UNIVERSITÀ DEGLI STUDI DI SALERNO

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

DIPARTIMENTO DI INFORMATICA

TESI DI LAUREA TRIENNALE IN INFORMATICA

Gestione dell'identità e dell'autenticazione sulla blockchain

Relatore:

Prof. Alfredo De Santis

Candidato:

Giacomo Cocozziello

0512103097

Anno Accademico 2017/2018

Abstract

Al giorno d’oggi, ogni individuo possiede molteplici identità digitali. La gestione di queste identità è molto importante perché il furto di identità è un evento fin troppo comune. Le nostre informazioni personali non sono sotto il nostro controllo ma risiedono in archivi che sono obiettivi per gli hacker. Queste violazioni sono dannose perché i dati rubati possono essere facilmente utilizzati per commettere frodi. Per risolvere questo problema abbiamo bisogno di un modello di identità decentralizzato che metta le persone sotto controllo e consenta alle aziende di ridurre significativamente le frodi attraverso uno scambio di dati sicuro e affidabile. La Blockchain pone le basi per un mondo migliore. La Blockchain è stata conosciuta come tecnologia di base delle cripto valute ma viene considerata come una tecnica funzionale per migliorare quelle esistenti e per la creazione di nuove applicazione mai utilizzate prima. In questa tesi andrò ad analizzare i pro e contro dell’utilizzo della Blockchain, i servizi, le caratteristiche ed in particolare come viene gestita l’identità analizzando in maniera dettagliata un’applicazione che gestisce l’identità e l’autenticazione basata sulla blockchain.

Sommario

Introduzione

In questa tesi è stato portato avanti uno studio incentrato sul tema di come la tecnologia Blockchain gestisce l'identità e l'autenticazione di tutti quei settori economici e industriali tra cui finanze e banche, assicurazioni, sanità, pubblica amministrazione e nell'IOT. Nello specifico, **nel capitolo 1** verrà spiegato che cos'è la Blockchain prendendo in considerazione molteplici punti di vista, inoltre verrà fatta una differenza partendo dai sistemi centralizzati ai sistemi decentralizzati, il funzionamento, vantaggi e svantaggi di questa tecnologia e i vari tipi di blockchain (pubblica e privata).

Nel **capitolo 2** sarà trattato il concetto di identità digitale, le proprietà e i ruoli che essa ricopre. Inoltre verrà spiegato in modo più dettagliato i vari problemi legati all'identità digitale soprattutto il furto di identità che oggi giorno è in continua crescita.

Nel capitolo 3 verrà spiegato come la tecnologia Blockchain gestisce l'identità digitale (self-sovereign identity) utilizzando il meccanismo Handshake che permette di eliminare la necessità di una terza parte di fornire l'autenticazione costruendo un'interazione diretta tra l'utente e il fornitore di servizi.

Nel capitolo 4 andremo ad approfondire come l'applicazione Blockpass verifica l'identità, analizzando vari use cases e scenari.

Capitolo 1 - Blockchain

1.1. Origine

La blockchain è una catena di blocchi che contiene informazioni. Questa tecnica è stata originariamente descritta nel 1991 da Stuart Haber e W.Scott Stornetta ed era inizialmente pensata per marcare i documenti digitali in modo che non fosse possibile retrodatarli o manometterli. Tuttavia è rimasta inutilizzata fino a quando non è stata impiegata da Satoshi Nagamoto nel 2008 sviluppata inizialmente per la cripto valuta digitale Bitcoin. Attraverso la rete peer-to-peer e al server di timestamping, la blockchain era in grado di gestirsi automaticamente, passando da una dimensione di 20gb a 162 gb. Nel 2014 si iniziò ad usare il termine "Blockchain 2.0" che si riferiva alla nuova versione distribuita di Blockchain. Questa nuova versione era differente dalla precedente in quanto permetteva lo scambio di valute senza l'intermediazioni di organizzazioni che muovevano denaro. L'aspettativa di base della blockchain era quella di permettere alle persone escluse dalla monetizzazione di entrare in possesso di un deposito monetario affidabile e sicuro con la possibilità di proteggere la privacy sulle loro informazioni.

1.2. Dai Centralized ai Distributed Ledger

Prima di spiegare le differenze tra i vari ledger occorre partire dal suo significato. Il ledger, in italiano "Libro Mastro", è la base della contabilità. Quando il libro mastro veniva rappresentato da pietre o legno, il ruolo di questo libro mastro era limitato. Con l'avvento dei computer i Ledger sono stati il centro di attenzione dell'informazione nelle grandi aziende e soprattutto nelle Pubbliche Amministrazioni. Ci sono 3 tipi di Ledger. Partiamo dai Centralized Ledger, ovvero un libro mastro centralizzato in cui tutte le transazioni vengono gestite da un'unica entità. Ad esempio, nel caso di transazioni bancarie pubblicate su un sistema centralizzato se l'entità si spegne bruscamente, tutte le transazioni verranno interrotte e non possono essere elaborate. Inoltre, un sistema centralizzato non prevede restrizioni sulle operazioni che possono essere eseguite nel libro mastro. Ad esempio, qualsiasi utente può modificare una transazione o una data. Ciò può portare ad attività finanziare errate e attività fraudolenti. Un altro tipo di libro mastro è il Decentralized Ledger, in italiano libro mastro distribuito. In questo libro mastro non esiste un grande soggetto centrale come nel libro mastro centralizzato ma ci sono tanti soggetti centrali. La fiducia anche in questo caso è delegata a un soggetto centrale, logicamente più vicino, ma comunque centralizzato. Per evitare questi tipi di errori possiamo utilizzare un Distributed Ledger. Un Distributed Ledger, libro mastro decentralizzato, utilizza una rete peer-to-peer per comunicare con i nodi sparsi in tutto il mondo e di un algoritmo di consenso che

permette l'aggiornamento del libro mastro decentralizzato solo se l'operazione ha avuto l'approvazione da un numero sufficiente di nodi. Ogni nodo è indipendente, possiede tutte le informazioni e ha il potere di validarle. Tutte queste operazioni una volta consentite sono irreversibili. Un esempio di libro mastro distribuito è la Blockchain.

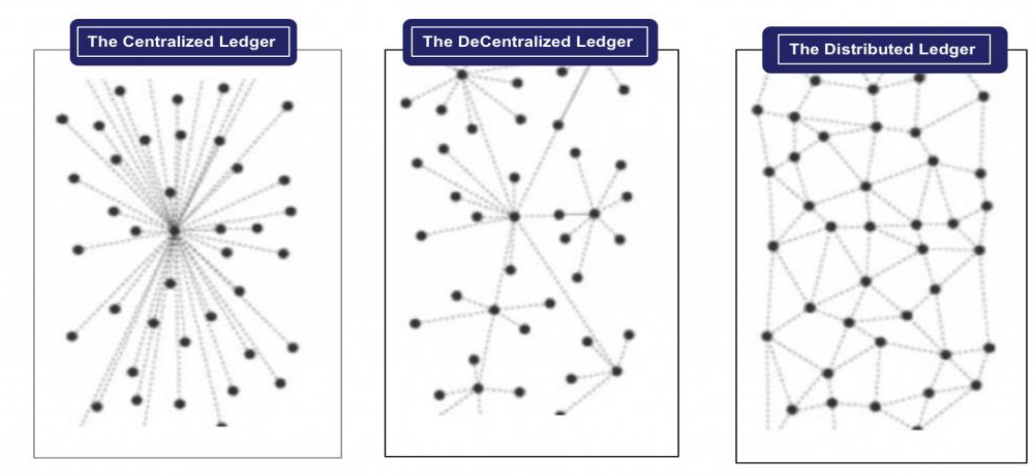

Figura 1: Differenza dei vari "Ledger"

1.3. Definizione di Blockchain

La Blockchain originariamente "Block" "Chain", traducibile in "catena di blocchi" che memorizza un insieme di informazioni validate e correlate da un marca temporale (timestamping). Questo servizio è costituito da una sequenza di caratteri che identifica in modo univoco, indelebile e immutabile una data e/o un orario ad un blocco per fissare l'avvenimento di un certo evento. Questa rappresentazione è sviluppata in un formato che ne permette la comparazione con altre date e stabilisce un ordine temporale. Le componenti principali della Blockchain sono:

- Nodo: partecipanti della Blockchain.
- Transazione: insieme di informazioni che vengono scambiate tra i nodi e hanno bisogno di essere verificate, approvate ed archiviate dai partecipanti
- Blocco: costituito da un insieme di transazioni.

1.4. Funzionamento

1.4.1. Blocco

Per capire come funziona la Blockchain prendiamo un blocco. Ogni blocco contiene i dati, l'hash del blocco e l'hash del blocco precedente. I dati memorizzati in un blocco dipendono dal tipo di blockchain che utilizziamo, ad esempio la blockchain "bitcoin" memorizza i dettagli di una transazione come mittente, destinatario e quantità di monete. Possiamo paragonare l'hash come un'impronta digitale. Una volta creato il blocco, viene calcolato l'hash. Cambiare qualcosa all'interno del blocco farà si che l'hash cambi. Quindi, gli hash sono molto utili quando bisogna rilevare le modifiche ai blocchi. Il terzo elemento fondamentale all'interno del blocco è l'hash del blocco precedente. Questo crea una catena di blocchi ed è questa tecnica che rende la blockchain così sicura.

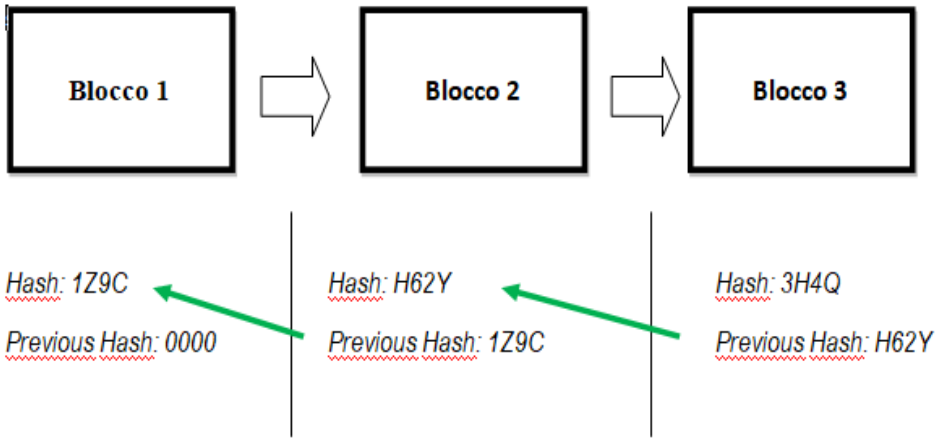

Figura 2: Blocco valido

Prediamo una catena costituita da 3 blocchi. Come si può vedere, ogni blocco contiene l'hash del blocco precedente, il nome e l'hash del blocco successivo. Quindi il blocco numero 3 punta al blocco numero 2 e il blocco numero 2 punta al blocco numero 1. Il 1 blocco non può puntare al blocco precedente perché è il primo. In questo caso viene chiamato blocco genesi (vedi Fig.2). Ora ipotizziamo che viene manomesso il secondo blocco e quindi per quanto detto prima anche l'hash del blocco cambia. A sua volta, il blocco 3 e tutti i blocchi successivi non saranno validi perché non memorizzeranno più un hash valido del blocco precedente. Pertanto, la modifica di un singolo blocco renderà non validi tutti i blocchi successivi (vedi Fig.3).

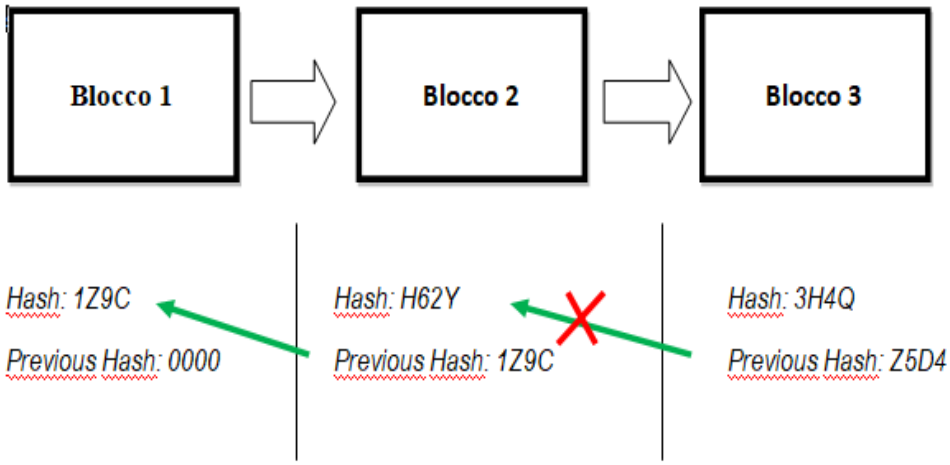

Figura 3: Blocco non valido

Un nuovo blocco per essere aggiunto alla Blockchain è necessario appunto che sia controllato, validato e crittografato. Per effettuare questo passaggio è necessario che ogni volta che un blocco viene composto deve essere risolto con un complesso problema matematico che richiede un cospicuo impegno in termine di potenza e di capacità elaborativa. Questa operazione viene definita "Mining" ed è svolta dai "Miner". Lo scopo principale di questa tecnica è di impostare la cronologia delle transazioni in modo che per l'attaccante risulta poco pratico modificare un blocco. Se il blocco raggiunge il consenso da parte di tutti i nodi della rete allora viene inserito nella Blockchain.

```
public class Block {
  private String hash;       // Block hash
  private String previousHash;  // Previous block hash
  private String data;       // Block data
  private long   timeStamp;     // As number of milliseconds
  private int    nonce;      // Number generated during mining

  // Block Constructor
  public Block(String data) {
    this.data = data;
    this.timeStamp = System.currentTimeMillis();
  }

  // Getter and Setter

  @Override
  public String toString() {
    return previousHash +
      Long.toString(timeStamp) +
      Integer.toString(nonce) +
      data;
  }
}
```

Figura 4: Struttura di un blocco

1.4.2. Transazione

La blockchain per gestire le transazioni utilizza la crittografia asimmetrica / chiave pubblica. Questa tecnica garantisce che la transazione sia legittima e che gli hacker non possono rubare i dati all'interno. La crittografia a chiave pubblica è un sistema crittografico nella quale sia la crittografia che la decrittografia utilizzano due chiavi differenti: una chiave privata che viene tenuta segreta e una chiave pubblica che viene trasmessa in rete. Un esempio di come la blockchain realizza questo con la crittografia asimmetrica è il seguente: Supponiamo che un utente Marco desideri inviare un messaggio a Paolo su un canale di comunicazione inaffidabile come Internet. Ciascun utente genera una coppia di chiavi da utilizzare per la crittografia e la

decrittografia delle informazioni. Ciascun utente inserisce la chiave pubblica in un registro pubblico o in un file accessibile e la chiave privata viene mantenuta segreta. Se Marco vuole inviare una transazione a Paolo, deve crittografarla utilizzando la chiave pubblica di Paolo. Quando Paolo riceve la transazione, la deve decrittografare utilizzando la propria chiave privata. Nessun altro può decrittografare la transazione poiché solo Paolo conosce la propria chiave privata. Seguendo questo approccio, le chiavi pubbliche saranno liberamente distribuibili mentre le chiavi private verranno generate localmente da ogni partecipante e non devono mai essere distribuite. Finchè la chiave privata di un utente rimane protetta e segreta, tutte le comunicazioni in ingresso rimangono sicure. Se un utente malintenzionato ruba la chiave privata di Marco, può decifrare tutti i suoi messaggi ma non può decifrare i messaggi inviati da Paolo perché ciò richiede la chiave privata di Paolo. Dopo di che, ogni transazione viene firmata con la firma digitale, simile alla firme effettive su un documento. La firma digitale aiuta a garantire che l'autore della transazione sia effettivamente l'individuo che detiene la chiave privata. Dopo essere stata firmata, viene verificata fornendo in output un booleano (V/F) a seconda che la firma sia autentica. Una volta firmata, la transazione viene elaborata dai "miners". I miners utilizzano la chiave pubblica del mittente per assicurarsi che la firma digitale sia autentica in modo che un hacker non può violare i dati al suo interno. Se la firma è verificata allora la transazione viene inserita nel blocco.

1.5. Distributed Consensus

Nelle applicazioni che utilizzano la Blockchain molto spesso si sente parlare di consensi distribuiti. Per "consenso" si intende ottenere l'affidabilità del sistema che sia tollerante ai guasti. Qui potrebbero sorgere due problemi più che leciti.

1) Risolvere il problema della doppia spesa
2) Problema Generale dei Bizantini

Il problema della doppia spesa significa utilizzare la valuta in due transazioni allo stesso tempo. Soltanto la prima transazione verrà accetta dai miners e aggiunta alla blockchain mentre la seconda verrà estratta. Il Problema Generale dei Bizantini consiste nel trovare un accordo, comunicando solo attraverso messaggi, tra componenti diversi nel caso in cui siano presenti informazioni discordanti. Questo problema descrive uno scenario in cui più generali si trovano a dover concordare sul momento preciso in cui attaccare un nemico comune su più fronti. Per poter comunicare e decidere in quale momento attaccare il nemico, il generale dovrà inviare un messaggio a tutti i suoi tenenti attraverso il campo nemico che comunicherà l'ora esatta in cui dovranno attaccare. Tuttavia, c'è la possibilità che il messaggero venga catturato dal nemico e quindi il messaggio non verrà consegnato. Questo potrebbe far sì che il generale attaccherà nell'ora stabilita mentre i suoi tenenti attaccheranno in un'ora diversa. Inoltre, anche se il messaggio riesce a giungere a destinazione, il generale dovrà riconoscere di aver ricevuto il messaggio, quindi ordinerà al

messaggero di tornare indietro con la risposta di ricevuta conferma. Così facendo, si può andare a ripetere lo scenario iniziale dove il messaggero può essere catturato. I generali non riusciranno mai a trovare un accordo sulle tempistiche dell'attacco. Questo problema è definito irrisolvibile. Per evitare ciò la blockchain utilizza alcuni importanti algoritmi di consenso tra cui proof-of-work(PoW) e proof-of-stake(PoS).

1.5.1. Proof-of-work(PoW)

Il Proof-of-Work, o PoW, è un protocollo che ha come obiettivo principale quello di difendersi dagli attacchi informatici, ad esempio un attacco denial-of-service (DDoS) distribuito che ha lo scopo di esaurire le risorse di un sistema informatico inviando più richieste false. Il concetto Proof-of-Work è stato utilizzato per la prima volta da Satoshi Nakamoto quando ha creato la valuta Bitcoin. Con questo protocollo i miners competono per verificare che tutte le transazioni all'interno del blocco siano legittime. Per fare questo, devono risolvere dei complessi algoritmi matematici che verificano l'integrità su ciascuna transazione. Il primo miner che risolve questo puzzle riceve una quantità di moneta, nota anche come ricompensa del blocco. Una volta risolto il problema, le transazioni vengono memorizzate sul blocco e il miner annuncia la soluzione all'intera rete. I vantaggi sono la difesa dagli attacchi denial-of-service (DDoS) ed inoltre impone alcuni limiti alle azione nella rete. Pertanto, l'attacco è possibile ma abbastanza inutile poiché i costi sono troppo alti.

1.5.2. Proof-of-stake(PoS)

La Proof-of-Stake(PoS) costituisce un altro metodo alternativo in cui i nodi raggiungono il consenso. La Proof-of-stake viene eseguita da un miner che mette su un blocco una grande quantità di moneta per verificare i blocchi della transazione. Il miner viene scelto dall'algoritmo in base alla quantità di moneta che possiede, da quanto tempo le possiede e come è strutturato l'algoritmo. Il PoS prevede 3 concetti chiave: nessuna ricompensa per il blocco, tutte le valute sono state create all'inizio e il loro numero non cambia mai e i miners ricevono solo le commissioni di transazione. Il PoS è meno costoso rispetto al PoW, perché i miners hanno bisogno di poca energia per risolvere calcoli complessi.

Figura 5: Proof-of-Work and Proof-of-Stake

1.6. Permissioned and Permissionless Ledger

Le Blockchain permissionless(pubblica) consentono a chiunque di creare un indirizzo ed iniziano ad interagire con la rete blockchain. Ad esempio, Internet è un sistema permissionless dove chiunque può creare un sito di sua scelta. In modo simile, nella Blockchain permissionless, qualsiasi persona, cosa o entità può interagire con altri membri, inoltre può partecipare alle verifiche delle transazioni (attraverso il meccanismo di mining), nonché creare contratti intelligenti. Le caratteristiche di un sistema permissionless sono:

- Decentralizzazione:
  I sistemi permissionless devono essere centralizzati e distribuiti, in modo che nessuna entità possa far cadere la rete.

- Trasparenza:
  La trasparenza è una caratteristica importanti dei sistemi permissionless poichè la gestione della rete viene eseguita dai partecipanti e non da un'autorità centrale.

- Anonimato:
  I miners e gli altri partecipanti della rete possono rimanere in gran parte anonimi. Questa caratteristica è utile in alcuni casi, ma non funziona bene in molti scenari.

Un altro tipo di blockchain è la Blockchain permissioned(privata) in cui ogni partecipante è ben definito. Soltanto questi possono eseguire i nodi che convalidano i blocchi di una transazione ed

eseguono smart contract. Questi tipi di Blockchain facilitano la condivisione di informazioni affidabili in un contesto sicuro. Le caratteristiche delle Blockchain permissioned sono:

- Decentralizzazione:
  Il grado di decentralizzazione per le blockchain permissioned si basa sul modo in cui i membri di un sistema privato scelgono di strutturare i loro rapporti commerciali. Le blockchain permissioned utilizzano l'algoritmo di consenso Byzantine Fault Tollerance che differisce dall'algortimo proof-of-work utilizzato nelle Blockchain permissionless.

- Trasparenza:
  Questa caratteristica nella blockchain permissioned potrebbe non essere tanto importante per i membri della rete come lo è nella blockchain permissionless. Tutto dipende da come vengono stabilite le relazioni commerciali e da come viene configurata la blockchain minimizzando il costo, il tempo e la facilità di condivisione delle informazioni.

- Scalabilità e consenso:
  Le blockchain permissioned utilizzano algoritmi di consenso computazionalmente poco costosi. Per questo motivo, godono di un'alta scalabilità rispetto alle blockchain permissionless.

1.7. Vantaggi e Svantaggi

La tecnologia Blockchain presenta vari vantaggi tra cui:

- Trasparenza:

  Uno dei motivi principali per cui la blockchain interessa alle imprese è che la sua tecnologia è quasi sempre open source. Questo significa che gli utenti e gli sviluppatori possono modificarla come meglio credono. Ma ciò che è più importante riguardo al suo open source è che rende l'alterazione dei dati registrati all'interno della blockchain incredibilmente difficile.

- Costi per le transazioni ridotti:

  Le transazioni all'interno della blockchain vengono portate a termine senza il bisogno di una terza parte, ciò significa che i costi delle transazioni sono ridotti, differente in un sistema centralizzato in cui le transazioni vengono verificate da una terza parte ed i costi sono elevati.

- Esecuzione rapida delle transazioni:

  Le transazioni all'interno della blockchain vengono elaborate in maniera rapida perché questa tecnologia è operativa 24 ore su 24.

- Decentralizzazione:

  Un altro motivo per cui la blockchain è avvincente è la sua mancanza di una banca dati centralizzata. Invece di gestire

un enorme centro di dati e di verificare le transazioni attraverso di esso, la blockchain consente alle transazioni individuali di avere la loro prova di validità personale e l'autorizzazione per applicare queste restrizioni. Ciò garantisce che se alcuni dati dovessero finire in mani sbagliate soltanto una piccola quantità di essi verrebbe compromessa e non l'intera rete.

- Reti controllati dall'utente:
  Gli investitori nelle cripto valute sono favorevoli alla blockchain perché il controllo viene gestito dagli utenti e/o sviluppatori e non da una terza parte.

  Oltre ai vantaggi la blockchain presenta anche alcuni svantaggi tra cui:

- Spreco:
  Questo svantaggio è legato soprattutto ai nodi perché ogni nodo ripete un compito più volte per ottenere il consenso rendendo il calcolo molto più lento e costoso. Ci sono vari modi alternativi per far sì che non ci siano attacchi da parte di utenti malevoli, uno di questo è utilizzare gli algoritmi di consenso tra cui PoW e il PoS.

- Mancanza di Privacy:

Le nostre transazioni diventano di dominio pubblico, quindi chiunque può conoscere ad esempio il saldo del Wallet, perché deve essere in grado di certificare la veridicità del dato.

- Inalterabilità delle transazioni:
  Da una parte la transazione rappresenta una funzionalità indispensabile per evitare contraffazioni, dall'altra è un limite nel momento in cui non si è più l'esecutore di tale transazione. Ad esempio, supponiamo che la nostra password venga rubata e un utente malintenzionato riesce ad effettuare una transazione. Il nostro denaro non tornerà più indietro.

- Rischio di contraffare la rete:
  È possibile che il 51% dei nodi della rete siano controllati da un'unica entità. In questo caso si disporrebbe della maggior parte della rete e si potrebbero creare dei blocchi contraffatti.

- La blockchain è lenta:
  Ogni transazione prima di essere validata deve essere controllata chiedendo a tutta la rete se essa è compatibile. In tal caso viene registrata e in seguito, passato un certo tempo, validata e scritta in modo indelebile.

1.8. Servizi

La tecnologia Blockchain opera in diversi settori partendo da quello finanziario, alla sanità, passando per IOT, Cybersecurity e Cloud. Analizziamo i più importanti:

- Banche:
  Alcune banche come Swiss e Barclays stanno sperimentando sistemi basati sulla tecnologia blockchain per migliorare i pagamenti collegando mittente e destinatario in modo da garantire che le transazioni siano rapide a tariffe agevolate.

- Sicurezza informatica:
  Una delle caratteristiche che rende la blockchain unica nel suo genere, è l'elevato standard di sicurezza che garantisce. Nonostante è costituita da un registro pubblico, ogni transazione è verificata attraverso elevati sistemi di crittografia che rende le informazioni affidabili e non duplicabili.

- Sistemi di votazione
  Ogni meccanismo elettorale richiede l'identificazione degli elettori attraverso il documento di riconoscimento, il tracciamento delle votazioni e un sistema che permette di determinare il risultato. Utilizzando una serie di strumenti basati sulla blockchain queste operazioni potrebbero essere compiute in maniera rapida e sicura, evitando ogni rischio di frode o alterazioni dei risultati del voto.

- Rete e IOT

  In questo caso l'utilizzo della blokchain potrebbe garantire a un numero molto elevato di dispositivi di comunicare e scambiare informazioni tra di loro senza la necessità di utilizzare un'unità centralizzata.

- Cloud

  Per chi offre servizi Cloud l'elemento fondamentale è la sicurezza. Questa però è messa a rischio dal fatto che la maggior parte dei dati memorizzati in servizi cloud vengono depositati in server centralizzati, quindi esposti agli attacchi hacker. Per risolvere questo problema, i servizi cloud possono essere memorizzati nella blockchain garantendo la conservazione decentralizzata dei dati.

Capitolo 2 - Digital Identity

Al giorno d'oggi veniamo definiti attraverso una serie di attributi come username e password che possono essere estranei agli attributi che utilizziamo nell'identificazione personale. Lo scopo dell'identità digitale è quello di saper riconoscere persone con documenti cartacei. Sul web molto spesso usiamo siti che richiedono la registrazione prima di offrirci il servizio e tutti i dati che forniamo finiscono in un database. Il sito web ha solamente bisogno di verificare l'identità di un utente ma l'abbondanza di credenziali che forniamo può rendere questo molto complicato perché risulta difficile gestire e mantenere tutte queste informazioni, soprattutto le password. Quindi, noi tendiamo a diventare sempre più pigri quando memorizziamo nuove password ad esempio inseriamo sempre la stessa password su siti diversi oppure creare password brevi non prestando attenzioni alle nostre credenziali. In questo caso potremmo avere un attacco a dizionario. Quindi deve esserci un modo migliore per entrare nei siti web senza dover immettere tutte le nostre informazioni ma soltanto username e password.

2.1. Caratteristiche

La rappresentazione dell'identità digitale deve essere tanto più completa quanto è complessa la transazione in cui è coinvolta. Un'identità digitale è costituita da due parti:

- Chi uno è (identità)
- Le credenziali che ognuno possiede (attributi dell'identità)

Le credenziali possono essere di differente utilizzo, la più semplice consiste in un ID (o username) e una password. In questo caso l'username è l'identità, mentre la password viene chiamata credenziale di autenticazione. Questo tipo di autenticazione, chiamata anche autenticazione ad un solo fattore, non è molto sicura perché la password potrebbe essere indovinata da qualcuno che non è il vero utente. Quella multi-fattore è più sicura, ad esempio la smart card ("qualcosa che possiedi) e una password ("qualcosa che sai").

2.2. Categorie

Ci sono 3 categorie che ci permettono di gestire l'identità digitale in maniera corretta ed efficiente: Federated Identity Management, User-Centric identity e Hybrid Identity Management. La Federated Identity Management consente agli utenti di accedere a più servizi basati su un'autenticazione singola. L'utente si registra una volta per accedere a tutti i servizi offerti dai diversi partner. È costituita da 2 parti: un provider di identità(Idp) e un fornitore di servizi (Sp). L'IdP gestisce l'identità dell'utente ed esegue il processo di autenticazione per convalidare l'identità dell'utente. L'SP fornisce uno o più servizi per gli utenti all'interno della federazione. Questo tipo di gestione consente l'adesione dei partner tra le aziende per fornire l'automazione del servizio a clienti e aziende. Ad esempio, per gestire l'assistenza sanitaria richiede lavoro e costi aggiuntivi se vengono eseguiti separatamente. Inoltre, utilizzando questo modello il cliente è responsabile della gestione dei propri utenti. In termini di

sicurezza è vulnerabile a vari attacchi alle applicazioni web, come attacchi man in the middle.

Nella user-centric identity, gli utenti sono in grado di scegliere quale delle loro identità utilizzare per ciascuna applicazione. Questo approccio mira a risolvere i problemi relativi alla sicurezza e alla privacy utilizzando credenziali basate sugli attributi (ABC). Il vantaggio è che consente agli utenti di selezionare gli attributi per condividerli con il fornitore di servizi. Quindi, migliora i problemi di privacy perché gli utenti hanno il pieno controllo sui loro dati e sanno quando utilizzarli. Anche se gli utenti sanno e possono controllare i loro dati in modo decentralizzato solo le parti relying come servizi o applicazioni conoscono il fornitore di identità. Mentre l'approccio Hybrid Identity Management fornisce un'alternativa quando sia l'approccio federated che user-centric non vanno bene. Ad esempio, nel settore sanitario, scambi di attributi e processi di delega non possono essere completamente user-centric, poiché in caso di incidenti gravi, gli utenti non possono dare il loro consenso. Quindi, il modello Hybrid consente agli utenti di configurare e tracciare l'accesso alla loro documentazione medica, mentre i fornitori di identità archiviano e gestiscono le credenziali dell'utente. Questo approccio è adatto per gestire ambienti instabili che richiedono flessibilità del sistema poiché gestisce tutto, inclusi utenti e dispositivi.

2.3. Proprietà dell'Identità Digitale

Per contribuire ad una soluzione più dettagliata e migliore per un sistema di identità digitale dovrebbero essere applicate queste 5 proprietà tra cui:

1. Entità:

Un'entità può essere un utente oppure un oggetto. Il comportamento dell'identità rappresenta il valore legale per il sistema ad esempio, individui, aziende, macchine, dispositivi. Le entità appartengono a 3 tipi di categorie: agenti di identità installati localmente vengono eseguiti su dispositivi come laptop e smartphone. Gli agenti di identità remota risiedono sulla rete, hanno le loro chiavi private e pubbliche e possono essere gestite da parti che hanno alcune credenziali dell'utente, ad esempio banche, università o altre entità considerate attendibili dall'utente. L'ultimo tipo di entità è costituito da parti Relying, in cui gli utenti interagiscono con un fornitore di servizi online; tuttavia, in un sistema peer-to-peer, le parti relying possono essere altri utenti.

2. Tipo di attributo:

Il tipo di attributo viene utilizzato per identificare l'entità. Di solito è composto da tre proprietà: chi sei, contesto e profilo. La proprietà "Chi Sei" identifica in modo univoco una singola identità in un contesto del mondo reale. Può includere dati, caratteristiche fisiche o elementi che l'entità possiede.

La proprietà “Contesto” si riferisce al tipo di transazione o organizzazione di come l’entità si identifica. Inoltre, determina la quantità e il tipo di informazioni sull’identità necessarie per fornire il livello appropriato di fiducia. L’ultima proprietà è rappresentata dal profilo. Un profilo consiste di dati necessari per fornire servizi agli utenti una volta che l’identità è stata verificata.

3. Ciclo di vita:

Per creare un identità digitale ci sono 3 passaggi fondamentali:

- Registrazione:

  Questa fase è divisa in due parti: iscrizione e convalida. Nella prima parte l’utente si registra inserendo i propri attributi (nome, cognome, data di nascita, sesso, indirizzo). Dopo di che, questa fase viene convalidata controllando gli attributi presentati rispetto a quelli esistenti.

- Emissione di documenti e credenziali;

  Prima che possa essere utilizzata da una persona, un’identità registrata passa attraverso la fase di emissione o processo di credenziali. In questa fase un identità per essere considerata digitale, le credenziali o i certificati(certificato di nascita, passaporto) emessi devono essere elettronici, nel senso che memorizzano e comunicano i dati elettronicamente.

- Autenticazione

  Dopo che gli utenti si sono registrati e si sono autenticati, possono usare le loro identità digitali per accedere a servizi pubblici o privati. Per accedere ai servizi, l'utente deve essere autenticato utilizzando uno o più fattori, ad esempio password, pin o impronta digitale.

4. *Politiche:*

   Le politiche vengono utilizzate per gestire le identità. Il livello di accesso è condizionato non solo dall'identità, ma è anche probabilmente vincolata da una serie di ulteriori considerazioni sulla sicurezza, come la politica aziendale, la posizione o l'ora del giorno.

5. *Tecnologia:*

   Per garantire l'usabilità, la sicurezza e la privacy è necessario implementare le identità utilizzando tecniche avanzate tra cui: tecniche di autenticazione, protocolli di sicurezza e token.
   Le tecniche di autenticazione vanno da quella a singolo fattore a quella a più fattori: le tecniche più importanti sono:

   - *Password/pin:*

     L'autenticazione della password è un metodo tradizionale in cui l'utente viene identificato con nome utente e password. Questa tecnica risulta inefficiente dal momento che il nome dell'utente e la password sono facili da indovinare o rubare.

Per rendere il processo di autenticazione più sicuro, viene utilizzata la tecnica One Time Password(OTP). L'utente inserisce una volta la password e deve richiederne un'altra al server al prossimo tentativo per accedere o effettuare una transazione. Questo metodo utilizza l'hashing e i dati vengono scambiati con il server e memorizzati. Il Pin utilizza lo stesso meccanismo della password. Un'autenticazione basata su Pin viene usato nei servizi finanziari come bancomat.

- *Biometria*

  La biometria è il processo di creazione che si accerta che le persone affermano chi sono. La biometria richiede sensori per prendere le caratteristiche dell'utente, ad esempio riconoscimento delle impronte digitali o dell'iride.

- *Protocolli di sicurezza:*

Questi vengono utilizzati per verificare l'identità e per trasferire l'autenticazione dei dati tra due entità. I protocolli di autenticazione più utilizzati per risolvere i problemi di sicurezza all'interno delle reti sono: Secure Sockets Layer(SSL) e Secure Shell (SSH). Entrambi utilizzano la crittografia per evitare che altri utenti della rete siano in grado di leggere le password o dati bancari. SSL è un modo per proteggere le informazioni che si sta visualizzando con un browser Web. Mentre, SSH viene utilizzato per inviare in

maniera sicuro i comandi di testo o file in un server Web su Internet.

2.4. Limitazioni

Le limitazioni sulla gestione dell'identità digitale sono:

- Clonazione dell'identità: ossia la sostituzione di un persona con l'obiettivo di creare una nuova identità utilizzando quelle credenziali.
- Furto di identità: noto come frode d'identità, è un crimine in cui impostore ottiene elementi chiave di identificazione personale, come la sicurezza sociale o il numero di patente di guida per impersonare qualcun altro. Le informazioni possono essere utilizzate per ottenere credito, merci e servizi in nome della vittima. Esistono molti esempi diversi di furto di identità, come ad esempio:
    - Furto di identità medica: un utente malintenzionato ruba informazioni mediche del paziente ed inoltre può ottenere le fatture fraudolente che si rifletteranno sul conto della vittima come servizi ricevuti.
    - Furto di identità minorile: in cui il numero di previdenza sociale del bambino viene utilizzato in modo improprio per richiedere sussidi governativi, aprire conti bancari e altri servizi. Le informazioni dei bambini sono spesso ricercate

dai criminali, poiché il danno può passare inosservato per un lungo periodo.

- Furto di identità criminale: uso dei dati della vittima per compiere atti pubblici illeciti di varia natura.

- Violazione dei dati: in cui i dati vengono divulgati in maniera non autorizzata. Un esempio è un hacker che si intromette in un sito web e ruba i dati sensibili da un database. Tuttavia, non tutte le violazioni sono così drammatiche. Se un dipendente non autorizzato osserva le informazioni sulla salute del paziente sullo schermo di un computer di un dipendente autorizzato, ciò costituisce anche una violazione dei dati. Le violazioni dei dati possono essere causate da password deboli, patch software mancanti che vengono sfruttati, persi o rubati dai computer portatili e/o da dispositivi mobili. Per prevenire ciò bisogna utilizzare pratiche di sicurezza di buon senso, ad esempio password complesse, utilizzo di software anti-malware, conduzione di penetration testing.

- Phishing: è un tipo di truffa effettuata su Internet in cui un malintenzionato attraverso la posta elettronica o SMS cerca di ingannare la vittima convincendola a fornire informazioni personali come ad esempio, il numero di carta di credito o la password per accedere ad un determinato servizio, fingendosi un ente affidabile.

- Esclusione di identità: è un altro problema legato all'identità digitale. Dal momento che essere in grado di mostrare una prova della propria identità è una necessità per partecipare all'attività sociale ed economica, non averne uno può avere conseguenze dannose per gli individui. Eppure, circa 1,5 miliardi di persone non hanno alcuna prova di identità riconosciuta ufficialmente. Oltre ai problemi personali non avendo dati demografici aggiornati ciò impedisce ai governi di sviluppare ed eseguire servizi sociali adeguati. Questo rappresenta una vere sfida e spesso la risoluzione di tali sfide inizia con la risoluzione del problema dell'identità.

Capitolo 3 - Digital Identity on Blockchain

3.1. Implementazione della blockchain basata sull'Identità Digitale

Nel mondo offline, l'identità e la privacy sono piuttosto semplici. Le "identità" delle persone vengono provate attraverso gli attributi con i quali un utente si identifica (nome, cognome, data di nascita, sesso) mentre la privacy ha la capacità di controllare ciò che gli altri sanno della loro identità. Mentre nel mondo online per dimostrare la nostra identità utilizziamo una password oppure l'autenticazione a due fattori. Il problema con questi metodi è che le password sono insicure e le autenticazione a due fattori generalmente si basano sull'invio di un messaggio via sms o su un servizio fornito da terze parti. Una soluzione a questo problema può essere la tecnologia blockchain. Il processo che utilizza la blockchain per gestire l'identità potrebbe essere richiedendo all'utente di creare un id e scaricare un'applicazione che gestisce l'autenticazione. Ad esempio, basta scattare una foto di un codice QR che codifica la richiesta di autenticazione e l'app deve firmare la richiesta e restituirla. In questa epoca in cui raramente rimaniamo senza i nostri smartphone, questa forma di autenticazione a 2 fattori sarebbe incredibilmente facile da adottare, non solo per l'utente esperto ma anche per il consumatore medio. Esistono alcune tecniche attualmente utilizzate per l'autenticazione a 2 fattori, i cui metodi, tuttavia, sono antiquati e pongono molte minacce alla sicurezza. Per esempio, uno dei metodi più comuni è quello di inviare un codice tramite sms. Questo metodo

è fantastico, tuttavia i messaggi sms sono notoriamente insicuri. Un potenziale aggressore potrebbe tracciare i messaggi da qualsiasi numero e leggerli. Questo è un grande problema perché se un utente malintenzionato sa che l'account utilizza messaggi di testo come metodo di backup di autenticazione e conosce il tuo nome potrebbe trovare i tuoi numeri di telefono elencati online e potrebbe intercettare quei messaggi ottenendo l'accesso a qualunque dispositivo. L'approccio decentralizzato offerto dalla blockchain elimina questo problema perché la catena dei blocchi è pubblica e nessun dato sensibile viene memorizzato in chiaro sulla blockchain. La blockchain gestisce l'identità attraverso il DID. Il DID è un insieme di attributi che definiscono in modo univoco un utente, un oggetto o un'organizzazione. Ogni record DID è protetto crittograficamente da chiavi private sotto il controllo del proprietario dell'identità quindi sono un elemento fondamentale per ciò che è generalmente noto come "identità autosufficiente" o "identità decentrata". Dal punto di vista tecnico, i DID sono URI (Uniform Resource Identifiers) validi, quindi sono compatibili con molte tecnologie web generiche. Non sono limitati a un singolo caso o protocollo. Un altro vantaggio è che i DID sono progettati per funzionare con diversi blockchain e altri sistemi di destinazione, fornendo quindi interoperabilità. I DID possono essere utilizzati per identificare qualsiasi risorsa digitale o reale, come un documento, un individuo, un'azienda o un oggetto fisico. Generalmente, un DID di per sé non prova l'unicità o qualcos'altro del suo proprietario. Un DID è semplicemente un identificatore. In molti casi è possibile

avere più DID per scopi, relazioni e transazioni diversi. Inoltre, la tecnologia blockchain potrebbe utilizzare l'identità digitale per rivoluzionare la democrazia adottando lo SPID (Sistema pubblico di identità digitale). Lo SPID per ora è solo in fase sperimentale, ma è stato pensato per sostituire la miriade di sistemi di identificazione dei vari servizi online della pubblica amministrazione ed unificarli in un unico pin tramite il quale si possa accedere a tutto. L'idea di fondo è che la blockchain potrebbe servire per rendere SPID più ampio e complesso, che comprenda servizi diversi non solo della Pubblica Amministrazione ma anche internazionali. Ad esempio, autenticandoci con una identità pubblica sovranazionale grazie alla blockchain, potremmo permettere al nostro smartphone di dialogare in modo sicuro con l'auto che stiamo per noleggiare in Giappone, trasferendo soltanto il nostro profilo utente. Inoltre, la blockchain potrebbe migliorare Spid, perché potrà permettere di eliminare la centralizzazione dei dati, favorendo lo sviluppo di nuovi servizi basati su attributi aggiuntivi dei cittadini. Un aspetto interessante dello SPID è il suo triplo livello di profondità che corrisponde anche al livello di sicurezza. Il primo livello è quello che consente all'utente di autenticarsi con un id e password, il secondo livello sempre gratuito, dove i provider mettono in campo le loro soluzioni particolari, richiede anche un codice temporale. Per il terzo livello, l'utente avrà bisogno anche di un dispositivo di accesso (smart card).

3.2. Handshake Protocol

Il protocollo HandShake elimina la necessità di una terza parte di fornire l'autenticazione costruendo un'interazione diretta tra l'utente e il fornitore di servizi. Il fornitore di servizi può essere un'app protetta che richiede il servizio. Il protocollo HandShake può essere diviso in 3 fasi principali:

- Login

  In questo passaggio, invece di utilizzare un nome utente e password per la registrazione, l'app utilizza un codice QR rendendo più facile la richiesta di autenticazione.

- Verifica e Risposta

  Questo passaggio contiene procedure che garantiscono l'autenticazione. I dati richiesti vengono verificati in modo che siano legittimi e che l'app è ciò che l'utente si aspetta di usare. La risposta permette all'app di firmare la richiesta,
  che viene poi pubblicata, tramite blockchain o un'autorità di certificazione. Successivamente, l'utente clicca sul pulsante "verifica login".

- Crea risposta

  L'ultima fase consiste nel creare una risposta dopo che l'utente clicca su "verifica login". La risposta viene firmata e la invia all'utente attraverso un percorso specificato nell'app.

Questa richiesta viene quindi verificata utilizzando un PKI sull'app protetta e l'utente viene quindi registrato.

3.3. Concetti sull'identità digitale

Ci sono 3 importanti concetti sull'identità digitale: richiesta, prova e attestazione. Una richiesta è un'asserzione fatta da una persona, ad esempio mi chiamo Andrea e la mia data di nascita è il 1 gennaio 1990. Una prova è una forma di documento che fornisce la prova per la richiesta. Le prove possono essere in tutti i formati. Di solito per gli individui è la carta di identità, passaporto mentre per le aziende è un insieme di documenti di costituzione o di proprietà. Un'attestazione è quando una terza parte convalida che in base alla loro documentazione le affermazioni sono vere. Ad esempio, un'università può attestare il fatto che qualcuno ha studiato lì e ha conseguito una laurea. Tuttavia, le attestazioni sono un onere per l'autorità in quanto l'informazione può essere sensibile. Ciò significa che le informazioni devono essere mantenute in modo che soltanto persone autorizzate possano accedervi. I problemi legati ai 3 concetti sono: le prove sono costituite solitamente da dati non strutturati (immagini). Ciò significa che qualcuno in banca deve leggere e scansionare manualmente i documenti per estrarre i dati. Quando i dati cambiano (ad esempio un cambio di indirizzo) il cliente è obbligato a comunicare ai vari fornitori finanziari. Inoltre, alcune forme di prova possono essere falsificate. Ciò

si traduce in processi lunghi, costosi e inaffidabili. Per migliorare questo tipo di soluzione, i dati non strutturati vengano archiviati e inviati in un formato leggibile dalla macchina. La soluzione per dimostrare l'autenticità delle prove di identità è che le attestazioni devono essere firmate digitalmente. Una prova firmata digitalmente è valida come un attestato perché la firma digitale non può essere falsificata. Una soluzione per la gestione dell'identità digitale è un autorità centrale, in cui una terza parte gestisce i dati dei clienti. Il cliente inserisce i dati nel sistema e chiunque abbia bisogno può accedervi (con il permesso del cliente) e può utilizzare questi dati nei propri sistemi. Se i dati cambiano, il cliente li aggiorna e invia la modifica all'autorità centrale. I problemi con le soluzioni centralizzate sono: - dati tossici: essere a capo di un'autorità centrale è un arma a doppio taglio. Da un lato, un operatore può chiedere denaro per un'utilità conveniente. Dall'altra parte, un operatore è responsabile dei dati dei clienti. Ad esempio, un hacker può entrare nel sistema e rubare dati dei clienti commettendo frodi e crimini, inoltre può vendere le identità digitali dei clienti.

- Politica giurisdizionale: i clienti vogliono che i dati personali vengono memorizzati entro i confini geografici. Quindi può essere difficile creare archivi di identità internazionali perché non sappiamo su quale paese memorizzare i dati e chi può accedervi. Per evitare questi tipi di problemi utilizziamo l'identità auto sovrana.

3.3. Self-Sovereign Identity

Il problema fondamentale sull'identità digitale è il modo in cui le organizzazioni (aziende) memorizzano e trasmettono i dati. Ogni volta che una persona effettua delle transazioni con una banca, con un'agenzia di credito, un rivenditore online, tale organizzazione genera e memorizza all'interno del database tutte le informazioni di quella persona. Ciò si traduce, in un pericolo per l'utente. Questi server o database centralizzati che contengono tutte le informazioni sono obiettivi per criminali informatici. L'identità auto-sovrana potrebbe essere il prossimo passo, in cui ogni persona crea e gestisce le proprie identità digitali.

L'identità auto-sovrana parte dall'idea che tutti noi siamo i creatori della nostra identità, ovvero persone e aziende possono memorizzare i propri dati su dispositivi e fornirli in modo efficiente a coloro che hanno bisogno per convalidarli senza fare affidamento su un'autorità centrale. L'identità auto-sovrana fornisce alle persone un maggiore controllo sulla propria identità, ma la persona è responsabile delle misure adottate per stabilire e mantenere sia la privacy che l'affidabilità. Se una persona utilizza un provider di identità come Facebook, la persona fornisce tutti i dati. Tuttavia, la persona ha una visione minima della gestione delle sue identità digitali. La tecnologia Blockchain fornisce una nuova base per creare un sistema SSI. I requisiti di questo sistema sono:

- Controllo dei dati da parte dell'utente.

In un sistema SSI l'utente deve avere il pieno controllo dei suoi dati non solo dove i dati vengono memorizzati ma anche chi ha accesso ad essi. Inoltre, l'utente dovrebbe essere in grado di aggiungere attributi di identità, modificarli ed eliminarli.

- Sicurezza e privacy.

  Tutti i dati devono essere archiviati ed elaborati in maniera sicura preservando la privacy dell'utente.

- Portabilità dei dati.

  L'utente deve essere in grado di utilizzare i suoi dati in qualsiasi luogo. Ad esempio, un sistema SSI può essere utilizzato come un provider di identità quando l'utente tenta di accedere ad un servizio online.

- Integrità dei dati.

  L'integrità può essere garantita utilizzando la tecnologia blockchain.

- Trasparenza dei dati.

  Tutte le modifiche ai dati nella blockchain sono trasparenti in modo che nessuno possa modificare i dati senza che qualcun altro se ne accorga.

- Persistenza delle identità digitali e dei registri delle transazioni per garantire totale trasparenza a lungo termine.

3.4.Principi chiave dell'identità auto sovrana

La blockchain può essere adottata come un sistema di identità digitale. Invece di memorizzare tutti i dati e le transazioni crea un'identità che rende più facile la gestione dell'identità degli utenti. Un sistema SSI gode di alcuni principi chiave:

- Controllo:

  Gli utenti devono controllare le loro identità. Ciò non significa che l'utente controlla tutte le affermazioni sulla propria identità ma può fare affermazioni su altri utenti.
- Accesso:

  Gli utenti devono avere accesso ai propri dati. Ciò non significa che un utente possa necessariamente modificare le informazioni sulla sua identità, ma deve essere a conoscenza. Inoltre, gli utenti non devono avere uguale accesso ai dati degli altri ma soltanto ai propri.
- Trasparenza:

  I sistemi devono essere trasparenti. I sistemi utilizzati per amministrare e gestire una rete di identità devono essere aperti sia nel loro funzionamento che nel modo in cui sono gestiti.
- Protezione:

  I diritti degli utenti devono essere protetti. Per garantire ciò, l'autenticazione dell'identità deve avvenire tramite algoritmi resistenti alla censura e gestiti in modo decentralizzato.

Rispettando i seguenti principi, un utente ha il pieno controllo della propria identità digitale indipendentemente dalle condizioni di vita attuali, incluso il luogo dove si trova attualmente l'utente o il fornitore si servizi. Inoltre, l'identità auto sovrana aumenta la libertà dell'individuo e potrebbe contrastare la struttura di Internet, in cui la gestione dell'identità è sotto controllo dei "Big Five" (Apple, Microsoft, Google, Amazon, Facebook).

3.5. Self Sovereign Identity per l'utente

Per creare un sistema SSI, utilizziamo un'applicazione su uno smartphone oppure su un computer, una sorta di "portafoglio di identità" i cui dati di identità vengono memorizzati sul dispositivo utente e non conservati in una repository centrale. All'inizio il portafoglio di identità è costituito soltanto da un numero identificativo generato automaticamente dalla chiave pubblica e privata (password). Queste chiavi sono autosufficienti perché sono state create dall'utente e nessun altro conosce il numero identificativo.

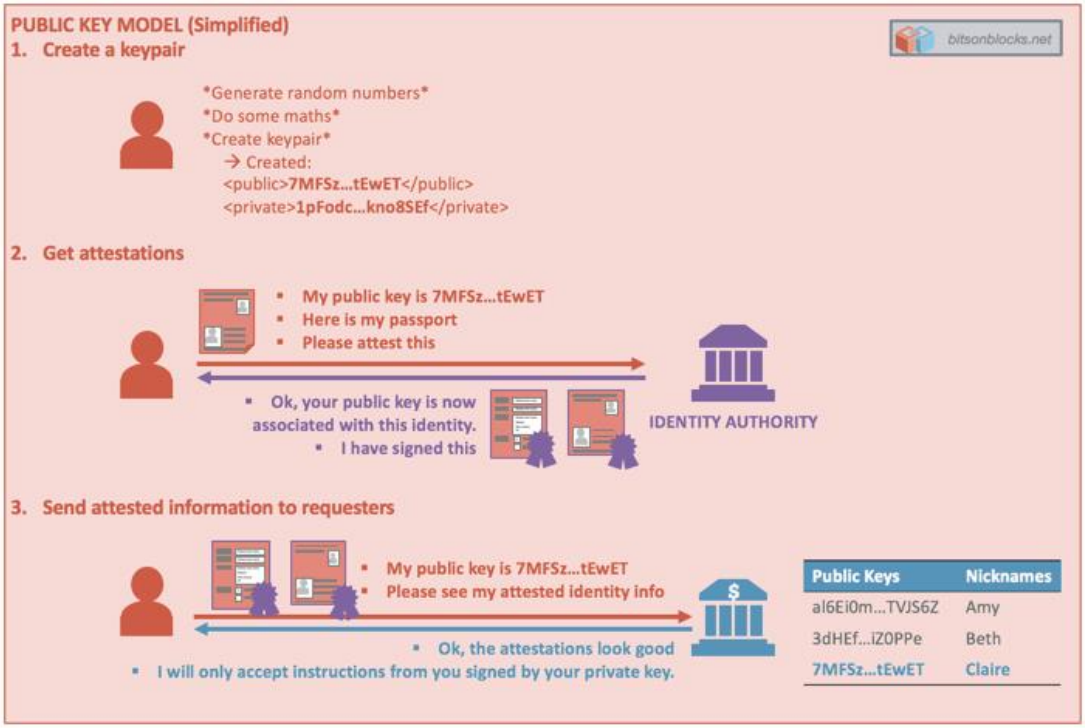

Figura 3: Public Key Model

I documenti sono leggibili a macchina, devono essere firmati digitalmente e sono valide entro un determinato periodo di tempo. L'autorità competente firma questi documenti con le firme digitali, ad esempio, ospedali, agenzie di passaporto. Il proprietario dell'identità deve essere in grado di scegliere quale informazione passare al richiedente. Ad esempio, se è necessario dimostrare di avere più di 18 anni, non è necessario condividere la data di nascita, è sufficiente una dichiarazione che dichiari di avere più di 18 anni, firmata dall'autorità competente. La condivisione di questo tipo di dati è più sicura sia per il provider di identità che per il destinatario. Il provider non ha bisogno di mostrare più di quanto è necessario ed il destinatario non ha bisogno di memorizzare dati sensibili inutilmente. Questi dati verrebbero memorizzati sul dispositivo dell'utente e poi quando

richiesti l'utente approverebbe una terza parte per raccogliere dati specifici, toccando una notifica sul dispositivo. Un esempio simile è l'utilizzo di Facebook, Linkedin in cui un utente accede ai server per raccogliere i suoi dati personali, mentre in un sistema SSI l'utente si collega direttamente al suo dispositivo. Per sfruttare l'auto sovranità, un sistema deve avere alcune caratteristiche importanti: - Persistente: l'identità che può essere tolta non è auto sovrana. L'identità auto sovrana non può essere utilizzata da altri utenti ed è di proprietà della persona che li crea. L'identità auto sovrana non viene utilizzata soltanto da privati ma anche da organizzazioni. – Peer-based: la sovranità definisce un confine entro il quale le persone possono utilizzare l'identità per interagire con altri. I sistemi SSI non sono client-server ma peer-to-peer. - Portabilità: gli identificatori e le credenziali associate devono essere portatili e i sistemi SSI devono essere interoperabili per proteggere la scelta ed il controllo.

Capitolo 4 – Blockpass

4.1. Che cos'è Blockpass?

Molte applicazioni utilizzano la tecnologia blockchain per la gestione dell'identità e dell'autenticazione. Una di queste è Blockpass. L'idea di questa applicazione è consentire agli utenti di memorizzare i propri dati attraverso l'app mobile basata sulla blockchain, inoltre eliminerà le lunghe procedure manuali di conformità. Blockpass crea una identità agli utenti utilizzando una procedura KYC che coinvolge la cancellazione dei dati in ogni fase di verifica e questi dati possono essere memorizzati soltanto sul dispositivo del cliente. L'identità può essere autenticata mediante una funzione hash derivante dall'albero Merkle e memorizzata sulla blockchain privata per il confronto con i dati memorizzati sul dispositivo dell'utente. I dati hash possono essere cancellati dalla blockchain privata su richiesta del cliente. Blockpass si basa sull'auto-sovranità in cui i dati non vengono controllati da terze parti ma dagli utenti stessi. Inoltre, gli utenti scelgono quali documenti devono essere verificati e firmati (ad esempio un documento di identità) e quali dati devono essere memorizzati (ad esempio sul dispositivo o nel cloud).

4.2. Componenti

L’applicazione Blockpass è composta da vari componenti:

- Applicazione Mobile:

L’applicazione utente front-end orientato al consumatore Blockpass. Dall’app gli utenti sono in grado di creare un nuovo account(profilo), presentare documenti per la verifica, presentare la loro identità digitale ai fornitori di servizi, accedere ai servizi dell’applicazione, firmare le transazioni. La configurazione dell’app è divisa in passi, il 1 passo è costituito dalla registrazione dell’utente, in cui inserisce il proprio indirizzo e-mail. L’applicazione invia l’indirizzo e-mail al server, che genera un codice e viene inviato all’indirizzo di posta elettronica. L’applicazione chiede all’utente di inserire il codice di verifica.

Nel 2 passo, l’utente deve scegliere una password. L’applicazione genera una coppia di chiave pubblica (UserPubKey) e privata (UserPrivKey). L’applicazione cifra UserPubKey con la password fornita. Nel passo 3, l’utente dopo aver scelto la password gli viene richiesto di attivare il TouchID o FaceID solo se il dispositivo ne è fornito. Dopo di che nella fase 4, viene creata l’identità Blockpass dell’utente e inviata alla Blockchain. Qualsiasi informazione inviata all’applicazione viene sottoposta ad un hash, creando un albero Merkle. La radice dell’hash di questo albero viene memorizzato su una blockchain privata. Quando l’utente utilizza l’identità per accedere ad un servizio, esso ricrea l’hash, ricostruisce l’albero di Merkle e ottiene la radice dell’hash. Questo hash viene confrontato con l’hash

iniziale memorizzato sulla blockchain per provare che i dati non sono stati modificati da terze parti. È importante sottolineare che l'utente ha la capacità di gestire la codifica dei dati utilizzando JSON-LD, che consente la serializzazione dei dati utilizzando un formato dati indipendente dal linguaggio. Sull'applicazione Blockpass è possibile avviare il backup manualmente. Il backup contiene tutte le informazioni dell'app, i certificati dell'utente e la chiave locale. Il backup è un file binario protetto da una password. Un altro componente importante è il certificato. Blockpass emette i certificati che dal punto di vista dell'utente rappresentano un miglioramento del profilo e sono necessari per soddisfare particolare requisiti KYC. Esso viene firmato con chiave privata da un notaio oppure da un'altra identità, le quali assicurano che le credenziali dell'utente siano corrette. Un certificato include tutti i dati dell'utente per emettere il certificato, un campo di testo libero in cui l'emittente definisce i termini del certificato, data di emissione, scadenza e la firma digitale dell'emittente. Quando un utente invia dei dati per la verifica oppure deve soddisfare determinati requisiti, un emittente invia un certificato sull'applicazione. In questo caso sul dispositivo utente viene inviata una notifica. L'utente può rivedere le informazioni del certificato prima che esso possa essere aggiunto al proprio profilo. Inoltre, l'utente potrebbe anche rifiutare un certificato.

- Blockpass ID Keys sono pulsanti ID che possono essere utilizzati da terze parti oppure da Dapps. Come i certificati, gli utenti possono aggiungere pulsanti id sul proprio profilo

Blockpass. Se un utente deve accedere ad servizio pubblico richiede una chiave pubblica e può decidere di condividerla. Altrimenti se un utente desidera firmare una transazione oppure un certificato da inviare ad un altro utente dell'applicazione può utilizzare la sua chiave privata.

- Blockpass KYC: è una funzionalità che permetta agli utenti di utilizzare Blockpass per verificare le informazioni scambiate dagli utenti. I dati vengono inviati ai servizi di verifica per essere validati. I certificati vengono generati e poi cancellati dalla Blockpass e viene inviata una richiesta agli agenti di verifica per eliminare ulteriori copie.

4.3. Blockpass for Business

L'applicazione Blockpass presenta alcune caratteristiche fondamentali:

- Rapid user OnBoarding

Con l'uso della tecnologia Blockchain e dei contratti intelligenti si risolve le noiose procedure di KYC e AML riducendo i tempi legati alla registrazione dell'utente e aumentando le conversazioni.

- Low Cost Pre-verificed Compliance

Con servizi di regolamentazione e conformità condivisi, gli utenti possono utilizzare più volte servizi diversi evitando costose e duplicate verifiche dell'identità.

- New Application Potential

Un nuovo protocollo di conformità consentirà nuovi livelli di efficienza e nuove possibilità di sviluppo delle applicazioni basate sulla blockchain.

- Simple Integration

Insieme di strumenti facilmente installabile incluso anche una funzionalità di verifica KYC. Tutto integrato perfettamente nella infrastruttura con i SDK.

4.4. Blockpass per l'utente

Il modo più semplice, più sicuro e veloce è quello di accedere a vari servizi che l'applicazione offre:

- Accesso rapido ai servizi conformi

Blockpass fornisce una gateway sicuro e veloce per accedere a ICO e servizi regolamentati senza la necessità di completare i requisiti di conformità ridondanti.

- Possiedi i tuoi dati personali

Blockpass è un servizio di verifica dell'identità che memorizza solo una rappresentazione crittografica della tua identità verificata su una lista della blockchain. I dati vengono memorizzati sul dispositivo dell'utente e condivisi soltanto con la persona scelta.

- Lista condivisa

Blockpass consente agli utenti di ottenere l'autorizzazione immediata senza dover registrarsi ogni volta che accedono all'applicazione.

4.5. Vantaggi

L’applicazione Blockpass oltre a proteggere i dati personali degli utenti ridurrà anche il costo della conformità per i professionisti della blockchain. Per fare ciò Blockpass fornirà agli utenti una “identità autosufficiente” evitando i rischi di pirateria informatica. Blockpass offre due importanti vantaggi:

- gli utenti mantengono il controllo della propria identità e soltanto loro possono decidere chi può accedervi.
- non esiste un server centralizzato che memorizza i dati degli utenti. Infatti quando un utente invia dei documenti sulla applicazione Blockpass per la verifica, una copia viene memorizzata localmente e crittografata con una password sul dispositivo dell’utente. L’utente è l’unica persona che detiene la password per decrittografarlo. Dopo che Blockpass ha ricevuto i dati li cancella dai server. Poiché i dati di ciascun utente vengono distrutti una volta verificati, se gli hacker riescono a violare i server Blockpass troveranno solamente file illeggibili che non hanno alcun valor per loro. Pertanto, questi dati esistono solo sul telefono dell’utente fino a quando non decidono di condividerlo con fornitori di terze parti. Questo offre agli utenti il controllo completo sui propri dati personali. Nel caso in cui si perda la password non è più possibile accedere a questa identità e bisogna crearne una nuova. Se si perde l’accesso al telefono e non si ha eseguito il backup, l’identità viene persa. Poiché l’applicazione Blockpass non conserva i dati. Inoltre, non è consigliabile utilizzare l’applicazione su più dispositivi perché i dati non

vengono memorizzati sul server ma vengono archiviati localmente. Se si utilizzano due o più dispositivi, i dati verranno suddivisi tra diverse posizioni e non sarà possibile unirli nuovamente in un'unica applicazione.

Conclusioni

Lo scopo di questa tesi di laurea è quello di fornire una panoramica sulla tecnologia blockchain per poi approfondire come viene gestita l'identità e l'autenticazione sulla blockchain. Partendo da queste si affrontano quali sono oggigiorno gli ambiti di applicabilità della blockchain facendo riferimento al supporto dei più recenti report e pubblicazioni da parte di enti di ricerca o osservatori, per poi analizzare quali potrebbero essere gli sviluppi futuri della stessa. Inoltre, essendo ancora nelle prime fasi di sviluppo esistono comunque numerose problematiche da affrontare. Innanzitutto deve raggiungere la massa critica. Le tecnologie legate alla blockchain beneficiano di un effetto rete, il che vuol dire che l'aggiunta di ogni utente in rete aumenta il valore della presenza nella rete per tutti gli altri. Sebbene l'effetto rete costituisca un vantaggio legato alla sicurezza della rete ma presenta anche uno dei principali svantaggi legato all'estrema difficoltà di avvio del processo, perché le piccole reti non hanno un valore paragonabile a quello delle grandi reti per il cliente finale. In secondo luogo si deve considerare l'elevato costo in termini energetici e di spazi di archiviazione. Dal momento che le blockchain sono libri mastri distribuiti e che tutti i dati sono memorizzati sui nodi, lo spazio di archiviazione di tale sistema cresce in modo esponenziale mano a mano che si aggiungono nodi/utenti al sistema. Per consentire alla blockchain di continuare a crescere, sarà necessaria apportare modifiche ai protocolli per ridurre i requisiti delle risorse coinvolte.

Infine, nell'ultimo capitolo viene analizzata l'applicazione Blockpass. Un'applicazione di identità basata sulla blockchain in cui gli utenti possono stabilire, verificare, archiviare e gestire le proprie identità, mantenendo il pieno controllo su tutti i dati coinvolti.

Bibliografia

1. Sovrin White Paper: https://sovrin.org/
2. Che cos'è la blockchain, come funziona e perché funziona bene : https://www.wired.it/economia/finanza/2016/02/22/blockchain-come-funziona/
3. A blueprint for digital identity – R.Jesse McWaters

4. Digital Identity : https://www.weforum.org/projects/digital-identity
5. Blockchain: perché e come sfruttarla: https://www.zerounoweb.it/cio-innovation/blockchain-perche-e-come-sfruttarla/
6. Self Sovereign Identity: a guide to privacy for your digital identity with Blockchain: https://medium.com/
7. Trasformed digital identity into identity: https://www.ibm.com/blockchain/solutions/identity
8. The New Internet: The Connection of Everything: https://www.entrepreneur.com/article/319088
9. https://www.blockchainews.it/
10. Blockpass Identity for a Connected World: https://www.blockpass.org/
11. What is Blockchain Technology: https://blockgeeks.com/guides/what-is-blockchain-technology/
12. Digital identity: https://www.techopedia.com/definition/23915/digital-identity
13. Blockchain and its impact on digital identity: https://www.rolandberger.com/en/Point-of-View/Blockchain-and-its-impact-on-digital-identity.html
14. Blockchains and Digital Identity: https://towardsdatascience.com/https-medium-com-shaanray-how-blockchains-will-solve-privacy-88944f3c67f0
15. https://www.wired.it/economia/finanza/2018/01/12/satoshi-nakamoto-bitcoin/

16. https://www.blockchain4innovation.it/mercati/pubblica-amministrazione/spidchain-identita-digitale-4-0-pa-aziende/
17. https://monetevirtuali.pro/ce-unalternativa-a-facebook-e-chiamata-lidentita-di-se-sovrano/
18. Cos'è la Blockchain e perché potrebbe cambiarci la vita : https://www.lastampa.it/2016/02/29/tecnologia/cos-la-blockchain-e-perch-potrebbe-cambiarci-la-vita-lI9xhVLT7AFGcpkUEmPBdI/pagina.html

Ringraziamenti

A conclusione di questo lavoro di tesi, è doveroso porre i miei più sentiti ringraziamenti alle persone che ho avuto modo di conoscere in questo importante periodo della mia vita e che mi hanno aiutato a crescere sia dal punto di vista professionale che umano. Ringrazio anzitutto il mio Prof. Alfredo De Santis (relatore) che mi ha insegnato, sostenuto, consigliato ed aiutato durante tutto lo svolgimento della tesi. Non so se trovo le parole giuste per ringraziare la mia famiglia, però vorrei che questo

traguardo raggiunto, per quanto possibile, fosse un premio anche per loro e per i sacrifici che hanno fatto. Senza di voi certamente non sarei la persona che sono. Per ultimi ma non meno importanti, i miei amici di infanzia e dell'università. Se ho raggiunto questo traguardo lo devo anche alla vostra presenza, per avermi fatto capire che potevo farcela, incoraggiandomi a non mollare mai.