come strumento di sicurezza e verifica. Comparando la privata con la

pubblica, in alcuni ambiti la prima può essere più funzionale. Infatti, se si desidera o bisogna cambiare o modificare alcuni codici nella blockchain, nella casistica di pochi nodi o solo uno è più veloce ed immediata. Nella blockchain privata solo il proprietario ne gestisce i diritti e l'accesso, mantenendo però poi al suo interno le altre caratteristiche della blockchain. Si crea in pratica un network privato, amministrato da uno o più soggetti amministratori. Ad esempio questa blockchain può svilupparsi all'interno di un'istituzione finanziaria per gestire i propri asset o per ragioni di controllo e auditing.

Consortium: Essenzialmente, questa tipologia di blockchain è un database dove il processo di consenso è controllato da un numero predefinito di nodi. Per esempio. si può immaginare un consorzio di 15 istituti finanziari, nel quale almeno il 50%+1 deve confermare la validità di ogni blocco che viene processato. Tuttavia, è possibile che questa blockchain rimanga pubblica, cioè scaricabile su qualsiasi PC in modo che chiunque può vedere i movimenti o i blocchi processati, senza partecipare attivamente al consenso. Questa tipologia è definita come "parzialmente decentralizzata".

Questo è il secondo modello, che a sua volta può ulteriormente svilupparsi nel momento in cui il network privato prenda forma di consorzio, dove il consenso è quindi, ad esempio, fornito, dalle istituzioni finanziarie facenti parti del consorzio e che possono decidere di avere un sistema permission o permissionless.

5. APPLICAZIONI DELLA BLOCKCHAIN

Di seguito elenchiamo alcune delle modalità attraverso cui le aziende cercano di sfruttare la potenza delle tecnologie blockchain.

Banking and 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. La 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.

Cybersecurity: anche se un registro di blockchain è pubblico, le comunicazioni di dati attuate al suo interno sono verificate e inviate utilizzando tecniche avanzate di cifratura (crittografia). Questo

assicura che i dati giungano corretti dalle fonti ai destinatari e che niente venga intercettato nel frattempo. Se la tecnologia blockchain venisse adottata su più ampia scala, la probabilità di hackeraggio o i tentativi di manomissione e intrusione dei database aziendali potrebbe ridursi, in virtù del fatto che i registri distribuiti sono, al momento, ritenuti più robusti rispetto a molti sistemi legacy. Un modo in cui si riduce il rischio legato all'utilizzo di tecnologie di protezione informatica convenzionali è legato all'eliminazione completa della necessità di interventi umani (nessun operatore, infatti, è previsto operare come garante delle procedure). Eliminando la necessità di mediatori si abbassano i potenziali problemi di sicurezza, dall'hackeraggio alla corruzione.

eVote: 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 e 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.

IoT. Alcune aziende leader del settore hanno lavorato su un concetto noto come ADEPT, che utilizza una tecnologia simile alle blockchain per formare la spina dorsale di una rete decentrata di dispositivi IoT. In queste applicazioni la blockchain servirebbe come un libro mastro pubblico per una massiccia quantità di dispositivi e questo permetterebbe di bypassare l'utilizzo di un hub centrale per gestire e mediare la comunicazione tra loro. Anche senza un sistema di controllo centrale per identificarsi l'un l'altro, quindi, i dispositivi IoT saranno in grado di comunicare tra loro in modo autonomo per gestire gli aggiornamenti del software, errori, oppure ottimizzare il consumo dell'energia.

Real Estate: Le criticità che si riscontrano nella compravendita immobiliare includono la scarsa trasparenza durante e dopo le operazioni; l'eccessivo ricorso alla carta e le possibili frodi ed errori dei registri pubblici. La blockchain offre un modo per ridurre la necessità di supporto cartaceo per la registrazione dei dati e porta, dunque, a una velocizzazione delle operazioni legate alla stesura dei contratti, all'identificazione delle controparti e dei dettagli precisi del bene oggetto di compravendita. I database decentralizzati applicati al settore della compravendita immobiliare possono aiutare a registrare, monitorare e trasferire titoli fondiari, atti di proprietà, privilegi ecc. e contribuiscono ad assicurare che i documenti siano accurati e verificabili.

Supply Chain Management: Uno degli aspetti più interessanti della tecnologia blockchain è che consente un controllo più sicuro e

trasparente delle operazioni. Le catene di approvvigionamento e fornitura sono fondamentalmente una serie di nodi transazionali che permettono di trasferire e spostare i prodotti dalla fabbrica al punto vendita. Grazie a questa tecnologia, infatti le transazioni che intercorrono tra i diversi operatori di una filiera (dalla produzione alla vendita) potranno essere documentate in un registro decentralizzato riducendo così i costi di trascrizione, i ritardi e i possibili errori umani. Diverse startup che operano nel comparto dei distributed ledger stanno sperimentando i benefici delle applicazioni di questa tecnologia al Supply Chain Management.

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. Si 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.