Il progetto si inserisce nell'ambito della collaborazione tra l'Università di Trento e l'azienda SEA Soluzioni Eco Ambientali (SEA) una PMI con sede a Villanova Canavese (TO) specializzata nel servizio di raccolta e trasporto di rifiuti solidi urbani (RSU). L'azienda opera prevalentemente il servizio di raccolta porta a porta di rifiuti differenziati ed è molto attiva nel ricercare ed implementare soluzioni che incentivino la massimizzazione dei conferimenti di rifiuto differenziato rispetto all'indifferenziato. Questo risulta essere un tema molto sentito considerando che l'azienda serve una popolazione di circa 1.200.000 persone.
SEA, dopo aver valutato diverse tecnologie, ha interesse a sperimentare i meccanismi crittografici basati sulla blockchain, come strumento per incentivare le attività aziendali sia interne che esterne. Proprio in quest'ottica, SEA ha coinvolto l'Università di Trento e il CryptoLabTN nella progettazione del design di una piattaforma basata sulla tecnologia blockchain per gestire una raccolta di cryptoasset destinati agli utenti che eseguono correttamente la raccolta differenziata nel proprio comune. In seguito i token raccolti dagli utenti possono essere riscossi come premi da alcuni partner territoriali, che hanno preso accordi privatamente con SEA.

Questo progetto deve essere sviluppato da un punto di vista crittografico: la sicurezza delle transazioni è garantita dalle primitive crittografiche che costituiscono la blockchain privata gestita da SEA e in particolare analizzare l'utilizzo di primitive crittografiche post-quantum in grado di resistere agli attacchi quantistici. Infatti al momento su quasi tutte le blockchain sono previste firme digitali la cui sicurezza è garantita dalla difficoltà computazionale di alcuni problemi che si sono tuttavia rivelati facilmente risolvibili tramite algoritmi basati sulla computazione quantistica, quali il problema della fattorizzazione di numeri interi e il problema del logaritmo discreto. Per questo è in corso un processo indetto dal NIST (National Institute of Standards and Technology) per la standardizzazione di algoritmi di firma digitale resistenti ad attacchi di tipo quantistico. Al momento i problemi sui quali si basano i finalisti a questa competizione sono relativi alla teoria dei Reticoli oppure sono metodi di crittografia multivariata. Finalisti alternativi invece basano la loro sicurezza su problemi relativi alle funzioni di hash o sulle zero-knowledge proof. In generale tutti i metodi post-quantum, rispetto agli algoritmi classici, hanno richieste più onerose sia in termini di memoria (dimensioni delle chiavi e dimensioni delle firme) sia in termini di costo computazionale. Tutti questi aspetti dovranno essere analizzati all'interno del progetto per identificare le soluzioni più adatte per la gestione dei dati nella piattaforma.

Inoltre, occorrerà approfondire lo studio di una o più blockchain per la gestione del sistema di ricompense tramite token crittografici. Nello specifico l'architettura da sviluppare sarà rivolta ai seguenti due ambiti di interesse della società SEA:

- monitoraggio della raccolta rifiuti e incentivazione di una corretta raccolta differenziata da parte degli utenti
- incentivazione di comportamenti corretti relativi alla salute dei propri dipendenti, favorendo il consumo di alimenti del territorio