PROPOSTE TESI TRIENNALI
GRUPPO DI RICERCA LAURA RICCI
MARZO 2022

Tesi di implementazione di strumenti/ambienti/servizi decentralizzati per web3

- ### Self Sovereign Identity (SSI): Selective Disclosure e Revocation

La Self-Sovereign Identity (SSI) è un approccio all'identità digitale che offre agli individui il controllo delle proprie identità digitali e delle proprie credenziali attraverso l'utilizzo della tecnologia blockchain. L'idea alla base di SSI è che l'identità di un individuo debba sempre essere sotto l'esclusivo controllo dell'individuo che ne è rappresentato, il quale può disporne in modo indipendente, senza la necessità di affidarsi ad intermediari terzi. Il concetto è strettamente legato al concetto di web decentralizzato, il web3. In un sistema di Self-Sovereign Identity una credenziale verificabile è un insieme di proprietà (come certificati, titoli, o attestazioni) emesse da un soggetto riconosciuto, e che possono essere verificate crittograficamente. Una credenziale verificabile posseduta da un utente (ad esempio la carta di identità) può essere presentata a un verificatore allo scopo di poter accedere ad un determinato servizio o risorsa. Legate a questa tematica si propongono diversi tipi di tesi:

- *Selective Discolsure:* Uno dei principali problemi delle credenziali verificabili e che non è possibile presentare al verificatore solo alcune parti della credenziale senza rivelare l'intero contenuto della stessa (ad esempio, non è possibile rivelare solo l'altezza presente nella carta di identità senza mostrare anche data di nascita, nome, cognome, etc.). La tesi riguarderà una tecnica di divulgazione selettiva delle informazioni contenute in una verifiable credential per preservare la privacy delle credenziali condivise dall'utente senza compromettere la loro verificabilità.
- *Revocation:* Data la natura decentralizzata della SSI, la revoca di una credenziale è un'operazione abbastanza complessa poichè deve garantire che qualsiasi utente possa identificare la credenziale come non piu' valida. Lo scopo principale della tesi è quello di analizzare le principali tecniche adottate per la revoca delle credenziali, testare il loro funzionamento, valutare le loro proprietà, e confrontare i diversi vantaggi e svantaggi offerti.
- *Partitioning:* Una tecnica che permette all'utente di avere un maggiore controllo dei dati presenti nella credenziale e' quella di partizionare i dati della credenziale in K insiemi distinti, e creare una credenziale verificabile per ogni insieme. La tesi analizzerà le tecniche di partizionamento presentate in letteratura per preservare la privacy dei dati delle credenziali condivise dall'utente. Il candidato dovrà implementare alcune delle

tecniche di partizionamento dei dati e valutare qual'è la giusta granularità di partizionamento in funzione del tipo e delle caratteristiche della credenziale

- **Strutture dati autenticate per Bitcoin light weight client**

La blockchain di Bitcoin ha attualmente una dimensione molto grande ed è impossibile che un client light-weigth, come uno smartphone, possa scaricare l'intera blockchain. Ogni nodo light fa quindi riferimento a un full node, che sincronizza l'intera blockchain e può inviare al nodo light solo le informazioni di suo interesse. Il light node invia al full node gli indirizzi di interesse ed il full node cerca nella blockchain le transazioni relative a quegli indirizzi e le invia al light node, insieme ad una prova crittografica che consentirà al client di verificare che l'informazione ricevuta è consistente. Il light node scarica solo una parte ridotta della blockchain (gli header di blocchi della blockchain), che associata alla prova ricevuta, consente di verificare la correttezza delle informazioni ricevute. Attualmente si utilizzano i Merkle Trees, ma recentemente sono state proposte nuove tecniche crittografiche, come quella degli accumulatori. Si tratta di una tesi di progetto in cui si utilizzeranno alcune librerie di crittografia avanzata per sperimentare nuove tecniche di autenticazione, la sperimentazione sarà effettuata facendo riferimento alla blockchain di Bitcoin, che offre un significativo data set per la fase di sperimentazione.

- **Individuazione di strategie di routing per payment channel per criptovalute**

La Lightning Network di Bitcoin (https://lightning.network/) è una rete P2P di pagamenti che consente di aumentare la scalabilità di Bitcoin, mantenendo la sicurezza garantita dalla blockchain. L'idea è che due utenti aprono un canale per effettuare le transazioni in Bitcoin direttamente tra loro e effettuano solo due transazioni sulla blockchain, una all'atto dell'apertura del canale ed una all'atto della chiusura del canale. E' possibile installare un client come C-Lightning, che consente di scaricare l'intera topologia della rete peer-to-peer Lightning. Una volta scaricata la topologia della rete, il client decide per ogni pagamento un cammino sulla rete, un po' come viene effettuato a livello IP dai protocolli "link state", basati su shortest path, solo che il routing avviene a livello applicazione dello stack TCP/IP. La differenza principale è che nella Lightning, i nodi richiedono una fee (un pagamento di pochi Satoshi), per consentire il passaggio di un pagamento sul canale che li collega.
La tesi riguarda lo studio di strategie di routing per la Lightning Network più sofisticate, che considerino, ad esempio, sia la lunghezza di un cammino di routing che l'ammontare delle fee necessarie per percorrere un certo cammino. La parte sperimentale riguarderà lo sviluppo di un simulatore (da sviluppare in un linguaggio a scelta, ad esempio JAVA) e che consenta di valutare la strategie di routing proposte.

- **Wallet integration in HCL Commerce**

Questa tesi verrà svolta in collaborazione con una azienda, la Professoressa Ricci seguirà comunque il progetto come relatore interno. L'idea è quella di integrare l'utilizzo di un

Wallet come Metamask o Coinbase Wallet nel profilo di un utente su un sito commerce B2C con l'obiettivo di immagazzinare gli NFT associati ai prodotti acquistati. L'idea è che un utente del sito B2C acquista un prodotto ed, al momento della chiusra dell'ordine, viene effettuato un processo di mint dell'NFT corrispondente. L'NFT prodotto dal minting permette di gestire il post vendita (Arianee, Everledger) e la presenza di metaversi
Si dovrà effettuare un'associazione tra i prodotti acquistati gli NFT, e poi visualizzarli in Metamask, trasformare il denaro accumulato in StableCoin. Le tecnologie utilizzate saranno Javascript, React, Ethereum.

Tesi di analisi di dati provenienti da blockchain

- **Individuazione automatica di betting pattern generati da Bitcoin on-chain betting services**

Scopo di questa tesi è quello d'individuare nel grafo delle transazioni della blockchain di Bitcoin possibili pattern generati da bot che effettuano automaticamente richieste a servizi di scommesse. Esiste infatti un insieme di pattern di scommessa noti, come D'Alambert, Martingale, utilizzati in generale quando si vuole massimizzare la ricompensa ottenuta da una serie di scommesse ed utilizzati precedentemente per servizi off-line ed ora trasferiti a servizi offerti su blockchain. Verrà dato a disposizione dello studente un file contenente una lista di address deanonimizzati di servizi di gambling presente su Bitcoin. In base a questi indirizzi, si potranno filtrare dalla blockchain di Bitcoin solo le transazioni che riferiscono almeno uno di questi indirizzi. Si prevede di utilizzare il servizio Google BigQuery (https://cloud.google.com/blog/topics/public-datasets/bitcoin-in-bigquery-blockchain-analytics-on-public-data) per evitare di sincronizzare l'intera blockchain, utilizzando un linguaggio SQL-like per il filtraggio dei dati. Sarà quindi costruito un grafo, a partire dalle transazioni filtrate, e sarà effettuata una analisi di tale grafo con il fine d'individuare particolari pattern corrispondenti a pagamenti effettuati automaticamente da bot. Per l'analisi del grafo si prevede di utilizzare librerie per l'analisi dei grafi come NetworKit (https://networkit.github.io/) o NetworkX (https://networkx.org/). Lo scopo finale della tesi è quello di utilizzare i pattern individuati per la deanonimizzazione di utenti della blockchain di Bitcoin. Ad esempio, un bot "scommettitore" utilizzerà gli indirizzi Bitcoin dell'utente che lo ha attivato. Tutti questi indirizzi potranno essere associati quindi ad uno stesso utente e, nel caso anche uno solo di questi indirizzi sia deanonimizzato, tutte le attività dell'utente risulteranno tracciate.

- **Graph-based analysis of the ERC-712 NFT Ethereum Token**

I non fungible Token (NFT) costituiscono una "proof of ownership" decentralizzata e rappresentano una delle più importanti "killer application" della blockchain Ethereum. L'idea di questa tesi è quella di analizzare la dinamica che avviene nello scambio di questo tipo di token, mettendo in evidenza se esistano caratteristiche simili a quelle che si verificano nelle rete sociali. La tesi comporterà lo scaricamento delle le transazioni relative a un insieme di NFT (selezionati tra i più importanti) dalla blockchain di Ethereum e la costruzione di un grafo che modelli i flussi di scambio degli NFT. Il grafo risultante sarà quindi analizzato con strumenti classici della graph analysis (diametro, centralità, distribuzione dei gradi di un nodo), e sarà analizzata anche l'evoluzione temporale delle interazioni. Gli strumenti che si prevede di utilizzare sono Google Table, per il reperimento delle transazioni, Networkit per l'analisi dei grafi, Graphia per la visualizzazione dei grafi.

ALTRE TESI

- **Distributed Ledger Technology Interoperability study (in collaboration with University of Cambridge)**

Distributed Ledger Technology has taken the world by storm, thanks to its decentralised nature and desirable properties that all fit perfectly with the sought after Industry 4.0 revolution. However, the many protocols and proposals, mainly revolving around blockchain technology, compete with each other in a heterogeneous landscape. The interoperability of systems employed by different organizations is often a must in many applications, such as decentralised supply chain management. However, interoperability of DLTs in general and blockchain protocols in particular, is still an elusive topic. The community has not even yet reached a consensus on what 'blockchain interoperability' even means, for example see [1, 2, 3] for competing definitions.
Aim of this thesis is a literature review to compile the state of the art on blockchain interoperability, including cross chain technologies and federation. The work should cover the study of three sides of the topic, i.e. the proposed definitions of the problem, the solutions (both from academia and industry) promising to solve it, and the application fields that would benefit from its adoption.

[1] Liu, Z.; Xiang, Y.; Shi, J.; Gao, P.; Wang, H.; Xiao, X.; Wen, B.; Hu, Y.-C. HyperService: Interoperability and Programmability across Heterogeneous Blockchains. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, London, UK, 11–15 November 2019; pp. 549–566.

[2] Scheid, E.J.; Hegnauer, T.; Rodrigues, B.; Stiller, B. Bifröst: A Modular Blockchain Interoperability API. In Proceedings of the IEEE 44th Conference on Local Computer Networks (LCN), Osnabrueck, Germany, 14–17 October 2019; pp. 332–339.
[3] Koens, T.; Poll, E. Assessing interoperability solutions for distributed ledgers. Pervasive Mob. Comput. 2019, 59, 101079.