

Blockchain-Based Smart Methodologies for Innovative Ledger Environments

Paolo Bottoni¹, Roberto Carlini², Claudio Di Ciccio¹, Remo Pareschi³

¹Sapienza University of Rome, Department of Computer Science, Rome, Italy

²Genesy Project, Ferrara, Italy

³University of Molise, Stake Lab, Pesche, Italy

info@bb-smile.net

Abstract

Le tecnologie blockchain rivestono un interesse in continua crescita presso enti ed industria in plurimi ambiti. Essendo in una fase espansiva anche in ambito di ricerca e sviluppo in area informatica, con rapidi aggiornamenti e migliorie, la loro integrazione con beni e servizi offerti richiede un know-how ancora elevato, così riducendone un'adozione più vasta. BB-SMILE (Blockchain-Based Smart Methodologies for Innovative Ledger Environments) è una start-up che si propone come fornitore di servizi esterno in grado di configurare tutta la tecnologia e l'infrastruttura blockchain necessarie su server propri. In particolare offre la produzione e distribuzione in modalità Blockchain as a Service (BaaS) che consentano ai clienti di creare le proprie applicazioni blockchain fornendo loro infrastrutture e strumenti per la configurazione e gestione in autonomia delle stesse.

1 Blockchain: concetti di base

Una blockchain è un protocollo per la gestione di transazioni scambiate tra peer. Ogni utente possiede uno o più account, generalmente raccolti in un cosiddetto portafoglio (wallet). Le transazioni riportano sullo scambio di valore o asset e sono firmate crittograficamente dal mittente per garantire l'autenticità del mandato a trasferire asset. Le transazioni sono raccolte in un *ledger*, ossia una lista di tipo *append-only* che sequenzia le transazioni scambiate. Una replica del ledger è salvata su tutti i nodi che partecipano alla rete blockchain. Per mantenere il registro aggiornato per tutte le parti, le sezioni del registro vengono incapsulate e trasmesse tra i nodi sotto forma di blocchi. Poiché i blocchi devono mantenere l'ordine esercitato dal ledger sulle transazioni, i blocchi stessi vengono sequenziati. A tal fine, ogni blocco contiene un collegamento al precedente (il blocco genitore) all'interno della sua intestazione. A tale scopo, mantiene l'hash (una stringa numerica che costituisce un'impronta digitale univoca e non può essere decodificata) di quest'ultimo. La sequenza hash che collega ogni blocco al suo genitore crea una catena che risale al primo blocco mai creato (il cosiddetto *genesis block*) dal blocco più recente. Da qui il nome, *blockchain*.

Poiché l'hash del blocco precedente si trova all'interno dell'intestazione del blocco, influisce sull'hash del blocco corrente. Se il blocco padre viene modificato, cambia anche il suo hash. L'hash modificato del genitore genera una modifica nel puntatore hash del blocco padre nel blocco figlio. Pertanto, anche l'hash del blocco figlio deve cambiare e così via. Questo effetto a cascata assicura che una volta che un blocco si trova a monte di diverse generazioni successive, non può essere modificato senza forzare un ricalcolo di tutti i blocchi successivi. Poiché un tale ricalcolo richiederebbe enormi sforzi computazionali, l'esistenza di una lunga catena di blocchi rende immutabile la storia della blockchain – una caratteristica fondamentale della sua sicurezza.

Essendo un sistema decentralizzato, non esiste un'entità centrale che lo controlli o lo gestisca. Si tratta invece di una rete *peer-to-peer* composta da nodi che comunicano tra loro e contengono al loro interno una copia della blockchain, che viene aggiornata ogni volta che vengono aggiunti nuovi blocchi. I nodi che propongono nuovi blocchi sono i cosiddetti *miner*, poiché vengono ricompensati per i loro sforzi con criptovaluta appena coniata. Un nuovo blocco, tuttavia, può essere aggiunto alla catena solo se c'è un consenso sulla maggioranza della rete. Il contenuto dei blocchi, inoltre, viene verificato nella sua integrità da ogni nodo nella rete. Le blockchain possono essere generalmente classificate in base a due proprietà, ovvero verificabilità (pubblica o privata) e concessione di accesso (*permissionless* o *permissioned*) [Wüst e Gervais, 2018]. La differenza tra blockchain pubbliche e private è la visibilità della rete: nel primo caso, la rete può essere acceduta e visionata da tutti, mentre la seconda solo da chi è invitato. Invece, le blockchain *permissioned* si differenziano dalle *permissionless* per la capacità di aggiungere blocchi alla catena: nelle prime, ogni peer della rete può aggiungere blocchi e partecipare al consenso, mentre nelle seconde solo alcuni hanno questo diritto.

La ridondanza delle informazioni garantisce che, anche se alcuni nodi smettono di funzionare, i dati non vanno persi poiché una loro replica esatta viene conservata in tutti i restanti nodi. Il decentramento avviene anche in termini di consenso sulle informazioni da inserire nel ledger: non c'è quindi né un'autorità centrale con potere decisionale né un singolo punto di attacco. Le transazioni registrate non possono essere modificate e possono essere ispezionate da chiunque nella rete. Il protocollo fornisce incentivi economici sotto for-

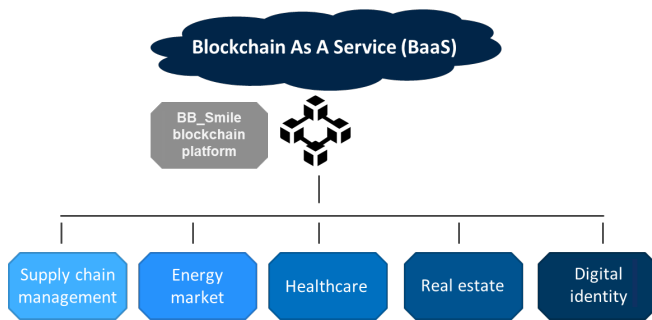


Figura 1: Blockchain as a Service tramite piattaforma BB-Smile

ma di criptovalute ai partecipanti per sostenere le transazioni nel registro distribuito, in modo da promuovere la partecipazione attiva alla manutenzione dell'infrastruttura nella sua interezza.

Alla luce di quanto sopra, tre elementi sono alla base della tecnologia blockchain: decentramento, immutabilità, trasparenza. Queste caratteristiche sono state sfruttate in un'ampia gamma di applicazioni. Bitcoin [Nakamoto, 2008], il primo protocollo blockchain, è stato definito come un sistema di interscambio e gestione di denaro elettronico peer-to-peer. Da allora, l'applicazione più conosciuta per le blockchain è stata la gestione decentralizzata e serverless dei pagamenti tramite scambi di criptovaluta. Tuttavia, la blockchain si è rivelata di ampia utilità in vari altri scenari, apertisi specialmente dopo l'avvento delle blockchain di seconda generazione quale Ethereum [Wood, 2014], che hanno tramutato la blockchain in una piattaforma programmabile per la gestione di applicazioni decentralizzate [Xu *et al.*, 2019]. I programmi disposti su blockchain prendono il nome di *smart contract*, in forma di artefatti software con stato che espongono variabili e metodi richiamabili da altri account su blockchain.

2 BB-SMILE: visione, sfide e opportunità

Le nuove opportunità offerte dalla blockchain hanno trovato sbocco in un elevato e sempre crescente numero di domini applicativi per blockchain, inclusi settori verticali come energia [AISkaif *et al.*, 2022], e-health [Mayer *et al.*, 2020] e mercato immobiliare [Creta e Tenca, 2021], nonché aree trasversali come le supply chain [Bottoni *et al.*, 2020], le identità digitali [Fdhila *et al.*, 2021], la gestione dei processi [Di Ciccio *et al.*, 2019].

L'estensione e la portata dell'adozione delle tecnologie blockchain viene a tutt'oggi ostacolata dalla natura sperimentale, altamente tecnica ed in continua evoluzione delle piattaforme che le supportano, il che rende il costo di integrazione delle piattaforme esistenti con il paradigma blockchain elevato [Prewett *et al.*, 2020].

La mission di BB-SMILE è proporsi come centro di competenza sulle tecnologie blockchain integrando gli skill operativi dei partner tecnologici con le conoscenze in ambito di ricerca e sviluppo dei partner accademici. Essi riguardano tre principali aree:

Servizi in BaaS (Blockchain as a Service): Le aziende sono sempre più orientate ad adottare la tecnologia bloc-

kchain, ma le complessità tecniche e le spese generali operative necessarie nella creazione, configurazione e gestione di una blockchain e nel mantenimento della sua infrastruttura sono spesso un deterrente. BB-SMILE si porrà come fornitore di servizi esterno in grado di configurare tutta la tecnologia e l'infrastruttura blockchain necessarie su server propri. Figura 1 descrive l'architettura ad alto livello e la sua relazione ai domini applicativi.

Sviluppo custom di piattaforme ibride interoperabili:

Esiste in molti casi la necessità di far convivere le caratteristiche di una blockchain privata (con identità certa, governance esplicita e canali riservati) come Hyperledger Fabric [Androulaki *et al.*, 2017] con quella pubblica Ethereum [Wood, 2014] (con accesso libero, trasparenza e tracciabilità pubblica). L'obiettivo è dunque quello di apportare soluzioni e architettare strumenti che permettano a un'applicazione decentralizzata ed agli smart contract con cui opera di scegliere quali dati scrivere su ciascuna delle piattaforme blockchain mantenendo coerenza, integrità, sicurezza, reperibilità dei dati – il tutto gestito da un server di backend che unificherà le web-app di interazione.

Enterprise consulting: Lo sviluppo di proof-of-concept e minimum viable products saranno il mattone fondamentale per lo sviluppo di progetti in sinergia con realtà di tipo enterprise. Inoltre, verrà guidata la migrazione di sistemi esistenti su piattaforme blockchain e al contempo l'integrazione di servizi e sorgenti informative off-chain tramite oracoli [Basile *et al.*, 2021].

Prodotti e servizi innovativi si basano sulla ricerca condotta dai membri accademici fondatori della start-up. Le investigazioni si orientano fondamentalmente in due direzioni.

La prima è lo sviluppo di **filieri industriali e commerciali di seconda generazione basate su blockchain** [Carlini *et al.*, 2020]. In questo ambito, lo scopo è supportare la supply chain tramite smart contract. Tale supporto è volto anche a rafforzare la collaborazione ottimizzando i ritorni finanziari della filiera stessa, calcolati e redistribuiti automaticamente secondo contratti condivisi tra le controparti [Bottoni *et al.*, 2021], con il fine ultimo di realizzare una Decentralised Autonomous Organization (DAO) per la gestione indipendente ed autofinanziata della piattaforma che coadiuvi gli attori coinvolti.

La seconda compete la **progettazione e l'implementazione su blockchain di processi aziendali collaborativi** [Mendling *et al.*, 2018]. L'approccio di tipo model-driven è orientato a consentire agli analisti aziendali di interfacciarsi con la blockchain attraverso un approccio basato su modelli, riducendo così la necessità di conoscere i dettagli dei linguaggi di codifica per creare, gestire e verificare smart contract alla base dei processi collaborativi [Magazzeni *et al.*, 2017]. Le tracce registrate dalle istanze di processo automatizzate su piattaforma blockchain divengono record chiave per l'auditing ed il monitoring dei processi stessi [Di Ciccio *et al.*, 2022].

L'evoluzione e le iniziative di BB-SMILE sono documentate su <https://www.bb-smile.net/>.

Riferimenti bibliografici

- [AlSkaif *et al.*, 2022] Tarek AlSkaif, Jose Luis Crespo-Vazquez, Milos Sekuloski, Gijs van Leeuwen, e João P. S. Catalão. Blockchain-based fully peer-to-peer energy trading strategies for residential energy systems. *IEEE Trans. Ind. Informatics*, 18(1):231–241, 2022.
- [Androulaki *et al.*, 2017] Elli Androulaki, Christian Cachin, Angelo De Caro, Alessandro Sorniotti, e Marko Vukolic. Permissioned blockchains and hyperledger fabric. *ERCIM News*, 2017(110), 2017.
- [Basile *et al.*, 2021] Davide Basile, Valerio Goretti, Claudio Di Ciccio, e Sabrina Kirrane. Enhancing blockchain-based processes with decentralized oracles. In *BPM (Blockchain and RPA Forum)*, volume 428 of *Lecture Notes in Business Information Processing*, pages 102–118. Springer, 2021.
- [Bottoni *et al.*, 2020] Paolo Bottoni, Nicola Gessa, Gilda Massa, Remo Pareschi, Hesham Selim, e Enrico Arcuri. Intelligent smart contracts for innovative supply chain management. *Frontiers Blockchain*, 3:535787, 2020.
- [Bottoni *et al.*, 2021] Paolo Bottoni, Remo Pareschi, Domenico Tortola, Nicola Gessa, e Gilda Massa. Distributed ledgers to support revenue-sharing business consortia: a hyperledger-based implementation. In *ISCC*, pages 1–6. IEEE, 2021.
- [Carlini *et al.*, 2020] Federico Carlini, Roberto Carlini, Stefano Dalla Palma, Remo Pareschi, e Federico Zappone. The genesis model for a blockchain-based fair ecosystem of genomic data. *Frontiers Blockchain*, 3:483227, 2020.
- [Creta e Tenca, 2021] Fabio Creta e Francesca Tenca. Tokenomics: A new opportunity in the real estate business? A qualitative approach to crowdfunding and blockchain interaction. *First Monday*, 26(10), 2021.
- [Di Ciccio *et al.*, 2019] Claudio Di Ciccio, Alessio Cecconi, Marlon Dumas, Luciano García-Bañuelos, Orlenys López-Pintado, Qinghua Lu, et al. Blockchain support for collaborative business processes. *Inform. Spektrum*, 42(3):182–190, 2019.
- [Di Ciccio *et al.*, 2022] Claudio Di Ciccio, Giovanni Meroni, e Luigi Plebani. On the adoption of blockchain for business process monitoring. *Software and Systems Modeling*, pages 1–23, 2022.
- [Fdhila *et al.*, 2021] Walid Fdhila, Nicholas Stifter, Kristian Kostal, Cihan Saglam, e Markus Sabadello. Methods for decentralized identities: Evaluation and insights. In *BPM (Blockchain and RPA Forum)*, volume 428 of *Lecture Notes in Business Information Processing*, pages 119–135. Springer, 2021.
- [Magazzeni *et al.*, 2017] Daniele Magazzeni, Peter McBurney, e William Nash. Validation and verification of smart contracts: A research agenda. *IEEE Computer*, 50(9):50–57, 2017.
- [Mayer *et al.*, 2020] André Henrique Mayer, Cristiano André da Costa, e Rodrigo da Rosa Righi. Electronic health records in a blockchain: A systematic review. *Health Informatics J.*, 26(2):1273–1288, 2020.
- [Mendling *et al.*, 2018] Jan Mendling, Ingo Weber, Wil M. P. van der Aalst, Jan vom Brocke, Cristina Cabanillas, Søren Debois, et al. Blockchains for business process management - challenges and opportunities. *ACM Trans. Manag. Inf. Syst.*, 9(1):4:1–4:16, 2018.
- [Nakamoto, 2008] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. Accessed: 2022-01-19.
- [Prewett *et al.*, 2020] Kyleen W. Prewett, Gregory L. Prescott, e Kirk Phillips. Blockchain adoption is inevitable – barriers and risks remain. *Journal of Corporate Accounting & Finance*, 31(2):21–28, 2020.
- [Wood, 2014] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger, 2014. Accessed: 2022-01-19.
- [Wüst e Gervais, 2018] Karl Wüst e Arthur Gervais. Do you need a blockchain? In *CVCBT*, pages 45–54. IEEE, 2018.
- [Xu *et al.*, 2019] Xiwei Xu, Ingo Weber, e Mark Staples. *Architecture for Blockchain Applications*. Springer, 2019.