DOI: 10.26314/GARR-Conf19-proceedings-15

Una soluzione basata sulla tecnologia blockchain per la validazione di attestati e titoli rilasciati tramite piattaforma di e-learning

Nicola Cannistrà, Fabio Cordaro, Fabrizio La Rosa, Francesco La Rosa, Roberta Maisano, Umberto Ruggeri, Salvatore Todaro, Riccardo Uccello

Università degli Studi di Messina

Abstract. Negli ultimi anni, le criptovalute e la tecnologia blockchain a supporto delle transazioni hanno attirato un crescente interesse. Spesso, le criptovalute come bitcoin vengono associate erroneamente alle blockchain come un unico concetto. In realtà la blockchain rappresenta uno strumento che prevede molteplici applicazioni e il cui scopo è quello di creare asset digitali unici dotati di particolari caratteristiche di integrità, affidabilità e non ripudio. Questa tecnologia cambierà radicalmente la modalità di gestione delle attività amministrative, finanziarie e di management con una gestione trasparente e democratica. In questo articolo proponiamo una soluzione basata sulla blockchain, ed in particolare sugli smart contract, finalizzata alla verifica dei certificati rilasciati come attestazione del successo formativo raggiunto o della partecipazione a corsi tenuti in modalità e-learning.

Keywords. Blockchain, ledger, smart contract, Ethereum

Introduzione

La necessità di avere un sistema in grado di garantire l'immutabilità delle informazioni registrate e la sicurezza delle transazioni, con il massimo livello di condivisione e trasparenza possibile, ha spinto gli addetti ai lavori verso un interesse sempre maggiore nei confronti della blockchain (Zheng et al. 2017). La blockchain permette la creazione di un database distribuito in cui le transazioni ed i dati vengono condivisi tra più nodi presenti in una rete (figura 1). Si tratta di un sistema strutturato a blocchi, concatenati l'uno all'altro per formare una lunga catena contenente tutte le transazioni e condivisa da tutti i nodi che sono deputati alla validazione, controllo ed approvazione.

L'elenco dei dati rappresentati dai blocchi della catena è in continua crescita e, grazie a un algoritmo di consenso distribuito su una rete peer-to-peer decentralizzata, le transazioni vengono verificate continuamente prima di aggiungere blocchi al libro mastro pubblico (Distributed Ledger).

Il processo di verifica consente che le transazioni appena aggiunte non siano in contrasto con le transazioni confermate nella blockchain e mantengano l'ordine cronologico corretto. La validazione avviene tramite un processo crittografico delle operazioni racchiuse nella blockchain. Ogni operazione avrà una sorta di impronta registrata nel blocco con un timestamp che risulta quindi immodificabile.

Possiamo affermare che con l'utilizzo della firma digitale, della crittografia e della

Torino, 4-6 giugno 2019 - ISBN: 978-88-905077-9-3

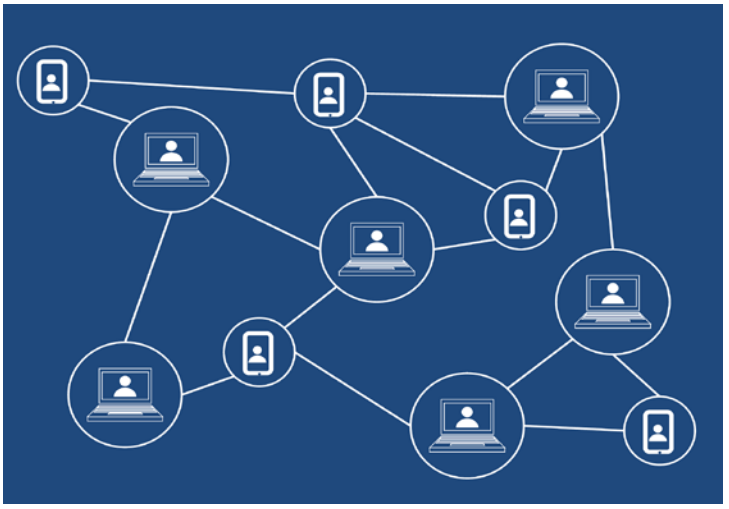


Fig. 1
Una rappresentazione dei nodi distribuiti a supporto di una blockchain

blockchain (Wright et al. 2015) il processo di validazione presenta le caratteristiche di integrità, trasparenza e non ripudio, necessarie per l'utilizzo in procedimenti affidabili e legalmente validi. Gli studi sulle potenzialità delle blockchain (De La Rosa et al. 2017) sono tuttora in corso e molto vivo è anche il dibattito su quale tipo di blockchain configurare, tuttavia esistono già diversi casi di possibile utilizzo (Faioli et al. 2016; Ølnes et al. 2017). Gli smart contract (Alharby et al. 2017) sono contratti scritti in un linguaggio di programmazione in modo da determinare, automaticamente, l'esecuzione delle clausole contrattuali all'avverarsi delle determinate condizioni inserite nel contratto stesso. A differenza di un contratto tradizionale in cui, dopo aver raggiunto un accordo, le parti devono "eseguire" il contratto per renderlo operativo, uno smart contract è autoeseguibile, cioè, una volta che le istruzioni sono state scritte su una blockchain, la transazione avverrà automaticamente quando vengono rilevate delle condizioni appropriate.

In questo articolo proponiamo una soluzione basata su blockchain, ed in particolare sugli smart contract, finalizzata alla verifica dei certificati rilasciati come risultato del successo formativo raggiunto o della partecipazione a corsi erogati tramite una piattaforma di e-learning.

1. Il sistema

In questo lavoro i certificati rilasciati ai partecipanti di alcuni corsi di formazione ospitati sulla piattaforma di e-learning dell'Università degli studi di Messina (che ospita corsi universitari, corsi di formazione destinati al personale tecnico amministrativo, master universitari, ecc.) come riconoscimento dei risultati formativi raggiunti vengono archiviati sulla blockchain di Ethereum e, se necessario, se ne può controllare la loro autenticità. La piattaforma Moodle è adottata dall'Università degli Studi di Messina dal 2005. Ai partecipanti al termine dei corsi, o al superamento delle prove d'esame, viene rilasciato un certificato. Gli strumenti di certificazione per Moodle già esistenti (Accredible, Simple Certificate, ecc.) non sono tutti gratuiti e molti non sono compatibili con la versione attuale (ver. 3.7.1). Inoltre, solo uno di questi strumenti (Accredible) ha tratto vantaggio dalla

funzione chiave pubblica-privata della tecnologia blockchain (Mikroyannidis et al. 2018). Ai fini di questo lavoro, una versione custom del modulo di certificazione del Moodle Learning Management System è stato realizzato per funzionare in conformità con uno smart contract definito su blockchain Ethereum. Nonostante ci siano diverse blockchain che supportano gli smart contract, i motivi per preferire l'Ethereum Blockchain sono l'utilizzo da parte di una grande comunità, la possibilità di un rapido accesso a soluzioni di possibili errori, la presenza di un ampio supporto API e la libreria di web3.js o web3.php (Ethereum per PHP) compatibile con Moodle.

1.1 Ethereum Blockchain

Ethereum, lanciata nel 2013 come idea di Vitalik Buterin, diventa operativa nel 2015. La caratteristica che distingue Ethereum dalle altre blockchain è che consente lo sviluppo e l'esecuzione di "smart contract" e "applicazioni autonome distribuite - DApp". Il linguaggio di programmazione utilizzato è chiamato "Solidity". Il programma è compilato e convertito in bytecode e inviato alla blockchain di Ethereum come smart contract. Contratti e applicazioni sulla blockchain vengono eseguiti su una Ethereum Virtual Machine (EVM). L'utilizzo di smart contract sulla blockchain e l'approvazione della transazione comportano costi in base alla dimensione del contratto in bytecode, la quantità di dati inviati e il numero di transazioni. Questi costi sono indicati come Ether o Gas, durante la spedizione e il funzionamento dello smart contract. Una verifica preventiva del corretto funzionamento del sistema avviene in ambienti di test denominati Testnet.

1.2 Ambiente di test

Per sviluppare uno smart contract sulla blockchain di Ethereum è stata installata e configurata l'applicazione Ganache. L'ambiente scelto per lavorare in combinazione con Ganache e per scrivere smart contract è Remix, che è un IDE dotato di interfaccia web. Dopo aver sviluppato lo smart contract di base, il processo di sviluppo del contratto è stato completato utilizzando MyEtherWallet. Lo smart contract, sviluppato con Remix e quindi inviato alla rete di test tramite l'interfaccia di MyEtherWallet, è costituito da due funzioni principali. La prima funzione registra il nome, il cognome, le informazioni sull'identità del partecipante, l'istituto che rilascia il certificato, il codice di autenticazione del documento e il valore hash md5 del documento che è ottenuto da Moodle, sulla blockchain di Ethereum. L'altra funzione consente, fornendo il codice di autenticazione del documento (specificato nel certificato), di verificarne l'autenticità e ottenere informazioni correlate richiamando l'hash della transazione inserita nella blockchain.

1.3 Learning System

Il modulo di certificazione sviluppato consente agli studenti di scaricare i propri certificati direttamente dalla piattaforma Moodle. Le informazioni relative al partecipante vengono elaborate dalla piattaforma ed utilizzate per produrre un file in formato PDF protetto da password. Quando gli studenti scaricano il loro certificato, le informazioni su candidato, istituto e file vengono registrate nella blockchain Ethereum mediante l'esecuzione dello

smart contract. Una volta completata la registrazione, il certificato diventa disponibile per il download e il codice di controllo del documento e il valore hash della transazione del processo vengono scritti in dei campi appositi del profilo dello studente in modo da consentire una verifica successiva.

2. Conclusioni

La tecnologia blockchain, mediante l'uso della crittografia, permette la riconciliazione e la replica dei dati, il controllo degli accessi, la trasparenza e la privacy. La blockchain, inoltre, trasforma l'organizzazione e le modalità di prestare il lavoro, incidendo sulla cultura giuridica, determinando una riorganizzazione della pubblica amministrazione e dei relativi modi di erogare servizi. Questo lavoro, grazie alla versatilità della tecnologia blockchain, rivoluziona il modo di tracciare le competenze, proponendo una soluzione innovativa basata sugli smart contract, finalizzata alla verifica dei certificati rilasciati tramite una piattaforma di e-learning.

Riferimenti bibliografici

Alharby M., van Moorsel A. (2017), Blockchain based smart contracts: A systematic mapping study, fourth International Conference on Computer Science and Information Technology.

De La Rosa J.L., Torres-Padrosa V., El-Fakdi A., Gibovic D., Hornyak O., Maicher L., Miralles F. (2017), A survey of blockchain technologies for open innovation, fourth Annual World Open Innovation Conference.

Faioli M., Petrilli E., Faioli D. (2016), Blockchain, contratti e lavoro. la ri-rivoluzione del digitale nel mondo produttivo e nella pa, Economia and lavoro, Rivista di politica sindacale, sociologia e relazioni industriali, 2, pp.139–158.

Mikroyannidis A., Domingue J., Bachler M., Quick K. (2018), Smart blockchain badges for data science education, IEEE Frontiers in Education Conference.

Ølnes S., Ubacht J., Janssen M. (2017), Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, Government Information Quarterly, 34(3), pp.355–364.

Wright A., De Filippi P. (2015), Decentralized blockchain technology and the rise of lex cryptographia, SSRN Electronic Journal.

Zheng Z., Xie S., Dai H., Chen X., Wang H. (2017), An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data, pp. 557–564.

Autori

Nicola Cannistrà - nicola.cannistra@unime.it

APM-GARR per l'Università di Messina. Responsabile dell'U.Op. "Infrastrutture ICT" dell'Università degli Studi di Messina, ha sviluppato competenze in ambito sistemistico, progettazione e gestione reti in ambito MAN, sistemi di WiFi centralizzato, sistemi VoiP, sicurezza e sistemi di autenticazione.

Fabio Cordaro - fabio.cordaro@unime.it

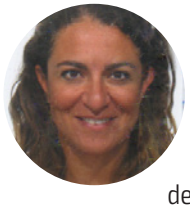
Responsabile dell'Unità Operativa "Sicurezza e Datacenter" presso l'Università degli Studi di Messina, Technical Contact per il dominio della stessa università, ha sviluppato competenze nell'amministrazione di sistemi Unix-like, progettazione e gestione reti, amministrazione di servizi di rete, implementazione di applicativi web.

Fabrizio La Rosa - fabrizio.larosa@unime.it

Laureato in Matematica c/o l'Università degli Studi di Messina. Negli ultimi anni ha ricoperto il ruolo di responsabile delle infrastrutture ICT, reti e datacenter per l'Università degli Studi di Messina ed il Comune di Milano e quello di APM per l'Ateneo messinese.

Francesco La Rosa - francesco.larosa@unime.it

Ha conseguito un dottorato di ricerca in Computer Science c/o l'Università degli Studi di Messina. E' coautore di decine di articoli pubblicati su atti di convegno e riviste internazionali. E' responsabile dell'Unità di Staff "Servizi di Rete" presso l'Università degli Studi di Messina.



Roberta Maisano - roberta.maisano@unime.it

Laureata in Engineering and Computer Science presso l'Università degli Studi di Messina dove ha conseguito anche un Dottorato di Ricerca. E' coautrice di diversi articoli scientifici su tematiche di data science, image processing e machine learning. E' vice-responsabile dell'Unità di Staff Servizi di Rete presso l'Università degli Studi di Messina.

Umberto Ruggeri - umberto.ruggeri@unime.it

Laureato in Ingegneria Elettronica presso l'Università degli Studi di Messina. Responsabile dell'Unità Organizzativa Sicurezza, Servizi Software e Gestione Energetica presso l'Università degli Studi di Messina. Ha sviluppato competenze in ambito sistemistico, virtualizzazione di sistemi, progettazione di reti, sicurezza e sistemi di autenticazione.

Salvatore Todaro - salvatore.todaro@unime.it

Vice responsabile dell'Unità Operativa "Sicurezza e Datacenter" presso l'Università degli Studi di Messina, si occupa di gestione delle identità, di sicurezza, gestione sistemi e infrastrutture di virtualizzazione. Ricopre il ruolo di referente tecnico di Ateneo e di membro del Comitato Tecnico Scientifico per la Federazione di Identità IDEM GARR AAI.

Riccardo Uccello - riccardo.uccello@unime.it

Laureato in Fisica presso l'Università degli Studi di Messina. Ha ricoperto negli ultimi anni ruoli di responsabilità nel settore dell'ICT, prima presso l'Università Mediterranea ultimamente presso il Centro Informatico dell'Università degli Studi di Messina. Ricopre il ruolo di APA-GARR per l'Ateneo messinese.