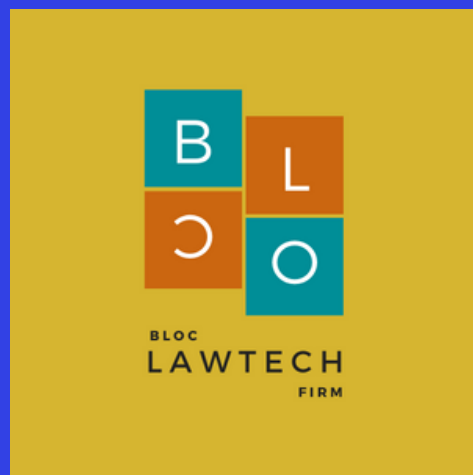


SONOSANO

Caso d'uso di PASS VACCINALE
collegato ad Identità digitale sovrana



Presentazione per
Hackathon "This is me 2021"
G2C



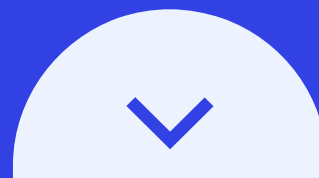


La Sfida

Conciliare i principi di autodeterminazione e riconoscimento univoco dell'individuo congiuntamente alla spendita di informazioni sanitarie, proponendo una soluzione tecnologica il più possibile conforme al quadro normativo vigente ed alle aspettative culturali del contesto sociale

Ecco "Sonosano", il Pass Vaccinale personale

che consente all'individuo di disporre delle proprie
credenziali in modo autonomo, di averne l'immediata
attribuzione al fine di poter gestire in modo agile le
informazioni sanitarie in esso contenute



Il perfetto connubio



Self Sovereign Identity

- diritto degli individui di determinarsi (esercizio esclusivo ed autonomo di attribuirsi una propria identità)
- diritto di possedere, dimostrare e spendere la propria identità (consentendo l'accesso o l'interazione con i terzi autorizzati dallo stesso ai dati e alle informazioni personali fornite)

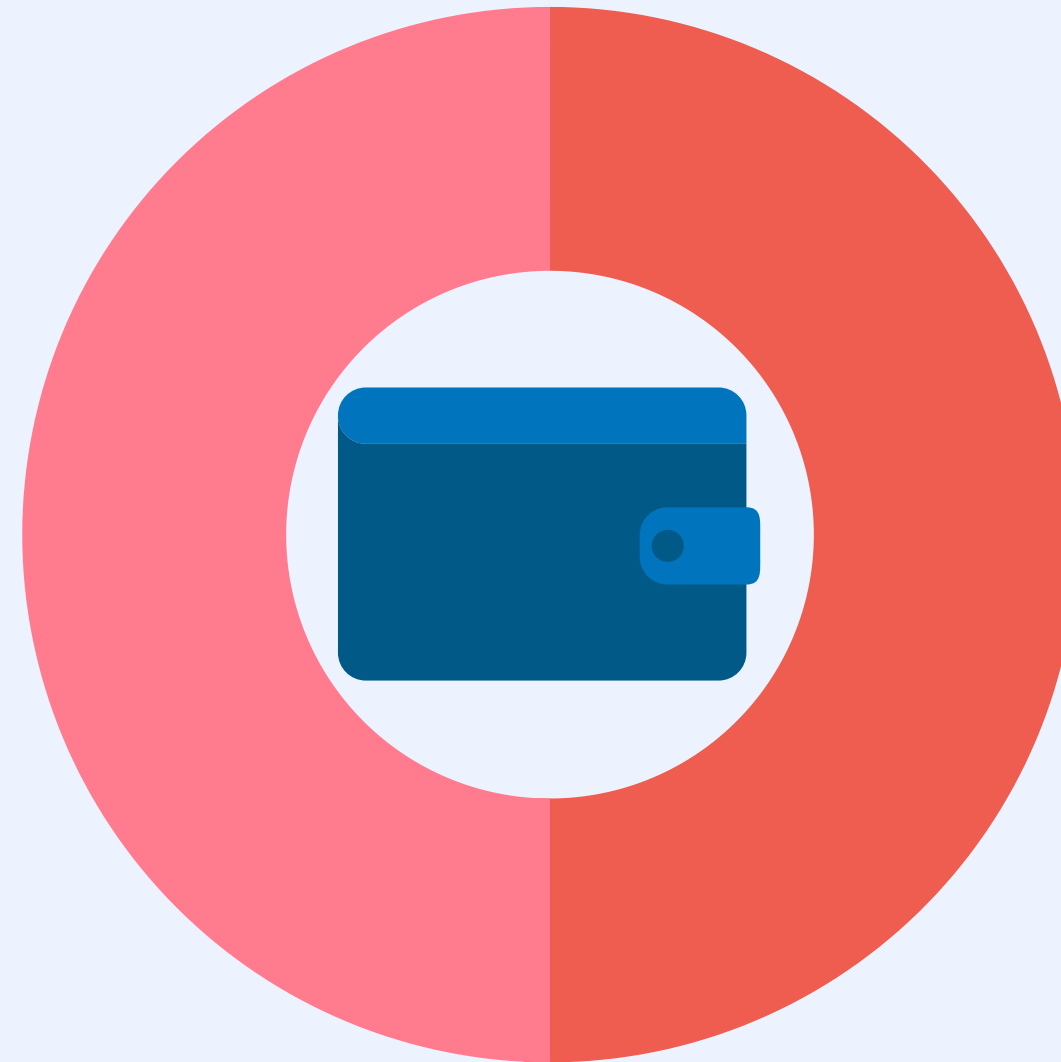
Trusted Service Providers

- Soggetto a cui è attribuito il potere di emettere il documento sanitario relativo alla vaccinazione dell'individuo
- ✗
- Diritto naturale
 - Costituzione Italiana
 - Decreto del Presidente della Repubblica n. 445 del 2000, artt.46-47



La sintesi nel Wallet Sonosano

TSP
50%



SSI
50%

La proposta di SONOSANO è di scollegare il certificato dal Data Base centralizzato del TSP e collegarlo alla SSI dell'individuo all'interno di un token complesso risiedente su blockchain pubblica, decentralizzata e distribuita, e richiamabile per ogni verifica necessaria.





Pain Point!

Non esiste attualmente un sistema basato su questa diade congiunta.

Oggi non è possibile generare un'identità senza fare affidamento ad un **provider di terze parti**.

Se l'ente o il provider cessassero di erogare i propri servizi o di esistere per assurdo (pensiamo all'anagrafe o a un servizio di firma digitale) sparirebbero tutte le identità degli utenti ad esse collegati.



La soluzione

Inversione della priorità dei soggetti (TSP al servizio del soggetto)

In un contesto di applicazione di Self Sovereign Identity gli individui certificano la propria identità sovvertendo il concetto di quadro di fiducia pubblico in quello di fiducia privata utilizzando il **TSP solo come mezzo** per l'impiego delle proprie credenziali in una sorta di self governable identity.



La scelta di SONOSANO

○ SSI IBRIDA (Me+TSP)

Il soggetto si autodetermina e convalida la propria identità facendo il match con l'identità fornita dal TSP. L'identità risiede completamente sul Wallet univoco.

○ TOKEN E BLOCKCHAIN

L'utilizzo di Token e del protocollo blockchain permettono l'identificazione univoca e la verificabilità dell'identità oltre che delle informazioni fornite dal TSP (documentazione vaccinale).

○ DATI FORNITI DAL TSP

I dati (certificati vaccinali) forniti dal TSP o dall'Ente preposto vengono ospitati all'interno del Token in modalità interagente con l'esterno. Il dato medico si collega alla SSI.



Art. 8 ter Decreto Semplificazioni:

- Riconoscimento DLT
- Effetti giuridici del Timestamp
- Riconoscimento della funzione Hash
- Riconoscimento Smart Contracts

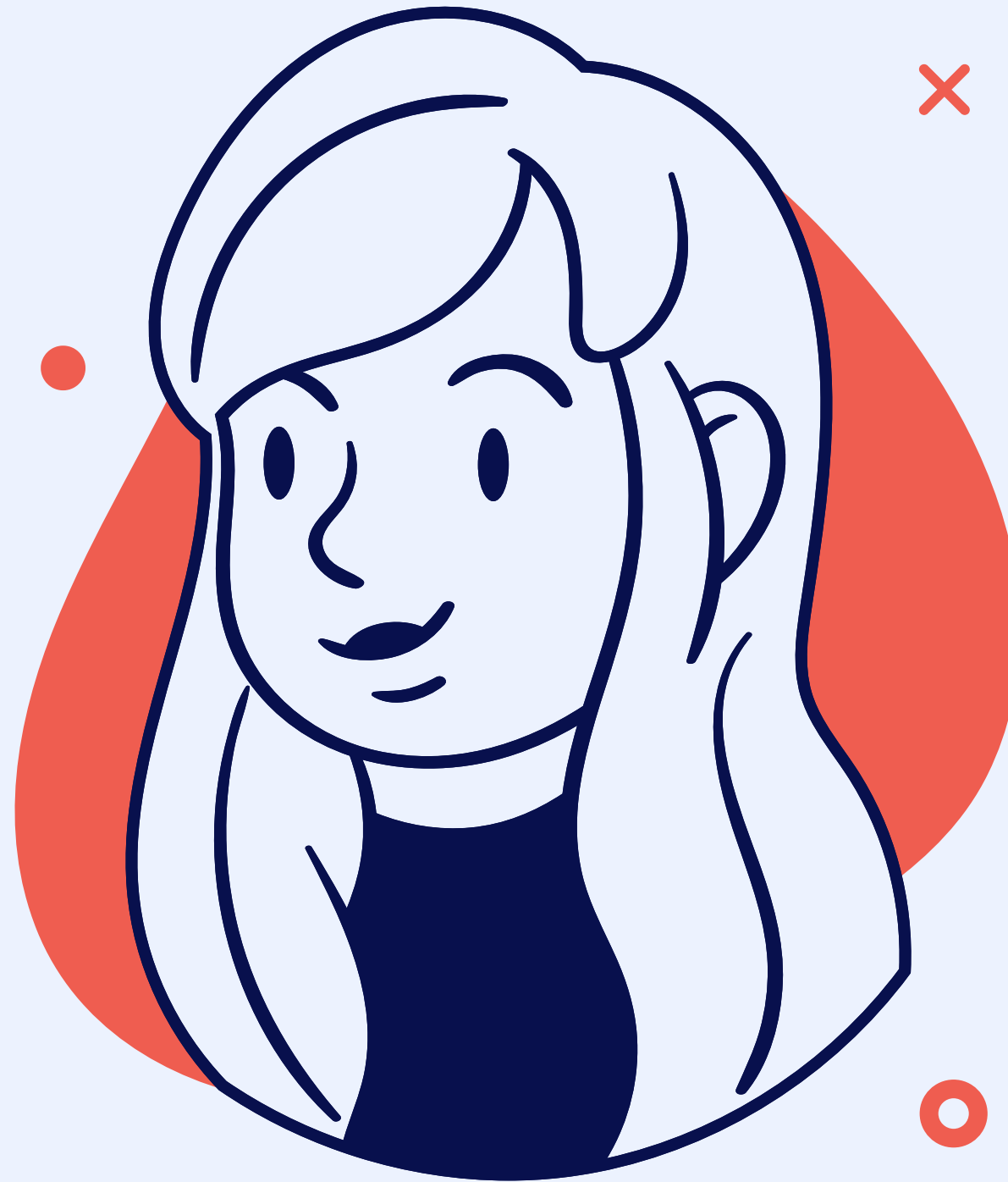


Cosa posso affermare di me?

ed inoltre

Nel nostro caso i token intendono rappresentare dati di identità e nascita. Ovviamente questi token possono essere tenuti al sicuro in forma digitale e preservati da contraffazioni.

Nasce in tal modo una NFI Non fungibile identity in cui i dati autocertificati risulteranno sempre collegati al soggetto emittente e mai modificabili in seguito.



Un NFT che diventa un NFI (non fungible identity)

Il sistema si basa sulla creazione di un SELF SOVEREIGN IDENTITY TOKEN da depositare nel proprio wallet. Gli NFT (Non Fungible Token) possono rendere univoca l'identità dell'individuo oltre che essere essi stessi richiamati ogni qual volta si necessiti di verificare la stessa identità.



Cosa afferma di me il soggetto Trusted?

quindi...

La creazione del certificato non può prescindere quindi dalla competenza ed attività di un soggetto medico accreditato presso un Ente preposto e definito TRUSTED che ne gestisca il rilascio. Tale dato risiede inizialmente in un Data Base centralizzato



Il documento medico

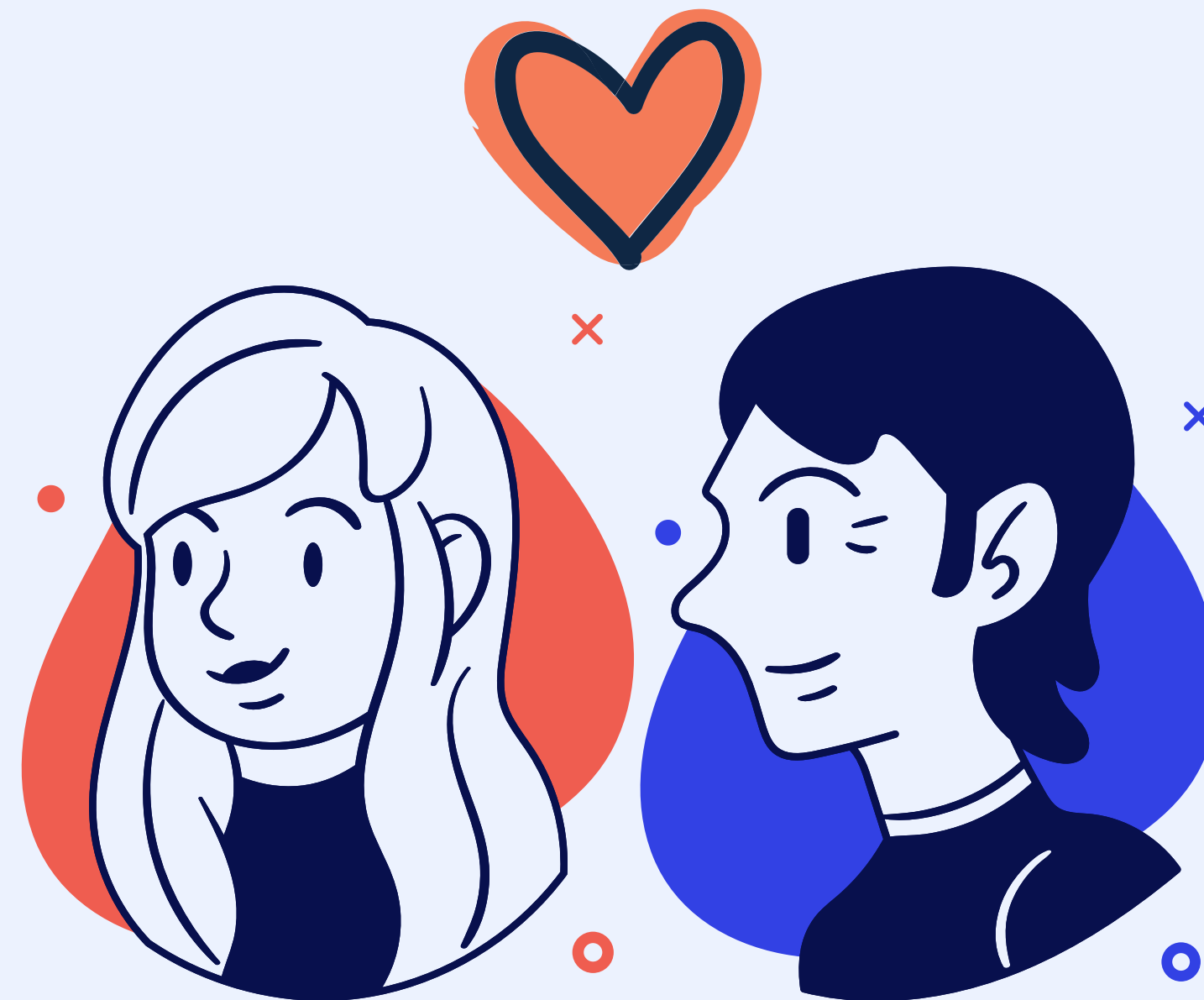
Il TSP o Ente fornisce i dati sanitari :
il **certificato vaccinale**

La composizione del dato sanitario relativo al Pass Vaccinale impegna professionalità mediche che necessariamente non possono ricadere sotto l'arbitrio dell'individuo che ne beneficia.



Cosa possono fare insieme...

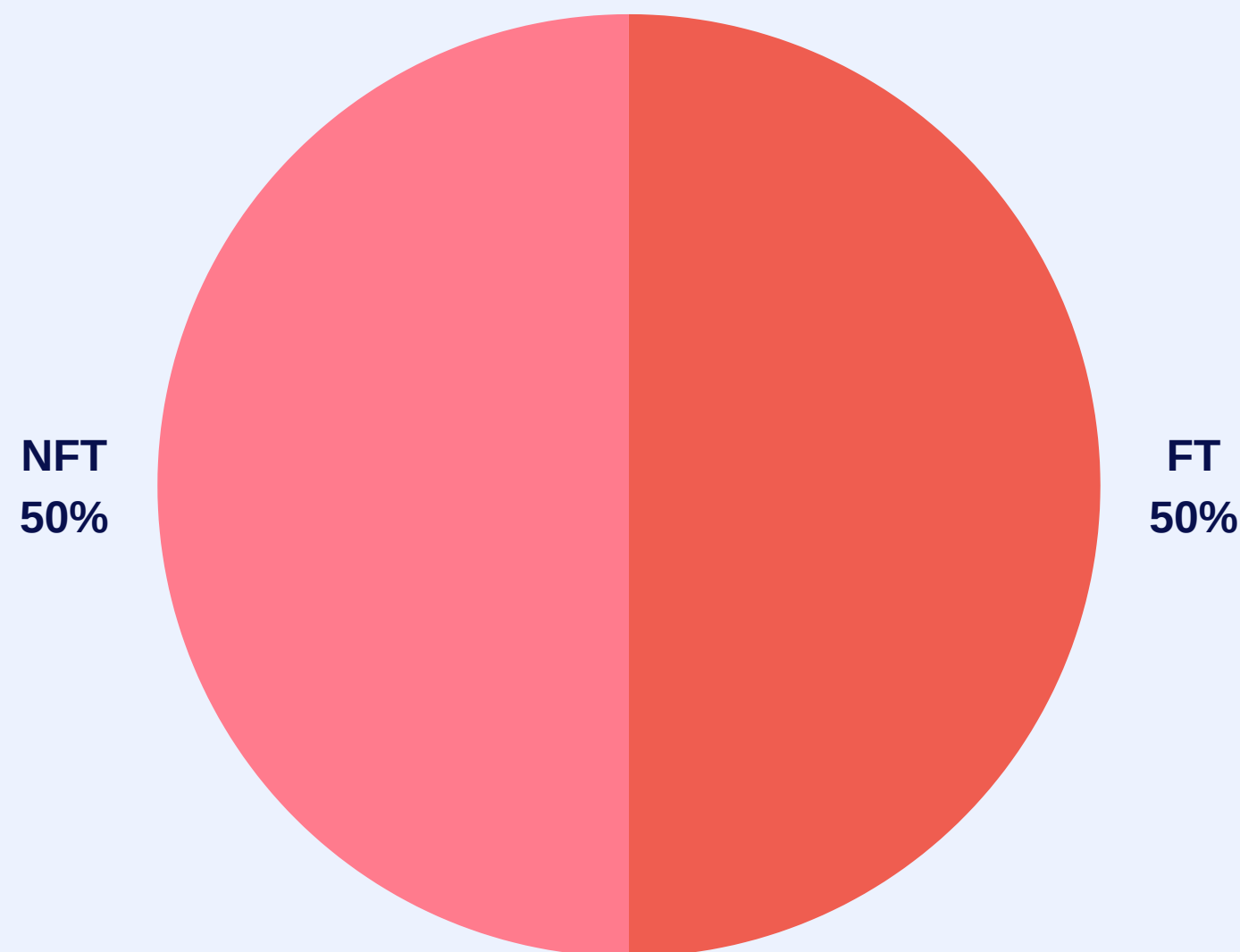
La proposta di SONOSANO è di scollegare il certificato dal Data Base centralizzato del **TSP** e collegarlo alla **NFI** dell'individuo all'interno di un **token complesso** che risiede su **blockchain** pubblica, decentralizzata e distribuita, e richiamabile per ogni necessaria verifica.



La tecnologia

Perché il sistema funzioni correttamente, esso deve soddisfare tre principi fondamentali: il **controllo individuale**, la **sicurezza** e la **piena portabilità**. Il sistema proposto lo permette contemporaneamente.

La sintesi:
il token...



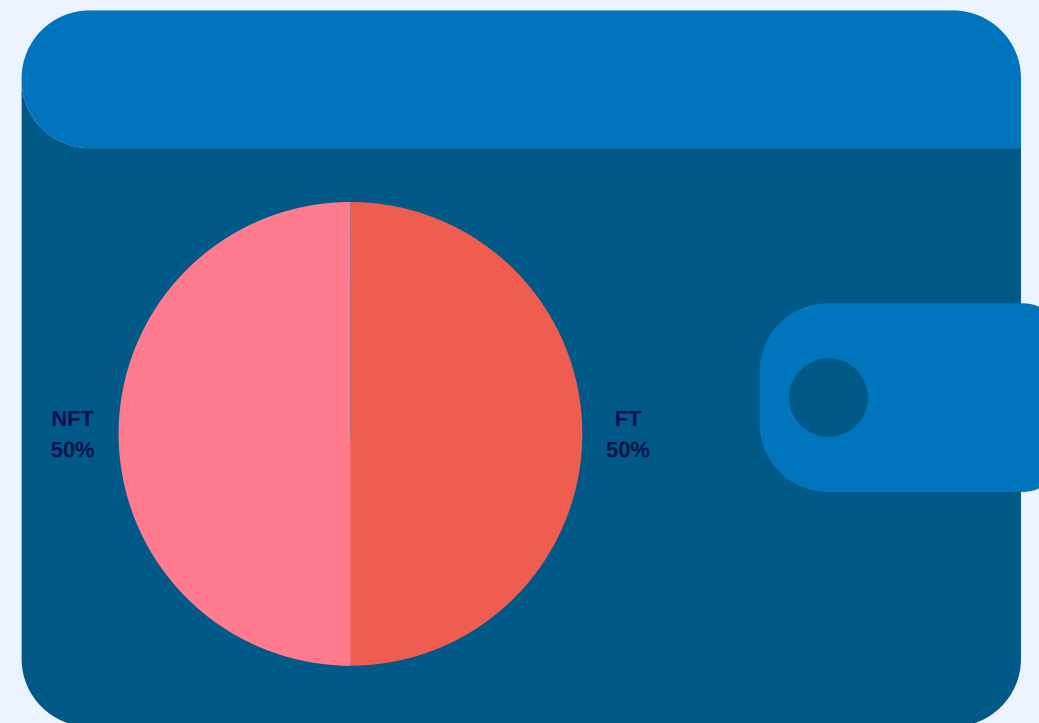
Lo Use Case SONOSANO prevede la realizzazione ed attribuzione a ciascun individuo di un token **ERC-1155** su blockchain di Ethereum che presenta **congiuntamente** le caratteristiche di un **token non fungibile** ma anche di un **token fungibile**.

I dati **univoci** dell'**NFT** sono connessi ai dati **interagenti** provenienti dall'esterno utilizzando **ERC-1155**



La collocazione all'interno del **medesimo token** di una **SSI (NFI)** e di un **certificato vaccinale** proveniente **da terze parti TSP**, con possibilità di aggiornamento costante, crea un **PASS individuale**, portabile, dinamico e sicuro che può essere custodito in un **Wallet**: il Wallet documentale di SONOSANO

L'infrastruttura, attraverso gli smart contract ibridi residenti sulla blockchain, è collegabile ai data base centralizzati o, ancora in seguito, alle blockchain stesse degli Enti.



La sintesi: ...ed il wallet documentale.

✗ L'uso del protocollo blockchain permette di soddisfare il requisito della firma elettronica avanzata secondo quanto previsto per lo stesso dal regolamento eIDAS. Art.25



DATI AL SICURO

Attraverso la creazione di una infrastruttura basata sul concetto di privacy by design

Il tema della applicazione del GDPR in ambienti basati su protocollo blockchain è tutt'oggi discusso.



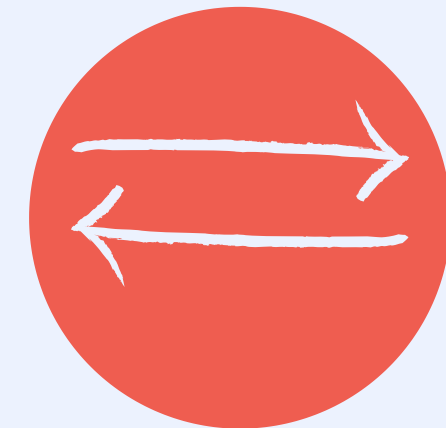
Il wallet personale

Il dato particolare dell'individuo risiede sul proprio wallet ed è protetto dal sistema di crittografia asimmetrica che utilizza chiave pubblica e chiave privata. Su blockchain sarà possibile verificarne attraverso la funzione di **HASH** l'univocità ed il collegamento al soggetto che ne permetterà l'accesso.



Il certificato vaccinale

Il documento medico sarà anche esso custodito all'interno del wallet a cui è collegato e sempre verificabile dai soggetti autorizzati dal possessore del wallet.



La circolazione

La circolazione del dato è completamente in capo al soggetto proprietario del wallet che decide di renderlo disponibile per le verifiche



Conclusioni

○ SONOSANO

E' un wallet documentale in cui risiede un combinato di una Self sovereign identity non fungibile NFI ed un documento proveniente da un provider definito Trusted che fornisce il certificato vaccinale.

○ BLOCKCHAIN

L'utilizzo combinato di NFT, Smart contract, e blockchain ambisce, in misura più possibilmente compliant alle norme vigenti, a garantire all'individuo possessore dell'accesso al proprio wallet di creare, spendere e circolarizzare secondo la propria volontà i propri dati in relazione all'esigenza che si manifesta.



Grazie per l'attenzione!



info@bloclaw.tech



bloclaw.tech

