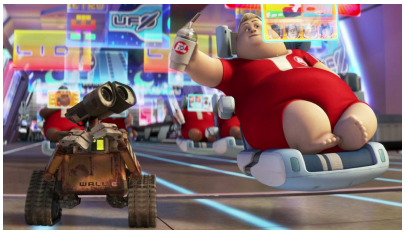
BLOCKCHAIN E NUOVE TECNOLOGIE

Una scuola superiore decide di organizzare un evento per parlare ai ragazzi dei pericoli a cui potrebbero incorrere con l'abuso di social network, intelligenze artificiali e nuove tecnologie. Per farlo decide di analizzare e discutere insieme ad esperti addetti al lavoro nel settore tecnologico e sociologi rinomati, due film d'animazione come WALL-E di Andrew Stanton e Ghost in the Shell di Mamoru Oshii. In contrapposizione a queste realtà distopiche presentate nei film, la scuola istituisce una raccolta fondi sfruttando una nuova tecnologia d'avanguardia che se ben usata può invece portare dei benefici attraverso un sistema paritario, sostenibile e utile: la **blockchain**.



BLOCKCHAIN

É una particolare tecnologia basata su un database condiviso e distribuito tra più nodi, supportato da codici crittografici che rendono le transazioni che vengono registrate praticamente impossibili da modificare o alterare.

Oggi viene utilizzata in molti modi: per registrare processi industriali, supportare criptovalute o sviluppare (come nel caso di questo progetto) smart contract.

Ma perché puntare sulla blockchain come tecnologia del futuro? Ci sono svariati vantaggi nel suo utilizzo rispetto ai modelli basati su sistemi tradizionali: quello che sicuramente salta subito all'occhio è la mancanza di una "terza parte", come può essere una banca, un notaio, o un'intera azienda che si occupa di archiviazione e registrazione di dati.

Pensiamo per esempio al mondo degli scambi di denaro: effettuare un pagamento tramite bonifico in euro significa affidarsi ad un istituto di credito al quale bisogna riconoscere una commissione, cosa che con bitcoin non avviene in quanto la buona riuscita passa attraverso un complesso processo algoritmico di decriptazione di un codice chiamato **hash**, che si genera ogni

qualvolta viene inizializzata una transazione. L'intera rete di nodi lavora simultaneamente fino a quando un minatore non riesce a trovare l'hash corrispondente a quello target. Da quel momento il blocco (una sorta di libro mastro contenente un certo numero di transazioni) viene *validato* e inserito nella blockchain. Questo processo riduce ai minimi termini il rischio di incorrere ad errori umani in quanto anche solo un singolo device dovesse commettere un errore computazionale, ci sarebbero altre migliaia di computer che non riconoscerebbero la transazione evitando di validarla.

Un beneficio strettamente collegato alla mancanza di intermediari è appunto la considerevole riduzione dei costi che si manifestano sottoforma di commissioni. Inoltre, anche gli intermediari hanno diritto a dei giorni di riposo: considerando che un bonifico ha bisogno di almeno un giorno lavorativo per essere preso in carico e completato, effettuandolo venerdì mattina dovrei aspettare fino a lunedì affinché il beneficiario lo riceva.

La decentralizzazione (più copie identiche della stessa informazione sono visibili all'interno della blockchain da migliaia di dispositivi diversi) porta ad un'impossibilità di manomettere il dato che viene registrato.

Questi sono solo alcuni dei vantaggi che la blockchain può apportare alla società.

SMART CONTRACT

I cosiddetti contratti intelligenti (termine coniato dall'informatico americano Nick Szabo) sono i programmi fondanti della rete Ethereum. Sono dei contratti automatizzati, decentralizzati e pubblici. Che differenze con i normali contratti redatti da notai o altre istituzioni competenti? La mancanza di intermediario rende lo smart contract totalmente affidabile, oltre ad essere contenuto nella blockchain e quindi le sue clausole non possono essere modificate da nessuno, si basa sul principio del "se questo, allora quello". Prendiamo ad esempio alcune clausole di questa raccolta fondi: la donazione di Ether è consentita solo se l'importo è maggiore di 0. Se questa ipotesi è verificata allora in modo totalmente automatizzato viene depositata la donazione. "Solo il manager della raccolta fondi può prelevare l'importo": provando a selezionare un indirizzo diverso da quello del manager, il contratto rende impossibile prelevare il saldo.

Essendo incastonato all'interno della Blockchain lo smart contract è per definizione pubblico e distribuito su tutti i nodi della rete, questo permette in qualunque momento di verificare i dettagli di una transazione. Tutti i dettagli tranne l'identità delle persone coinvolte: essendo Ethereum un rete basata su codici criptati, la privacy viene salvaguardata.

ETHEREUM, UNA BLOCKCHAIN ECOSOSTENIBILE

Ethereum è passato da un meccanismo di consenso proof-of-work (PoW), quello su cui si basa bitcoin sopracitato al proof-of-stake (PoS). Nel PoW i miner sono chiamati a risolvere complessi

problemi matematici computazionali per validare transazioni e creare un blocco, utilizzando un elevato dispendio di risorse. Nel contesto di PoS, il processo di selezione del nodo che sarà incaricato di validare e creare il nuovo blocco è basato sulla quantità di criptovaluta posseduta (stake) da quel partecipante. In altre parole, più monete crittografiche una persona o un nodo possiede, maggiore è la probabilità che venga scelto per creare un nuovo blocco e convalidare le transazioni.

Il 15 settembre 2022 la rete principale di ethereum basata su un meccanismo di consenso PoW e quella secondaria (la Beacon Chain, basata sulla PoS) che prima agivano in parallelo si sono fuse, originando una nuova versione di ethereum basata esclusivamente sul PoS, al cui interno continuano però a comparire tutte le informazioni contenute nella precedente versione.

La *Fusione* ha portato una riduzione delle emissione di carbonio pari al 99,95%.

MyContract

Ho iniziato nominando le tre variabili di stato di tipo numerico, indicate dalla sigla “uint”, che contrassegna un numero intero POSITIVO.

Le variabili *TotalAmount* e *TotalDonor* indicano rispettivamente l’ammontare delle donazioni raccolte ed il totale dei contribuenti. Entrambe si aggiornano ad ogni donazione, fino al raggiungimento dell’obiettivo (variabile *Goal*) prefissato dal creatore del contratto che ammonta a 10 Ether.

```
uint public TotalAmount = 0 ether;
uint public TotalDonor = 0;
uint public Goal = 10 ether;
```

Grazie alla funzione “**donate**”, resa payable, è possibile inviare Ether al contratto. Il valore della donazione (msg.value) deve essere superiore di 0, come espresso nella funzione **require** (altrimenti **donate** si blocca) e, va ad incrementare il saldo raccolto (dell’importo della donazione) e il totale dei donatori (di una una unità per donatore).

```
function donate() payable public {
    require(msg.value > 0, "Donations must be positive!");
    owner.transfer(msg.value);
    TotalDonor++;
    TotalAmount += msg.value;
}
```

Grazie alla funzione **getTotalAmount** è possibile ritirare il saldo raccolto e, implementata con modifier onlyOwner permette SOLO al manager della raccolta fondi di ritirarlo una volta raggiunto l’obiettivo della raccolta.

```
modifier onlyOwner() {
    require(msg.sender == owner, "Only manager can get the amount");
    _;
}

function getTotalAmount() public view onlyOwner returns(uint) {
    require(TotalAmount >= Goal);
    return TotalAmount;
}
```

La funzione **checkGoal** permette di confrontare il saldo raccolto con l'obiettivo della raccolta, qualora quest'ultimo dovesse venire eguagliato o superato dai fondi raccolti, la funzione restituisce la stringa "The fundraising is over!", se invece dovesse essere inferiore, restituisce "Goal not achieved" e, quindi, è necessario aspettare altre donazioni prima di poter ritirare il saldo.

```
function checkGoal() public view returns(string memory) {
if(TotalAmount >= Goal) {
    return "The fundraising is over!";
} else {
    return "Goal not achieved";
}
}
```