



APPLICAZIONE BASATA SULLA TECNOLOGIA BLOCKCHAIN PER I PROCESSI DI CERTIFICAZIONE ISO

Relatore: Paolo Giaccone

Candidato: Stefano Suraci

Introduzione

Oggi molte imprese reputano la blockchain uno degli strumenti più rivoluzionari a loro disposizione: il *business* si basa sulle informazioni e tanto più queste sono accurate migliori sono le negoziazioni. La blockchain si presenta come un sistema neutro e affidabile, in grado di spostare la fiducia dai singoli individui alle applicazioni. A questo proposito le macchine risultano avvantaggiate: gli elementi alla base di ogni negoziazione sono i contratti, cioè degli accordi legali tra le parti. Gli *smart contracts* permettono di assolvere in modo automatizzato le condizioni dei contratti, prevenendo la possibilità di azioni non corrette da parte delle entità coinvolte. La logica di queste applicazioni modella le caratteristiche di un contratto reale e il linguaggio di programmazione con il quale sono scritti è per definizione privo d'incertezze. Un sistema di questo tipo non è perciò condizionato da eventi esterni come la corruzione o l'incapacità di compiere scelte eque tipica degli esseri umani. La blockchain, quindi, non rappresenta solamente un periodo di transizione tecnologico, ma cambia completamente gli schemi: i modelli centralizzati e chiusi lasciano spazio alla decentralizzazione e all'*open source*. L'introduzione del sistema blockchain nei processi di certificazione ISO permette di aumentare la fiducia nello strumento di accreditamento: le relazioni tra soggetto accreditato ed ente di certificazione e la valenza internazionale dei certificati vanterebbero le proprietà di veridicità e immutabilità dei dati memorizzati. Oggigiorno le certificazioni possono essere volontarie o previste dalla legge. La certificazione ISO 9001, ad esempio, non è obbligatoria, ma è un requisito indispensabile per tutte quelle imprese che desiderano essere competitive sul mercato. Il possesso di un certificato garantito dalla tecnologia blockchain permetterebbe di aumentare le opportunità lavorative poiché assicurerebbe un punteggio migliore ai bandi pubblici. A giovarne sarebbe anche l'immagine dell'azienda nei confronti degli *stakeholders* poiché dimostrerebbe l'effettiva capacità organizzativa e la volontà di trasparenza. Inoltre, anche i costi assicurativi sarebbero ridotti, si avrebbero delle agevolazioni fiscali e i processi produttivi sarebbero più efficienti.

Scopo

Lo scopo di questa tesi è quello di progettare e realizzare un'applicazione basata sulla tecnologia blockchain per i processi di certificazione ISO. L'applicazione viene realizzata su richiesta dell'organizzazione Bechain, una società che si occupa di accompagnare le aziende nel processo di transizione digitale. L'introduzione di Bechain come organizzazione che fornisce il servizio ha influenzato le scelte progettuali.

Scelte progettuali

Lo studio del processo di certificazione ISO 9001 ha mostrato che alla base dell'iter di certificazione vi è uno scambio di documenti tra un ente terzo e un cliente. Partendo da questo campione, sono state identificate le fasi che richiedono maggiore trasparenza ed è stato definito un modello astratto rappresentativo di un qualsiasi processo di certificazione. La logica ottenuta dalla macchina a stati è stata successivamente utilizzata per l'implementazione degli *smart contracts*.

Per lo sviluppo dell'applicazione è stata utilizzata Hyperledger Fabric (HF). HF è una piattaforma che permette di creare blockchain *permissioned* particolarmente interessanti per casi d'uso aziendali. In questo contesto è importante garantire la fiducia decentralizzata su un sottoinsieme di entità note e mantenere confidenziali i dati e le transazioni. La peculiarità di questa piattaforma è la possibilità di definire protocolli di consenso altamente configurabili e quindi di adattare l'applicazione a schemi di fiducia eterogenei.

L'architettura è composta da tre organizzazioni: B, Org1 e Org2. B è Bechain, Org1 è l'insieme degli enti di certificazione e Org2 è l'organizzazione dei clienti. B fornisce l'infrastruttura di rete e ospita l'*orderer* OB, ma non partecipa alle negoziazioni. Org1 e Org2 comunicano privatamente tramite i rispettivi *peer* P1 e P2 connessi al canale privato C1. Ciascun peer possiede il *ledger* L1 e il *chaincode* S1, invocati rispettivamente tramite le *applicazioni client* A1 e A2. Ciascuna organizzazione ha la propria *certificate authority* CA che distribuisce le identità digitali nel formato standard X.509.

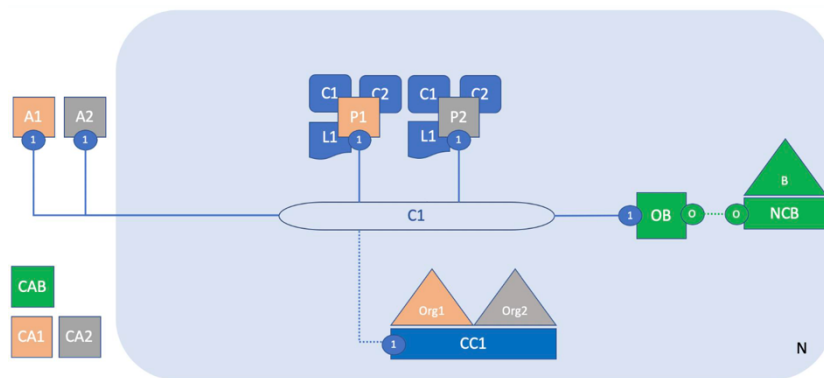


Figura 2 Architettura di Rete.

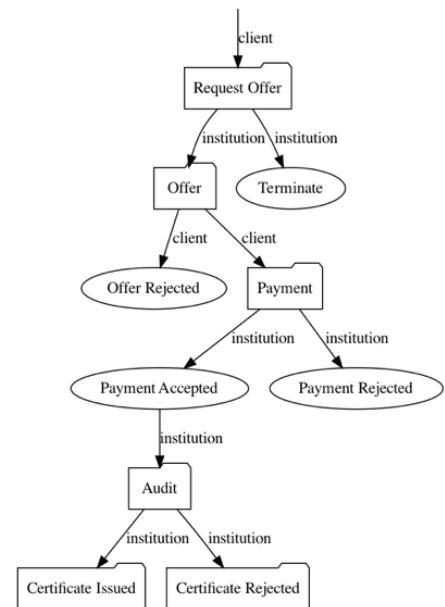


Figura 1 Modello astratto del processo di certificazione ISO.

L'*endorsement policy* richiede che i peer di entrambe le organizzazioni approvino una transazione affinché possa essere considerata valida. Analogamente la *Life cycle Endorsement policy* richiede il consenso sia di Org1 che di Org2 per approvare la definizione di un chaincode.

Per comprendere come è stata implementata la privacy, introduciamo il concetto di ledger: il ledger in HF è composto dalla blockchain e dal *world state*. Il world state è un database che contiene gli ultimi stati di ciascun oggetto aziendale nella blockchain. Per assicurare tra i membri di Org1 la riservatezza dei dati e delle transazioni, sono stati utilizzati i *chaincode namespaces*. Lo spazio dei nomi garantisce ad ogni chaincode definito nel canale un proprio stato mondiale. Segue che ogni smart contract definito all'interno di uno stesso chaincode può accedere unicamente allo stato mondiale riservato per il suo chaincode. Definendo un chaincode per ogni ente di certificazione è stato possibile mantenere private le informazioni tra ogni istituzione.

Le informazioni nello stato mondiale sono memorizzate come coppie chiave-valore. La chiave è stata suddivisa in tre parti per effettuare *query* più efficienti nel database di stato ed evitare di leggere tutti i record fuori catena. La scelta d'includere il nome del cliente come parte della chiave ha permesso di effettuare un confronto con l'identità contenuta all'interno del certificato X.509. In questo modo è stata garantita a ciascun cliente una visibilità limitata solamente ai propri dati. Il valore è invece composto da una serie d'informazioni generali tra cui l'*hash* del documento che include anche il *salt*.

a-	ISO contract name	Client's name	TransID	DeclarantID	StateID	NextStates	Attached	HashDocument
----	-------------------	---------------	---------	-------------	---------	------------	----------	--------------

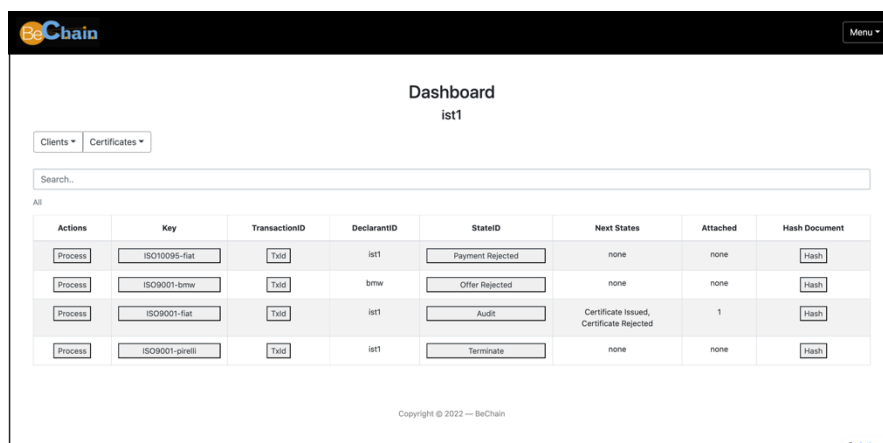
Figura 3 Oggetto aziendale.

Le prestazioni di un sistema blockchain dipendono dalla dimensione delle transazioni e dei blocchi. Includere l'hash del documento, invece che il documento stesso, ha avuto un duplice obiettivo: aumentare le prestazioni e impedire a B di comprendere le transazioni: B ospita OB, il quale ordina le transazioni non ancora convalidate in blocchi. Il sale serve per impedire a B di risalire al documento tramite l'hash: se più di un documento fosse compilato nello stesso modo, l'hash risultante sarebbe lo stesso. A questo punto nasce la necessità da parte di ogni istituzione di memorizzare i documenti nel proprio database locale e di garantire un riferimento agli stessi tramite una chiave. Il valore della chiave deve coincidere con quello usato nella blockchain. Pertanto, se il documento originale fosse rimosso dal database, l'hash del documento nella blockchain sarebbe una prova inconfutabile della sua presenza.

Nonostante i propositi iniziali, l'evoluzione delle norme nel tempo e le caratteristiche specifiche di ciascuna certificazione potrebbero richiedere di modificare il modello unico. Per rispondere a queste esigenze e nella volontà di lasciare libero arbitrio a Bechain nell'implementazione della macchina a stati, sono stati creati due strumenti di supporto. Il primo permette di generare un file sintatticamente compatibile con il software Graphviz, uno strumento in grado di rappresentare le informazioni strutturate come grafi; il secondo utilizza le informazioni fornite da Graphviz per generare automaticamente il codice relativo a un chaincode. Questi due strumenti permettono di adattare l'applicazione alle diverse esigenze aziendali ed eliminano la necessità di competenze tecniche nell'implementazione degli smart contracts.

Risultati sperimentali

Per l'implementazione delle applicazioni client A1 e A2 si è scelto di realizzare un'applicazione web. L'interfaccia grafica ricorda quella di un'applicazione *Blockchain Explorer*, ma con l'aggiunta di funzionalità specifiche per il programma. In particolare, l'applicativo consente di: registrarsi alla rete blockchain, invitare un nuovo cliente, avviare un processo di certificazione, effettuare una transazione, annullare l'ultima transazione effettuata, visualizzare la storia di un oggetto aziendale nella blockchain ed effettuare una ricerca sulla base del cliente, del certificato e di chiavi multiple. Per l'annullamento delle transazioni si distinguono gli errori umani dai tentativi di violazione contrattuale. Inoltre, l'annullamento è di tipo logico in quanto le transazioni fisiche sulla blockchain sono permanenti. La realizzazione di questo programma ha permesso di valutare l'efficacia delle scelte implementative, il corretto funzionamento del programma e la gestione puntuale degli errori.



The screenshot shows the BeChain Dashboard for user 'ist1'. It features a search bar and a table with columns: Actions, Key, TransactionID, DeclarantID, StateID, Next States, Attached, and Hash Document. The table contains four rows of transaction data.

Actions	Key	TransactionID	DeclarantID	StateID	Next States	Attached	Hash Document
Process	ISO10095-flat	Txid	ist1	Payment Rejected	none	none	Hash
Process	ISO9001-bmw	Txid	bmw	Offer Rejected	none	none	Hash
Process	ISO9001-flat	Txid	ist1	Audit	Certificate Issued, Certificate Rejected	1	Hash
Process	ISO9001-pirelli	Txid	ist1	Terminate	none	none	Hash

Copyright © 2022 — BeChain

Figura 4 Home Page.

Considerazioni

Attualmente la persona che fa da garante rispetto alle questioni legali di un contratto è il notaio. L'impiego della blockchain e degli smart contracts introduce la necessità di figure che sappiano verificare l'idoneità dei contratti informatici e in generale dei processi che governano la blockchain. Gli smart contracts possono autonomamente verificare le difformità contrattuali, ma questo non esclude la verifica della loro efficacia da parte degli enti di accreditamento.