



Applicazioni della blockchain

Y2Y: BLOCKCHAIN E SMART CONTRACT

Organizzatori: Massimiliano Sala, Andrea Gangemi e Christopher Spennato

Speakers: Robbie Daniels, Daniele De Bernardini, Andrea Gangemi, Enrico Guglielmino, Francesco Romeo, Chiara Spadafora, Christopher Spennato

7 e 11 Dicembre, 2023

Sommario

- 1 Introduzione alle applicazioni
- 2 Digital Notary
- 3 Contract Lifecycle Management (CLM)
- 4 Automotive
- 5 E-voting
- 6 Raccolta differenziata e impronta ecologica
- 7 Decentralised Identifiers
- 8 Charity
- 9 Dhali

Introduzione alle applicazioni

Scopo iniziale della blockchain

- La *blockchain* nasce nel 2008 su idea di Satoshi Nakamoto, per gestire le transazioni di bitcoin.
- Questa tecnologia impedisce di:
 - Ripudiare le transazioni eseguite;
 - Spendere soldi che non si possiedono;
 - Spendere due volte gli stessi soldi.

Proprietà della blockchain

- Le proprietà principali garantite dalla *blockchain* sono:
 - Immutabilità delle informazioni inserite a registro;
 - Assoluta trasparenza dei dati inseriti.
- Questo ha portato all'utilizzo della tecnologia per un'ampia gamma di applicazioni.

Panoramica veloce I

- La *Digital Notary* consiste nell'utilizzo della *blockchain* per notarizzare documenti.
- La blockchain può essere usata all'interno del *Contract Lifecycle Management* (CLM) per accompagnare le varie fasi del ciclo di vita di un contratto.
- La *blockchain* può essere usata nel tracciamento di filiera per garantire uno storico del prodotto acquistato.
- *Smart contract* e *blockchain* possono essere usati per implementare un'asta automatica a busta chiusa.

Panoramica veloce II

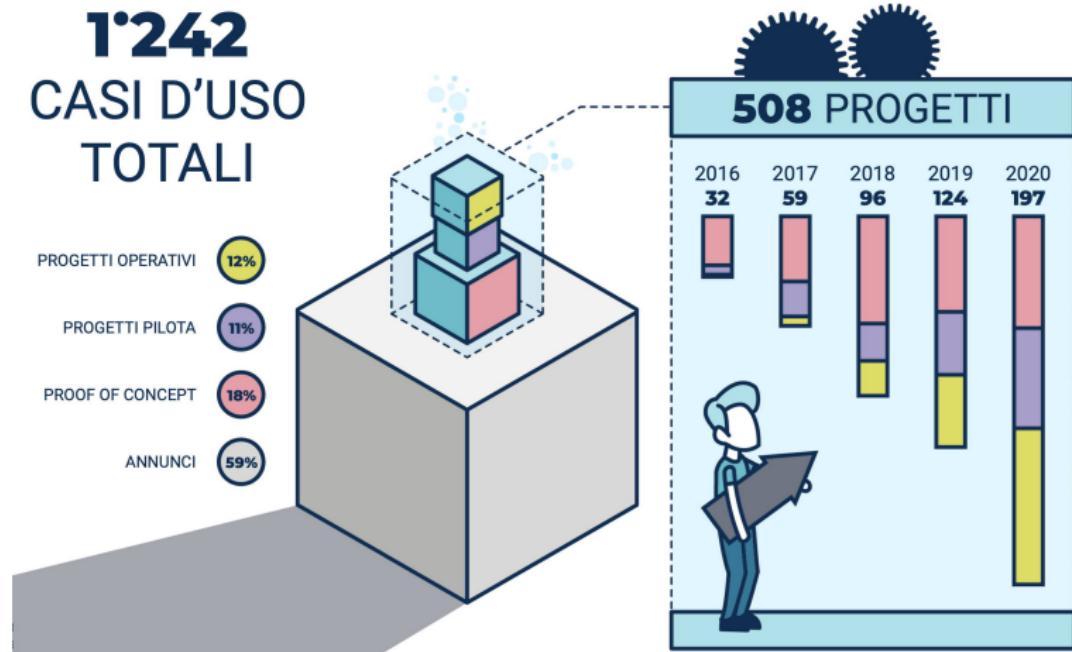
- Attraverso la *blockchain* è possibile implementare un protocollo di voto elettronico che soddisfi le proprietà necessarie a un sistema di votazione.
- In ambito *Automotive*, si possono raccogliere sulla *blockchain* dati riguardanti le condizioni della strada, sul traffico, sulla vettura stessa e sui comportamenti degli utenti, per migliorare la tracciabilità e la sicurezza.
- La *blockchain* può essere impiegata nella raccolta differenziata per incentivare i cittadini ad eseguirla correttamente, tramite l'utilizzo di *token*.

Panoramica veloce III

- La *blockchain* può consentire la definizione di un'identità digitale, consentendo di gestirne efficientemente tutto il *lifecycle*.
- Attraverso la monetizzazione su *blockchain* si è in grado di creare store digitali di noleggio.

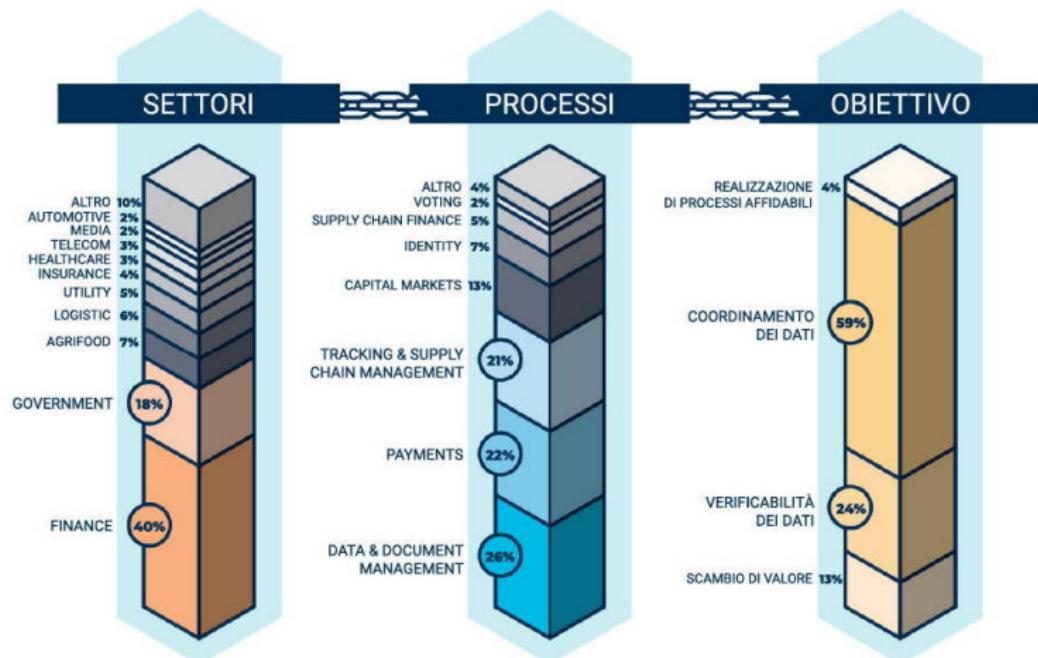
Una tecnologia dirompente

La *blockchain* può considerarsi una tecnologia dirompente e il *trend* sul numero di progetto attivi è in crescita, come si osserva nella seguente figura (dati fino al 2020).



Una tecnologia dirompente

I settori in cui la tecnologia *blockchain* sono vari (percentuali aggiornate al 2020).



Digital Notary

Obiettivo

- La *Digital Notary* ha lo scopo di garantire l'integrità nel tempo di documenti importanti.
- Per fare ciò, si salva su *blockchain* l'*hash* del documento.
- In questo modo, chiunque possiede il documento può calcolarne l'*hash* e verificare che coincida con quello salvato su *blockchain*.
- Se anche il documento fosse cambiato di una virgola, il riferimento nella *blockchain* non corrisponderebbe.

Dove notarizzare?

Ci sono due possibilità per scegliere la tipologia di *blockchain* su cui notarizzare i documenti.

1. Utilizzare una *blockchain* pubblica.
2. Utilizzare una *blockchain* privata.

In linea di massima in un contesto aziendale è preferito l'utilizzo di una *blockchain* privata.

Blockchain privata

L'uso di una *blockchain* privata:

- Garantisce di avere contezza di tutti i partecipanti al *network*;
- Impedisce ad utenti sconosciuti di partecipare alla rete;

D'altro canto, tramite *blockchain* privata si perde la proprietà di assoluta trasparenza per la quale viene utilizzata la *blockchain*.

Ancoraggio a una blockchain pubblica

- Per mantenere le garanzie offerte dalla *blockchain* privata, e al contempo non perdere le potenzialità offerte dalla *blockchain* è necessario effettuare l'ancoraggio a una *blockchain* pubblica.
- Per ancoraggio si intende l'azione di inserire nella *blockchain* pubblica le informazioni presenti in quella privata.

Osservazioni

1. I dati scritti sulla *blockchain* pubblica lasciano trasparire informazioni riguardanti i documenti prodotti dall'azienda?

No! Sono infatti protetti dalla resistenza alla controimmagine delle funzioni di *hash*.

2. Come fa l'azienda a garantire l'esistenza di una versione di un dato documento?

- Ogni qualvolta si ha un'interazione con la *blockchain* pubblica, viene generata una ricevuta che garantisce il corretto inserimento nella *blockchain* pubblica.
- Le transazioni sulla *blockchain* pubblica hanno un timestamp che indica il momento in cui sono state effettuate.

3. Viene garantita la veridicità dei documenti?

No, la *blockchain* può garantire soltanto l'integrità.

Per garantire la veridicità sono necessari *smart contract* ad hoc.

Contract Lifecycle Management (CLM)

Notazione

Per descrivere questa applicazione si distingueranno tre tipologie di contratto:

1. Contratti tipizzati: contratti già prefissati, in cui cambiano soltanto i nomi e gli indirizzi dei contraenti (ad esempio quelli delle compagnie telefoniche).
2. Contratti standard: contratti con un *template* già stabilito, dove possono cambiare contraenti, cifre economiche, clausole contrattuali, motivazioni alla base del contratto, etc.
3. Contratti su misura: contratti totalmente liberi scritti a seconda delle specifiche esigenze.

Per *Contract Lifecycle Management* (CLM), si intende la gestione di tutte le varie fasi che costituiscono il ciclo di vita di un contratto:

1. Creazione;
2. Negoziazione;
3. Approvazione;
4. Esecuzione;
5. Monitoraggio e tracciamento;
6. Chiusura.

- Per creare un contratto è necessario scegliere un *template*.
- Nel *template* del contratto ci sono sempre alcuni elementi:
 - Contraenti;
 - Formula di accettazione della proposta;
 - Causa;
 - Oggetto dell'obbligazione principale;
 - Forma specifica della tipologia contrattuale.
- Il *template* standard di un contratto deve prevedere tutti gli elementi da inserire.
- A partire da qui, il *template* va personalizzato.

- Tramite *smart contract* si può automatizzare la scrittura di un contratto standard o tipizzato.
- Un utente compila alcuni campi prefissati (ad esempio durata, contraente, etc).
- Questi valori sono passati come input a uno *smart contract*, che genera automaticamente il contratto sulla base di queste specifiche.

Creazione III

- Ogni volta che è necessario un nuovo contratto non occorre scriverlo *ex novo* (purché sia tipizzato standard o tipizzato).
- È sufficiente passare allo *smart contract* le specifiche con le proprie esigenze.
- La versione del contratto generato dallo *smart contract* è automaticamente notarizzata.
- L'utente che ha inviato la transazione è crittograficamente riconosciuto (una transazione su *blockchain* è valida soltanto se firmata digitalmente).
- L'automazione di un contratto su misura risulta invece di difficile attuazione data la totale libertà del suo *template*.

Negoziazione I

- La negoziazione è la fase in cui si definiscono gli obiettivi da raggiungere in termini:
 - economici,
 - temporali,
 - di gestione dei rischi.
- Durante la fase di negoziazione il compratore analizza l'offerta del venditore.
- Se non è soddisfatto avanza una controproposta.
- Il venditore deciderà se accettare o proporre nuove modifiche.
- La fase di negoziazione termina con l'accordo sulle ultime modifiche proposte (oppure con la decisione dell'impossibilità di proseguire nella contrattazione).

Negoziazione II

- Attraverso la *digital notary* è possibile tracciare su *blockchain* tutte le offerte e controfferte.
- In questo modo sarà sempre possibile risalire all'intero processo di negoziazione che ha portato al contratto in essere.
- L'intero processo che ha creato le varie versioni può essere gestito da uno *smart contract*.
- Questo *smart contract* è una semplice estensione di quello usato nella creazione della prima versione del contratto.

Approvazione I

- Una volta conclusa la fase di negoziazione è necessaria l'approvazione formale.
- Solitamente, l'approvazione definitiva del contratto viene notificata prima informalmente e poi attraverso uno scambio di mail formali.
- Dopo l'approvazione, il contratto sarà firmato, e gli ordini d'acquisto saranno approvati.

Approvazione II

- Grazie agli *smart contract* è possibile imbastire un sistema di firme digitali.
- Si può registrare il contratto sulla *blockchain* effettuando una transazione che viene firmata digitalmente.
- La transazione può contenere l'intero contratto, oppure un *hash* dello stesso.
- Occorre inoltre un semplice *smart contract* che verifichi le firme digitali.
- Volendo, si può legare lo *smart contract* di verifica delle firme a quello che ha aiutato la gestione delle versioni.
- In tal modo, entrambi i processi saranno fluidamente collegati.

- Superata l'approvazione, il contratto viene preso in carico dai responsabili.
- Per tutto quello che concerne l'esecuzione di un contratto, gli *smart contract* possono risultare utili.
- La loro forza risiede proprio nel fatto che al verificarsi delle clausole contrattuali, gli obblighi vengono adempiuti automaticamente.
- Vedremo più avanti alcune criticità di questi *smart contract*.

Monitoraggio e tracciamento I

- La fase di monitoraggio verificare che tutti gli obblighi contrattuali vengano rispettati.
- Per il corretto avvio di un contratto è previsto un *kick-off meeting* in cui si discute la forma e la frequenza dei vari *deliverable*.
- Una volta avviato il contratto saranno necessari dei *meeting* periodici di allineamento.
- Durante questi *meeting* si controlla se le varie parti stanno rispettando le tempistiche dichiarate in fase di contrattazione e se le spese in corso d'opera rientrano nei vincoli stabiliti.

Monitoraggio e tracciamento II

- È possibile anche usare la tecnologia *blockchain* per tenere traccia delle consegne dei *deliverable*.
- Lo *smart contract* non potrà mai valutare la qualità di un *deliverable*.
- Tuttavia può accertarsi del suo arrivo e registrare i verbali delle riunioni relative.
- Lo *smart contract* potrebbe anche tracciare la fase di fatturazione:
 - Può tenere traccia di tutti i pagamenti effettuati e delle loro date.
 - Può notificare gli utenti interessati dell'avvicinarsi delle scadenze.

Chiusura I

- La chiusura è la fase finale del CLM.
- Si verifica che tutti i beni e/o servizi richiesti siano stati ricevuti e che tutte le fatture emesse siano state pagate.
- Si recupera tutto il materiale che il compratore ha messo a supporto del venditore.
- Si appura che non vigano reclami irrisolti.
- In caso di controversie, si deciderà se iniziare una nuova negoziazione oppure accettare le modifiche proposte.
- Se il contratto prevedesse la possibilità di rinnovo il ciclo ricomincerebbe dalla fase di approvazione.

- La *blockchain* può essere usata per certificare l'approvazione di un contratto firmandolo digitalmente.
- Analogamente può essere usata per certificare la chiusura del contratto.
- Una volta appurato che tutte le parti coinvolte siano soddisfatte (pagamenti avvenuti e no reclami irrisolti) uno *smart contract* può certificare sulla *blockchain* la chiusura del contratto.
- Per farlo può inviare una transazione di chiusura contratto firmata digitalmente da tutti i contraenti.
- Questa transazione può essere visualizzata da tutte le parti (compresi subappalti e autorità di vigilanza, etc.).

Riassunto I

Abbiamo visto come la *blockchain* può essere adoperata per supportare le varie fasi del ciclo di vita di un contratto.

- Uno *smart contract* può notarizzare una prima versione del contratto, riconoscendo crittograficamente l'utente che ha inviato la transazione.
Un contratto su misura può essere notarizzato su *blockchain* senza uso di *smart contract*.
- Attraverso la *blockchain* si può gestire la fase di negoziazione e tenere traccia di tutte le proposte e modifiche approvate tra le parti. Una volta che il contratto ha raggiunto una formulazione definitiva, si potrebbe selezionare tramite la *blockchain* un fornitore (se previsto).

Riassunto II

- Al momento dell'approvazione finale, il contratto può essere registrato su *blockchain* effettuando una transazione firmata digitalmente, mentre un apposito *smart contract* verifica le firme digitali e conferma la legittimità e autenticità del contratto.
- Uno *smart contract* non può valutare la qualità di un *deliverable*, né se è un elaborato, tantomeno se è un oggetto fisico.
Tuttavia, può certamente conservare le ricevute di consegne degli stessi.
- La *blockchain* può certificare la corretta chiusura di un contratto, una volta ricevuti tutti i servizi/prodotti previsti ed effettuati tutti i pagamenti.

A nostro avviso, questo approccio garantisce un passo avanti rispetto alla contrattualistica attuale.

Eventuale salto di qualità

- Una volta definito un accordo tra più parti, si può scrivere uno *smart contract* che contenga le clausole contrattuali automatizzabili e gli effetti che queste comportano.
- In questo modo si unirebbero tutte le funzionalità descritte precedentemente all'esecuzione automatica di un contratto.

Eventuale salto di qualità II

Questo approccio presenta tre criticità:

1. Il verificarsi di alcune clausole potrebbe non dipendere da eventi esterni alla *blockchain*. In tal caso è necessario collegare lo *smart contract* con oracoli. Questo implica la necessità di fidarsi di sistemi esterni alla *blockchain*.
2. La traduzione delle clausole contrattuali in linguaggio di programmazione può non essere fedele.
3. L'esecuzione del contratto potrebbe essere inficiata da errori informatici a vari livelli: piattaforma, librerie, compilatore, etc.

Eventuale salto di qualità III

Per affrontare il primo problema ci sono almeno tre strumenti:

1. Si potrebbero prevedere più oracoli, considerando così "valida" un'informazione trasmessa dalla maggioranza di essi.
2. Ci si potrebbe affidare a un "oracolo umano" e sottoscrivere con esso un contratto per disciplinarne la responsabilità.
3. Si potrebbe allocare il rischio su una delle parti in base al principio di maggior controllo sulla gestione del rischio stesso.

Per affrontare il secondo problema possono entrare in gioco i Ricardian Contracts: particolari *smart contract* dotati di valore legale leggibili sia da una macchina sia da un essere umano.
Questi strumenti esulano dallo scopo del corso.

Eventuale salto di qualità IV

- La terza criticità è intrinseca alla natura degli *smart contract*.
- Uno *smart contract* è immodificabile, quindi un contratto legato a uno *smart contract* che effettua errori di esecuzione rimane comunque vincolato allo stesso.
- In passato, errori di programmazione degli *smart contract* hanno causato la perdita di milioni di dollari.
- Uno degli esempi più famosi è l'attacco DAO alla *blockchain* Ethereum che permise a un *hacker* di prelevare ether per un valore di 60 milioni di dollari.
- Oltre agli errori di programmazione in senso stretto, ci potrebbero essere errori di esecuzione derivanti da altre componenti del sistema, quali il compilatore, le librerie, la piattaforma, etc.

Automotive

Automotive - Introduzione

Oggi, grazie alla connessione a internet, le automobili sono in grado di analizzare una mole incredibile di informazioni in tempo reale, prendere decisioni istantanee senza l'aiuto o l'intervento dell'uomo, ma soprattutto sono una fonte inesauribile di dati.

Nei prossimi anni questa tendenza è destinata ad aumentare, tanto che ogni auto avrà sensori che raccoglieranno dati sulle condizioni della strada, sul traffico, sulla vettura stessa e sui comportamenti e le preferenze dei guidatori.

Un recente studio dell'IBM evidenzia come la blockchain introdurrà miglioramenti e innovazione in aree quali l'**esperienza dei clienti**, i **servizi accessori**, l'**autenticazione** dell'accesso alle auto e quelli relativi alle **transazioni finanziarie**. L'obiettivo è quello di contare su un migliore accesso e **trasparenza** delle informazioni e sulla loro **sicurezza**.

Problematiche relative all'utilizzo di sistemi tradizionali

Gli **smart vehicles** sono sempre più connessi alla infrastruttura stradale, agli altri veicoli nelle immediate vicinanze, e più in generale all'Internet of things (IoT). Tuttavia l'alto grado di interconnettività di tali veicoli può compromettere la sicurezza del veicolo e quella del passeggero.

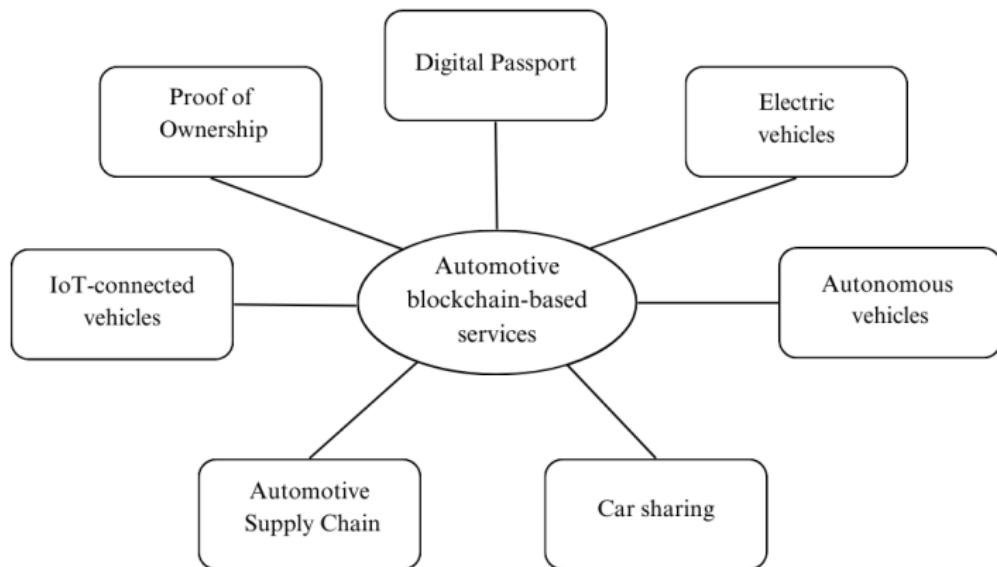
I metodi convenzionali di sicurezza e privacy tendono spesso ad essere inefficaci a causa di:

- Centralizzazione;
- Mancanza di privacy;
- Minaccia alla sicurezza.

Diagramma di flusso per valutare l'idoneità della tecnologia blockchain per un caso d'uso specifico



Servizi basati su blockchain per il settore automotive



MOBI (Mobility Open Blockchain Initiative)

MOBI è un consorzio globale il cui obiettivo è accelerare l'adozione delle tecnologie blockchain e in generale DLT nel settore automobilistico e della mobilità.

Il consorzio MOBI è impegnato in varie attività, tra le quali:

- Economia circolare e passaporto globale della batteria;
- Identità digitale del veicolo;
- Supply Chain;
- Mercato dei dati;
- Integrazione della rete dei veicoli elettrici;
- Manutenzione e riparazione del veicolo.

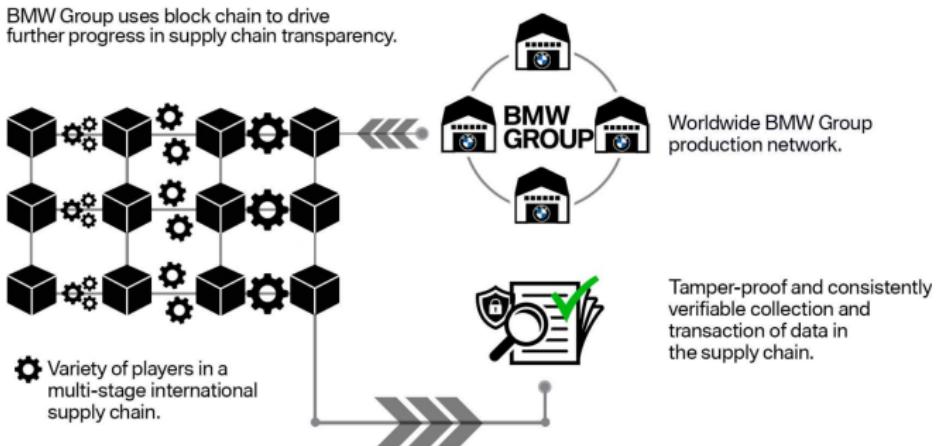
Tra le aziende partner di MOBI abbiamo numerose aziende del settore automobilistico come BMW, Ford, General Motors, Honda, Marelli, Mazda, Nissan, Renault, Stellantis e Toyota, e molte altre aziende leader come Accenture, Reply, Amazon Web Services, Bosch e IBM.

Nel 2019, il **BMW Group** ha annunciato l'adozione della tecnologia blockchain per ottimizzare diversi processi:

- Migliorare la tracciabilità delle parti e delle materie prime nell'ambito delle **supply chain**;

BLOCKCHAIN

BMW Group uses block chain to drive further progress in supply chain transparency.



- Ricaricare le auto elettriche più facilmente;
- Sviluppo di un passaporto digitale dei veicoli.

Per quanto riguarda le supply chain, l'azienda ha introdotto un progetto Blockchain noto come [PartChain](#). Tra i vari obiettivi di questo progetto, vi è anche quello di creare una piattaforma aperta che faciliti lo scambio sicuro e anonimo dei dati.

PartChain sfrutta non solo le soluzioni Blockchain ma anche le tecnologie Cloud come Amazon Servizi Web e Microsoft Azure. Questa combinazione consente il tracciamento continuo dei componenti tra tutti i partner partecipanti, garantendo che non vi sia alcun rischio di manipolazione dei dati.

Inoltre, è importante sottolineare che il BMW Group è stato uno dei principali co-fondatori di MOBI nel 2018.

Porsche è stata una delle prime case automobilistiche ad esplorare e successivamente ad implementare la tecnologia blockchain nei loro sistemi.

Nel 2018, Porsche ha presentato il risultato del contest Porsche innovation dell'anno precedente, vinto dalla start-up XAIN. A seguito del successo di un test nel dicembre 2017, Porsche e XAIN hanno infatti approfondito la loro collaborazione per sviluppare ulteriormente e testare la Blockchain di XAIN sui veicoli ibridi.

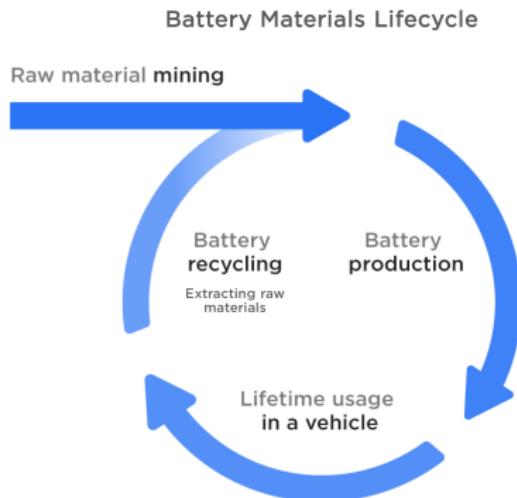
Lo sviluppo ha portato a un algoritmo di consenso brevettato da XAIN chiamato PPKW (Practical Proof of Kernel Work).

Integrando reti e sistemi diversi (sia all'interno che all'esterno dell'auto) con la tecnologia Blockchain, sono state introdotte diverse funzionalità per i clienti:

- Registrazione dei dati sul traffico;
- Blocco/sblocco dell'auto sicuro e più veloce;
- Concessione di accesso temporaneo a un'altra parte;
- Notifiche in tempo reale.

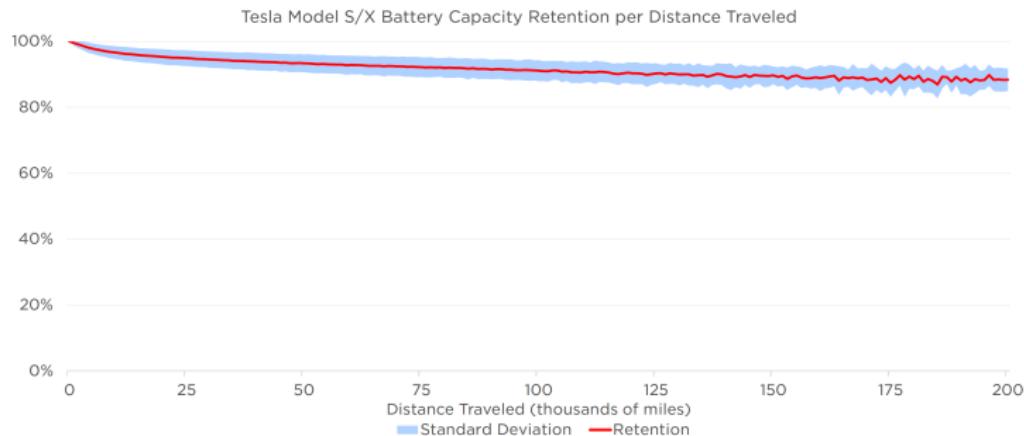
Inoltre, l'integrazione di un Ethereum Virtual Machine (EVM) per l'esecuzione di smart contracts basati su Solidity ha consentito l'implementazione di soluzioni sofisticate e processi automatizzati all'interno dell'ecosistema del veicolo.

La direzione di Tesla nel percorso di adozione della tecnologia Blockchain è quella di incentivare la trasparenza, la tracciabilità e la sostenibilità lungo tutta la catena di fornitura delle batterie.



Nel suo [report](#) annuale del 2020, Tesla ha espresso il suo vivo interesse per lo sviluppo della tecnologia Blockchain attraverso due progetti di collaborazione:

1. Re|Source Blockchain Collaboration for Cobalt;
2. BHP Blockchain Collaboration for Nickel.



Nel 2019 il gruppo Volkswagen ha aderito al Responsible Sourcing Blockchain Network (RSBN), insieme a Stellantis e Ford.

Allo stesso modo, Volkswagen ha collaborato con la società Minespider per puntare alla trasparenza delle **supply chain**. L'infrastruttura è composta da tre layers:

1. contiene informazioni generalmente accessibili;
2. contiene blocchi di dati privati che non possono essere modificati;
3. layer crittografico.

Questo approccio abilita fornitori, subfornitori ed entità responsabili dell'estrazione o del riciclaggio delle materie prime a collaborare e interagire tramite un'infrastruttura condivisa e uno scambio trasparente di informazioni.

A causa della crescita nell'adozione di veicoli elettrici, Volkswagen sta realizzando nuovi sistemi per una mobilità urbana sostenibile, che in futuro sarà sempre più elettrica, connessa, condivisa e autonoma. Ad esempio, grazie alla connettività del servizio [We Connect](#) è possibile gestire tutta una serie di micropagamenti e servizi pay-per-use dal wallet dell'automobile.

Volkswagen sta inoltre testando la blockchain per semplificare i contatti commerciali tra fornitori e i clienti per la ricarica elettrica dei veicoli.

Nel contesto dei contratti di noleggio, la blockchain potrà essere utilizzata anche per verificare in tempo reale il chilometraggio effettuato, lo stile di guida, la diagnostica di bordo e la pianificazione degli interventi periodici in officina.

Infine, il gruppo Volkswagen sta estendendo ulteriormente l'uso della blockchain nelle catene di fornitura dei ricambi, al fine di contrastare l'ingresso di componenti contraffatti nel sistema.

E-voting

Voto Elettronico

Con la locuzione **voto elettronico (e-voting)** si intendono i diversi metodi finalizzati a permettere l'espressione del voto e il conteggio delle preferenze mediante tecnologie elettroniche e informatiche. Questa votazione può avvenire sia in modalità **remota** che in **presenza** attraverso l'utilizzo di apposite macchine per il voto.

In questa presentazione con *voto elettronico* ci riferiremo sempre al *voto elettronico remoto*.

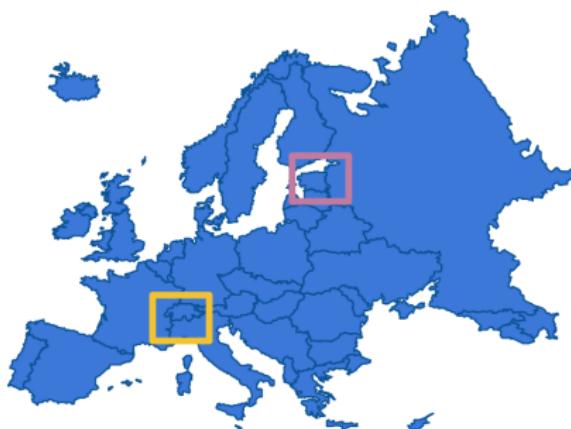
La tecnologia blockchain potrebbe rendere il voto elettronico uno strumento adeguato per la **democrazia del futuro** e aprire delle prospettive di **democrazia partecipativa** attualmente non disponibili.

Voto elettronico

Esistono già delle realizzazioni pratiche di **voto elettronico**.

In Europa, le più note sono:

- Svizzera: **Swiss Post**
- Estonia: **IVXV**



Per quanto riguarda il **voto elettronico via blockchain**, questo è stato già sperimentato da vari paesi tra cui:



- Corea del Sud
- India
- Thailandia
- USA

Voatz è un'applicazione statunitense per il voto elettronico che utilizza la tecnologia **blockchain per memorizzare** i voti e la biometria per identificare gli elettori.

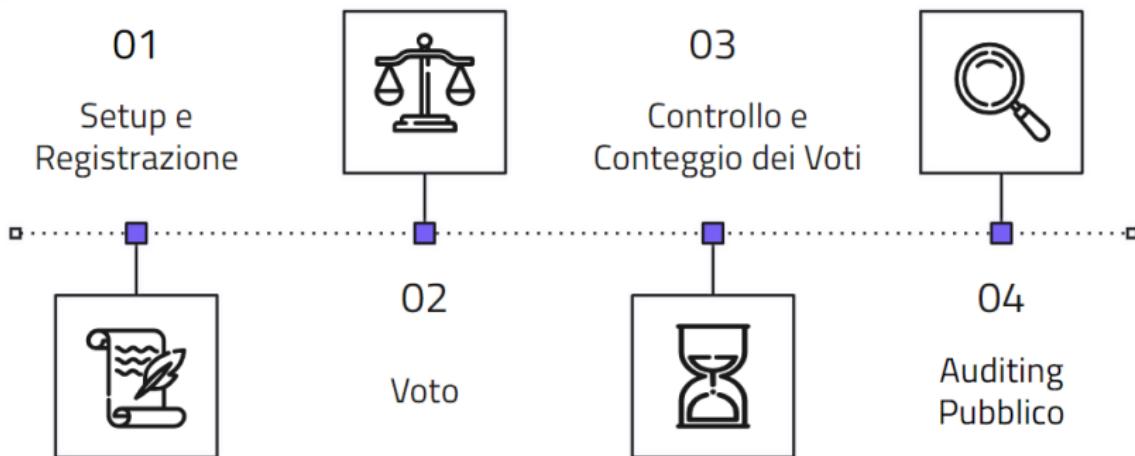
- La blockchain utilizzata è di tipo *permissioned* e costruita su **Hyperledger**.
- L'infrastruttura blockchain comprende 32 nodi ed è distribuita tra i datacenter di Amazon AWS e Microsoft Azure.
- I voti inviati vengono **stampati** su una scheda cartacea (meccanismo utilizzato per il conteggio), e contemporaneamente **memorizzati** sulla blockchain.

Le **motivazioni a favore** dell'utilizzo di un sistema di un voto elettronico sono:

- **Comodità**: si può votare quando si vuole e da dove si vuole;
- **Risparmio**: il voto elettronico è molto più veloce e meno costoso;
- **Estensione del diritto di voto**: può votare chiunque, anche chi è fuori sede o all'estero, o chi ha problemi di mobilità;
- **Partecipazione**: data la maggiore comodità del voto e la riduzione del numero di persone escluse, potrebbe crescere la percentuale dei votanti.

Voto elettronico

Sebbene non esista uno standard, una votazione elettronica può essere divisa nelle seguenti **fasi**:



Al fine di garantire una votazione **sicura**, è necessario che alcune proprietà vengano soddisfatte.

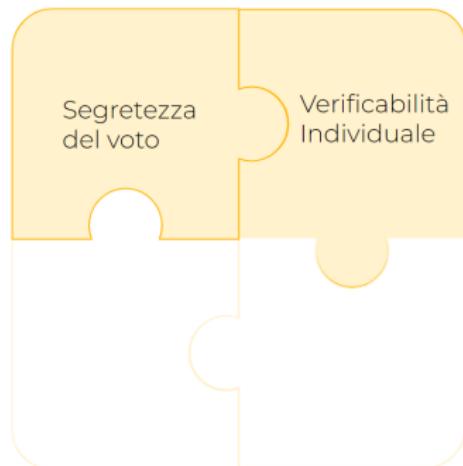
Voto elettronico

La **segretezza del voto** è definita come l'incapacità dell'avversario di distinguere, dati due candidati, per quale l'elettore ha votato.

La **segretezza "perpetua" o "perenne"** è una variante della proprietà di segretezza del voto che richiede che la segretezza del voto venga preservata anche dopo la conclusione della votazione.



Voto elettronico



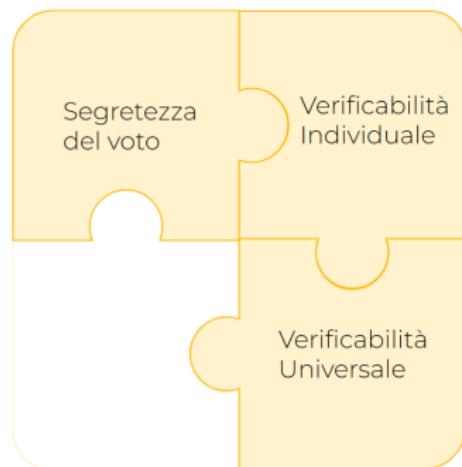
La **verificabilità individuale** è definita a partire da tre proprietà:

- *Cast-As-Intended*
- *Recorded-As-Cast*
- *Tallied-As-Recorded*

Voto elettronico

La **verificabilità universale** richiede che chiunque abbia la possibilità di verificare che le elezioni si siano svolte correttamente.

La **verificabilità di idoneità** richiede che chiunque possa verificare che solo votanti con diritto di voto abbiano inviato un voto valido.



Voto elettronico



La resistenza alla coercizione

richiede che un avversario non possa apprendere alcuna informazione aggiuntiva sui voti inviati rispetto a quelle rivelate dai risultati della tabulazione.

In altre parole, gli elettori non possono dimostrare se o come hanno votato, anche se interagiscono con l'avversario durante il voto.

Vediamo ora un **esempio** di protocollo di **voto su blockchain**.

Gli attori coinvolti sono:

1. Un numero finito di votanti.
2. Due candidati distinti.
3. Due autorità.

Il protocollo di voto è stato sviluppato per una infrastruttura blockchain con le seguenti **caratteristiche**:

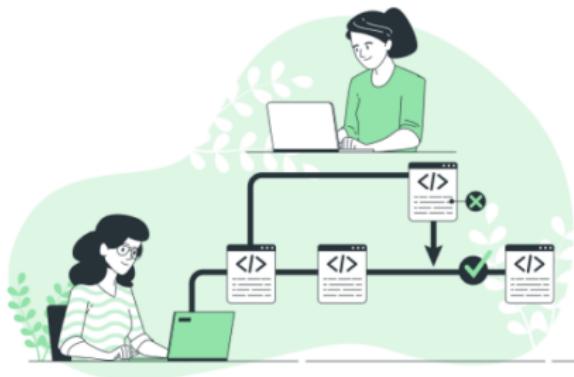
- **Pubblica.** Il contenuto della blockchain è pubblico.
- **Permissioned.** Solo un votante autenticato può votare.
- **Append-Only.** Un utente malintenzionato può solo inserire una nuova transazione ma non è in grado di riordinare, eliminare o modificare le transazioni passate.

Caratteristiche chiave del protocollo:

- **v-token:** token posseduto dal votante e necessario per esprimere la propria preferenza.
- **Votare** vuol dire **spendere** i propri v-token. Un voto è considerato valido solo se tutti i v-token vengono spesi in un'unica transazione a candidati distinti.

Ogni votante ha un numero di v-token pari al numero candidati. Di questi v-token, uno solo è valido, gli altri sono **fittizi ma sono indistinguibili** ad una terza parte.

In fase di conteggio, *i voti inviati con v-token fittizi non vengono conteggiati.*



Setup

Le autorità inizializzano il sistema creando i valori per la generazione dei token.

Voto elettronico

Registrazione

Il votante crea un wallet sulla blockchain e lo registra con le autorità.

Le autorità costruiscono i 2 *v-token* e comunicano all'utente qual è il token valido e quale quello fittizio.

Il votante non riesce a dimostrare ad altri quale sia il *v-token* valido.



Voto elettronico



Voto

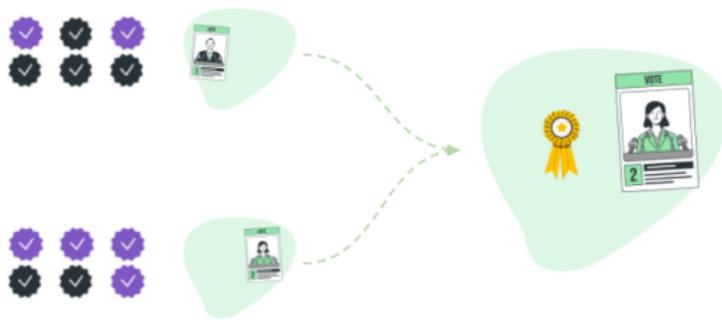
Il votante vota spendendo entrambi i suoi *v-token*.

Il votante riceve una ricevuta della transazione.

Conteggio

Terminata la fase di voto,
i voti vengono processati
dalle autorità.





Conteggio e Controllo di Correttezza

Le autorità pubblicano il numero di voti validi ricevuti da ogni candidato.

Viene fornita una dimostrazione di correttezza dell'elezione.

- **Segretezza del voto.** La preferenza dell'elettore non viene mai rivelata, neanche durante la fase di conteggio.
- **Verificabilità Individuale.** Ogni votante può controllare che il suo voto sia stato acquisito, registrato e conteggiato correttamente.
- **Verificabilità Universale.** Subito dopo la fine della fase di voto, chiunque può contare il numero di voti validi ricevuti da ogni candidato.
- **Resistenza alla Coercizione.** I *v-token* sono indistinguibili: il coercitore non può essere sicuro che l'elettore abbia votato con il *v-token* valido per il candidato scelto.

Voto elettronico - Il Problema del Logaritmo Discreto

Il problema del logaritmo discreto consiste nel trovare, dati due elementi g e h di un gruppo \mathbb{G} , un esponente intero s tale che $g^s = h$.

In alcuni casi questo problema può essere risolto facilmente, ma, scegliendo opportunamente il gruppo, se s non è piccolo diventa un problema praticamente insolubile.

Molte applicazioni, tra cui il voto elettronico, basano la loro sicurezza su questa difficoltà.

Voto elettronico - Schema a Soglia

In molti contesti, è preferibile non permettere ad una singola entità di accedere ad un dato segreto.

Consideriamo uno schema di cifratura asimmetrica: se una singola entità ha accesso alla chiave di decifratura, essa può decifrare tutti i messaggi ricevuti e questo, nel caso specifico del voto elettronico, violerebbe la segretezza del voto.

Per impedire ciò, si può utilizzare uno schema a soglia per la condivisione di un dato segreto, ovvero, un protocollo crittografico che permette di dividere il segreto s in più segreti s_i . In questo modo possiamo far sì che la decifratura sia possibile solo se un numero minimo di autorità collabora.

Gli schemi a soglia aumentano anche la resilienza: un attacco a poche autorità non compromette l'intero sistema.

Voto elettronico - Dimostrazioni a Conoscenza Zero

Una dimostrazione a conoscenza zero (ZKP) è un protocollo crittografico tra due entità, un Dimostratore ed un Verificatore, che permette al Dimostratore di convincere il Verificatore della veridicità di una certa affermazione, senza rivelare nient'altro.

Queste dimostrazioni possono essere:

- *Interattive*. Il Dimostratore e il Verificatore devono essere entrambi attivi durante la dimostrazione.
- *Non-Interattive*. Il Dimostratore pubblica una dimostrazione di veridicità che può essere verificata in seguito in modo indipendente da uno o più Verificatori.

Prima della fase di conteggio.

Prima della fase di conteggio dei voti, i *v-tokens* del votante v_i sono della forma:

$$\left(g^{y_i(x_i+k)}, g^{y_i(x_i+\lambda)} \right)$$

con

- x_i e y_i parametri privati specifici del votante v_i .
- k e λ parametri segreti e comuni a tutti i *v-token*. Definiscono rispettivamente il *v-token* valido e quello falso.

La posizione del *v-token* valido e falso è scelta in modo randomico durante la creazione dei *v-tokens*.

Fase di conteggio.

Nella fase di conteggio, i *v-token* vengono processati dalle autorità inserendo la maschera del candidato a cui vengono inviati.

$$g^{y_i(x_i+k)} \Rightarrow g^{\omega(x_i+k)}$$

Il wallet del candidato Ω , la cui maschera è il valore ω , riceverà un *v-token* per votante (i.e. 3 *v-token*). Moltiplicando il valore dei *v-tokens* ricevuti da Ω otteniamo:

$$\prod_{i=1}^3 g^{\omega(x_i+\sigma_{i,j})} = (g^{\omega k})^{\text{valid}_\omega} (g^{\omega \lambda})^{\text{fake}_\omega} (g^{\omega \cdot \text{sum}})$$

con $\sigma_{i,j} = k$ o λ e $\text{sum} = x_1 + x_2 + x_3$.

Da questa espressione, possiamo facilmente ricavare il numero di voti validi ricevuti da Ω .

Raccolta differenziata e impronta ecologica

Nel campo dell'ecologia, grande spazio è dedicato alla **raccolta differenziata**, in quanto si riesce a dare nuova vita a molti materiali, riducendo allo stesso tempo **l'impronta ecologica** globale.

Le società che si occupano dello smaltimento di rifiuti cercano sempre nuove soluzioni per spingere gli utenti a differenziare correttamente. Un approccio è quello di ricompensare gli utenti con premi ogni volta che si comportano in maniera virtuosa.

Un grande impulso allo sviluppo di questi atteggiamenti costruttivi è dato dall'utilizzo di metodi moderni ed innovativi per la gestione della raccolta punti, e un esempio è dato dalla blockchain.

Programmi di fidelizzazione tradizionali

Attualmente, la maggior parte dei programmi di fidelizzazione tradizionali può essere ricondotta in una delle seguenti categorie:

- **Tessera fedeltà:** ogni qual volta un cliente acquista uno specifico bene o servizio, viene applicato un “timbro” sulla tessera. Quando questa tessera è riempita, il cliente può restituirla e ottenere in cambio un omaggio. Il problema fondamentale di programmi di questo tipo è il supporto cartaceo che viene utilizzato: spesso la tessera viene persa, oppure dimenticata.
- **Raccolta punti:** essi si basano sull'accumulo di punti fedeltà a seguito di alcune transazioni oppure con l'acquisto di determinati prodotti. Il problema di queste tessere è che gli utenti si ritrovano spesso con diverse carte di accumulo punti, facendo poca presa sugli utenti che effettuano acquisti saltuari.

Programmi di fidelizzazione tradizionali

- **Raccolta punti a livelli:** anche in questo caso gli acquirenti accumulano punti in base agli acquisti che effettuano e che potranno poi spendere per richiedere premi. La differenza sta nel fatto che i clienti vengono diversificati in base al livello all'interno del programma di fedeltà nel quale si trovano.
- **Programmi fedeltà con quota d'iscrizione:** per avere accesso a questo tipo di programmi un utente deve pagare una quota d'ingresso, ottenendo in cambio tutti i benefici immediatamente. Questo tipo di stratagemma invoglia gli utenti ad usufruire del servizio ripetutamente in quanto già pagano per esso.
- **Programmi con Cashback:** molti programmi di fidelizzazione di carte di credito prevedono un rimborso periodico di una piccola percentuale di quanto speso direttamente sul proprio conto.

Piattaforme user-rewarding basate su blockchain

I maggiori problemi delle raccolte punti elencate in precedenza sono:

- il numero di possibili raccolte a cui un utente può partecipare;
- la presenza di supporti fisici che possono venire dimenticati o persi;
- la perdita di interesse da parte degli utenti nel proseguire con la raccolta.

Tutti questi problemi hanno visto una soluzione con lo sviluppo della blockchain: dato il carattere immutabile di questa tecnologia, i punti possono essere salvati nel proprio wallet senza ricorrere a supporti fisici se non il proprio smartphone o il pc dove consultare la app relativa.

Applicazioni di questo tipo possono essere usati nel contesto della gestione dei rifiuti. Vediamone alcune.

Recereum (RCM) è una piattaforma Ethereum-based che si pone l'obiettivo di premiare i cittadini che fanno bene la raccolta differenziata, con un innovativo sistema di user-reward che premia con un token chi, al centro di raccolta rifiuti, smista i propri rifiuti in maniera corretta.

L'obiettivo è fare in modo che ogni cittadino possa guadagnare dei soldi per ogni bottiglietta, batteria o pezzo di hardware in maniera completamente trasparente.

Il token RCM deve essere depositato su un wallet apposito, e ogni volta che si conferisce un rifiuto nell'apposita area il wallet va collegato attraverso un indirizzo al cassonetto di riferimento che distribuisce i token.

Questo token può poi essere utilizzato dai cittadini per svariati scopi, tra cui il pagamento delle bollette o la tassa dei rifiuti.

Plastic Bank è una azienda canadese che si occupa di raccogliere la plastica con lo scopo di dargli nuova vita. Il modello di business dell'azienda prevede di remunerare le persone che raccolgono la plastica, per poi trasformare la plastica e rivenderla.

Il ruolo della blockchain è quello di garantire che l'intero processo avvenga in maniera sicura, decentralizzata, immutabile e trasparente. Plastic Bank registra tutti i conferimenti, le rivendite alle aziende manifatturiere e la vendita al dettaglio attraverso transazioni blockchain.

Plastic Bank utilizza Hyperledger Fabric, piattaforma open source sviluppata da IBM. Grazie alla tecnologia blockchain, Plastic Bank è in grado anche di gestire tutti i pagamenti in maniera completamente automatizzata.

RecycleGo è una startup con l'obiettivo di dare trasparenza alla filiera del riciclo dei rifiuti. Questa azienda utilizza software blockchain-based allo scopo di rendere più efficiente il percorso di riciclo dei rifiuti da parte delle aziende.

Tra i servizi offerti, ci sono:

1. Ottimizzazione dei percorsi di raccolta rifiuti ;
2. Compliance automatica grazie alla tecnologia blockchain;
3. Trasparenza lungo tutta la filiera;
4. Possibilità di implementare smart contract tra gli attori della filiera.

Per fare ciò, RecycleGo utilizza Hyperledger Fabric. La blockchain permette a clienti, fornitori, raccoglitori e tutti gli attori della filiera di collaborare in maniera completamente trustless utilizzando smart contracts che permettono di ottimizzare i processi e prendere decisioni più informate.

Troventum è un progetto digitale orientato allo sviluppo sostenibile, che si pone l'obiettivo di connettere ogni partecipante della filiera dei rifiuti attraverso una piattaforma trustless completamente decentralizzata.

Troventum consiste in una serie di moduli implementati sulla blockchain di Ethereum. Uno di questi offre un sistema di rewarding che garantisce ai conferitori di rifiuti una ricompensa in base ai rifiuti conferiti negli appositi contenitori.

Un altro modulo permette invece ai raccoglitori di rifiuti di registrare sulla blockchain il conferimento dei rifiuti, con transazioni ad hoc in base al tipo di rifiuto.

Questo sistema modulare permette di operare in maniera dinamica e integrare tutti i processi che si svolgono lungo la filiera in maniera completamente decentralizzata, sicura e trasparente.

Un possibile modello

L'università di Trento ha progettato una applicazione che ha come obiettivo l'incentivazione della raccolta differenziata per conto di un'azienda italiana. Descriviamo più in dettaglio come funziona.

Gli attori in gioco saranno quattro: **utenti, operatori, partner e l'azienda di riferimento.**

L'architettura prevede tre gruppi di smart contract, nel seguente modo:

- Un primo gruppo di smart contract dovrà permettere il passaggio di token tra l'azienda e gli utenti, nel momento del conferimento da parte degli operatori;
- Un secondo set di smart contract per permettere il passaggio di token tra gli utenti e i partner;
- Un terzo insieme di smart contract tra i partner e l'azienda, per raccogliere i punti e ricompensare i partner che partecipano al programma.

Un possibile modello

L'azienda avrà a disposizione un **wallet**, a cui corrisponde un indirizzo ed una chiave privata, quest'ultima necessaria per poter riscattare il possesso dei propri token.

L'utente che decide di registrarsi al servizio, invece, dovrà in fase di registrazione indicare il **codice RFID** legato ai suoi bidoni. L'utente viene identificato con questo codice, in quanto è sufficiente per segnalare l'avvenuto conferimento da parte dell'operatore.

Ogni utente e ogni partner avranno a loro volta a disposizione un loro wallet, nel quale accumuleranno i token previsti dallo schema come ricompensa.

Gli utenti e i partner verranno registrati anche su uno smart contract, accessibile soltanto dall'azienda.

Un possibile modello

Gli operatori non avranno a disposizione un wallet personale, in quanto non hanno bisogno di possedere token.

Essi, dopo avere appurato che l'utente ha conferito correttamente un rifiuto nel bidone, lo comunicheranno all'azienda, che provvederà a versare la quantità di token prevista nel wallet dell'utente.

Infine, anche l'elenco degli operatori viene memorizzato su uno smart contract.

Flusso delle transazioni

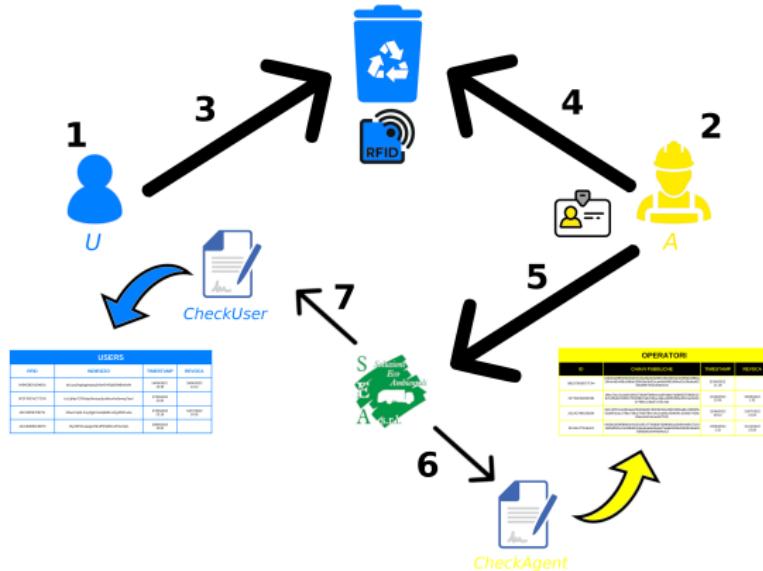


Figure 1: STEP 1: Conferimento dei rifiuti - Tratta operatore-utente

Flusso delle transazioni

Il processo di ritiro del rifiuto e conferimento dei token avverrà nel modo seguente:

- L'utente U espone il rifiuto differenziato correttamente (umido, vetro, carta, etc) nel giorno di raccolta designato;
- L'operatore O ritira il rifiuto e controlla che sia il giorno di raccolta corretto. In caso affermativo, legge con un lettore collegato alla rete il codice RFID del cassetto (che è lo stesso dell'utente);
- L'azienda A riceve la richiesta di inviare i token tramite una transazione da parte di O ;
- A invia quindi questa transazione ad uno smart contract, che controlla la presenza di U all'interno del database;
- Se tutto è corretto, A autorizza il pagamento.

Flusso delle transazioni

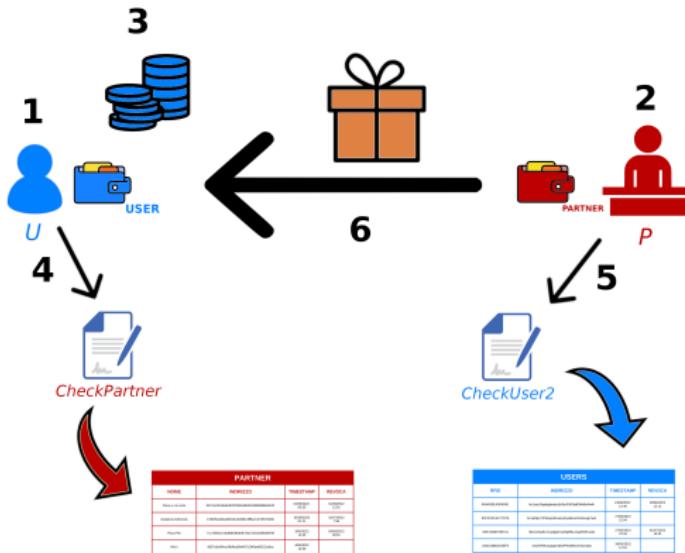


Figure 2: STEP 2: Tratta utente-partner

Flusso delle transazioni

Il riscatto della premialità può avvenire per esempio nel seguente modo:

- Quando U ha raggiunto la quantità di token t necessaria al riscatto del premio a cui è interessato, si reca dal partner P per ottenerlo;
- U effettua una transazione verso uno smart contract che controlla se P è iscritto al database;
- Contemporaneamente, P controlla se l'utente U è iscritto nel database, e che possegga almeno t token;
- Se i check passano, viene effettuata una transazione per l'importo t , chiamando un ulteriore smart contract. P fornisce a U il bene o servizio scelto come premio.

Flusso delle transazioni

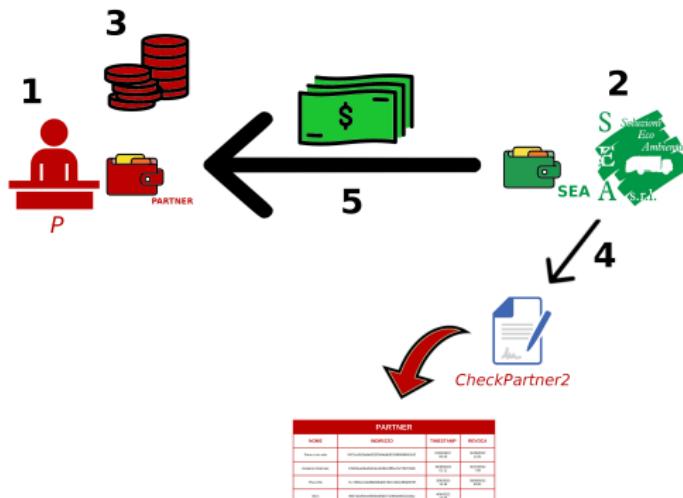


Figure 3: STEP 3: Tratta partner-azienda

Flusso delle transazioni

In questa tratta, infine, viene descritto lo scambio di token tra i partner e l'azienda.

A invia una transazione allo smart contract per verificare che P sia veramente iscritto al database e, se il check passa, lo ricompensa in base agli accordi presi.

Alla conclusione di questo flusso, A ha ricevuto indietro un certo numero di token dal partner P . Questi stessi token potranno poi di nuovo essere utilizzati per ricompensare gli utenti che effettuano la raccolta differenziata correttamente, iniziando un nuovo ciclo di scambio di asset crittografici.

Impronta ecologica

Nel corso degli ultimi anni, la Commissione Europea ha definito varie azioni contro i problemi causati dal cambiamento climatico. Tra le tante, è necessario ottimizzare la gestione dei rifiuti solidi urbani all'interno di tutto il territorio europeo.

Recentemente sono stati compiuti molti studi sulla gestione dei rifiuti solidi urbani. La metodologia più utilizzata per calcolare le emissioni dei gas a effetto serra è nota come **Life Cycle Assessment**.

Essa permette di valutare, per ciascuna tecnologia utilizzata, il loro effetto in termini di cambiamento climatico, tramite il calcolo dell'**impronta ecologica** (EF).

Impronta ecologica

Per abbassare l'impronta ecologica è importante incentivare sia i cittadini sia gli operatori. Un possibile metodo è l'incentivazione tramite token crittografici, gestiti da una blockchain.

La blockchain può essere utilizzata per memorizzare vari dati provenienti dalle tre fasi di raccolta, trasporto e smistamento, come per esempio il chilometraggio, il peso trasportato da un camion o la percentuale di rifiuti riciclati in modo corretto.

Questi dati possono essere utilizzati sia per vedere quanto varia l'impronta ecologica (per esempio, mese per mese), sia per premiare gli operatori che hanno inserito i dati.

Impronta ecologica

Esistono progetti che utilizzano la tecnologia blockchain e che hanno come obiettivo la riduzione delle emissioni. Un esempio è dato da [ClimateTrade](#).

Esso consente alle grandi multinazionali di ridurre l'impronta di io, grazie all'uso di API e della crittografia. La tecnologia garantisce sia un consenso, sia regole chiare tra i fornitori, e si può utilizzare per incoraggiare i fornitori stessi.

L'utilizzo di strumenti come la blockchain per combattere contro il cambiamento climatico è consigliato anche dalla Commissione Europea. La blockchain è uno strumento potente che può migliorare significativamente la trasparenza e la tracciabilità delle emissioni di gas serra.

Inoltre, è possibile individuare in modo chiaro i contributi che i singoli attori apportano per ridurre l'impronta di io.

Decentralised Identifiers

L'identità digitale è [...] la rappresentazione virtuale dell'identità reale utilizzabile durante interazioni elettroniche [...]

L'identità digitale deve dunque contenere tutti i **dati** e tutte le **informazioni** che siano necessarie a identificare un individuo, tra cui anche:

- Patenti;
- Certificati;
- Etc.

Sarebbe inoltre auspicabile avere completo controllo su queste informazioni e su chi vi può accedere.

Proprietà attese

Un buon metodo di identificazione *dovrebbe* soddisfare i seguenti requisiti:

1. Sia ottenibile velocemente;
2. Sia sempre disponibile;
3. Ne sia possibile verificare l'autenticità;
4. Sia utilizzabile per quanto più tempo possibile;
5. Sia sotto il controllo del proprietario.

A queste proprietà possiamo poi aggiungere anche le generica richiesta che il metodo sia sicuro.

Metodi di identificazione

Attualmente possiamo affidarci a svariati metodi per identificarci (sia *online* sia *offline*) tra cui:

- **Documenti fisici** (cartacei e tessere);
- **Email/password**;
- **SSO** (*Single Sign On*).

Questi metodi garantiscono le proprietà sopra menzionate?

- Ottenibili velocemente? **No**
- Sempre disponibile? **Sì**
- È possibile verificarne l'autenticità? **...**
- Longevo? **Sì**
- Sotto il controllo del proprietario? **...**

NB: È sempre possibile fare una copia di un documento fisico.

Email e password

- Ottenibile velocemente? **Sì**
- Sempre disponibile? ...
- È possibile verificarne l'autenticità? **No**
- Longevo? ...
- Sotto il controllo del proprietario? **No**
- Sicuro? **No**

NB: *Password burden*, legata al numero crescente di credenziali da gestire per accedere a servizi diversi.

- Ottenibile velocemente? **Sì**
- Sempre disponibile? ...
- È possibile verificarne l'autenticità? **Sì**
- Longevo? ...
- Sotto il controllo del proprietario? **No**

NB: Necessaria talvolta l'iscrizione a molteplici *service provider*.

Cos'è una DID - I

Per risolvere i problemi sottolineati in precedenza possiamo considerare di definire un'identità digitale all'interno di una *blockchain*, cosicché tale identificativo sia:

- Facilmente generabile e sempre disponibile;
- Globalmente unico e valido;
- Crittograficamente sicuro.

Un tale costrutto viene chiamato *Decentralized Identifier (DID)*.

NB: I DID non forniscono alcun tipo di informazione riguardo al soggetto in questione.

Cos'è una DID - II

I DID sono usati in combinazione con le cosiddette *Verifiable Claims* (**VC**) che consentono la trasmissione delle informazioni necessarie a soddisfare una richiesta. Tali informazioni sono condivise cifrate (e.g. *digital signatures*, ZKP) sulla base di:

- La VC in questione;
- Il soggetto di tale DID/VC;
- Colui che ha generato la VC.

NB: Per semplicità d'ora in avanti identificheremo i DID con le identità digitali.

Proprietà di una DID

Essendo immerso in una *blockchain*, ogni DID ha intrinsecamente le seguenti proprietà:

- Elimina la necessità di un'autorità centrale e il problema del *single point of failure*;
- Massimo controllo sui propri dati e sulle proprie informazioni (*privacy compresa*);
- Consente di emettere prove crittografiche dell'autenticità della DID;
- Vasta interoperabilità grazie alla sempre maggiore integrazione delle *blockchain* nei servizi di uso comune.

Struttura di una DID

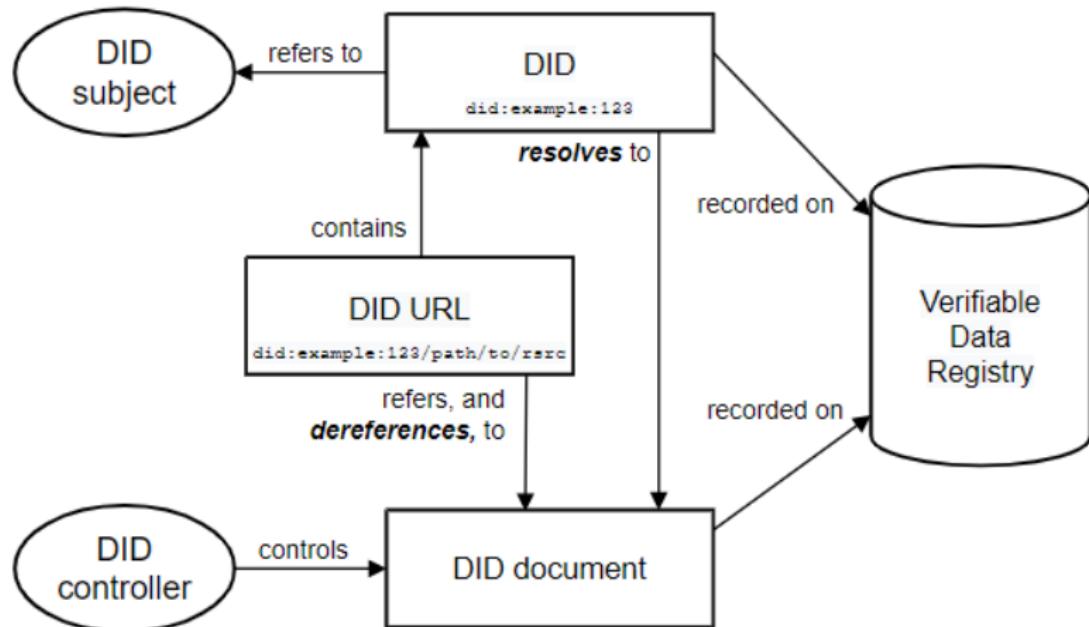


Figure 4: Struttura di un'architettura DID. Per una descrizione più dettagliata si veda w3.org/TR/did-core/.

Applicazioni della DID

Alcuni esempi di uso di DID:

- eIDAS;
- The & company;
- Fractal ID;
- Heirloom.

Charity

What is Ripple?

- From Wikipedia, “*Ripple is a real-time gross settlement system, currency exchange and remittance network... created by Ripple Labs Inc.*”;
- Different story with respect to Bitcoin (OpenCoin);
- Its Ledger is not properly a Blockchain;

XRP LEDGER

Cryptocurrencies ▾		Exchanges ▾	Watchlist	
Rank	Name	Symbol	Market Cap	Price
1	Bitcoin	BTC	\$522,322,017,161	\$26,768.71
2	Ethereum	ETH	\$185,758,419,048	\$1,544.71
3	Tether USDT	USDT	\$83,478,899,633	\$0.9995
4	BNB	BNB	\$31,574,243,412	\$205.23
5	XRP	XRP	\$25,660,094,405	\$0.4802
6	USDC	USDC	\$25,078,081,797	\$0.9999

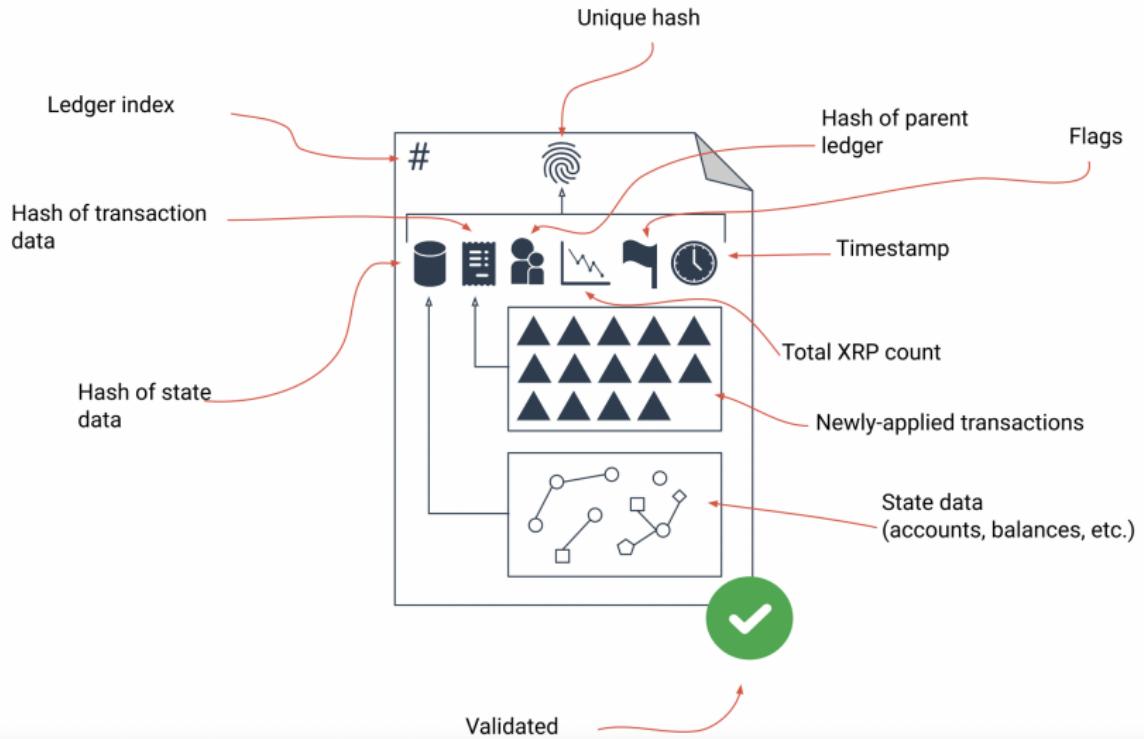
Main Characteristics

- Transactions are validated through consensus;
- Fast and efficient;
- “Limited” number of Ripple;
- Exchange between other currencies;

Structure

- Big Ledger;
- “*decentralized cryptographic ledger powered by a network of peer-to-peer servers*”;
- Is a “public permissioned” blockchain;
- Only validated operations can modify the ledger;
- The operations are validated by servers called *Rippled*.

XRP LEDGER



Transactions

- Only transactions can modify the Ledger;
- Any transaction has cost (*fee*) in XRP;
- Also failed transaction are taxed with the fee;
- Transactions are characterized by digital signatures between parties.

Fees

- Ripple and Ledger have a fee to create (and validate) transactions;
- Fees are immediately destroyed;
- They grow with the growth of the network;
- The fee is specified into the transaction ;
- The standard is 0.00001 XRP (10 drops).

XRP LEDGER

```
Response(status=<ResponseStatus.SUCCESS: 'success'>, result={'Account': 'rKA3LZLs3nE61GcXdd3itQUa9UDkMup4d7', 'Amount': '22000000', 'Destination': 'rPT1Sjq2YGrBMTttX4GZHjKu9dyfzbpAYe', 'Fee': '10', 'Flags': 0, 'LastLedgerSequence': 42086992, 'Sequence': 42086948, 'SigningPubKey': 'ED8EC4DCB6EDCE0AE613B7F1D372DC28F74CC5C523A92D0491861175CFA8EF57AB', 'TransactionType': 'Payment', 'TxnSignature': 'D57E64576399C9CB7F20BFD9589C079F5D7E94221898026D77E24D55A02AC4C4C0FB34AF1B2A79A5DF5537C28D8DC8981DFC90D3B5758680FFFDFE86E19DB402', 'ctid': 'C282323E00070001', 'date': 750764160, 'hash': '6C5A0D92779AF1A923DA33BFAA350C5C3E970EF0091BC698914C2B0FE20C482E', 'inLedger': 42086974, 'ledger_index': 42086974, 'meta': {'AffectedNodes': [{ModifiedNode': {'FinalFields': {'Account': 'rPT1Sjq2YGrBMTttX4GZHjKu9dyfzbpAYe', 'Balance': '81743487061016025', 'Flags': 0, 'OwnerCount': 0, 'Sequence': 6773975}, 'LedgerEntryType': 'AccountRoot', 'LedgerIndex': '31CCE9D28412FF973E9AB6D0FA219BACF19687D9A2456A0C2ABC3280E9D47E37', 'PreviousFields': {'Balance': '81743487039016025'}, 'PreviousTxnID': '34728FDFAAFA1B9842D5D77656DB0D299D3526EE066DDFDEC94546FD643057A3', 'PreviousTxnLgrSeq': 42086967}], 'ModifiedNode': {'FinalFields': {'Account': 'rKA3LZLs3nE61GcXdd3itQUa9UDkMup4d7', 'Balance': '9977999990', 'Flags': 0, 'OwnerCount': 0, 'Sequence': 42086949}, 'LedgerEntryType': 'AccountRoot', 'LedgerIndex': '5667BE04ADB5FEA20AD9730C9CF175266ED27A959AB8ADCA0595D36608CA5B59', 'PreviousFields': {'Balance': '10000000000', 'Sequence': 42086948}, 'PreviousTxnID': '7B4410158601F4F4FA0A6DA67C2D40FF8164361324DE5C525EC3B81DF954A9B5', 'PreviousTxnLgrSeq': 42086948}}], 'TransactionIndex': 7, 'TransactionResult': 'tesSUCCESS', 'delivered_amount': '22000000', 'validated': True}, id=None, type=<ResponseType.RESPONSE: 'response'>)
```

Differences with Bitcoin

- Security:
 - Bitcoin uses the Proof of Work;
 - Ripple uses Validation Servers
- Transaction speed:
 - Bitcoin validates operations every 10 minutes;
 - Ripple validates transactions in few seconds;
- Privacy: in both systems one can retrieve user identities through transactions;
- Decentralization:
 - Bitcoin can be centralized by entities having 50% of the nodes (unfeasible);
 - Ripple Labs have most of the servers → centralized **de facto**.

XRPL CHARITY

DELFT XRP HACKATON 2023



XRPLCharity



Challenges

Solution

Clarity brings value to charity

Challenges faced by charities today

Approximately only 71-90 % of the donations actually go to the charity work

source: [/ \(2023\)](#)





Administrative costs for
charities

If we don't have accurate data
how do we improve?

There is a wide gap between
90% and 71%.

How Nonprofits Get Really Big

- Since 1970, over 200,000 U.S. nonprofits have emerged, but just 144 reached \$50 million in yearly revenue.
- There is no transparent accountability in charities, which can lead to mission drift.
- Mission drift won't help with already existing budget inefficiencies.
- Source: https://ssir.org/articles/entry/how_nonprofits_get_really_big

Let the tech track

- Donators can track the movement of funds and ensure they are being used for their intended purposes
- The NFT is minted when a charity lists a project on our platform
- Live status of all the charity projects
- When the target amount is reached:
 - The funds will automatically transfer to the pre-specified retailer
 - The NFT is burned
 - The project will close itself for new funds

XRPL CHARITY: HOME

Pages / Home

Home

Search... AV

-  Home
-  Charities
-  Retailer
-  Sign In
-  Add Charity



XRPL CHARITY: SIGN IN

[Back to Home Page](#)

Sign In

Sign in with just one click with GemWallet now!



Sign In

or



Sign in as a Retailer

Do not have a GemWallet? [Join GemWallet now!](#)



XRPL CHARITY: PROFILE

Pages / Retailer

Retailer

Search... 



Amazon
Retailer

5 Open Charities 57k Total donations 27 Previous charities

Open Charities

NAME	COMPLETED	DATE	DONATED FUNDS
Books for first graders	✓ Completed	04 Jul 2023	<div style="width: 100%;"><div style="width: 100%;"></div></div>
Food for abandoned gods	✗ Collecting Funds	1 Jun 2023	<div style="width: 100%;"><div style="width: 100%;"></div></div>
Tents after the earthquake	✗ Collecting Funds	22 Jul 2023	<div style="width: 100%;"><div style="width: 100%;"></div></div>

alhest-3000/horizon-ui-chakra#

XRPL CHARITY: ADD CHARITY

The screenshot shows a web-based application for adding a new charity. At the top right, there is a breadcrumb navigation "Add Charity / Pages" and a main title "Add Charity". On the left side, there is a user profile icon with "AV", a notification bell icon, a search icon, and a search bar with the placeholder "...Search". The main content area has a heading "Add new charity". Below it are four input fields, each with a label and a required indicator (*). The first field is for "Location", the second for "Description", the third for "Category", and the fourth for "Total Amount". Each input field is represented by a large, light-blue rounded rectangle.

Add Charity / Pages

Add Charity

...Search

AV

Location *

Description *

Category *

Total Amount *

XRPL CHARITY: CHARITIES & DONATION

Charities

Explore charities:



Tap Water for Everyone

Africa
Tap Water

Amount needed: 1000000
Amount left: 999950.000102
Charity Address:
rDoNaTEAYnFQCQYdg6UP3WkVmLtq7HAMrHf
Retailer: Infrastructure
Retailer Address:
rakpXz6bfWvTEyFD6w3mQmulbWDz5lxNHy



Food for abandoned dogs

Brazil
Animals

Amount needed: 20000
Amount left: 19750.000022
Charity Address:
rhELP7Xtb65MjGzp3a5W39a5NsZDSq5gWK
Retailer: Pet Shop
Retailer Address:
rB2fLhDLZQyaM5T58mVz89d4KnuMiwpml6Q

Tap Water for Everyone
Retailer: Infrastructure
Retailer address:
rakpxF6pTqIEFD6w3mQmubWdZ5tNhlyQ
Total amount needed: 999950.000102
Charity address:
rDoNaTEAMfQCQYdg6UP3WkVmLtq7HAMrH

Enter amount

Dhali

Web3 API Authentication

David Simmons & Robbie Daniels
Co-Founders
Dhali



APIs power the world

Web2 API authentication

Web3 API authentication

Introduction



What are APIs?

“Application programming interfaces”

Rules for how to communicate

Powers the internet

HTTP APIs most common for internet



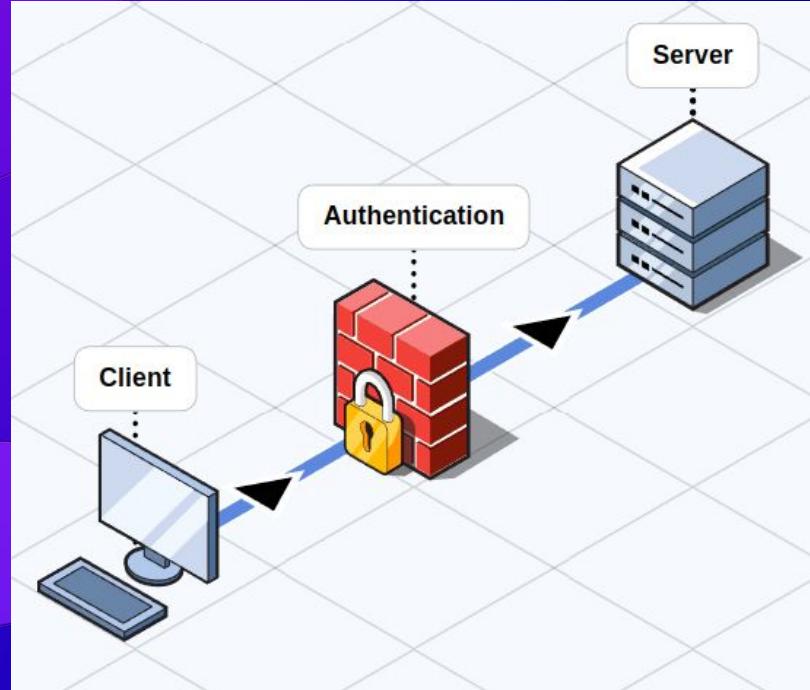
What are APIs?

Sometimes open

Free! 😊

Other times closed!

Needs registration, logins,
data harvesting, or
subscriptions 😢



What are APIs?

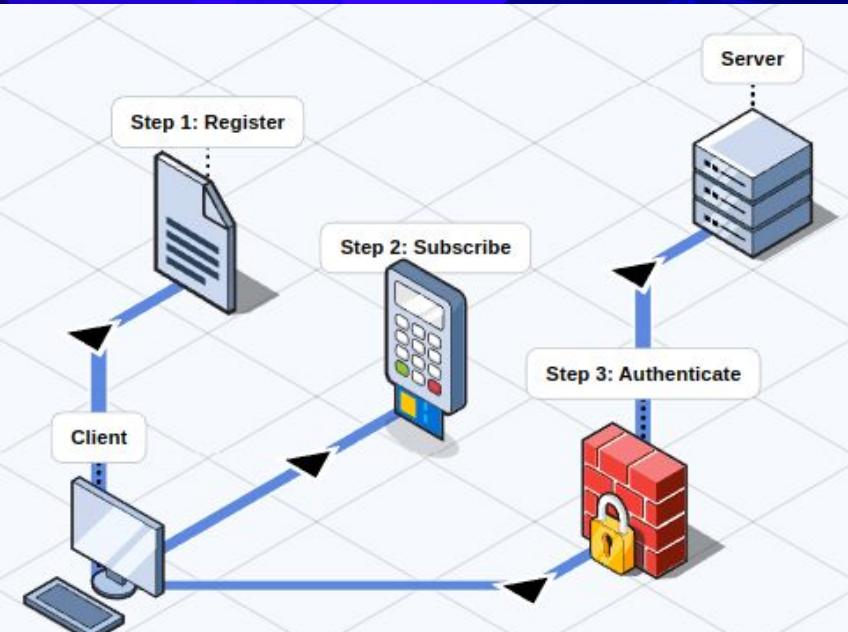


If an API is closed

Authentication is required!



Standard authentication for paid APIs



Step 1: Give your personal details

Step 2: Give your payment details.
Bulk pay

Step 3: Access



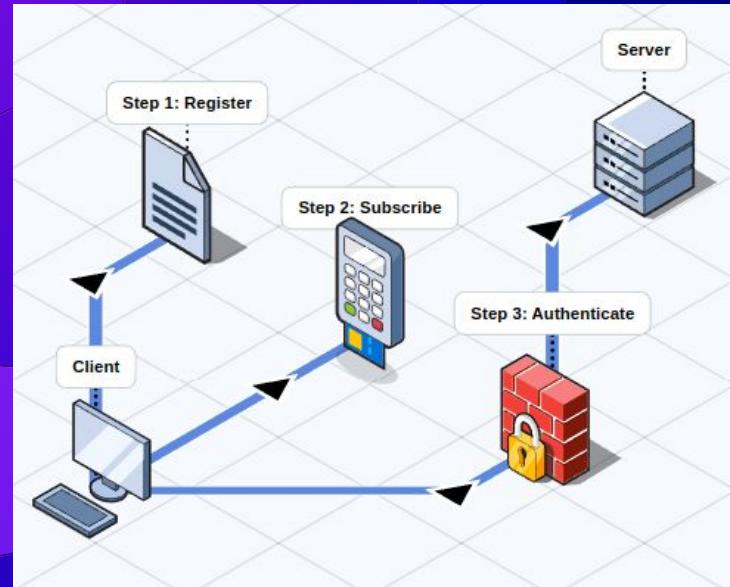
WHY!?



Payments are inefficient!

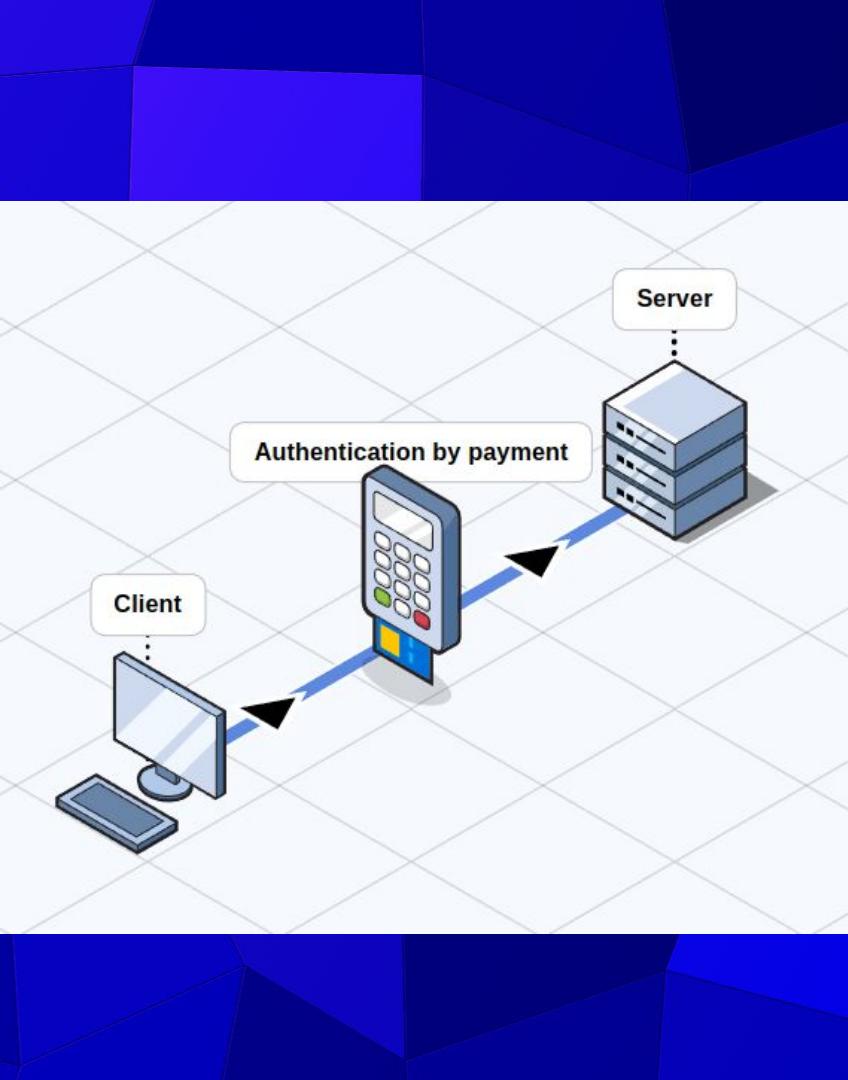
Step 1: Your data is harvested

Step 2: You're required to bulk pay



Blockchain powered APIs

3 steps become 1!



**No secret
management on API
user's behalf**

**API owners require
less supporting infra**

Reduced security risk

“Authentication by Payment”



How?

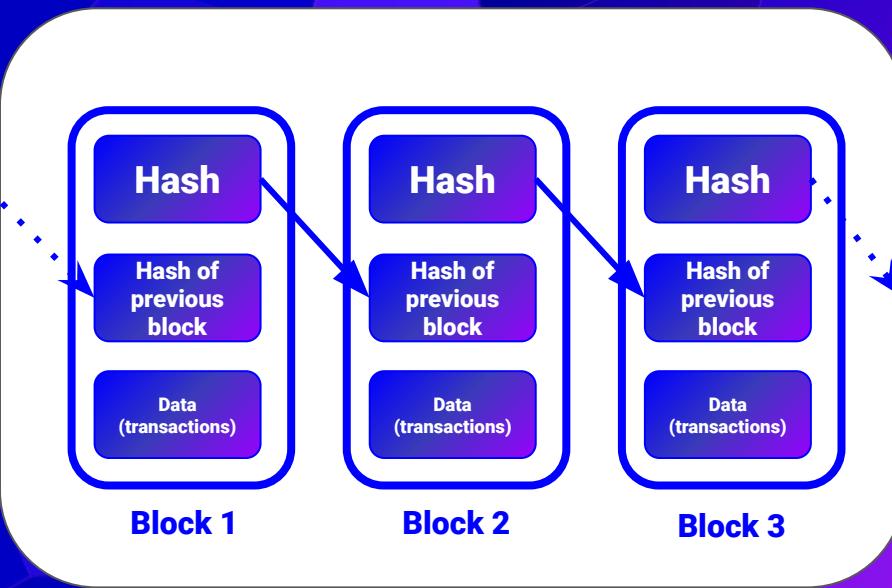


Blockchains

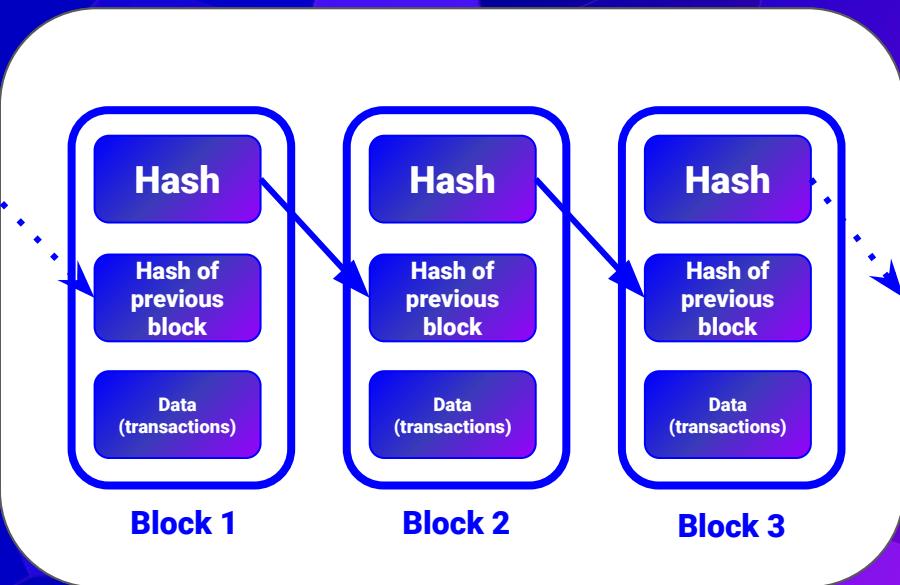
A chain of blocks

Solves the "double spend problem

Each block represents a ledger state



Blockchains



Proof-of-work (PoW)

Power from compute

Proof-of-stake (PoS)

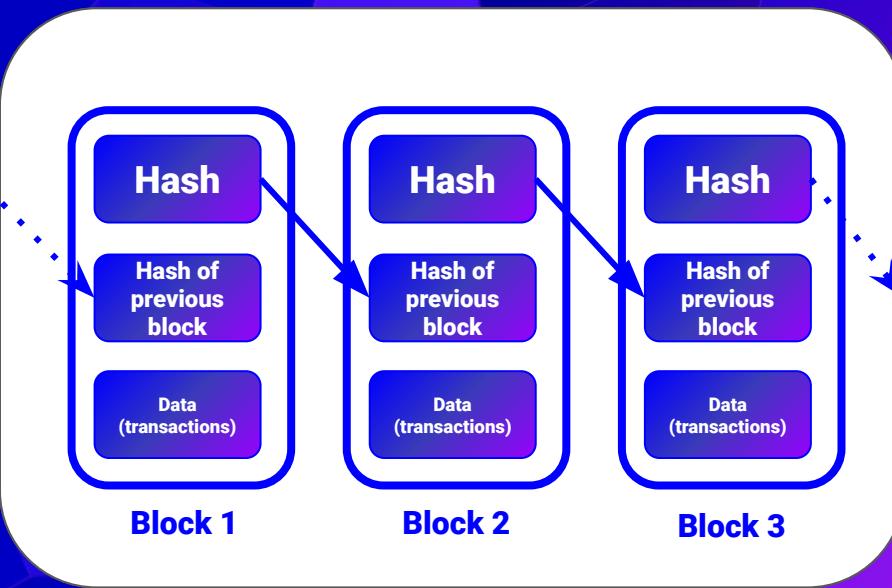
Power from wealth

XRPL consensus

Power from trustworthiness



Blockchains



Proof-of-work (PoW)

Power from compute

Proof-of-stake (PoS)

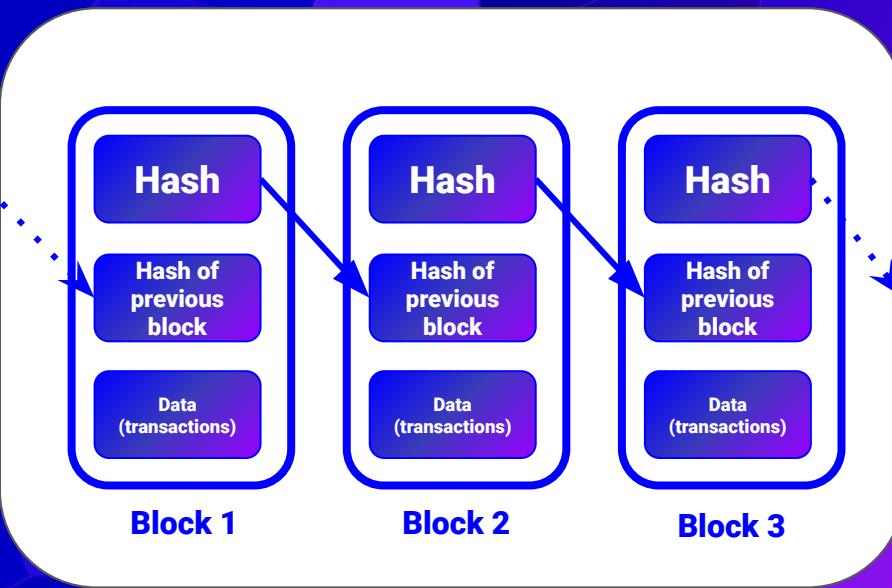
Power from wealth

XRPL consensus

Power from trustworthiness



Blockchains



Proof-of-work (PoW)

Power from compute

Proof-of-stake (PoS)

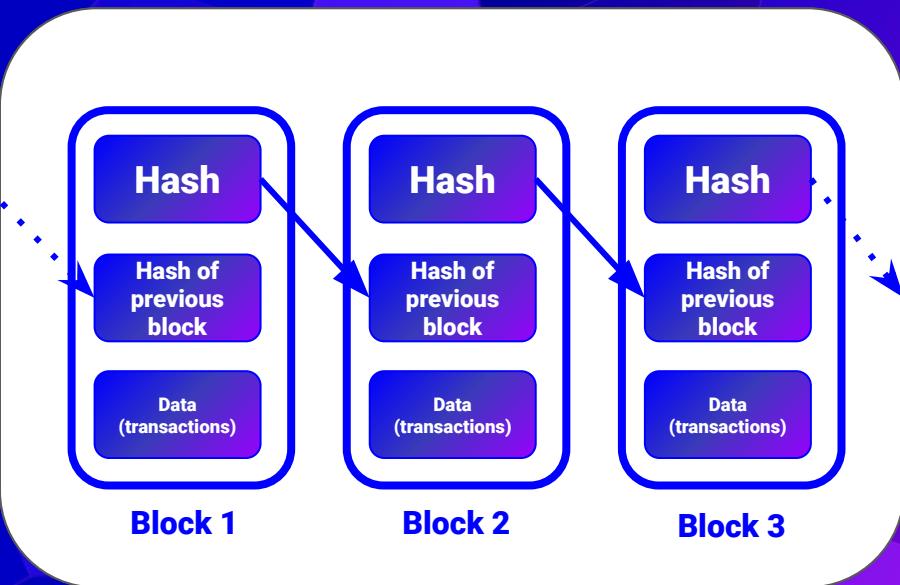
Power from wealth

XRPL consensus

Power from trustworthiness



Blockchains



Inefficient

Expensive

Slow



Solution

Accumulate transactions off-ledger

Submit cumulative transactions less often



Payment Channels

Keep costs low

Secure and off ledger

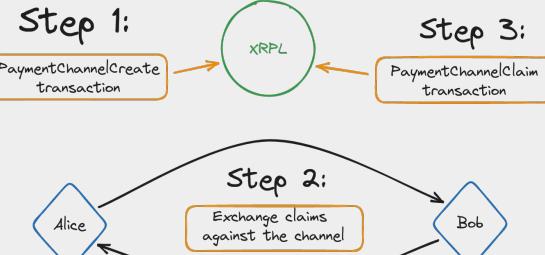
Check out: “Advanced Payment Features of the XRPL”



A shared locked box of money



Payment Channels



The transaction flow



Payment Channels

Step 1:
PaymentChannelCreate transaction

Step 3:
PaymentChannelClaim transaction

XRPL

Step 2:
Exchange claims
against the channel

Alice

Bob

Blockchains enable
authentication-by-payment

Embed payment claims into request
headers

Authenticate the claim



What else do we do?





We use NFTs!



NFTs

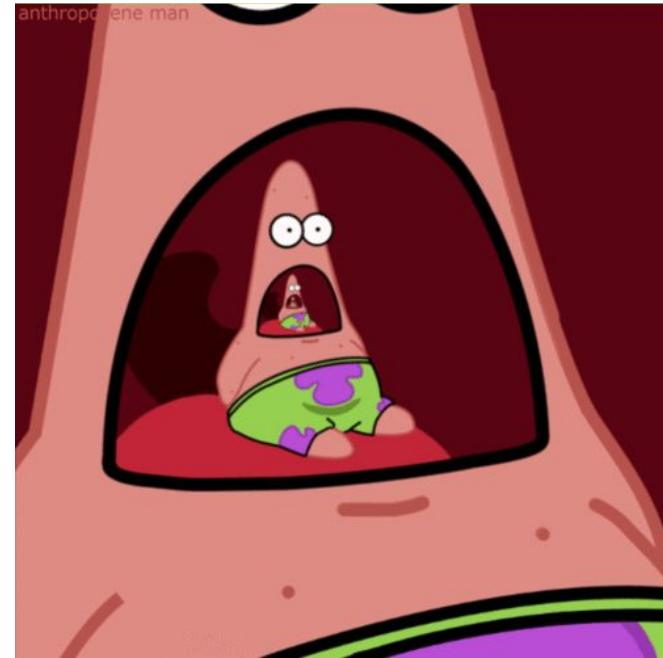
Transparency for buyers and sellers

Transact on a global, open market

Simplified software asset sales



**But wait,
there's
more...**



NFTs

They improve
security!

**Users choose wallet
provider**

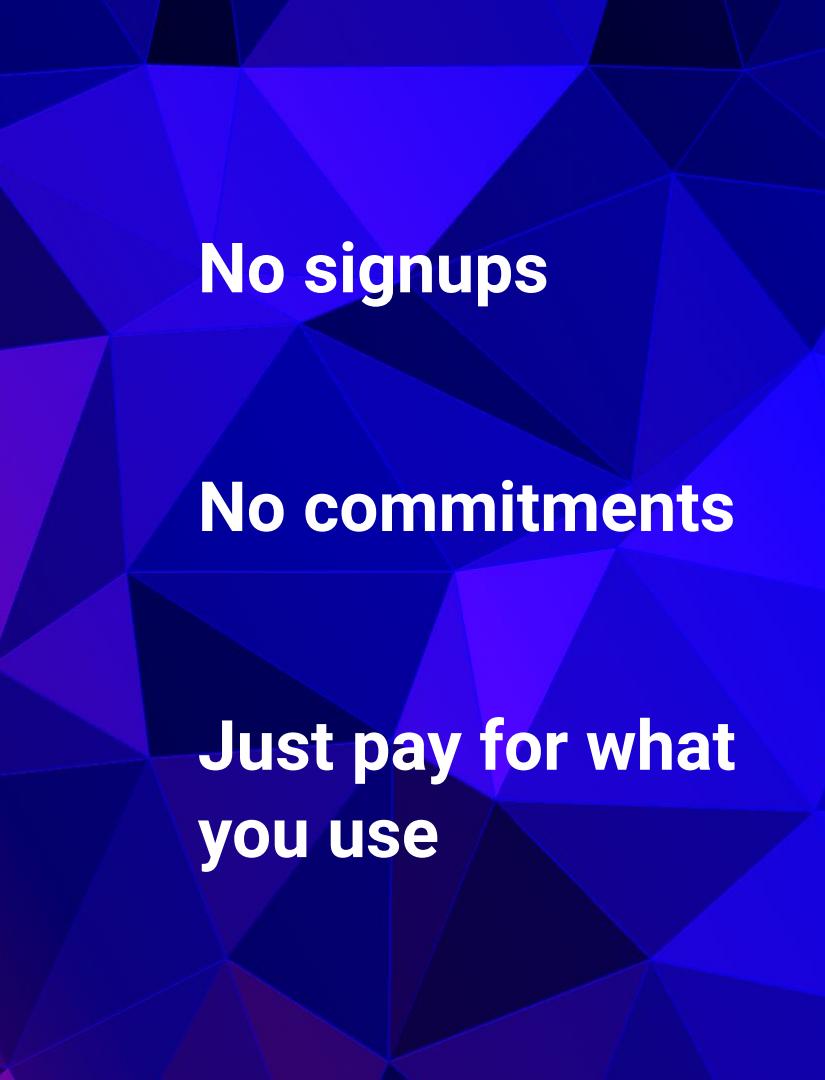
**Dhali just inspects the
XRPL**

**Dhali not involved in NFT
transactions**



“The Web3 approach”





No signups

No commitments

**Just pay for what
you use**

Web3

“It’s like going into a supermarket”



Web 2.0 vs Web3

Web 2.0

- Need to be banked
- Registration and OAuth
- Deal with costly payment provider (e.g., PayPal)
- Lock-ins, subscriptions, opaque charges

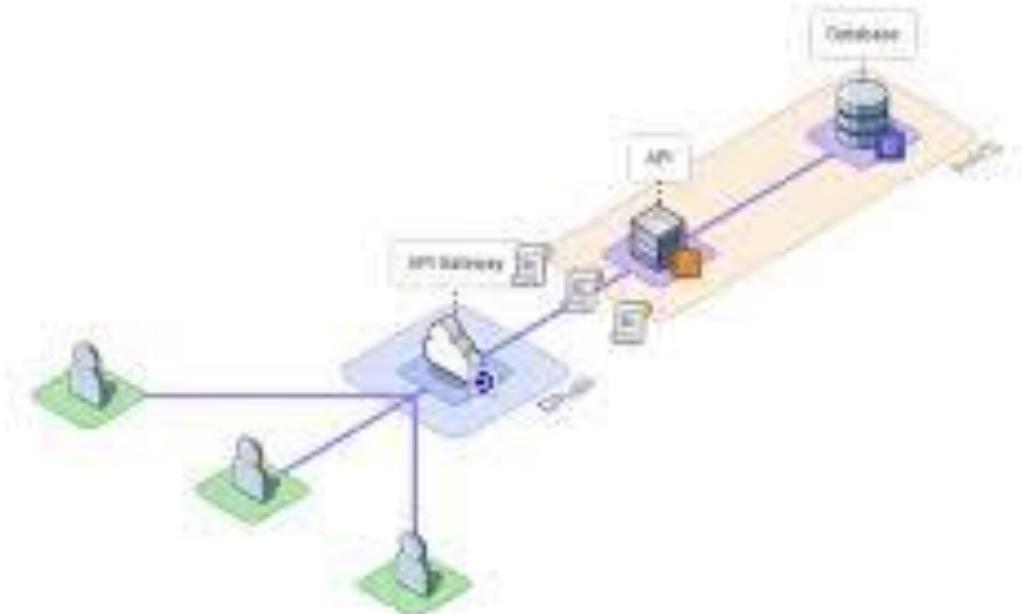
Web3

- Have a funded crypto wallet
- Flexible, on-demand systems
- Transparent, publicly auditable charges



Our project: Dhali









Thanks!
← - - - Scan me

Contact:

Twitter: @dhali_io

Email: info@dhali.io

Discord

