Lezione 13 modulo 3

In questa lezione parleremo di 'Blockchain', vedremo anche un'applicazione di alcune tecniche che abbiamo visto per gestire aspetti di sicurezza, in particolare, in questo caso, noi vorremmo garantire delle transazioni, la registrazione di alcune informazioni in un database, che sarà un database distribuito in un caso in cui l'ambiente in cui ci troviamo è un ambiente in cui non c'è una fiducia fra i diversi partecipanti e vogliamo avere una gestione delle informazioni delle transazioni che viene effettuata utilizzando un meccanismo 'Peer to peer', quindi senza avere una particolare autorità che conferma la validità delle transazioni. Parleremo, quindi, di una tecnologia che si sta affermando in questi anni, che è la tecnologia del Blockchain. Passeremo a vedere adesso alcune slide e cominceremo con la definizione di alcuni concetti principali. Allora, innanzitutto, quando parliamo di Blockchain, abbiamo detto, vogliamo avere le transazioni che vengono registrate in un database distribuito. Questo database distribuito ha delle caratteristiche particolari: abbiamo detto che non vogliamo avere un'autorità centrale che lo controlla, quindi questo viene definito come 'politicamente decentralizzato', senza un'autorità che controlli le transazioni. 'Architetturalmente decentralizzato': dobbiamo avere un sistema su più nodi, che vedremo avranno un'architettura appunto di tipo 'peer to peer', saranno distribuiti nella rete. Ma vogliamo anche, invece, avere una coerenza dei dati, quindi il database sarà 'logicamente centralizzato', quindi effettivamente dovremo essere sicuri che una transazione quando viene registrata nel database distribuito sia effettivamente registrata e questo abbia una validità per tutti i nodi che partecipano al sistema. Le tecnologie su cui è basato il sistema del Blockchain sono alcune tecnologie che abbiamo già avuto modo di vedere, nell'ambito della sicurezza. In particolare la firma digitale dei documenti, la funzione di Hash e a questo aggiungeremo qualcosa che ci serve per avere dei meccanismi per raggiungere un consenso quando le parti non sono fidate, quindi un consenso distribuito e le interazioni saranno di tipo peer to peer. Prima di tutto, che cosa sarà una transazione per noi? Qua c'è un esempio: la transazione dovrà essere svolta fra due parti, quindi avremo due indirizzi e ad esempio qua una transazione è il trasferimento di denaro da un indirizzo A ad un indirizzo B. Quello che è importante è che la transazione deve essere firmata, quindi se è una transazione fra due controparti, questa transazione dovrà avere la firma di entrambe le controparti che la confermano. La transazione può anche essere effettuata da parte di un unico agente nella rete che effettua una convalida, una certa operazione. La transazione sarà identificata da un identificatore e il meccanismo su cui si baserà la convalida sarà il fatto che questa transazione, appunto, sia firmata. La firma sarà una firma crittografica come abbiamo visto con chiave privata e chiave pubblica, quindi sostanzialmente l'associazione fra l'indirizzo dell'agente e la sua chiave pubblica consentono di identificare tutte le transazioni che provengono da un certo agente che è presente nella rete. Non abbiamo, in questo caso, un meccanismo tipo la 'Public Key Infrastructure', ma sostanzialmente abbiamo un meccanismo per cui abbiamo associato una chiave pubblica a un certo agente, tutte quelle che saranno le transazioni successive che arriveranno con quella chiave pubblica e che saranno confermate col meccanismo di cifratura, saranno considerate valide. Quindi uno dei temi che ci saranno ovviamente nell'effettuare le transazioni su un sistema a Blockchain, sarà la necessità di verificare che le firme delle transazioni siano corrette, quindi documento firmato, firmato con la chiave privata da parte dell'agente che l'ha firmato e verifica della firma utilizzando la chiave pubblica corrispondente a quell'agente. Quando parliamo di Blockchain, però, abbiamo detto che avremo, lo vediamo nel nome, una catena di blocchi: quindi dobbiamo definire che cos'è un blocco e che cos'è una catena, quindi dobbiamo parlare di quello che è il meccanismo di funzionamento della Blockchain. Innanzitutto quello che vogliamo vedere è che abbiamo appunto una rete di nodi pari e qui sostanzialmente vengono rappresentati in questo modo, abbiamo delle transazioni che vengono iniziate da una certa parte, oppure appunto firmate con un contratto fra due parti e queste vengono registrate, appunto, sulla rete. Cosa vuol dire che vengono registrate sulla rete? Innanzitutto verranno raccolte, non ci sarà un'unica registrazione, mi ci saranno più registrazioni di più transazioni che arriveranno alla rete e verranno raccolte in quelli che vengono chiamati 'i blocchi' e quindi

un blocco tipicamente contiene un certo numero di transazioni. I blocchi vanno riempiti di transazioni, quando un blocco è pieno, sostanzialmente vorremo aggiungerlo a una catena; quindi la catena è una catena di blocchi e ognuno di questi blocchi ha un certo numero di transazioni. Le transazioni all'interno del blocco, però, dovranno essere state approvate da parte dei vari peer e questo appunto consisterà nel verificare che la transazione sia firmata correttamente. Quando avremo un insieme di transazioni che sono state verificate e vengono aggiunte alla catena, appunto, avremo questa catena di blocchi che conterranno tutte le transazioni a partire da un momento iniziale in poi. Quindi ogni blocco è un insieme di transazioni. Quello che è importante, però, che vedremo alla base del meccanismo, è che questo blocco viene aggiunto alla catena, di nuovo con dei meccanismi crittografici, legando le informazioni del blocco a quelli che sono le informazioni del blocco precedente. Quindi all'interno di quello che viene registrato nel blocco, noi avremo delle informazioni che sono legate al blocco (n-1), se questo è il blocco (n) e quindi non sarà facile cambiare uno di questi blocchi all'interno di una catena, perché tutti questi saranno concatenati uno all'altro quindi cambiare un blocco vorrebbe dire cambiare anche tutti quelli successivi, quindi se volessi cambiare questo blocco dovrei cambiare in modo coerente tutti quelli successivi e questo vedremo che è un'operazione che sostanzialmente non è praticamente fattibile. Quindi il nostro 'Distributed ledger' conterrà una serie di blocchi i quali contengono delle transazioni. Vediamo come sono fatte, innanzitutto, come risultato le transazioni. Le transazioni alla fine di questo processo potranno essere o confermate, come operazioni di commit, quindi il risultato sarà valido per tutti, oppure rifiutate e in questo caso tutti i peer dovranno considerare rifiutata questa transazione, quindi non potrà esserci il caso di una transazione che viene confermata da uno dei peer e non confermata da altri. Quindi questo succederà seguendo le proprietà chiamate 'ACID', (Atomicità, Consistenza, Isolamento, e Durabilità) che hanno le transazioni sulle basi dei dati che garantiscono che appunto i valori che vengono registrati sono valori corretti. Come funziona il meccanismo di inserimento all'interno di una catena? Abbiamo già accennato prima che abbiamo un inserimento di transazioni, di più transazioni, abbiamo una rete peer to peer, abbiamo una fase di validazione della transazione e di costruzione dei blocchi e di aggiungere i blocchi fino alla completezza transazione. In più, noi possiamo associare alle transazioni anche un altro meccanismo che è un utilizzo di cripto valute; questo in particolare sarà importante perché nel momento in cui i vari pari avranno da effettuare delle operazioni, che vedremo sono computazionalmente molto onerose, quindi costose, per poter raggiungere la convalida delle transazioni, vorremo anche fare in modo che vengano ricompensati per questa attività onerosa e quindi abbiamo un meccanismo di cripto valute che va a compensare appunto con una valuta che è valida all'interno di questo sistema di pari, che potrà essere registrata e utilizzata in altre transazioni, quindi sostanzialmente una forma di pagamento del lavoro che viene svolto. Quindi uno degli obiettivi dei pari nel fare le operazioni che abbiamo detto, che sono necessarie di verifica e poi di calcolo di informazioni per la creazione del blocco, potrà essere legato al pagamento in cripto valute. Quindi, oltre a registrare ovviamente le varie transazioni, avremo le informazioni relative anche a questi pagamenti e qualora si utilizzi un metodo di questo tipo. Vediamo adesso però che cos'è la struttura di un blocco, che cosa contiene un singolo blocco, perché è su questo che noi andremo a ragionare. Innanzitutto, abbiamo detto ci sono più transazioni al blocco, supponiamo qua che ce ne siano 4, ovviamente il numero sarà tipicamente superiore. Delle transazioni quello che ci interesserà conservare è la traccia del loro Hash, l'Hash, vi ricordo, è il modo per riassumere in un blocco di dimensioni fisse il contenuto di un documento, quindi avremo degli Hash che quindi sono di lunghezza predeterminata per ciascuna delle transazioni partecipanti. Verrà costruito quello che viene chiamato un 'MERKLE TREE', quindi una composizione di più Hash, di coppie di Hash fino ad arrivare, appunto, all'insieme delle transazioni che sono considerate. Questa è la prima parte di questo blocco; in più abbiamo detto vogliamo legare il blocco, supponiamo il nostro sia il blocco 50, al blocco precedente. Come possiamo fare? Di nuovo usiamo un Hash. Un Hash, come al solito, è il modo per fare un riassunto di quello che è il contenuto di un certo documento, quindi in questo caso il blocco precedente. Aggiungiamo, quindi, all'Hash dell'albero delle transazioni precedente, l'Hash del blocco 49. Aggiungiamo un 'time stamp' che è sempre necessario quando si registrano delle transazioni e poi vedremo che dovremo aggiungere, utilizzando un meccanismo che è il meccanismo, abbiamo detto,

computazionalmente oneroso, che sarà alla base della costruzione di un blocco, quello che viene chiamato un 'Nonce'. Un Nonce è sostanzialmente un numero che viene aggiunto al blocco, in modo che poi l'Hash di questo blocco inizi con un certo numero di zeri, quindi il problema del costruire un blocco, consiste nel verificare tutte le transazioni, verificare e costruire con le transazioni che arrivano, ovviamente siamo in una rete peer to peer e quindi vari nodi potranno costruire blocchi di forma diversa man mano, costruire dei blocchi con un insieme di transazioni e trovare un Nonce. Trovare un Nonce vorrà dire trovare questo numero che consente di avere l'Hash di questo blocco con un certo numero di zeri iniziali, supponiamo sei zeri all'inizio dell'Hash del blocco. Questa è un'operazione molto onerosa perché sostanzialmente non sarà possibile calcolarlo in modo algoritmico, bisognerà andare per tentativi e quindi questo è computazionalmente oneroso. Nel momento in cui viene trovato questo numero, da parte di un nodo della rete, questo potrà consentire a questo nodo della rete di dichiarare che è un blocco completo e gli altri potranno consentire, sarebbe accorto, se questo è un blocco che è valido oppure no. Questo come lo faranno? Con un meccanismo che è di verifica di quello che è stato trovato, nell'operazione che è stata fatta nella creazione del blocco. Come viene fatta la verifica? Sostanzialmente gli altri ripeteranno le operazioni che sono state fatte, utilizzeranno il Nonce proposto e verificheranno che effettivamente ha questa proprietà, di avere un Hash con un certo numero di zeri. Se si raggiunge il consenso e vediamo poi più avanti cosa vuol dire raggiungere il consenso in questi casi, allora il blocco potrà essere aggiunto alla catena e sarà premiato chi ha trovato per primo, appunto, un blocco corretto. Quindi i concetti principali sono quello del Blocco, che abbiamo visto adesso, composto appunto dagli Hash risultanti dagli Hash delle transazioni, l'Hash del blocco precedente, il Nonce, la Conferma, conferma delle transazioni e poi delle operazioni finali e poi abbiamo le operazioni di 'Mining', appunto per scoprire il Nonce. Il Nonce è uno dei modi che possiamo avere per risolvere un problema matematico oneroso, per potere dare una complessità computazionale al fatto di poter aggiungere un blocco alla catena, il che è necessario per rendere sicura la Catena, perché è necessario che venga risolto un problema matematico per poter raggiungere appunto un blocco alla catena. Questo, che vi ho raccontato, basato sul calcolo di un numero, in particolare del Nonce con queste proprietà, viene chiamato 'Proof of Work', cioè, noi abbiamo dei nodi che appunto fanno quest'operazione di Mining di cercare il Nonce, che lavorano e quindi il Nonce quando viene trovato viene presentato come risultato e quindi può essere premiato appunto come lavoro svolto e questi nodi, visto che fanno queste operazioni di Mining del Nonce, vengono tipicamente chiamati 'Miners'; quindi sostanzialmente quello che abbiamo come risultato alla fine di questa operazione è il fatto che abbiamo dei blocchi che sono stati trovati e che potenzialmente possono essere agganciati a questa catena. Abbiamo detto, ci troviamo in un sistema distribuito non fidato, cosa vorrà dire, una volta che sono stati trovati i blocchi, aggiungere il blocco alla catena? Ovviamente dovranno essere d'accordo un certo numero di nodi, perché questo venga considerato valido e quindi, abbiamo detto, devono verificare che effettivamente il blocco ha delle proprietà che si sono dette e poi il sistema deve essere fatto in modo che la catena sia unica e quindi se, visto che in un sistema distribuito i nodi non sempre saranno tutti collegati, quindi con tutti i problemi di un sistema distribuito, quello che potrebbe succedere è che si creino delle zone della rete che temporaneamente vengono isolate quindi delle catene parallele che vengono formate dai noti. Quindi come possiamo risolvere questo problema? prima cosa: il 'meccanismo di voto'. Noi vogliamo combattere l'introduzione di transazioni false, che questo in un ambiente non fidato viene chiamato anche il problema dei 'generali bizantini', cioè il problema che abbiamo è che alcuni nodi della rete potrebbero mettersi d'accordo per introdurre delle transazioni false. La Blockchain è basata su dei meccanismi di voto: dei risultati che sono noti nell'ambito dei sistemi distribuiti è che se si hanno (3n+1) votanti, per avere una transazione falsa è necessario che (2n+1) si mettano d'accordo, però se introduciamo la firma digitale con (2n+1) votanti, è necessario che (2n+1) si accordino per introdurre una transazione falsa, quindi più della metà dei partecipanti. Quindi se come abbiamo detto che tutti i nostri meccanismi di identificazione degli agenti all'interno del Blockchain sono basati su una firma digitale dei partecipanti, in questo caso siamo in questa situazione. Un' altra cosa, però, sempre all'interno di un sistema distribuito che abbiamo è che se la nostra Blockchain, la Blockchain cosiddetta pubblica, quindi in cui abbiamo dei peer che si possono

aggiungere liberamente senza un controllo centralizzato, in genere far votare tutti i partecipanti è impossibile, quindi si usano delle varianti dell'algoritmo dei generali bizantini che vengono chiamate 'practical byzantine fault trust', quindi possiamo utilizzare un sottoinsieme dei votanti per il sistema di voto. C'è un altro caso di Blockchain che si sta diffondendo, che è quello che viene chiamato delle 'Permissioned ledgers': sono sempre dei ledgers distribuiti, quindi dei database distribuiti, ma sono Blockchain private. In questo caso, quello che va a cambiare è che c'è un controllo dell'insieme dei noti e quindi ci può essere un proprietario, ad esempio alcuni grandi player all'interno del settore informatico sviluppano i propri ambienti appunto di Blockchain con un controllo dei partecipanti, nel senso che il sistema di approvazione poi non è vincolato alla maggioranza di tutti i partecipanti, ma un numero limitato di attori che vengono definiti come 'Attori fidati', quindi abbiamo un controllo dell'insieme dei nodi e alcuni di questi nodi vengono considerati fidati e il meccanismo poi per il resto è quello che abbiamo visto prima, quindi la ricerca di un Nonce per formare il blocco e una maggioranza che approva appunto l'inserimento di questo blocco. Altra cosa che abbiamo detto è che potrebbero formarsi delle catene collaterali appunto nel momento in cui troviamo la possibilità di creare delle sotto-parti delle reti e fra i partecipanti a queste sotto-parti dei percorsi alternativi. Quando le varie parti della rete poi si ricongiungono, possiamo trovarci in questa situazione, allora dobbiamo scegliere tra quelle che sono le transazioni che vengono effettivamente considerate valide e verrà sempre scelta come valida in questi casi la catena più lunga. E quindi questa è quella che dà la garanzia che la catena viene a svilupparsi lungo un unico percorso non lungo un albero, è quindi una catena unica. Questo è ovviamente necessario per avere una unica conferma di tutte le transazioni. A livello applicativo, dove utilizziamo questi meccanismi? Abbiamo in questo modo un meccanismo per fare nelle transazioni fra attori che non si conoscono, quindi senza alcun meccanismo anteriore di fiducia e possiamo utilizzare questo meccanismo per definire quelli che vengono chiamati degli 'Smart Contract': sostanzialmente del codice che rappresenta un contratto che consente di fare interagire fra di loro direttamente o indirettamente degli attori. Il contratto registra quindi il progresso di una collaborazione fra più parti che interagiscono direttamente o indirettamente perché sono all'interno di un certo processo in rete. Ad esempio, in un contratto, possiamo avere ad esempio un ordine con più prodotti, quello che viene registrato è ad esempio l'arrivo di un prodotto e quello che si vuole fare è ad esempio pagare il fornitore di questo prodotto solo quando tutti i prodotti sono arrivati. Quindi noi possiamo registrare eventi che vengono man mano inseriti nel tramite delle transazioni all'interno del nostro sistema e fare scatenare poi delle attività sulla base di certe condizioni che si sono raggiunte. Tipicamente un contratto inizia con una transazione di richiesta di un servizio da parte di un partecipante, poi viene svolto. Questo è molto simile a quello che abbiamo già visto e infatti la comunità della rappresentazione dei processi sta studiando le Blockchain con molta attenzione, con i processi. I processi, abbiamo visto, possono avere diverse Bulk. Una Bulk rappresenta attori di tipo diverso, quindi ad esempio qua vediamo un tipico caso in cui questo tipo di meccanismo può essere interessante. Abbiamo un processo, in questo caso di formulazione di un ordine, in cui noi abbiamo l'ordine, poi la consegna e noi vediamo che ad esempio questo ordine viene fatto a un fornitore di un certo prodotto che dovrà produrre questo prodotto utilizzando del materiale che viene fornito da vari fornitori; quindi è sostanzialmente qua ad esempio abbiamo un caso in cui abbiamo, a fronte della ricezione di un ordine, la richiesta di quello che deve essere richiesto a un intermediario, in termini di fornitori di materie prime e poi quello che abbiamo è la possibilità di produrre, sulla base dei componenti richiesti o materie prime quello che è necessario, consegnarlo. Questo viene consegnato a un distributore, quindi abbiamo un altro attore che viene inserito, che viene contattato dall' intermediario e che si aspetta appunto di fare delle consegne e quindi arrivano, diciamo, i vari messaggi di accordo sulla consegna fino a quando viene poi consegnato l'ordine. A questo punto l'ordine arriverà al produttore che potrà fare la produzione e consegnare il prodotto. Perché è importante in questi casi avere un controllo della transazione distribuita? Perché in questo caso non abbiamo un unico attore che ha un sistema che mette in contatto tutte queste parti, il manifacturer non sa quali sono i suppliers che vengono contattati, si aspetta di ricevere quello che ha chiesto all'intermediario in una consegna e non ha conoscenza degli altri suppliers. Abbiamo però un vincolo a sostanzialmente pagare

questi prodotti ordinati ai suppliers che è un vincolo indiretto che verrà fatto tramite l'intermediario, quindi quello che vogliamo seguire in questi casi sono dei processi appunto distribuiti in cui le parti non si conoscono, ma vogliamo avere conferma che le varie transazioni sono state fatte. Quindi il supplier che comincia a produrre sa che l'ordine che è arrivato non potrà essere cancellato successivamente, è un ordine che è stato confermato e così via. Quindi c'è un interesse, un forte interesse a utilizzare meccanismi di questo tipo in ambienti applicativi di tipo diverso. Ad esempio transazioni bancarie, c'è un forte interesse per transazioni bancarie complesse soprattutto a livello internazionale quindi fra sistemi bancari diversi, nell'ambito dei trasporti appunto una gestione di catene di ordine che portano poi a una consegna di quanto è stato richiesto, eventualmente anche unendo varie richieste di trasporto in combinazione più grande, ad esempio un container o interi mezzi di trasporto e poi abbiamo un interesse, un forte interesse da parte della grande distribuzione in generale e alcuni player tecnologici, ad esempio IBM e SAP sono particolarmente interessati a questi tipi di tecnologie soprattutto nella loro forma permissioned in cui abbiamo delle transazioni che comunque sono gestite a livello distribuito, quindi danno un notevole livello di sicurezza, non c'è la registrazione su un'unica piattaforma, ma abbiamo comunque una registrazione distribuite le transazioni fra attori non fidati, quindi con partecipanti anche non fidati e con garanzia diciamo delle proprietà transazionali delle varie transazioni. Quindi quello che abbiamo visto è sostanzialmente un meccanismo per gestire transazioni in rete e con un buon livello di sicurezza anche se l'ambiente è di tipo non fidato. Uno dei problemi che abbiamo però è quello della cosiddetta 'scalabilità' di questo tipo di sistemi. La scalabilità è una proprietà che abbiamo già visto. Quanto riusciamo a gestire? Che numeri di transazioni noi riusciamo a gestire per sistemi di questo tipo? Tipicamente una delle forme che sono state inizialmente create e che ha portato poi a questo tipo di tecnologia, è quella della cripto valuta, quindi bitcoin è la prima cripto-valuta e vediamo che le transazioni al secondo sono tre o quattro, quindi un blocco viene costruito nei circa 10 minuti, quindi tempi piuttosto lunghi, possiamo andare a una velocità maggiore su reti più recenti, tipo Ethereum, stiamo sempre però parlando di creazione di un blocco ogni 15 secondi, quindi di venti transazioni al secondo. Quando confrontiamo questo con le transazioni tipicamente commerciali di pagamento, ad esempio della VISA, noi abbiamo più di un migliaio di transazioni al secondo, quindi il livello diciamo di velocità che abbiamo in questo tipo di sistemi è chiaramente, in questo momento, non confrontabile con la velocità dei tipici sistemi di pagamento. Questo perché abbiamo visto abbiamo introdotto un meccanismo che per dare le garanzie e sicurezza appunto della validità e transazioni in un ambiente distribuito non affidato richiede un calcolo che può essere effettuato appunto dai nodi in modo distribuito che è computazionalmente oneroso e intenzionalmente computazionalmente necessariamente oneroso per dare questa garanzia. Si sono ovviamente altre soluzioni allo studio, ad esempio sostituire il meccanismo computazionale con altri meccanismi di cui noi non andremo a parlare in questo caso e vorrei concludere con questo invito a guardare un video di funzionamento del Blockchain che vi fa vedere sostanzialmente come viene costruito un blocco, facendo un esempio semplice quindi supponendo di avere un unico testo, non si vede il MERKLE TREE, però dà una buona idea di cosa vuol dire fare il mining e creare un blocco e concatenarlo con gli altri.