UNIVERSITÀ DEGLI STUDI DI SALERNO

FACOLTÀ DI SCIENZE MATEMATICHE,FISICHE E NATURALI

DIPARTIMENTO DI INFORMATICA

TESI DI LAUREA TRIENNALE IN INFORMATICA

Studio sulla blockchain come servizio per gestire l' identità digitale.

Relatore :

Alfredo De Santis

Candidato :

Aniello Giugliano

0512103007

Anno Accademico 2017/2018

Sommario

Introduzione

In questa tesi è stato fatto uno studio sul tema della gestione dell'identità digitale , in particolare viene analizzato il concetto di Self Sovreign Identity(identità autosovrana), e viene dimostrato come la tecnologia blockchain possa essere utilizzata per realizzare un sistema di autosovranità. Nel capitolo 1,andremo ad analizzare le origini della blockchain,che cos'è un libro mastro decentralizzato ,come lavora la blockchain e come vengono memorizzati i dati in essa,cos'è la regola del consenso e come vengono aggiunti i blocchi alla catena. Inoltre analizzeremo anche quali sono i punti di forza e quali sono gli svantaggi nell'utilizzo della blockchain,ed i vari campi di applicazione di questa tecnologia. Nel capitolo 2 andremo ad analizzare il concetto di identità digitale e le sue proprietà. Inoltre studieremo le varie fasi in cui si è evoluta l'identità digitale, ed alcuni dei problemi legati alla sua gestione. Nel capitolo 3 analizzeremo nel dettaglio il concetto di Self Sovreign Identity,spiegando come funziona questo sistema per l'utente. Nel capitolo 4 andremo ad analizzare l' applicazione ShoCard, che elimina la necessita di memorizzare nome utente e password all'interno di un database centrale,utilizzando un processo di autenticazione digitale basato su blockchain.Vedremo nello specifico alcuni casi d'uso ed alcuni scenari della suddetta applicazione.

Capitolo 1 – Blockchain

1.1. Storia della Blockchain

Il primo lavoro su una catena di blocchi crittografata è stato descritto nel 1991 da Stuart Haber e Scott Stornetta. Nel 1992 venne incorporato il Merkle Tree alla progettazione, che ne migliorò l' efficienza consentendo di raccogliere diversi documenti in un unico blocco. La blockchain pare essere stata ideata da Satoshi Nakamoto (pseudonimo dell'inventore della blockchain e del suo codice sorgente), e resa famosa dal suo protocollo più conosciuto, la moneta virtuale Bitcoin. Satoshi Nakamoto rivela il proprio progetto e la propria visione nell'ottobre del 2008 con la pubblicazione di un white paper che parla e descrive la possibilità di sviluppare una digital currency indipendente da ogni ente o istituzione centrale.

1.2. Database Distribuito(Distribuited Ledger)

La blockchain è un'implementazione del database distribuito, ma facciamo un passo indietro e vediamo che cos'è un Distribuited Ledger e come funziona. Nel momento in cui parliamo di Distributed Ledger ci troviamo davanti un database che non si trova fisicamente solo su un server , ma che invece si trova su più computer nello stesso momento, tutti perfettamente sincronizzati su tutti gli stessi documenti. In questo modo l'informazione è reperibile in maniera molto rapida, in quanto la potenza di calcolo sfrutta la potenza di tutti i computer connessi. Ci sono fondamentalmente due processi che permettono ai database distribuiti di funzionare correttamente, e di non perdere dati per strada. Questi processi sono:

– Replica del database: ovvero un software è incaricato di analizzare il database per identificare cambiamenti. Una volta identificati questi cambiamenti, il software fa in modo che questi cambiamenti vengano replicati e che tutti i database siano identici.

– Duplicazione: è un processo che assicura che tutti i database abbiano gli stessi dati. In pratica identifica un database master, che poi duplica i dati su tutti gli altri database, in modo da renderli uguali. Gli utenti possono modificare soltanto il database master, garantendo che i dati locali non vengano sovrascritti erroneamente.

1.3. Permissionless e Permissioned Ledger

Esistono due tipi di Ledger, le Permissionless Ledger e le Permissioned Ledger. Le Permissionless Ledger, di cui l'esempio più famoso e diffuso è rappresentato dal Bitcoin, sono aperte, non hanno una "proprietà" o un attore di riferimento e sono concepite per non essere controllate. L'obiettivo delle Permissionless Ledger è quello di permettere a ciascuno di contribuire all'aggiornamento dei dati sul Ledger e di disporre, in qualità di partecipante, di tutte le copie immutabili di tutte le operazioni. Ovvero di disporre di tutte le copie identiche di tutto quanto viene approvato grazie al consenso.

Questo modello di Blockchain impedisce ogni forma di censura, nessuno è nella condizione di impedire che una transazione possa avvenire e che possa essere aggiunta al Ledger una volta che ha conquistato il consenso necessario tra tutti i nodi (partecipanti) della Blockchain. Le Permissionless Ledger possono essere utilizzate come database globale per tutti quei documenti che hanno la necessità di essere assolutamente immutabili nel tempo a meno di aggiornamenti che richiedono la massima sicurezza in termini di consenso, come ad esempio i contratti di proprietà o i testamenti. Le Permissioned Ledger possono invece essere controllate e dunque possono avere una "proprietà". Quando un nuovo dato o record viene aggiunto il sistema di approvazione non è vincolato alla maggioranza dei

partecipanti alla Blockchain bensì ad un numero limitato di attori che sono definiti Trusted. Questo tipo di Blockchain possono essere utilizzate da istituzioni, grandi imprese che devono gestire filiere con una serie di attori, imprese che devono gestire fornitori e subfornitori, banche, società di servizi. In questo caso le Permissioned Ledger rispondono alle necessità di un aggiornamento diffuso su più attori che possono operare in modo indipendente, ma con un controllo limitato a coloro che sono autorizzati. Le Permissioned Ledger permettono poi di definire speciali regole per l'accesso e la visibilità di tutti i dati. In altre parole le Permissioned Ledger introducono nella Blockchain un concetto di Governance.

1.4. Funzionamento della Blockchain

Come funziona la Blockchain? Possiamo dividere il suo funzionamento in più aspetti.

- Struttura

  Una blockchain è una contabilità digitale decentralizzata, distribuita e pubblica che viene utilizzata per registrare transazioni su più computer in modo che il record non possa essere modificato retroattivamente senza la modifica di tutti i blocchi successivi e della collusione della rete.

  Ciò consente ai partecipanti di verificare e controllare le transazioni a basso costo. Un database blockchain è gestito in modo autonomo utilizzando una rete peer-to-peer e un server timestamping distribuito. Sono autenticati da una collaborazione di massa alimentata da interessi collettivi. Il risultato è un robusto flusso di lavoro in cui l'incertezza dei partecipanti riguardo alla sicurezza dei dati è marginale. L'uso di una blockchain rimuove la caratteristica di riproducibilità infinita da una risorsa digitale. Conferma che ogni unità di valore è stata trasferita una

sola volta, risolvendo il problema di vecchia data della doppia spesa. Le blockchain sono state descritte come un protocollo di scambio di valori. Questo scambio di valori può essere completato più rapidamente, in modo più sicuro e più economico rispetto ai sistemi tradizionali.

- Blocchi

I blocchi contengono batch di transazioni valide che sono hash codificati in un Merkle Tree. Ogni blocco include l'hash crittografico del blocco precedente nella blockchain, che collega i due. I blocchi collegati formano una catena. Questo processo iterativo conferma l'integrità del blocco precedente, fino al blocco di genesi originale. A volte blocchi separati possono essere prodotti contemporaneamente, creando una forcella temporanea.

Oltre a una cronologia hash sicura, ogni blockchain ha un algoritmo specifico per il punteggio di diverse versioni della cronologia, in modo che uno con un valore più alto possa essere selezionato rispetto ad altri. I blocchi non selezionati per l'inclusione nella catena sono chiamati blocchi orfani. I peer che supportano il database hanno di volta in volta versioni diverse della cronologia. Mantengono solo la versione con punteggio più alto del database a loro nota. Ogni volta che un peer riceve una versione con punteggio più alto (solitamente la vecchia versione con un singolo nuovo blocco aggiunto) estende o sovrascrive il proprio database e ritrasmette il miglioramento ai propri pari.

Figura 1: Blocchi all'interno di una Blockchain

```java
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 2: Struttura dei dati di un blocco

- Tempo di blocco

Il tempo di blocco è il tempo medio impiegato dalla rete per generare un blocco ed aggiungerlo alla blockchain. Al momento del completamento del blocco, i dati inclusi diventano verificabili. Nel mondo delle criptovalute, ciò si verifica quando avviene la transazione monetaria, quindi un tempo di blocco più breve significa transazioni più veloci. Il tempo di blocco per Ethereum è impostato tra 14 e 15 secondi, mentre per Bitcoin è di 10 minuti.

```
public static String applySha256(String input){
  try {
    MessageDigest digest = MessageDigest.getInstance("SHA-256");

    //Applies sha256 to our input,
    byte[] hash = digest.digest(input.getBytes("UTF-8"));

    return Hex.encodeHexString( hash );

  } catch(Exception e) {
    throw new RuntimeException(e);
  }
}
```

Figura 3: Calcolo della funzione hash

Come funziona la decentralizzazione di una Blockchain? Memorizzando i dati attraverso la sua rete, la blockchain elimina i rischi associati ai dati che vengono conservati centralmente. La blockchain decentralizzata può utilizzare il passaggio di messaggi ad-hoc e la rete distribuita.

La rete non ha punti di vulnerabilità centralizzati che i cracker informatici possono sfruttare; allo stesso modo, non ha un punto centrale di fallimento. I metodi di sicurezza blockchain includono l'uso della crittografia a chiave pubblica. Una chiave pubblica (una lunga stringa di numeri a caso) è un indirizzo sulla blockchain. I token di valore inviati attraverso la rete sono registrati come appartenenti a quell'indirizzo. Una chiave privata è come una password che consente al suo proprietario di accedere alle proprie risorse digitali o ai mezzi per interagire altrimenti con le varie funzionalità che ora le blockchain supportano.

I dati memorizzati sulla blockchain sono generalmente considerati incorruttibili. Mentre i dati centralizzati sono più controllabili, e quindi sono possibili le modifiche ai dati, la blockchain rende i dati trasparenti a tutti i soggetti coinvolti. Ogni nodo in un sistema decentralizzato ha una copia della blockchain. La qualità dei dati è garantita da una massiccia replica del database e dalla fiducia computazionale. Nessuna copia "ufficiale" centralizzata esiste e nessun utente è "fidato" più di un altro. Le transazioni vengono trasmesse alla rete tramite software. I messaggi

vengono consegnati in base al miglior sforzo. I miner convalidano le transazioni, le aggiungono al blocco che stanno costruendo e quindi trasmettono il blocco completato ad altri nodi.

1.5. Consenso Distribuito

La blockchain utilizza un algoritmo di consenso per aggiungere un nuovo blocco alla catena di blocchi.Questo algoritmo è conosciuto col nome di Proof of Work(PoW). In una Blockchain, questo algoritmo viene utilizzato per confermare le transazioni e produrre i nuovi blocchi della catena. La PoW incentiva i miner a competere tra loro nell'elaborazione degli scambi, ricevendo in cambio una ricompensa. All'interno della Blockchain un registro decentralizzato raccoglie ogni singola transazione: tuttavia, per poter essere considerate valide, queste transizioni devono essere prima approvate e organizzate in blocchi. Tale responsabilità ricade su speciali nodi chiamati miner. L'intero processo viene invece definito mining. Alla base di questo sistema troviamo complessi problemi matematici e la necessità di dimostrarne semplicemente la soluzione. Si tratta di una sorta di enigma, che richiede un'enorme potenza di calcolo per essere risolto.
Ne esistono di varie tipologie:
-Funzione di hash, ovvero dover trovare un input partendo da un output;
-Scomposizione in numeri primi, vale a dire rappresentare un numero come moltiplicazione di altri due numeri;
-Guided tour puzzle protocol, che in caso di attacco DoS richiede, ad alcuni nodi ed in un certo ordine, il calcolo di una funzione di hash. In questo caso, bisogna riuscire a trovare una catena partendo da una stringa alfanumerica.
Col il termine 'hash' solitamente s'intende sia il problema matematico che la sua soluzione. Quando la rete si espande i problemi pian piano di

complicano, e l'algoritmo necessita di maggiore potenza di calcolo per poterli risolvere. La difficoltà dei problemi è una questione parecchio complessa e delicata. La velocità e l'esattezza di un sistema Blockchain dipendono dalla difficoltà dei problemi. Ma i problemi non dovrebbero essere eccessivamente complessi, poiché in tal caso la generazione di nuovi blocchi richiederebbe troppo tempo, le transazioni non verrebbero elaborate ed il flusso della rete si bloccherebbe. Se il problema non ha un tempo di risoluzione ben definito, generare nuovi blocchi sarebbe praticamente impossibile. Al contrario, se il problema fosse troppo semplice, la rete diverrebbe estremamente vulnerabile ad attacchi esterni. Inoltre la soluzione deve poter essere controllata con estrema semplicità da ogni macchina, in quanto non tutti i nodi potrebbero essere capaci di appurare che i calcoli siano stati eseguiti correttamente. In tal caso questo nodi dovrebbero far affidamento su altri utenti, violando uno dei principi fondamentali della Blockchain ossia la trasparenza. I miner quindi risolvono il problema, danno vita ad un nuovo blocco e confermano tutte le transazioni al suo interno.

La complessità del problema dipende dal numero di utenti, dalla potenza di calcolo disponibile e dal carico della rete. La hash di ogni blocco contiene la hash del blocco precedente, incrementando la sicurezza ed impedendo ogni sorta di violazione informatica. Quando un miner riesce a risolvere il problema, il nuovo blocco viene creato e le transazioni vengono piazzate al suo interno. I principali vantaggi offerti da un sistema PoW sono un'ottima difesa contro gli attacchi DoS e l'impatto marginale delle quote nel mining.

Difesa contro gli attacchi DoS.

La PoW impone parecchi limiti alle azioni che è possibile intraprendere sulla rete, ed un attacco efficiente richiederebbe moltissimo tempo ed una potenza di calcolo incredibile. Nonostante quindi gli attacchi DoS ad una

Blockchain siano in teoria possibili, in pratica i risultati sarebbero deludenti ed i costi estremamente elevati.

Mining

Non importa quanto sia alta la percentuale delle quote nel proprio portafoglio: in un sistema PoW l'unica cosa che conta è la potenza di calcolo utilizzata per risolvere i problemi matematici e generare nuovi blocchi. Chi possiede grosse quantità di denaro, quindi, non ha maggiore controllo sulla rete.

I principali svantaggi di un sistema PoW sono invece i costi elevati, la totale inutilità dei calcoli e il rischio di attacchi del 51%.

Costi elevati.

Il processo di mining richiede macchine altamente specializzate, capaci di risolvere in tempi brevi algoritmi estremamente complessi. Questi dispositivi sono estremamente costosi e consumano anche enormi quantità di energia elettrica, incrementando ulteriormente i prezzi.

Inutilità dei calcoli.

I miner consumano moltissimo tempo ed energie per generare nuovi blocchi, eseguendo calcoli fini a se stessi, non applicabili a nessun altro settore. I problemi garantiscono quindi la sicurezza della rete, ma non possono essere utilizzati in campo economico o scientifico.

Attacco del 51%

Con attacco del 51%, o attacco di maggioranza, s'intende il caso in cui un singolo utente o un gruppo di individui riesca a controllare la maggior parte della potenza di mining di una rete. Gli aggressori ottengono una tale influenza nella rete da poter controllare l'esito degli eventi che avvengono al suo interno. Potrebbero ad esempio monopolizzare la generazione di nuovi blocchi, ostacolando gli altri miner e impedendo loro di ricevere le ricompense oppure potrebbero addirittura annullare le transazioni.

```
public ArrayList<Block> blockChain = new ArrayList<Block>();

public void addBlock(String data) {
  Block block = new Block( data );
  if ( blockChain.isEmpty() ) {
    block.setPreviousHash( "0" );
  } else {
    block.setPreviousHash( blockChain.get( blockChain.size() - 1 ).getHash() );
  }
  block.setHash( calculateHash( block ) );
  blockChain.add( block );
}

public String calculateHash( Block block ) {
  return Utils.applySha256( block.toString() );
}
```

Figura 4: Esempio di codice del Mining

1.6. Vantaggi e Svantaggi della Blockchain.

I principali vantaggi nell'utilizzo della Blockchain sono:

- Immutabilità:

  Con la Blockchain è possibile effettuare transazioni irrevocabili, e allo stesso tempo più facilmente tracciabili. In questo modo si garantisce che le transazioni siano definitive, senza alcuna possibilità di essere modificate o annullate.

- Trustless :

  Blockchain consente alle transazioni digitali di accadere tra parti che non si fidano l'una dell' altra. Immagina una moneta digitale memorizzata in un file sul tuo computer. Puoi copiare e incollare il file un numero infinito di volte. Il valore di questa valuta digitale sarebbe vicina allo zero. In passato, le autorità centrali (le banche) hanno agito da mastro, mantenendo registrazioni del numero di monete che ciascuno di noi ha a disposizione come libro mastro centralizzato, per evitare il problema della duplicazione. Distribuendo il Ledger a molti nodi e sincronizzando questo Ledger tramite il consenso, blockchain consente alle parti che non si fidano l'una dell'altra, di credere che la transazione sia reale e non priva di valore. Nel tempo, la fiducia può essere ulteriormente aumentata, attraverso processi condivisi e registrazioni

immutabili delle transazioni. Ciò facilita una vasta gamma di potenziali transazioni digitali che sarebbero potute essere realizzate prima senza un'autorità centrale che le gestisse.

- Trasparenza:
  Le transazioni effettuate attraverso la Blockchain sono visibili a tutti i partecipanti, garantendo così trasparenza nelle operazioni.
- Convenienza:
  Effettuare transazioni attraverso la Blockchain è conveniente per tutti i partecipanti, in quanto vengono meno interlocutori di terze parti, necessari in tutte le transazioni convenzionali che avvengono tra due o più parti (ovvero le banche e altri enti simili).
- Digitalità:
  Con la Blockchain tutto diventa virtuale. Grazie alla digitalizzazione, gli ambiti applicativi di questa nuova tecnologia diventano tantissimi.
- Decentralizzazione
  Blockchain sostiene anche la riduzione dei monopoli centralizzati e rimuove i costi. Distribuendo le reti, la blockchain può trovare economie di scala, senza un singolo investimento centralizzato. Ciò aumenta la concorrenza nel mercato, riducendo le barriere all'ingresso, facendo pressione su tutti i partecipanti affinché diventino più efficienti. Inoltre, consentire ai peer di effettuare transazioni senza alcun obbligo di fiducia interrompe le pratiche commerciali correnti delle organizzazioni che facilitano la fiducia, come ad esempio le banche.

Nell'utilizzo della blockchain esistono anche degli svantaggi, di seguito vengono esposti i principali.

- Spreco di energia :

Ogni nodo gestisce la blockchain per mantenere il consenso. Ciò offre livelli estremi di tolleranza agli errori, assicura tempi di fermo zero e rende i dati memorizzati sulla blockchain sempre immutabili e resistenti alla censura. Ma tutto ciò è uno spreco di energia, poiché ogni nodo ripete un compito per raggiungere il consenso bruciando elettricità e tempo lungo la strada. Ciò rende il calcolo molto più lento e costoso rispetto a un singolo computer tradizionale. Ci sono molte iniziative che cercano di ridurre questo costo focalizzandosi su mezzi alternativi per mantenere il consenso, come il proof-of-stack.

- Velocità e costo della rete.

  Le reti blockchain richiedono l'esecuzione di nodi. Ma poiché molte delle reti sono nuove, mancano del numero di nodi per facilitarne l'uso diffuso. Questa mancanza di risorse si manifesta in costi più elevati poiche i nodi ricercano ricompense più elevate per il completamento delle transazioni in uno scenario di domanda e offerta ed inoltre le transazioni sono più lente , dato che i nodi danno priorità alle transazioni con premi più elevati, i backlog delle transazioni si accumulano. Nel tempo, reti di blockchain pubbliche riusciranno a incentivare i nodi, creando allo stesso tempo costi favorevoli per gli utenti, con transazioni completate in un periodo di tempo rilevante. Questo equilibrio è la chiave per l'economia di ogni blockchain.

- Dimensione del blocco.

  Ogni transazione o blocco aggiunto alla catena aumenta le dimensioni del database. Poiché ogni nodo deve mantenere una catena da gestire, i requisiti di elaborazione aumentano a ogni utilizzo.

- Potere speculativo

Le blockchain come Ethereum vengono eseguite utilizzando modelli valutari per finanziare lo sviluppo o gestire l'economia dei nodi. Le valute basate su blockchain stanno cercando di posizionarsi come alternativa alle valute tradizionali come dollaro o euro, tuttavia le queste ultime sono fortemente sostenute dalle solide condizioni economiche del paese di origine mentre la blockchain non ha un tale supporto e quindi le valute basate sulla blockchain sono altamente speculative sul mercato.

1.7. Applicazioni della blockchain

La tecnologia blockchain può essere integrata in più aree. L'uso principale delle blockchain oggi è quella di libro mastro distribuito per criptovalute, in particolare bitcoin. Tuttavia essa può essere utilizzata in tantissimi campi. Vediamo un elenco di alcuni dei vari utilizzi possibili delle Blockchain:

- Leggittimazione del voto elettorale:
  Le blockchain possono servire come strumento utile per la selezione, il monitoraggio e il conteggio dei voti in modo specchiato, sgomberando il campo da qualsiasi probabile tentativo di frode elettorale, trucchetti o perdita di dati e voti.
- Compravendita di automobili:
  Il potenziale cliente sceglie l'auto che vuole ottenere in leasing e la transazione viene immessa sul registro pubblico della blockchain. Una volta sedutosi al posto di guida, il cliente firma un contratto di locazione e una polizza assicurativa e il distribuited ledger viene aggiornato con le informazioni relative.
- Compravendita immobiliare:
  La blockchain offre un modo per ridurre la necessità di supporto cartaceo per la registrazione dei dati e porta, dunque, a una

velocizzazione delle operazioni legate alla stesura dei contratti, all'identificazione delle controparti e dei dettagli precisi del bene oggetto di compravendita. I database decentralizzati applicati al settore della compravendita immobiliare possono aiutare a registrare, monitorare e trasferire titoli fondiari, atti di proprietà, privilegi ecc. e contribuiscono ad assicurare che i documenti siano accurati e verificabili.

- Sanità:

  Le blockchain applicate al settore della sanità permettono a ospedali, contribuenti e altre strutture sanitarie di condividere l'accesso ai loro network senza compromettere la sicurezza e l'integrità dei dati.

- Gestione delle risorse umane:

  Se i curriculum precedenti sono stati conservati in un registro distribuito, impossibile da falsificare, i professionisti dell'organizzazione vedranno semplificarsi all'improvviso l'iter del processo di selezione e valutazione dei candidati.

Capitolo 2 – Digital Identity

L'identità è un concetto unicamente umano. È quell'ineffabile "io" dell'autocoscienza, qualcosa che è compreso in tutto il mondo da ogni persona che vive in ogni cultura. Tuttavia, la società moderna ha confuso questo concetto di identità. Oggi, le nazioni e le multinazionali confondono le patenti di guida, le tessere di previdenza sociale e altre credenziali rilasciate dallo stato con l'identità; questo è problematico perché suggerisce che una persona può perdere la propria identità se uno stato revoca le sue credenziali o anche se attraversa i confini dello Stato. L'identità nel mondo digitale è ancora più complicata. Soffre dello stesso problema del controllo centralizzato, ma è allo stesso tempo molto balcanizzato: le identità sono frammentarie, differiscono da un dominio Internet a un altro. Mentre il mondo digitale diventa sempre più importante per il mondo fisico, presenta anche una nuova opportunità; offre la possibilità di ridefinire i moderni concetti di identità. Potrebbe permetterci di ricollocare l'identità sotto il nostro controllo - ancora una volta ricongiungendo l'identità con l'ineffabile "io".

2.1. Proprietà dell' identità digitale.

Il concetto di identità può essere visto da diverse prospettive ed è applicabile in diversi domini, a seconda dell'obiettivo per cui viene utilizzata l'identità digitale. In generale, l'identità personale in filosofia si riferisce alla risposta alla domanda "Chi sono io?" ,si riferisce cioè a quelle proprietà che rendono l'individuo unico e diverso dagli altri. Precisamente, l'identità si riferisce a un insieme di qualità e caratteristiche che rendono un'entità definibile, distinguibile e riconoscibile rispetto ad altre entità. Tuttavia, nel mondo digitale, "identità" è un insieme di record digitali che rappresenta un utente. Questi record vengono salvati e gestiti in un formato

standard da entità che forniscono le informazioni sull'identità o assicurazioni necessarie per completare le transazioni. Un'identità digitale accetta e integra anche nuovi record per creare una visualizzazione completa dell'utente. Di seguito c'è un elenco di cinque proprietà che dovrebbero essere applicate per contribuire ad una soluzione più dettagliata per migliore il sistema digitale di identità.

Entità

Secondo la sua definizione, un'entità è un oggetto che esiste. In un sistema digitale, alcuni tipi di entità richiedono identità digitali, incluse persone, macchine o dispositivi, organizzazioni, e agenti. Quelle entità possono essere categorizzate in modo specifico in tre tipi. Gli agenti di identità installati localmente vengono eseguiti su dispositivi con utente, come smartphone e laptop. Gli agenti di identità remota risiedono sulla rete. Hanno le loro chiavi private e pubbliche e possono essere gestiti da parti che hanno alcune credenziali dell'utente, come banche, università o altre entità considerate attendibili dall'utente. L'ultimo tipo è costituito da parti Relying, che rappresentano una parte con la quale l' utente intende interagire, in sostanza, un fornitore di servizi online; tuttavia, in un sistema peer-to-peer, le parti relying possono essere altri utenti.

Tipo di attributo

Il tipo di attributo è usato per identificare l'entità. Di solito è composto da tre attributi; chi sei, contesto e profilo.

- Chi sei.

  Questo è l'attributo che identifica in modo univoco una singola entità in un contesto del mondo reale. Può includere conoscenze o dati che sono

conosciuti solo da quell'entità,caratteristiche fisiche uniche di quell'entità o elementi che l'entità possiede.

- Contesto.

Questo può riferirsi al tipo di transazione o al modo in cui viene effettuata la transazione. Diversamente sono i vincoli sull'identità digitale che potrebbero essere implementati a seconda del contesto. Il contesto è anche usato per determinare la quantità e il tipo di informazioni sull'identità necessarie per fornire il livello appropriato di fiducia.

- Profilo.

Un profilo consiste dei dati necessari per fornire servizi agli utenti una volta che l'identità è stata verificata. I profili utente possono includere ciò che le entità possono fare: di quali gruppi sono membri, i loro servizi selezionati, ecc. Un profilo utente può cambiare nel corso di un'interazione con il fornitore di servizi.

Ciclo Di Vita

Ci sono 3 passaggi fondamentali per creare un identità digitale:

1. Registrazione: che include iscrizione e validazione;
2. Emissione di documenti e credenziali:
3. Autenticazione.

- Iscrizione

Questa fase è divisa in due parti: iscrizione e convalida. L'iscrizione comporta le fasi di registrazione: acquisizione e registrazione degli attributi di identità chiave di una persona che rivendica una certa identità. Questo può includere dati biografici (ad es. nome, data di nascita, sesso, indirizzo, email), dati biometrici (ad es. impronte digitali,

scansione dell'iride), e gli altri attributi. Una volta che una persona ha richiesto un'identità durante l'iscrizione, questa identità viene quindi convalidata controllando gli attributi presentati rispetto a quelli esistenti.

- Emissione

Prima che possa essere usato da una persona, un'identità registrata passa attraverso un'emissione o processo di credenziali. Un identità per essere considerata digitale, le credenziali o certificati (ad es. 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. Ad esempio, i cittadini possono utilizzare il proprio numero di identificazione elettronica per pagare le imposte attraverso un portale online, mentre in banca i clienti possono utilizzare carte di debito intelligenti o servizi finanziari mobili. Per accedere ai servizi, l'utente deve essere autenticato utilizzando uno o più fattori, ad esempio password, pin o impronta digitale. Durante le fasi del ciclo di vita, i fornitori di identità digitali gestiscono e organizzano l'identità del sistema, compresi i suoi impianti e personale, tenuta dei registri, conformità e controllo, e aggiornare lo stato e il contenuto delle identità digitali. Ad esempio, gli utenti potrebbero aver bisogno di aggiornare vari attributi di identità, come indirizzo, stato civile, professione, ecc. Inoltre, i provider di identità potrebbero aver bisogno di revocare un'identità, che comporta invalidare l'identità digitale per motivi di frode o di sicurezza o terminare un identità nel caso della morte dell'individuo.

Politiche

Le politiche sono utilizzate per gestire le identità. Questo è un insieme di regole, definito dal proprietario di risorse, per la gestione dell'accesso a una risorsa (risorsa, servizio o entità) e per quali scopi può essere utilizzato. 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.

Tecnologia

Per garantire l'usabilità, sicurezza e privacy, è necessario implementare le identità digitali usando metodi tecnologici avanzati. Pertanto, la tecnologia deve essere applicata almeno a tre aree: autenticazione, protocolli di sicurezza e miglioramenti della memorizzazione.

- Tecniche di Autenticazione

Le tecniche di autenticazione vanno da quella a singolo fattore a più fattori. Le tecniche più importanti sono:

1. Password/pin

L'autenticazione della password è un metodo tradizionale in cui viene fornito all'utente con un nome utente e una password. Tuttavia, molti hanno dimostrato che questa tecnica è inefficace dal momento che il nome utente e la password sono spesso facili da indovinare o rubare. Al fine di rendere il processo di autenticazione più sicuro, viene utilizzata un'altra tecnica denominata 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 avanzato utilizza l'hashing e i dati vengono scambiati con il server e memorizzati. Il PIN ha lo stesso meccanismo di una password, ma consiste solo in un termine numerico (di solito con quattro o sei cifre). Un'autenticazione basata su PIN è comunemente usato per servizi finanziari come bancomat.

2. Token

Funziona utilizzando il principio dell'autenticazione a due fattori (2FA). Invece di usare un nome utente e una password, viene aggiunto un livello per ottenere token a tempo limitato (in genere una chiave o una password crittografica) utilizzata per ulteriori transazioni durante la sessione. Generalmente, ha un display fisico per l'autenticazione l'utente inserisce semplicemente il numero visualizzato per accedere. Il dispositivo fisico per i token per lo più non richiede una connessione internet perché comunica usando servizi di telecomunicazione mobile come chiamate vocali, SMS o USSD.

3. Crittografia a chiave pubblica

Questo metodo utilizza meccanismi crittografici che, come teoria sottostante, coinvolge una coppia di chiavi asimmetriche: una chiave pubblica e una chiave privata. La crittografia a chiave pubblica utilizza coppie di chiavi per la crittografia e la decrittografia. La chiave pubblica è resa pubblica ed è distribuito ampiamente e liberamente. La chiave privata non è mai distribuita e deve essere tenuta segreta.

4. Biometria

L'autenticazione biometrica richiede uno stile di completamente differente rispetto al processo di autenticazione. L'autenticazione biometrica, o solo la biometria, è il processo di creazione che si accerta che le persone siano chi affermano di essere. Questo approccio è basato sulle caratteristiche biologiche uniche che possono essere utilizzate per l'identificazione biometrica di una persona utilizzando, ad esempio, il riconoscimento delle impronte digitali o dell'iride. La biometria richiede di sensori per prendere le caratteristiche dell’utente.

5. Smart Card

Quando viene utilizzato per l'accesso logico, la tecnologia delle smart card viene in genere in due forme: una tessera di plastica di dimensioni di una

carta di credito o un dispositivo USB, ciascuna incorporato con un chip del computer. L'uso di una smart card per archiviare i file delle password è la sua applicazione più semplice.

- Protocolli di sicurezza

Questi sono apprezzati per la loro forte verifica dell'identità e attributi di autenticazione. In particolare, sono progettati per trasferire l'autenticazione dei dati tra due entità. I protocolli di autenticazione più utilizzati per affrontare i problemi di sicurezza all'interno delle reti aperte sono Secure Sockets Layer (SSL), IP Sec, Secure Shell (SSH) e Kerberos.

- Memorizzazione dei dati

Le nuove tecnologie che contribuiscono al miglioramento della memorizzazione vengono utilizzati per la creazione di robusti sistemi di identità digitali. Ci sono due nuove tecnologie che possono offrire metodi migliorati nell'archiviazione del database. Il primo è una tecnologia ledger distribuita o blockchain combinata con crittografia e cloud , ciò consente di conservare e trasferire le informazioni da punto ad un altro in una rete immutabile. Il secondo è costituito da standard di identità federati, come SAML 2.0, che crea interoperabilità tra reti di gestione delle identità e applicazioni esterne, consentendo ai sistemi di identità federati di adattarsi un gran numero di provider di identità e parti fidate.

2.2 L’evoluzione dell’ identità digitale.

I modelli per l'identità online sono avanzati attraverso quattro grandi fasi dall'avvento di Internet: identità isolata, identità centralizzata, identità federata, identità centrata sull'utente.

Fase 1 : Identità Isolata

L'evoluzione dei modelli di identità è iniziata con il modello di identità isolato, che è ancora il modello più comune. Il suo concetto principale esprime la combinazione del servizio provider (SP) e il provider di identità (IdP), il che significa che l'SP gestisce dati di identità dell'utente e le loro credenziali. In questo caso, l'utente si autenticherà direttamente presso la SP.

Fase 2 : Identità Centralizzata

In contrasto con il modello isolato, il modello di identità centrale separa l'IdP dal SP. Questa separazione è la principale differenza perché i dati di identità sono memorizzati presso l'IdP. Quando un utente vuole accedere a un servizio online, deve prima farlo autenticarsi all'IdP e successivamente i dati di identità vengono trasferiti all'SP.

In questo modello, l'utente non ha alcun controllo sui propri dati di identità. Un esempio per questo scenario utilizza Facebook perché l'utente non ha il controllo sui propri dati memorizzati su Facebook.

Nei primi tempi di Internet, le autorità centralizzate divennero emittenti e autenticatori dell'identità digitale. Poi, a partire dal 1995, le autorità di certificazione (CA) si sono intensificate per aiutare i siti di commercio su Internet a dimostrare di essere chi dicevano di essere. Alcune di queste organizzazioni hanno fatto un piccolo passo oltre la centralizzazione e creato gerarchie. Tuttavia, la radice aveva ancora il potere principale: stavano solo creando nuove centralizzazioni meno potenti sotto di loro. Sfortunatamente, concedere il controllo dell'identità digitale alle autorità centralizzate del mondo online soffre degli stessi problemi causati dalle autorità statali del mondo fisico: gli utenti sono rinchiusi in una singola autorità che può negare la propria identità o addirittura confermare una falsa identità. La centralizzazione conferisce innata potenza alle entità centralizzate, non agli utenti. Man mano che Internet cresceva, con il potere

accumulato tra le gerarchie, veniva rivelato un ulteriore problema: le identità erano sempre più balcanizzate. Si sono moltiplicati come hanno fatto i siti Web, costringendo gli utenti a destreggiarsi tra decine di identità su dozzine di siti diversi, pur non avendo il controllo su nessuno di essi. In larga misura, l'identità su Internet oggi è ancora centralizzata, o nella migliore delle ipotesi, gerarchica. Le identità digitali sono di proprietà di CA. Tuttavia, negli ultimi due decenni c'è stata anche una crescente spinta a restituire identità alle persone, in modo che potessero effettivamente controllarle.

Fase 3: Identità Federata

La gestione delle identità federate consente agli utenti di accedere a più servizi basati su un'autenticazione singola. Concettualmente, coinvolge un gruppo di organizzazioni che impostano una relazione di fiducia che consente loro di condividere asserzioni sulle identità degli utenti, per garantire agli utenti l'accesso alle loro risorse. L'utente si registra una volta per accedere a tutti i servizi offerti da diversi partner attraverso l'impresa federata.La Federated identity Architecture (FIA) consiste essenzialmente in 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 delle identità consente l'adesione dei partner tra le aziende per fornire l'automazione del servizio a clienti e aziende. Utilizzando questo modello, possono sfruttare l'autenticazione del portale aziendale dei dipendenti per fornire accesso ai loro servizi. Inoltre, in questo modello il datore di lavoro è responsabile della gestione dei propri utenti e password.Tuttavia la Federated identity deve ancora affrontare

alcuni problemi, specialmente in termini di sicurezza e privacy. In relazione alla sicurezza, è vulnerabile a vari attacchi alle applicazioni web, come attacchi di replay, attacchi di man-in-the-middle e session hacking. Per quanto riguarda la privacy, il fornitore di servizi può ottenere più informazioni dell'utente di quanto richiesto, perché consente agli utenti di distribuire l'identità in modo dinamico su domini di sicurezza, aumentando la portabilità.

Fase 4 : Identità centrata sull' utente

In questo sistema, gli utenti sono in grado di scegliere quale delle loro identità utilizzare per ciascuna applicazione. Consente agli utenti di memorizzare identificativi e credenziali per diversi fornitori di servizi in un unico dispositivo hardware anti-manomissione, che potrebbe essere una smart card o qualche altro dispositivo personale portatile. Questo modello centrato sull'utente può essere distinto dal modello federato poiché è più probabile che si concentri su quali sono gli utenti nel contesto rispetto alle organizzazioni o alle imprese. Un ulteriore avanzamento pratico di questo tipo di sistema è l'identità basata sugli attributi. Questo approccio mira a risolvere i problemi relativi alla sicurezza e alla privacy utilizzando credenziali basate sugli attributi (ABC). La tecnologia ABC ha una visione diversa dell'identità e dell'autorizzazione; abilita gli attributi da emettere e memorizzare con l'oggetto dei dati (l'individuo). Inoltre, è necessario solo il sottoinsieme rilevante e spesso non identificativo di questi attributi da mostrare nel contesto di una particolare istanza di verifica e autorizzazione. L'individuo non può modificare i suoi valori di attributo; questo garantisce che i sistemi che utilizzano ABC per prendere decisioni di accesso. Il chiaro vantaggio è che consente all'utente di selezionare gli attributi da condividere con la parte richiedente. Quindi, migliora i problemi di privacy

perché gli utenti hanno il pieno controllo sui loro dati e sanno chi li usa e quando. 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; altrimenti non avrebbero basi per prendere la decisione.

2.3. Problemi e rischi legati alla gestione di un'identità digitale.

L'identità online presenta svariati problemi legati alla sua gestione:

- Il problema della prossimità: quando hai a che fare con persone a distanza, poiché non stiamo interagendo fisicamente con loro, i nostri metodi tradizionali per sapere con chi abbiamo a che fare sono inutili, quindi abbondano le frodi.
- Il problema di scala: i sistemi di identità online si basano su relazioni commerciali e integrazioni tecniche per le autorità di trust di base. Tutto questo è costoso e viene fatto solo per casi d'uso di alto valore.
- Il problema della flessibilità: gli attuali sistemi di identità sono rigidi, con schemi fissi e casi d'uso.
- Il problema della privacy: gli identificatori condivisi, come i cookie del browser, consentono di accumulare e correlare le informazioni personali dietro le nostre spalle. Gli hack in corso dimostrano in modo convincente che i grandi depositi centralizzati di informazioni personali non sono sicuri.
- Il problema del consenso: i sistemi di identità si basano su identificatori universali come indirizzi e-mail, numeri di telefono e persino numeri di previdenza sociale che rendono facile per le terze parti correlare il comportamento e tenere sotto controllo le persone senza il loro permesso.

Tutti questi problemi, portano a due rischi principali, il furto di identità e la violazione dei dati.

Furto di identità

Il furto d'identità, noto anche come frode d'identità, è un crimine in cui un 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, merce e servizi in nome della vittima, o per fornire al ladro false credenziali. Oltre a indebitarsi, in rari casi, un impostore potrebbe fornire una falsa identificazione alla polizia, la creazione di un casellario giudiziario o il rilascio di mandati di arresto eccezionali per la persona la cui identità è stata rubata. Il furto di identità è suddiviso in due categorie: vero nome e acquisizione dell'account. Il furto di identità di un vero nome significa che il ladro utilizza le informazioni personali per aprire nuovi account. Il ladro potrebbe aprire un nuovo conto di carta di credito, stabilire un servizio di telefonia cellulare o aprire un nuovo conto corrente per ottenere assegni in bianco. Il furto di identità dell'acquisizione di account implica che l'impostore utilizza le informazioni personali per accedere agli account esistenti della persona. In genere, il ladro cambierà l'indirizzo postale su un account ed eseguirà un conto enorme prima che la persona la cui identità è stata rubata si accorga che c'è un problema. Internet ha reso più facile per un ladro di identità utilizzare le informazioni che hanno rubato, perché le transazioni possono essere effettuate senza alcuna interazione personale.
Esistono molti esempi diversi di furto d'identità, come ad esempio:
furto di identità fiscale, laddove un ladro presenta una falsa dichiarazione dei redditi con l'Internal Revenue Service (IRS) utilizzando un numero di Social Security rubato; furto di identità medica, laddove un ladro ruba informazioni, inclusi numeri di membri dell'assicurazione sanitaria, per

ricevere servizi medici; furto d'identità minorile, in cui il numero di previdenza sociale di un bambino viene utilizzato in modo improprio per richiedere sussidi governativi, aprire conti bancari e altri servizi; furto di identità senior, in cui un anziano è il bersaglio di un ladro di identità.

Data Branches

Una violazione dei dati è un incidente confermato in cui dati sensibili, riservati o altrimenti protetti sono stati consultati o divulgati in modo non autorizzato. Le violazioni dei dati possono riguardare informazioni sulla salute personale, informazioni personali identificabili, segreti commerciali o proprietà intellettuale. Le esposizioni comuni alla violazione dei dati includono informazioni personali, come numeri di carta di credito, numeri di previdenza sociale e anamnesi sanitaria, nonché informazioni aziendali, come elenchi di clienti, processi di produzione e codice sorgente software. Se qualcuno che non è specificamente autorizzato a farlo vede tali dati, si dice che l'organizzazione incaricata di proteggere tali informazioni abbia subito una violazione dei dati. Se una violazione dei dati provoca un furto di identità o una violazione dei mandati di conformità del governo o dell'industria, l'organizzazione che ha commesso l'infrazione può essere soggetta a multe o altre cause civili. Un esempio familiare di violazione dei dati è un hacker che si intromette in un sito Web aziendale e ruba dati sensibili da un database.

Capitolo 3 – Blockchain Identity Management

3.1. Identità Autosovrana(Self-Sovereign Identity)

L'identità di auto-sovranità parte dall'idea che tutti noi siamo i creatori della nostra identità, online e offline. Poiché non fanno affidamento su un'autorità centralizzata, i sistemi di identità autosufficienti sono decentralizzati, rispecchiando il modo in cui l'identità funziona nella vita reale. Offline, le nostre interazioni supportano in modo flessibile l'uso di attributi e credenziali di numerose terze parti, poiché la persona che estrapola le proprie credenziali da un portafoglio le presenta a qualcun altro per verificarle. Le informazioni importanti sono confezionate in modo da rendere facile l'autenticazione e difficile la falsificazione. Questi dati verificabili sono il cuore dell'identità autosufficiente. L'identità autosovrana non significa che hai il completo controllo sull'identità, ma definisce i confini entro i quali prendi le decisioni e al di fuori del quale comunichi con gli altri alla pari. I sistemi di identità autosufficienti risolvono tutti i problemi legati alla gestione dell'identità usando il decentramento e la crittografia. La sovranità è, per definizione, un potere o un'autorità suprema, che governa se stessa senza eventuali influenze esterne. La sovranità per la gestione delle identità significa che l'utente possiede tutti i suoi dati e li controlla. Il concetto di identità di Sé Sovrano può essere visto come il prossimo stadio di evoluzione nella gestione dell'identità. L'identità decentralizzata è stata difficile da ottenere perché uno dei requisiti fondamentali dell'identità funzionale è la ricerca dell'identità, ossia dato un identificatore, ho bisogno di cercarlo. In passato, questo ha sempre portato a directory centralizzate, che hanno portato a sistemi di identità centralizzati. Ma la tecnologia blockchain ha cambiato tutto questo poiché fornisce una buona base per creare un sistema SSI.

I requisiti di tale sistema sono i seguenti:

•Controllo da parte dell’utente sui dati.

Ogni utente deve avere il pieno controllo sui propri dati di identità. Questo include non solo dove i dati di identità vengono memorizzati, ma anche chi ha accesso a questi dati. L'utente dovrebbe essere in grado di aggiungere o importare attributi di identità e di eliminarli o revocarli a suo piacimento. Inoltre, tutti gli accessi ai dati di identità di un utente devono essere registrati per una successiva verifica.

•Sicurezza e privacy dei dati dell’utente

Tutti i dati di identità devono essere archiviati ed elaborati in maniera altamente sicura. Inoltre, la privacy dell'utente deve essere preservata. Ad esempio, eliminare il collegamento tra il portafoglio utente e i suoi dati di identità aumentano la privacy dell'utente.

•Completa portabilità dei dati

Questo requisito descrive che l'utente dovrebbe essere in grado di utilizzare i suoi dati di identità ovunque loro vogliono. Ad esempio, un sistema SSI può essere utilizzato come provider di identità quando l'utente tenta di accedere a un servizio online.

•Mancata fiducia in un’autorità centrale

La sottostante tecnologia blockchain risolve il trust richiesto relativo a una centrale autorità.

•Integrità dei dati

L'integrità dei dati di identità può essere garantita utilizzando la tecnologia blockchain.

•Trasparenza dei dati

La tecnologia blockchain fornisce la trasparenza dei dati di tutti.

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

3.2. Dieci principi chiave dell' identità autosovrana

La Blockchain ha il potenziale per essere adottato come un sistema di identità digitale. Invece di memorizzare tutti i dati e le transazioni in modo sicuro e aperto, creare un'identità su blockchain rende più facile per le persone gestire la propria identità e garantire il controllo di chi ha le loro informazioni personali e in che modo accedono ad esse. Questi principi tentano di assicurare il controllo all'utente che è al centro dell'identità autosufficiente. Tuttavia, riconoscono anche che l'identità può essere un'arma a doppio taglio - utilizzabile sia a scopo benefico che a fini malefici. Pertanto, un sistema di identità deve bilanciare la trasparenza, l'equità e il supporto dei beni comuni con protezione per l'individuo.
Di seguito sono esposti i 10 principi chiave per un sistema di identità autosufficiente:

- Esistenza:

  Gli utenti devono avere un'esistenza indipendente. Ogni identità di auto-sovranità si basa in ultima analisi sull'ineffabile "io" che è al centro dell'identità. Non può mai esistere interamente in forma digitale. Questo deve essere il nucleo di sé che viene sostenuto e supportato. Un'identità autosufficiente rende semplicemente pubblici e accessibili alcuni aspetti limitati dell '"io" che già esiste.
- Controllo:

  Gli utenti devono controllare le loro identità. Sottoposto a algoritmi ben compresi e sicuri che garantiscono la validità continua di un'identità e delle sue affermazioni, l'utente è l'autorità suprema della sua identità. Ciò non significa che un utente controlla tutte le affermazioni sulla propria identità: altri utenti possono fare affermazioni su un altro utente, ma questo non dovrebbe essere centrale per l'identità stessa.

- Accesso:

  Gli utenti devono avere accesso ai propri dati. Un utente deve essere sempre in grado di recuperare facilmente tutte le richieste e altri dati all'interno della sua identità. Non ci devono essere dati nascosti. Ciò non significa che un utente possa necessariamente modificare tutte le rivendicazioni associate alla sua identità, ma significa che deve esserne a conoscenza. Inoltre, non significa che gli utenti abbiano uguale accesso ai dati degli altri, ma solo ai propri.

- Trasparenza:

  I sistemi e gli algoritmi 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 e aggiornati. Gli algoritmi devono essere liberi, open source, ben noti e il più indipendenti possibile da ogni particolare architettura; chiunque dovrebbe essere in grado di esaminare come funzionano.

- Persistenza:

  I sistemi e gli algoritmi 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 e aggiornati. Gli algoritmi devono essere liberi, open source, ben noti e il più indipendenti possibile da ogni particolare architettura; chiunque dovrebbe essere in grado di esaminare come funzionano.

- Portabilità:

  Informazioni e servizi sull'identità devono essere trasportabili. Le identità non devono essere detenute da una singola entità di terze parti, anche se si tratta di un'entità fidata che si prevede lavori nel migliore interesse dell'utente. Il problema è che le entità possono scomparire - e su Internet, la maggior parte alla fine lo fa. I regimi possono cambiare, gli utenti possono trasferirsi in diverse

giurisdizioni. Le identità trasportabili garantiscono che l'utente mantenga il controllo della propria identità indipendentemente da questi fattori.

- Interoperabilità:

  Le identità dovrebbero essere il più ampiamente utilizzabili possibile. Le identità hanno poco valore se funzionano solo in regioni limitate. L'obiettivo di un sistema di identità digitale del 21 ° secolo è rendere le informazioni sull'identità ampiamente disponibili, superando i confini internazionali per creare identità globali, senza perdere il controllo dell'utente. Grazie alla persistenza e all'autonomia queste identità ampiamente disponibili possono quindi essere continuamente disponibili.

- Consenso:

  Gli utenti devono accettare l'uso della loro identità. Ogni sistema di identità è costruito attorno alla condivisione di tale identità e delle sue affermazioni e un sistema interoperabile aumenta la quantità di condivisione che si verifica. Tuttavia, la condivisione dei dati deve avvenire solo con il consenso dell'utente. Sebbene altri utenti come un datore di lavoro, un ufficio di credito o un amico possano presentare reclami, l'utente deve comunque offrire il proprio consenso affinché diventi valido. Si noti che questo consenso potrebbe non essere interattivo, ma deve essere ancora deliberato e ben compreso.

- Minimizzazione:

  La divulgazione delle richieste deve essere ridotta al minimo. Quando i dati vengono divulgati, tale divulgazione dovrebbe comportare la quantità minima di dati necessari per svolgere l'attività in questione. Ad esempio, se è richiesta solo un'età minima, allora l'età esatta non dovrebbe essere rivelata, e se viene richiesta solo

un'età, allora la data di nascita non dovrebbe essere rivelata. Questo principio può essere supportato con rivelazioni selettive, prove di intervallo e altre tecniche di conoscenza zero, ma la non correlabilità è ancora un compito molto difficile (forse impossibile); il meglio che possiamo fare è utilizzare la minimizzazione per supportare la privacy nel miglior modo possibile.

- Protezione:

  I diritti degli utenti devono essere protetti. Quando c'è un conflitto tra le esigenze della rete di identità e i diritti dei singoli utenti, allora la rete dovrebbe errare per preservare le libertà e i diritti degli individui rispetto alle esigenze della rete. Per garantire ciò, l'autenticazione dell'identità deve avvenire tramite algoritmi indipendenti resistenti alla censura, resistenti alla forza e gestiti in modo decentralizzato.

3.3. Architettura SSI

La blockchain offre la possibilità di realizzare un sistema senza parti semi-attendibili come autorità di certificazione centrale (CA) o autorità di registrazione (RA). Tuttavia, il grado di fiducia richiesto dipende dalla specifica implementazione della blockchain. Solo blockchain pubbliche o prive di licenza forniscono un ambiente affidabile. Se una blockchain è privata o autorizzata, solo le parti autorizzate hanno accesso al libro mastro, che richiede almeno un qualche tipo di relazione di fiducia con queste entità. Anche se le parti autorizzate sono indipendenti l'una dall'altra, la fiducia nelle parti scelte o nel processo di selezione di diventare una parte fidata è ancora necessaria. Le autorità indipendenti dovrebbero ospitare una copia del libro mastro che aiuti a ridurre la fiducia richiesta. Il ledger della blockchain è la parte centrale di un tale sistema SSI. Tuttavia, ci sono parti aggiuntive necessarie per supportare pienamente tutte le funzionalità. Pertanto, il libro mastro distribuito deve essere esteso da almeno due parti aggiuntive, vale a dire la memorizzazione dei dati sul libro mastro e la

parte di importazione dei dati. Memorizzare dati sensibili nella blockchain potrebbe non essere una buona idea anche se questi dati sono criptati. Il problema che si verifica memorizzando i dati nella blockchain è che questi dati non possono più essere modificati o eliminati in seguito. Questa potrebbe essere una caratteristica importante in alcuni casi, ma non quando si tratta di dati sensibili.

Nel sistema SSI, i dati relativi alle persone vengono memorizzati al di fuori del registro e solo un identificatore univoco è memorizzato nella blockchain. Questo identificatore speciale è collegato crittograficamente all'archiviazione dei dati fuori dal libro mastro. Come memorizzazione off-ledger è possibile utilizzare diversi servizi di archiviazione come gli archivi cloud. La seconda parte è l'estensione di importazione dei dati. Un sistema SSI si occupa dei dati di identità. Questi dati possono avere diversi livelli di qualità. Ad esempio, un'autorità nazionale può emettere dati di identità qualificati di una persona. Al contrario, una persona inserisce i dati relativi a se stesso da solo. L'autenticità di questi dati auto inseriti non può essere garantita. Pertanto, può essere utile per un utente che il sistema SSI supporti l'importazione di dati qualificati. L'importazione dei dati qualificati non è semplice perché deve essere eseguita una trasformazione speciale dei dati durante il processo di importazione. Questo processo di trasformazione converte il formato dei dati dal formato ricevuto al formato supportato dal sistema SSI. Il formato dei dati ricevuti può variare a seconda della fonte. Questo è un passo necessario per fornire una rivelazione selettiva e l'attestazione degli attributi in un secondo momento.

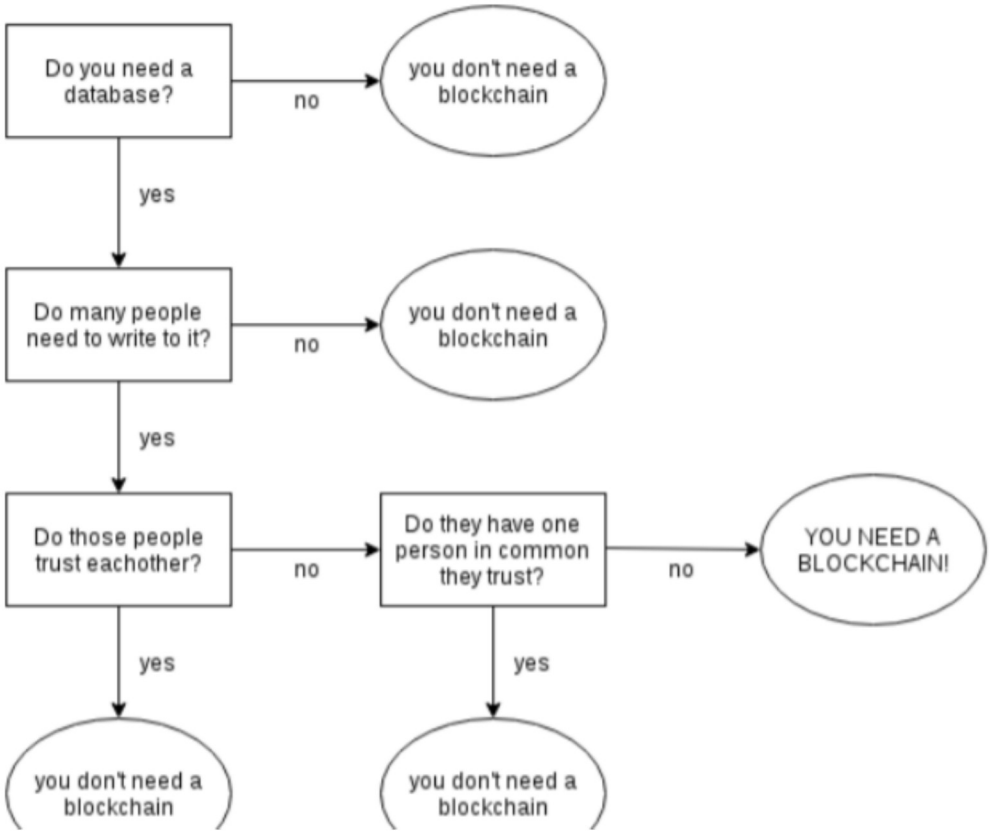

Figura 5: Why use Blockchain for SSI

3.4. Identificatori decentralizzati e reclami verificabili

Fino ad ora, l'unico modo per ancorare gli identificativi per un utente su Internet era farlo all'interno di uno spazio dei nomi gerarchico. Ad esempio, in uno spazio dei nomi privato, sei soggetto ai termini di servizio di un'azienda.Tuttavia in questo modo si può interrompere l' identità digitale dell' utente in qualsiasi momento e per qualsiasi motivo e non si può effettuare praticamente alcun ricorso legale.Questo è il caso degli indirizzi e-mail di Google, degli handle di Twitter, degli account di Facebook, dei profili di LinkedIn, degli account Instagram e praticamente di qualsiasi sito in cui si crea un nome utente e una password che poi vivono sotto lo spazio e il controllo di una terza parte. Quindi ci sono spazi dei nomi globalmente gerarchici.

Oggi, tuttavia, esiste la possibilità di un' identità autosufficiente radicata negli identificatori non sotto il controllo di un'altra entità ma realmente

controllata dall'individuo,questi identificatori vengono chiamati DID(Identificatore Decentralizzato).L'emergere della tecnologia blockchain, offre l'opportunità di implementare una gestione dell'identità completamente decentralizzata. In questo ecosistema, tutti i partecipanti con identità (chiamati proprietari di identità) condividono un Common Trust Anchor sotto forma di un libro mastro globalmente distribuito (o una rete P2P decentralizzata che fornisce funzionalità simili). Ogni proprietario di identità può essere identificato su un libro mastro con una coppia chiave-valore. La chiave dell'indice è un Identificatore decentrato e il valore è l'oggetto descrittore DID associato. Insieme formano un record DID. Ogni record DID è protetto crittograficamente da una chiave privata sotto il controllo di un proprietario dell'identità (nel caso di un'identità gestita dal proprietario) o di un tutore (nel caso di un'identità gestita da un tutore). Una chiave pubblica corrispondente viene pubblicata nell'oggetto descrittore DID utilizzando una descrizione della chiave. Un oggetto descrittore DID può anche contenere un insieme di endpoint di servizio per l'interazione con il proprietario dell'identità. Seguendo i dettami di Privacy, ciascun proprietario dell'identità può disporre di tutti i record DID necessari per rispettare la separazione desiderata tra identità, persone e contesti del proprietario dell'identità. Per utilizzare un identificatore decentralizzato con un particolare registro o rete distribuita è necessario definire una specifica del metodo DID.Questo design elimina la dipendenza dai registri centralizzati per gli identificatori e dalle autorità di certificazione centralizzate per la gestione delle chiavi. Con i record DID su un libro mastro distribuito, ciascun proprietario di identità può fungere da proprio ancoraggio di affidabilità: un'architettura denominata DPKI (PKI decentralizzato).Ogni Identificatore Decentrato utilizza un metodo di identificazione decentralizzato specifico, definito in una specifica del metodo DID separata, per definire in che modo l'Identificatore

Decentralizzato è registrato, risolto, aggiornato e revocato su una specifica Rete o Tecnologia Distributed Ledger. Esistono diverse varietà di DID e diversi metodi, ma tutti seguono lo stesso schema di base. Quindi, ora che abbiamo un modo per creare identificatori univoci a livello globale, dove vengono memorizzati? E come le persone accedono ad essi?Questi identificatori vengono memorizzati sulla blockchain,che è appunto la tecnologia che ha reso possibile la creazione di un sistema di identità autosufficiente. Pertanto, quando si crea un DID e lo si memorizza in un libro mastro condiviso, non è possibile, a tutti gli effetti, essere cancellato. Può essere aggiornato solo dall'utente . Utilizzando l'infrastruttura DID, individui e istituzioni possono creare identificatori unici e monouso a livello globale che, attraverso PKI, consentono canali di comunicazione sicuri tra l'individuo e l'istituzione.Quindi se, ad esempio, il database della tua banca è compromesso e la tua chiave privata è esposta, allora solo quell'account è interessato. La chiave privata è inutile da qualsiasi altra parte, diversamente da un numero di previdenza sociale oggi. L'istituto può anche stabilire nuove chiavi pubbliche e private e una nuova connessione sicura con voi.Questa tecnologia non blocca le violazioni dei dati, ma riduce l'impatto perché ogni relazione ha i propri identificatori univoci anziché un identificatore utilizzato in più contesti. Ora abbiamo l'infrastruttura sottostante che l'utente non tocca. Successivamente, abbiamo bisogno di servizi. Quindi, con tutti questi identificatori distribuiti e decentralizzati, come facciamo a conoscere delle informazioni chiave che sono rilevanti per determinate le transizioni? Le entità che hanno una conoscenza autorevole sull'utente possono emettere un reclamo verificabile e registrare che lo hanno fatto in un libro mastro distribuito.Altre affermazioni verificate potrebbero includere una licenza per guidare, una credenziale educativa come una laurea o qualcosa di super-specifico come il superamento di una particolare classe, o la prova che sei un dipendente di

una particolare azienda. Gli standard su come eseguire questa operazione si stanno spostando nel W3C nel gruppo di lavoro sui reclami verificabili e nel gruppo di comunità delle credenziali. In passato, qualsiasi soluzione al problema dei reclami verificabili comportava che il verificatore verificasse presso l'emittente se effettivamente emetteva tale richiesta. Questo è noto come il problema della "phone home".Per dirla in termini concreti: vuoi prendere un drink al bar. Al giorno di oggi, il barista guarda la patente di guida e in genere crede alla data di nascita (a meno che non sia un evidente falso).Ma se fosse una licenza digitale, come potrebbe "crederci"? Dovrebbe domandare all'emittente per verificare se l'asserzione digitale che hai superato i 18 anni sia vera. Questo non è qualcosa che vuoi che succeda, perché allora l'emittente del reclamo conoscerebbe tutti i luoghi in cui hai usato il tuo reclamo verificato in digitale. In altre parole saprebbe sempre quali luoghi frequenti. Supponiamo invece che la prova dell'emissione dei crediti da parte dell'emittente sia archiviata in un libro mastro pubblico distribuito che sia individuabile dal verificatore. Pertanto, il verificatore può stabilire la veridicità del credito e che proviene dall'emittente, senza interagire effettivamente con il sudetto emittente. Come si dimostra che un reclamo è vero e come evitare di condividere tutte le informazioni in esso? Tornando all'esempio della birra, come provate di avere più di 18 anni e quindi avere la possibilità di acquistare alcolici ma senza mostrare il documento completo? Quando una rivendicazione di prova di conoscenza zero (ZKP) viene rilasciata al singolo utente , egli può presentare nuovamente il reclamo al verificatore, che può crederlo, a causa di come è stato codificato crittograficamente tale reclamo. L'utente può utilizzare tali reclami verificati per condividere alcuni aspetti, ma non tutti, con un emittente. Ciò preserva la privacy dell'individuo perché non tutte le informazioni sono condivise con il verificatore, che può ancora fidarsi della veridicità della richiesta.Non tutte le prove durano per sempre, però. Ci

sono casi speciali ed abbiamo bisogno del potere di revocare le richieste. Le prove di conoscenza zero funzionano molto bene per i tipi di reclamo che non possono essere revocati come la data di nascita (lo stato non può affermare che una persona non è nata). Tuttavia, non funzionano bene per i reclami che prevedono la revoca. Ad esempio, una persona è dipendente di una determinata azienda, ma potrebbe non esserlo più l'anno successivo. Questo in passato era impossibile da affermare utilizzando lo ZKP, perché sapere se qualcosa è vero ora, non se fosse vero in passato, è una parte fondamentale della richiesta. La prova CL è un pezzetto di matematica ancora più elaborato che completa lo ZKP. CL offre agli emittenti il potere di revocare le attestazioni e ai verificatori di vedere tali revoche anche se sono ZKP. Quindi ora puoi usare ZKP per una gamma più ampia di attestazioni.


```
{
  "@context": "https://w3id.org/did/v1"
  "id": "did:btcr:xkrn-xzcr-qqlv-j6sl",
  "service": [
    {
      "type": "agent",
      "serviceEndpoint": "https://azure.microsoft.com/dif/hub/did:btcr:xkrn-xzcr-qqlv-j6sl"
    },
    {
      "type": "xdi",
      "serviceEndpoint": "https://xdi03-at.danubeclouds.com/cl/+!:did:btcr:xkrn-xzcr-qqlv-j6sl"
    }
  ],
  "authentication": {
    "type": "EdDsaSASignatureAuthentication2018",
    "publicKey": [
      "did:btcr:xkrn-xzcr-qqlv-j6sl#key-1"
    ]
  },
  "publicKey": [
    {
      "id": "did:btcr:xkrn-xzcr-qqlv-j6sl",
      "type": "Secp256k1VerificationKey2018",
      "publicKeyHex": "024a63c4362772b0fafc51ac02470dae3f8da8a05d90bae9e1ef3f5243180120dd"
    }
  ]
}
```


Figura 6: DID code example

Example:

```
{
  "@context": "https://w3id.org/security/v1",
  "id": "http://example.gov/credentials/3732",
  "type": ["Credential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov",
  "issued": "2017-01-01",
  "claim": {
    "id": "did:sov:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "signature": {
    "type": "LinkedDataSignature2015",
    "created": "2016-06-18T21:19:10Z",
    "creator": "https://example.com/jdoe/keys/1",
    "domain": "json-ld.org",
    "nonce": "598c63d6",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez8RwDg/+
    MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
    PRdW+gGsutPTLzvueMWmFhwYmfIFpbBu95t501+rSLHIEuujM/+PXr9Cky6Ed
    +W3JT24="
  }
}
```

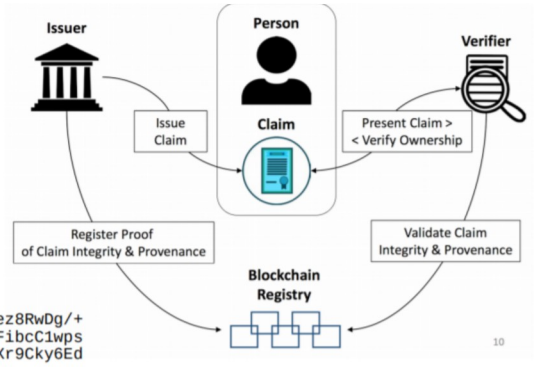

Figura 7: Verificable Claims code example

3.5. Come funziona la Self Sovereign Identity per l'utente.

Per creare un sistema basato sulla Self Sovereign Identity, utilizziamo un'app su uno smartphone o un computer, una sorta di "portafoglio di identità" in cui i dati di identità vengono archiviati sul disco rigido del dispositivo utente, ma non conservati in un repository centrale. Il portafoglio di identità inizialmente sarebbe vuoto, solo con un numero di identificazione generato automaticamente dalla chiave pubblica e una chiave privata corrispondente (come una password, utilizzata per creare firme digitali). Questa coppia di chiavi si differenzia da un nome utente e una password poiché viene creata dall'utente facendo alcuni calcoli matematici piuttosto che richiedere una combinazione nome utente e password di terze parti. In questa fase, nessun altra persona conosce questo numero di identificazione. Nessun autorità centrale lo ha emesso, poiché l'utente stesso lo ha creato, quindi è autosufficiente. Le leggi dei grandi numeri e della casualità assicurano che nessun altro generi lo stesso numero di identificazione dell'utente. Quindi si utilizza questo numero di identificazione, insieme alle dichiarazioni di identità per ottenere attestazioni dalle autorità competenti. È quindi possibile utilizzare queste affermazioni attestate come informazioni di identità.

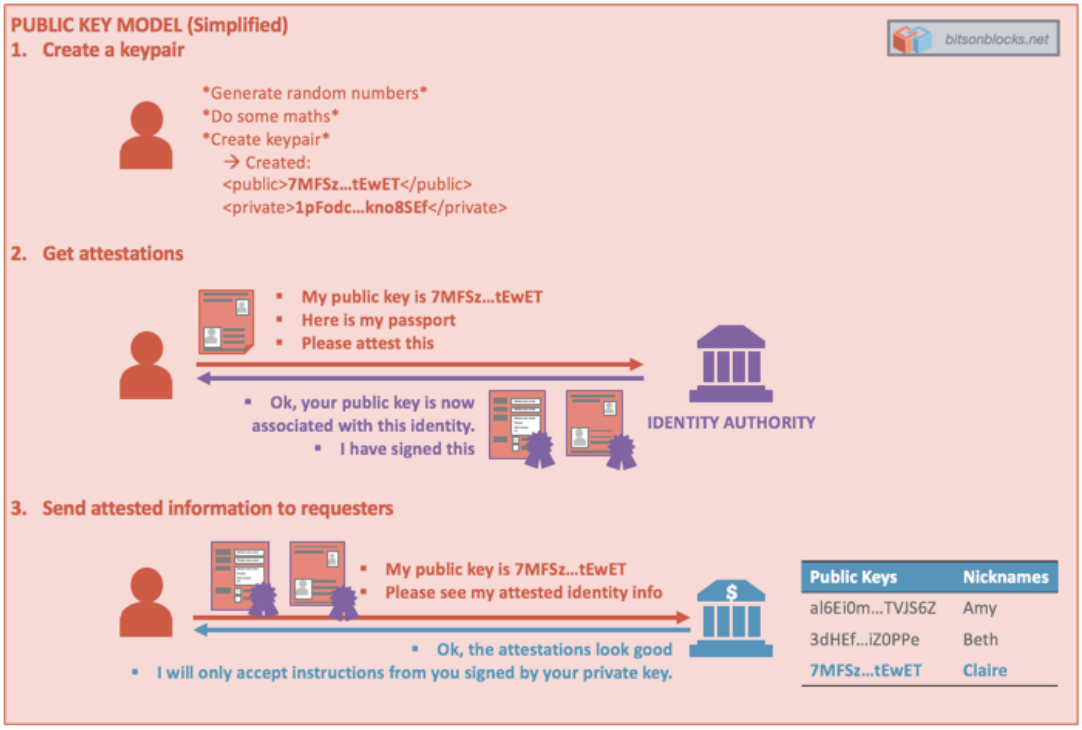

Figura 8: Public Key Model

Le prove vengono archiviate salvando scansioni o foto di documenti di prova. Gli attestati vengono memorizzati anche in questo portafoglio. Queste sono informazioni leggibili a macchina, firmate digitalmente, valide entro determinate finestre temporali. L'autorità competente deve firmare questi documenti con le firme digitali - ad esempio, agenzie di passaporto, ospedali, autorità competenti per la patente di guida , polizia ecc. Il proprietario dell'identità è in grado di scegliere quale informazione passare a qualsiasi 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 piu di quanto è necessario ed il destinatario non ha bisogno di memorizzare dati sensibili inutilmente, ad esempio l'utente se deve

dimostrare di avere piu di 18 anni, mostrerà un flag che attesta la sua età, non la data di nascita.

I dati vengono archiviati sul dispositivo dell'utente (cosi come i documenti cartacei vengono conservati all'interno del portafoglio), e poi quando richiesto, l'utente approva ad una terza parte di raccogliere dei dati specifici, toccando una notifica sul proprio dispositivo. Abbiamo già qualcosa di simile a questo, ad esempio quando utilizziamo un applicazione "collegando" il nostro account a Facebook o LinkedIn per reperire i nostri dati, tuttavia con l'identità autosovrana, invece di andare sui server di Facebook per raccogliere i dati personali dell' utente , questi vengono presi dal dispositivo utente ed in questo modo l'utente stesso ha un controllo granulare su quali dati sono condivisi.

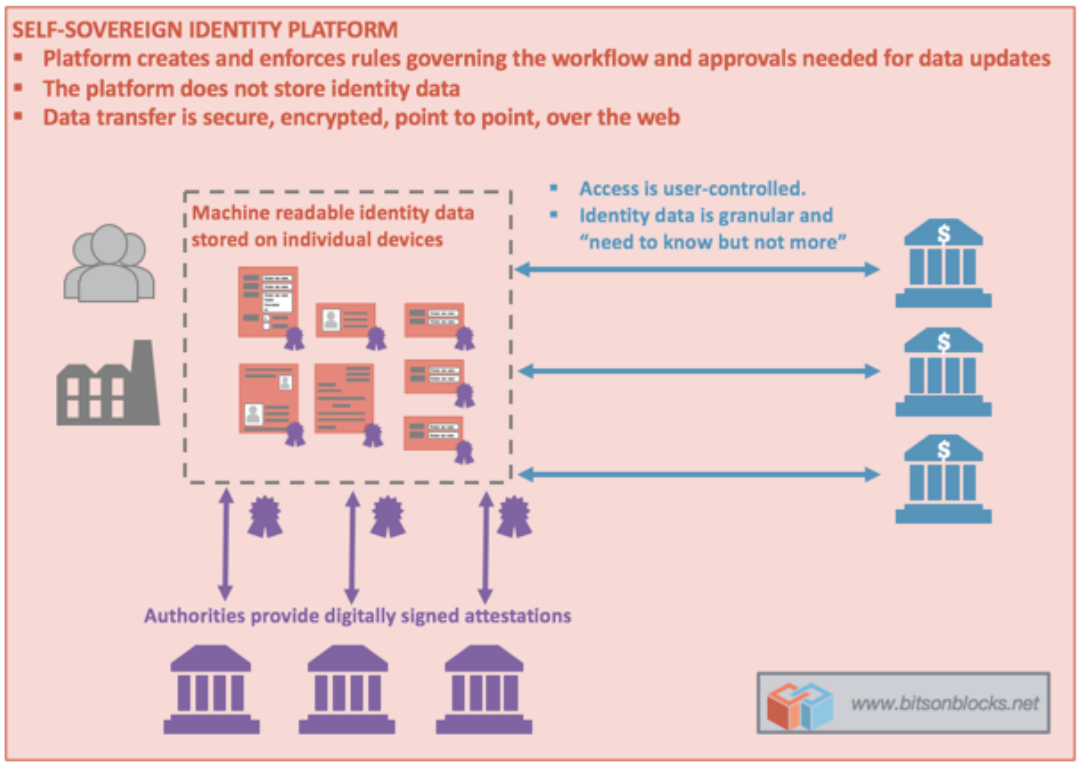

Figura 9: Struttura del SSI

3.6. Utilizzi futuri dell' identità autosovrana.

Ecco alcuni campi di utilizzo della Self-Sovereign Identity.

- Login su siti web:

  In futuro, potremmo non dover utilizzare servizi di autorizzazione centralizzati per accedere a Internet come Twitter, Google o Facebook e utilizzeremo invece la nostra Identità autosovrana per convalidare la nostra identità senza dover fare affidamento su terze parti, ad esempio utilizzando un dispositivo mobile. Questo ci consentirà di utilizzare la nostra "vera identità" o uno pseudonimo, a seconda del contesto.

- Banking:

  Le banche sono sottoposte ad un controllo sempre maggiore da parte delle autorità di regolamentazione nell'ambito dei processi KYC (Know-your-Customer) e AML (Antiriciclaggio), pertanto devono soddisfare urgentemente i crescenti costi. A causa di questa pressione, le istituzioni finanziarie di tutto il mondo stanno esplorando soluzioni per aiutare i loro clienti a trasportare le loro identità da una banca all'altra. Ciò consentirà a qualsiasi banca di beneficiare del precedente lavoro di KYC e AML effettuato da una banca precedente nella stessa giurisdizione riconosciuta.

- Dati Medici:

  Simile al web, le nostre informazioni sulla salute sono anche distribuite in vari database. La Self Sovereign Identity aspira a renderci i proprietari di tutte le nostre informazioni sulla salute per poter scegliere a chi dare un ulteriore accesso e permetterci di avere accesso alle nostre informazioni ogni volta che ne abbiamo bisogno. In futuro, questo dovrebbe consentire al medico o all'ospedale l'accesso ai nostri dati ogni volta che lo desideriamo. Questo metodo potrebbe anche essere usato per aiutare a sviluppare nuovi farmaci senza mettere a rischio la nostra privacy. Un dispositivo tecnologico potrebbe misurare il nostro polso e la pressione sanguigna in tempo

reale e noi potremmo decidere di donare o vendere queste informazioni a fini scientifici o in cambio di prodotti e servizi. Questa è solo una selezione di un numero infinito di potenziali casi d'uso, infatti, come già è stato detto nel capitolo precedente,la blockchain è una tecnologia che può essere applicata a tantissimi ambiti e quindi molteplici sono i suoi utilizzi in termini di servizi offerti.

Capitolo 4 – Sho Card

4.1. Che cos’è Sho Card?

Alcune aziende hanno fatto da pioniere nello sviluppo delle applicazioni basate sulla blockchain per la gestione delle identità e dell’autenticazione.
In questo studio andiamo ad analizzare l’ applicazione ShoCard in maggior dettaglio. ShoCard è una piattaforma di autenticazione e identità digitale costruita su un livello di dati blockchain pubblico, che utilizza la crittografia a chiave pubblica / privata e l'hashing dei dati per archiviare e scambiare in modo sicuro i dati di identità, tra cui dati biometrici come impronte digitali, viso, iride e voce. L'approccio all'identità di ShoCard è diverso dalle soluzioni esistenti in quanto l'utente possiede e trasporta i propri dati all'interno della sua app mobile ed è l'unica persona che decide con chi condividerla e quali pezzi di identificazione condividere. La blockchain viene quindi utilizzata per convalidare tali informazioni e confermare altre terze parti che hanno definitivamente certificato l'identità dell'utente. Non esiste una sede centrale privata che raccolga informazioni private dell'utente e parti di identificazione di un utente non devono essere diffuse in altri servizi al fine di autenticare o provare la proprietà di un account. L'app mobile è facile e intuitiva da utilizzare come patente di guida, ma abbastanza sicura per una banca.
ShoCard consente agli utenti e alle imprese di stabilire le proprie identità tra loro in modo sicuro e verificato, in modo che qualsiasi transazione, sia che si tratti di accedere, condividere informazioni personali o completare

una transazione finanziaria, può essere eseguita rapidamente, in modo trasparente e con tranquillità.

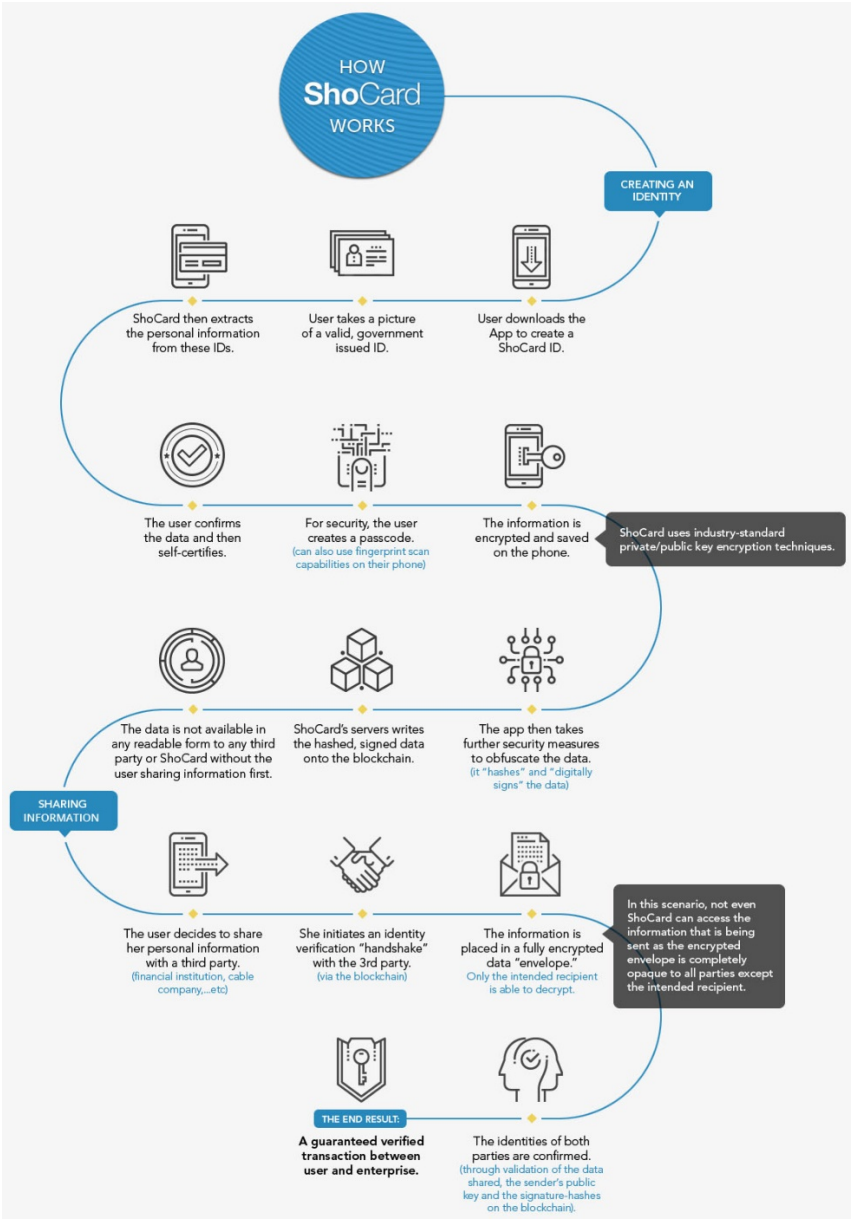

Figura 10: ShoCard Model

Il processo di certificazione può essere eseguito come parte del processo "Know Your Customer" di una terza parte.

Figura 11: Verifica credenziali utente

- Le credenziali dell'ID dell'utente vengono verificate per verificarne l'autenticità.
- All'utente possono essere fatte ulteriori domande per verificare che siano, in realtà, chi dicono di essere.
- Come passaggio di sicurezza finale, la terza parte può rivedere le informazioni nell'app.

Una volta che una terza parte autorevole (come un istituto finanziario, un governo o altra entità fidata) certifica l'ID dell'utente, tutte le altre parti future possono fare riferimento a questa certificazione ed essere certi che le informazioni fornite dall'utente tramite l'App sono precise e appartengono a loro.

4.2. Scenari e casi d'uso di ShoCard

Login

Il login ShoCard offre la possibilità per un utente di accedere a un sito Web (abilitato con la piattaforma ShoCard), senza la necessità di ricordare le password. La prima volta che l'utente visita un sito, sarà necessario collegare il proprio ID ShoCard al sito Web e registrarsi. Una volta completata la registrazione, sarebbero in grado di interagire normalmente con il sito web. Qualsiasi successiva visita al sito Web può essere completata mediante la scansione del codice QR per l'accesso o

immettendo il nome utente senza password e tentando un accesso. Ciò consentirebbe loro di autorizzare il login tramite la loro app ShoCard.
Inizio: L'utente inserisce Username o scansiona il codice QR.

- L'utente riceve quindi un avviso per l'autenticazione tramite Touch ID.
- L'utente verifica il Login.

L'autenticazione sicura è completata.

Identify Verification

La verifica dell'identità può essere un primo passo nel processo di conoscenza del cliente per gli istituti finanziari, le compagnie aeree o i fornitori di servizi sanitari. Questi controlli sono più sicuri e più robusti rispetto ai metodi offline standard, poiché i documenti fisici possono essere falsificati o obsoleti, ma non sono stati revocati fisicamente. Con ShoCard, il vero stato dei dati può essere verificato e persino confrontato con la biometria dell'individuo per garantire che la persona che presenta i dati sia il vero individuo che li possiede.

Inizio: Con ShoCard, la verifica dell'identità è un processo semplice e diretto. A seconda delle informazioni da verificare, l'individuo seleziona i campi appropriati nell'app ShoCard (un'immagine, nome, indirizzo, età o qualsiasi altra combinazione di informazioni personali identificabili).

- Altre carte possono essere aggiunte all'app ShoCard, come carte di sicurezza sociale, tessere sanitarie, carte verdi, carte di lavoro.
- Le immagini effettive delle carte, così come le informazioni selezionate su ciascuna carta, possono essere condivise con l'Agente che sta eseguendo il controllo.
- Per ogni campo o scheda in corso di verifica, ogni parte di dati viene sottoposta a hash e confrontata con l'hash firmato delle stesse

informazioni presenti sulla Blockchain, nonché le eventuali certificazioni correlate condivise che autenticano i dati.

Fine: Tutte le informazioni che superano il processo di certificazione verranno visualizzate come certificate e tutte le informazioni non certificate saranno evidenziate come non certificate sul dispositivo dell'agente.

Automated Registration

La registrazione online viene spesso studiata a causa dell'alto livello di drop-off che si verifica in un processo di registrazione. La registrazione del sito Web può essere notevolmente supportata utilizzando il sistema ShoCard, con il trasferimento automatico pre-compilato e il trasferimento controllato delle informazioni direttamente al sito Web in registrazione. La registrazione con un clic potrebbe essere uno dei modi più efficaci per migliorare l'esperienza dell'utente e consentire agli utenti di partecipare immediatamente come membri registrati a questi siti Web.

Inizio: Il processo di registrazione inizierà dalla schermata di accesso per il sito web. L'individuo dovrebbe eseguire la scansione di un codice QR visualizzato su tale schermata o fare clic sul pulsante "Registrati ora". La seguente schermata di installazione avrebbe un altro codice QR, che potrebbe essere scansionato.

- L'utente riceverà una richiesta sul proprio dispositivo mobile per confermare che viene richiesto un set specifico di informazioni per completare la richiesta di accesso.

Fine: Se la persona conferma, il modulo viene compilato automaticamente e l'utente deve solo premere "Invia" per diventare un utente registrato.

Questo processo funziona anche per deroghe e iscrizioni in luoghi come un club sportivo o una palestra di arrampicata. Viene scansionato un codice

QR sul dispositivo utilizzato per raccogliere i rinvii, al dispositivo mobile dell'utente viene richiesto di fornire una firma e altre informazioni pertinenti e, se l'utente accetta, il processo è completo.

Proof of age

La piattaforma ShoCard consente agli utenti di condividere solo le informazioni pertinenti e di tenere tutte le altre informazioni di identificazione personale (PII) nascoste e sicure con l'individuo.
Inizio: Nell'app ShoCard, l'individuo seleziona di voler condividere il fatto che ha superato 18, 21 o 55 anni (per gli anziani) e seleziona "Condividi".

- Un codice QR viene generato sul telefono dell'utente, che viene quindi scansionato dal dispositivo dell'agente.

Fine: L'agente riceve quindi una verifica (assegno verde) o una negazione della verifica (X rossa) che l'individuo sottoposto a verifica ha superato l'età appropriata.

Conclusioni

È tempo di evolvere i paradigmi di gestione dei dati da quelli basati su un'architettura web centralizzata a quelli funzionanti dal web decentralizzato. Solo in questo modo è possibile garantire la sovranità individuale in un mondo in cui le autorità centralizzate esercitano un controllo irreversibile sulle infrastrutture digitali e le violazioni della sicurezza diventeranno più comuni. Le blockchain stanno diventando le architetture decentralizzate più rapidamente adottate dalle quali possono emergere pratiche di gestione dei dati sicure e autonome. I destinatari ora hanno la proprietà privata delle proprie risorse digitali in un modo che prima non era possibile. Con il passaggio a Identificatori decentralizzati e reclami verificabili, i destinatari hanno anche identità digitali permanenti e indipendenti e possono scegliere esattamente quando, come e a chi divulgare i propri dati privati. Come standard pubblici, tutte queste specifiche risolvono la massima interoperabilità e portabilità di documenti e dati, senza sacrificare la privacy o il controllo individuale. Grazie alla tecnologia Blockchain abbiano le risorse necessarie per i sistemi basati su principi di auto-sovranità, e sta a noi assicurarci che siano utilizzati nelle architetture educative, economiche e di governance delle generazioni future.

Bibliografia

1. Towards Self-Sovereign Identity using Blockchain Technology-Djuri Baars
2. Sovrin White Paper : https://sovrin.org/
3. Self-Sovereign Identity and Distributed Ledger Technology Framing the Legal Issues : PerkinsCoie.com/Blockchain
4. SelfKey White Paper: https://selfkey.org/
5. Decentralized Identifier – Marco Sabadello : https://danubetech.com/
6. Che cos'è la blockchain, come funziona e perché funziona bene : https://www.wired.it/economia/finanza/2016/02/22/blockchain-come-funziona/
7. A blueprint for digital identity - R. Jesse McWaters
8. Digital Identity : https://www.weforum.org/projects/digital-identity
9. Self Sovereign Identity—a guide to privacy for your digital identity with Blockchain : https://medium.com
10. Self-sovereign identity on the block – ideal or no deal? : https://www.computerweekly.com
11. Self-sovereign identity delivers MyData in practice : https://perspectives.tieto.com/blog/2017/08/self-sovereign-identity-delivers-mydata-in-practice/
12. Trasformed digital identity into trusted identity: https://www.ibm.com/blockchain/solutions/identity
13. Blockchain and digital identity : https://towardsdatascience.com
14. 21 Companies Leveraging Blockchain for Identity Management and Authentication : https://gomedici.com
15. Shocard White Paper : https://shocard.com/

16. Public key model – bitsonblocks.net