EGG Net

The sustainable blockchain

Powered by EGG CHAIN

ecosistema digitale basato su blockchain

per la tokenizzazione delle business community

Overview

Introduzione **3**

Glossario **4**

Modello **5**

Community 5

Token 5

Attori e Profilazione 6

Profili e Ruoli 7

Badge 7

Architettura **8**

Componenti dell'ecosistema eggNet 8

eggHome 8

eggIdentity 9

Infrastruttura 10

Server farm 10

Blockchain network 11

Introduzione

Questo documento descrive le caratteristiche e le funzionalità di **eggNet**: ecosistema digitale integrato, basato su *blockchain*, al servizio delle reti di imprese e cittadini e, più in generale, delle *business community* che desiderano introdurre asset o token digitali liberamente circolanti all'interno della community per facilitare le interazioni e gli scambi di valore tra i membri delle community e con gli utenti/consumatori finali dei beni e dei servizi prodotti dalla community stessa.

Alcuni esempi di *business community network* possono essere:

- I circuiti regionali di credito mutuale
- Le aziende di un distretto coinvolte nella medesima filiera produttiva
- Libere associazioni di cittadini e/o imprese per lo sviluppo del territorio
- Associazioni di categoria, associazioni di impresa
- Reti di produttori e consumatori (prosumer) di energia rinnovabile
- Comunità di Pratica che producono e si scambiano asset digitali unici pagandoli in token (baratto digitale)

Glossario

eggID	Identificativo Univoco di una Persona (fisica o giuridica) all'interno dell'ecosistema generato e salvato sulla blockchain eggNet.
eggWallet	Borsellino Digitale associato ad una Persona fisica o giuridica dotata di identificativo univoco eggID all'interno del quale vengono conservati tutti i token delle community di affiliazione. Ad un eggID possono essere associati più eggWallet (ad esempio, il Titolare di una Azienda può operare sul Wallet aziendale con una opportuna delega e anche un Wallet personale, individuale).
ERC20	Standard Ethereum per la gestione di token digitali scambiabili come "moneta digitale" → https://en.wikipedia.org/wiki/ERC-20
ERC721	Standard Ethereum per la gestione di asset digitali unici, collezionabili e scambiabili → https://en.bitcoinwiki.org/wiki/ERC-721

Modello

Il modello generale di **eggNet** prevede alcune entità fondamentali che possono essere specializzate e configurate per ogni specifico contesto di business consentendo alla piattaforma di potersi adattare al business e di supportare processi anche molto diversi.

Community

La piattaforma **eggNet** consente di definire Community cioè aggregati di soggetti (da intendersi come persone fisiche o giuridiche) aventi un comune interesse o scopo.
La Community può essere, a sua volta, suddivisa in Community di secondo livello in funzione di articolazioni di tipo territoriale o tematiche o altro.
Tutte le Community fanno parte della Community globale *eggNet* alla quale sono associati i processi e i servizi generali comuni come la gestione delle identità degli utenti e la sicurezza.
Ogni Community può definire e gestire i suoi Token Digitali che saranno utilizzabili da tutti i soggetti che appartengono alla Community e a tutte le sotto-Community.
Ogni Token ha le sue caratteristiche e le sue regole di circolazione.

Token

Un Token è un asset digitale univoco gestito su Blockchain e possiede caratteristiche e regole diverse di circolazione.
Ogni token ha regole di emissione, di assegnazione, di circolazione, di distruzione.
Queste regole sono implementate nello Smart Contract che governa il funzionamento del token a run-time.
Parametri di un Token Digitale implementato su eggChain:

Community Owner	La Community che definisce il Token e ne gestisce la sua circolazione
tokenName	Il codice o simbolo del Token
tokenType	Uno tra i seguenti valori: ● Credito regionale ● Currency ● Buono sconto ● Gift Card ● Titolo
tokenStandard	Lo standard tecnico di riferimento per l'implementazione

	del Token
Descrizione	Descrizione estesa del Token
Attributi	Nel caso di Token ERC721, elencare la lista degli attributi che caratterizzano ciascuna istanza del token
Assegnazione wallet	Regola che stabilisce in quale modo il token viene abilitato al wallet degli utenti e quali sono i wallet abilitati
Regole di emissione	Regola che stabilisce in quale modo il token viene “coniato” cioè creato dal nulla da parte della Community che lo gestisce
Regole di assegnazione	Regola che governa l’assegnazione di token ai wallet a valle della loro creazione
Regole di circolazione	Regola che governa la circolazione del token da un wallet all’altro
Regole di distruzione	Regola che stabilisce come e quando i token vengono ritirati dal mercato e distrutti.
SmartContract	Indica il nome dello Smart Contract che implementa il token su Blockchain

Attori e Profilazione

Gli attori serviti dalla piattaforma **eggNet** sono:

- Amministratore di una Community di primo o secondo livello
- Operatori di una Community
- Titolare Azienda iscritta a una o più community
- Operatori aziendali
- Utenti finali, cittadini, consumatori

La profilazione è un processo predisposto dal sistema e gestito dagli amministratori della community per definire l’operatività di ogni tipologia di attore.
Questa attività è particolarmente importante perché definisce le regole di accesso ai dati sensibili.

Profili e Ruoli

La profilazione delle soluzioni verticali viene gestita tramite la definizione di profili e ruoli.

Un profilo è un insieme di funzionalità del sistema che rappresenta un processo completo (es: inserimento di un'azienda).

Un ruolo è un gruppo di utenti della community (es: amministratori, operatori, etc …) a cui vengono attribuiti diversi livelli di utilizzo del sistema identificati da specifici profili.

Ad ogni ruolo bisogna associare uno o più profili definendone il livello di operatività:

- Non visibile
- Lettura
- Lettura e scrittura
- Lettura, scrittura e esecuzione

Un utente senza alcun ruolo non può utilizzare le soluzioni verticali.
Un utente appartenente ad uno o più ruoli può accedere a tutte le funzionalità definite nei profili associati al ruolo purché siano di livello superiore a "Non visibile".

Badge

Le applicazioni generali di ecosistema (community eggNet), non verticali per uno specifico dminio, trattano solo dati generali relativi alla persona e quindi il perimetro di accesso ai dati viene definito automaticamente dopo la fase di autenticazione.
Può essere invece necessario limitare l'utilizzo di alcune funzionalità e questo risultato si ottiene tramite la definizione di un ***badge***.

Un ***badge*** è un attestato che viene riconosciuto dal sistema a seguito di un suo determinato utilizzo (es: il badge "autenticazione" si ottiene dopo aver validato l'account con un numero di cellulare) e non può essere trasferito ad un altro utente.

Architettura

Componenti dell'ecosistema eggNet

APP	DESCRIZIONE	LIVELLO
eggHome	Home Page dell'intero ecosistema applicativo, punto di ingresso centralizzato, gestisce le funzioni di login, logout, preferenze utente, controllo ACL, virtual desktop per l'accesso a tutti gli altri servizi integrati nell'ecosistema. Da ogni sistema e da ogni pagina deve essere sempre possibile ritornare ad eggHome, con un click ("back to a safe place").	Ecosistema eggNet
eggIdentity	Sistema che gestisce l'identità degli utenti e il ciclo di vita delle identità. Le identità sono definite a livello di Ecosistema e gli identificativi univoci (eggID) sono persistenti sulla Blockchain eggNet. Gli utenti dotati di eggID possono accedere a tutte le applicazioni che vivono all'interno dell'Ecosistema. E' compito delle applicazioni verticali definire ruoli e permessi per abilitare una identità ad accedere alla applicazione stessa e a compiere determinate azioni o accedere a specifici dati. eggIdentity è l'unico componente dell'intero ecosistema che conosce le identità delle persone e conserva gli attributi identificativi (Personal Data) in formato cryptato. Tutti gli altri componenti dell'ecosistema utilizzano solo l'identificativo eggID ma non trattano e non conservano i dati personali.	Ecosistema eggNet
eggBoard	Applicazione di backoffice utilizzata dagli Amministratori e dagli Operatori di ogni singola Community di primo o di secondo livello con funzioni specifiche di dominio. Attraverso eggBoard gli amministratori e gli operatori delle Community gestiscono le anagrafiche e i wallet degli iscritti e i token circolanti all'interno della Community.	Soluzione verticale di dominio
eggPay	Applicazione mobile-first di pagamento multi-wallet, multi-valuta, multi-circuito. Ad uso del singolo utente, della singola identità a livello di ecosistema.	Ecosistema eggNet

eggHome

eggHome è il punto di accesso centralizzato a tutto l'ecosistema digitale.

Su eggHome troviamo le funzioni di registrazione e di login, la funzione per gestire il profilo personale, il punto di ingresso a tutte le altre applicazioni dell'ecosistema alle quali l'utente è abilitato e a cui si accede, con un click, in single-sign-on.
Attraverso eggHome gli utenti gestiscono il loro profilo personale e le politiche di sicurezza e di abilitazione dei device.

eggIdentity

Le funzioni di eggIdentity sono:

1. Registrazione (con accettazione del consenso informato e assegnazione di eggID)
2. Gestione dati personali (e alcuni dati aziendali solo per utenti autorizzati)
3. Login/Logout
4. Sicurezza

Ad ogni utente registrato è associato un identificativo univoco (eggID) valido per l'intero ecosistema eggChain e per tutti i servizi che esso contiene.

I Dati Personali associati all'eggID sono conservati in un unico database cryptato (NON su blockchain) e tutte le applicazioni e le transazioni del sistema si basano solo sul valore di eggID (le applicazioni e le transazioni non tracciano dati personali).

Per aumentare la sicurezza dei dati personali e dell'accesso ai servizi, per ogni eggID saranno salvati in forma cryptata:

- la password corrente di accesso
- i diversi device da cui l'utente può collegarsi (mac address)
- la pass-phrase (seconda password di sblocco)

La pass-phrase consente all'utente di cambiare le impostazioni generali di sicurezza: cambiare password, bloccare device smarriti, attivare nuovi device, cambiare pass-phrase, e deve essere conservata e custodita dall'utente fuori sistema.

Per l'accesso ad alcuni servizi, quindi, l'utente dovrà:

- possedere una coppia valida di credenziali (username e password)
- accedere da un device registrato (la registrazione del device chiede la phass-prase)

Processo di "**Registrazione**":
1. Utente compila dati anagrafici (con mail e mail di recovery facoltativa)
2. Sistema invia OTP via mail

3. Utente digita OTP
4. Sistema completa la registrazione, assegna eggID, genera pass-phrase, registra mac-address del device corrente
5. Sistema invia pass-phrase via mail

Funzione "**Sicurezza**":
- si accede alla funzione solo da un device registrato oppure (se il device è nuovo) con richiesta di pass-phrase (generata al momento della registrazione)
- dopo l'accesso alla funzione l'utente vede elenco dei device registrati e il device da cui l'utente è collegato e la data/ora del login corrente e data-ora dell'ultimo logout
- l'utente può cambiare password (*)
- l'utente può bloccare un device (*)
- l'utente può registrare il nuovo device dal quale è collegato (*)
(* per confermare l'operazione viene spedita via mail una OTP da digitare e viene chiesta la pass-phrase)

Infrastruttura

eggNet "vive" su una infrastruttura digitale distribuita ibrida che comprende una o più reti blockchaim private attivabili in funzione delle specifiche esigenze delle business community.

L'infrastruttura è composta da due layer complementari ("cloud & ground"):

- **server farm** ("cloud")
- **blockchain network** ("ground")

Server farm

La parte di server farm (cloud) è a sua volta composta da due livelli:

- sezione pubblica: nodi esposti sulla rete internet esterna
- sezione privata: nodi protetti dalla rete internet esterna

Lo scopo dei nodi pubblici è quello di filtrare le richieste provenienti dall'esterno in modo tale da proteggere tutto l'ecosistema da client malevoli.

Solo sui nodi privati gireranno i servizi, alcuni dei quali comunicheranno il layer blockchain "sottostante".

Blockchain network

E' una rete ***blockchain privata e permissioned composta da nodi Ethereum*** che possono essere di due tipi:

- nodi validatori
- nodi minatori

I ***nodi validatori*** devono soltanto verificare e validare le transazioni generate dagli utenti (ad esempio: lo scambio di crediti tra i diversi wallet) e contenute nei blocchi creati dai nodi minatori e quindi richiedono una minore potenza computazionale rispetto ai nodi minatori.

I ***nodi minatori*** svolgono lo stesso compito dei nodi validatori ma, in più, hanno il compito di creare i blocchi di transazioni che formano la *catena di blocchi* (*block chain*) replicata su tutti i nodi della rete e formano registro condiviso delle transazioni (shared ledger).

L'attuale stima di dimensionamento ci porta alla conclusione che dovrà essere attivato un nodo minatore almeno ogni 25 nodi validatori.

Sul registro distribuito residente in replica su tutti i nodi della rete blockchain privata, sono censiti anche gli identificativi univoci di tutti gli utenti accreditati all'ecosistema (eggID) e che hanno quindi una Identità Digitale valida generale e trasversale ai diversi applicativi verticali e, con quella unica identità, possono accedere a tutti i sistemi ai quali sono stati autorizzati con gli opportuni permessi di accesso.

L'identità digitale, quindi, è unica e valida a livello globale, di ecosistema, basata su blockchain. Gli identificativi univoci degli utenti (eggID) sono censiti sul registro della blockchain e sono, quindi, immutabili. Diversi sistemi verticali, anche di diversi circuiti di credito mutuale o diverse community, possono quindi dare accesso alla medesima persona fisica identificandola con il medesimo eggID e questo consente alla persona di essere riconosciuta da tutti i circuiti e di poter gestire in modo unitario e univoco tutti i suoi conti e i suoi wallet a partire da una unica interfaccia di gestione personale (eggPay, eggBoard).

Sul registro distribuito residente in replica su tutti i nodi della rete blockchain privata, sono registrati tutti gli scambi di crediti (nelle diverse valute complementari dei diversi circuiti) tra i diversi wallet digitali degli utenti di tutti i circuiti. Il registro delle transazioni di credito mutuale è unico, distribuito e condiviso tra tutti i nodi della rete ed è quindi, per definizione, "multivaluta", "multiwallet", "multicircuito" consentendo di ottenere una soluzione scalabile in modo *additivo* al crescere dei circuiti che aderiscono al progetto.

La rete blockchain è composta da server fisici detti ***nodi*** con le caratteristiche hardware e software sotto indicate.

I nodi sono fisicamente installati presso le sale server delle aziende iscritte ai circuiti che, su base volontaria, e previa verifica del possesso dei requisiti tecnici minimi, manifestano il loro interesse ad ospitare un nodo della rete e a farlo funzionare in modo ottimale.

Ogni azienda che ospita un nodo è chiamata ad ospitare, presso il suo CED, il server fisico fornito e già configurato come nodo della rete blockchain.

L'azienda deve fornire alimentazione elettrica e connettività internet sufficiente per garantire il pieno funzionamento del nodo e deve garantire un necessario livello di cura e di custodia del server per garantire il suo pieno funzionamento nel tempo.

I nodi sono tele-monitorati dagli operatori di eggChain e, su di essi, vengono svolti degli interventi di manutenzione programmata, da remoto o in presenza.