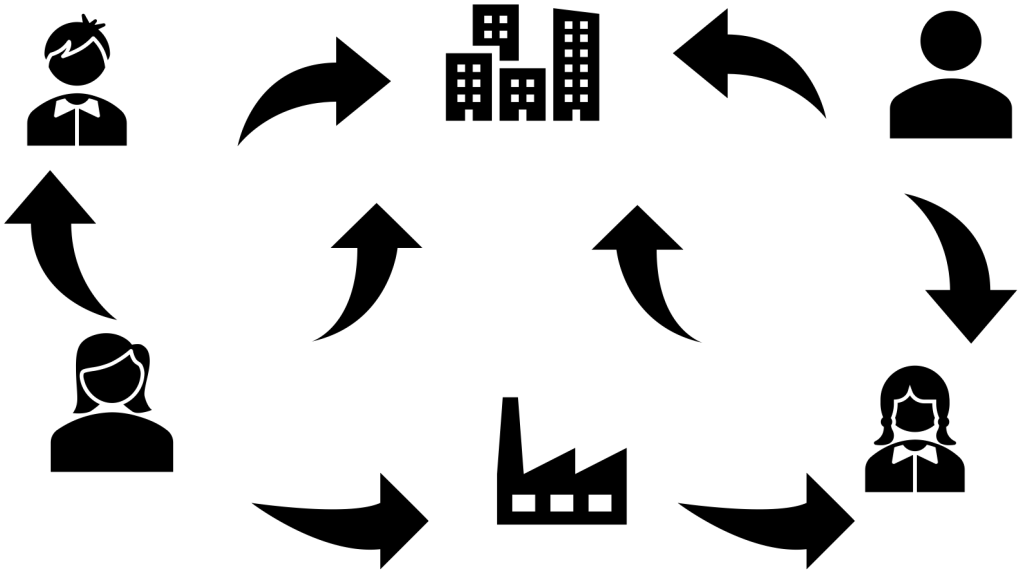
Introduzione a Blockchain, Smart Contract e NFT

Dr Sara Migliorini

sara.Migliorini@univr.it

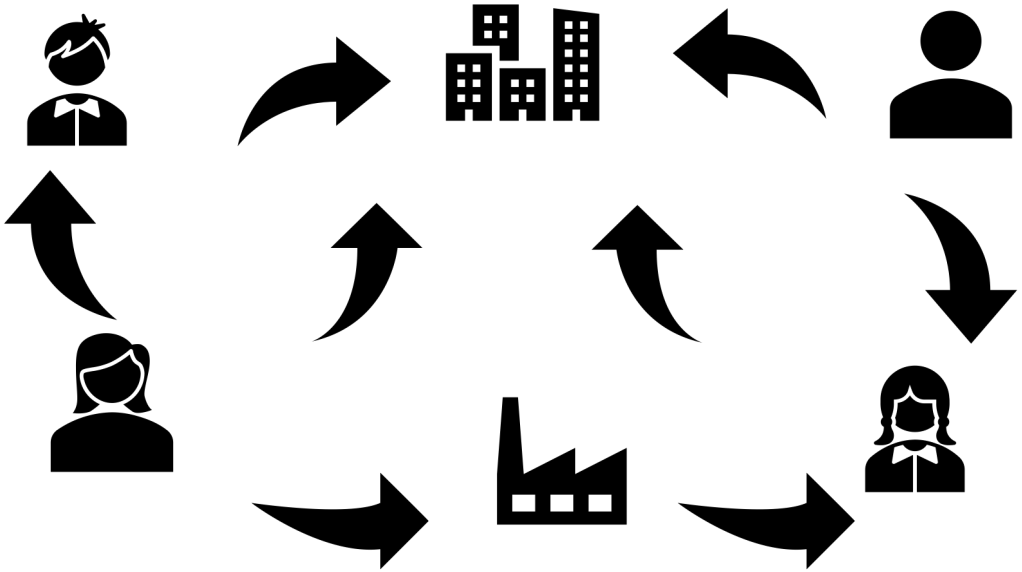
Che cos’è una blockchain e a cosa serve?

- Supponiamo di voler creare un consorzio per scambiare beni e servizi.



Che cos’è una blockchain e a cosa serve?

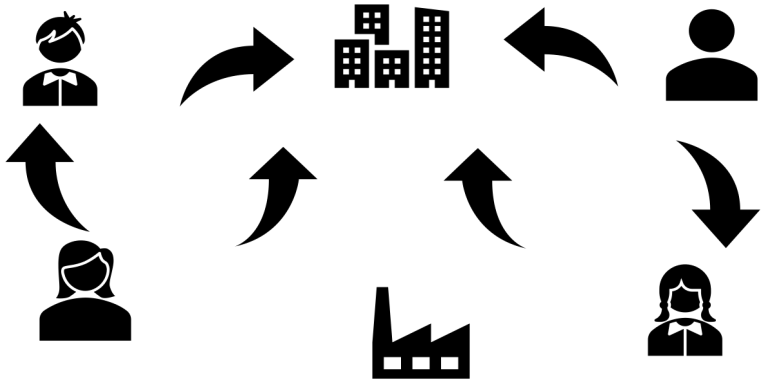
- Supponiamo di voler creare un consorzio per scambiare beni e servizi.



Di cosa abbiamo bisogno per gestirlo?

Che cos’è una blockchain e a cosa serve?

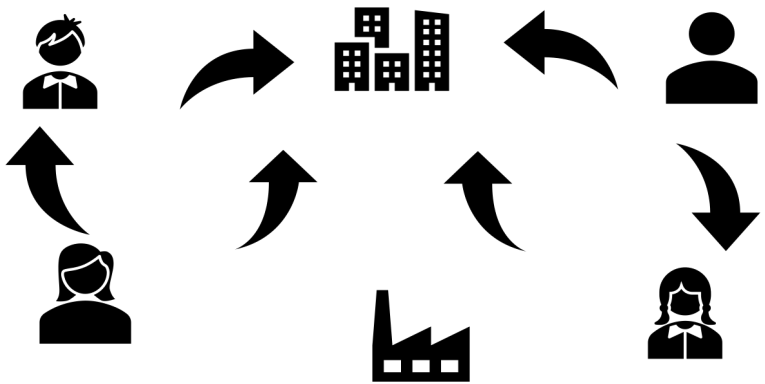
- Ci serve un registro (o libro contabile) in cui memorizziamo tutti gli scambi che vengono effettuati tra i vari partecipanti.
- Per ogni transazione vengono memorizzate informazioni come: quando, cosa, quanto, ecc…



Che cos’è una blockchain e a cosa serve?

- Ci serve un registro (o libro contabile) in cui memorizziamo tutti gli scambi che vengono effettuati tra i vari partecipanti.
- Per ogni transazione vengono memorizzate informazioni come: quando, cosa, quanto, ecc…

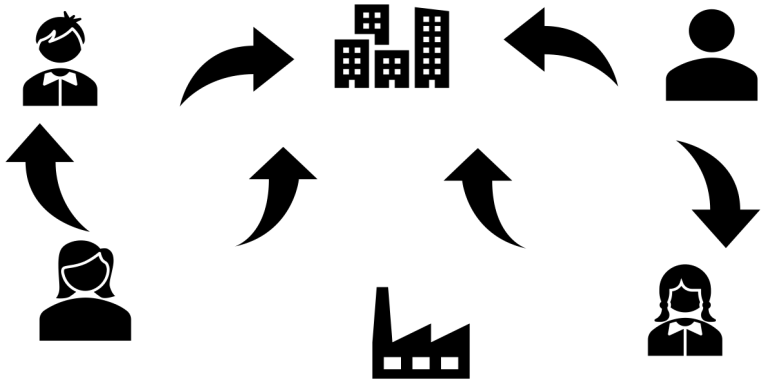
Problema:
Chi tiene il registro?

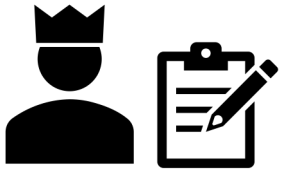


Che cos'è una blockchain e a cosa serve?

- Ci serve un registro (o libro contabile) in cui memorizziamo tutti gli scambi che vengono effettuati tra i vari partecipanti.
- Per ogni transazione vengono memorizzate informazioni come: quando, cosa, quanto, ecc…

Problema:
Chi tiene il registro?





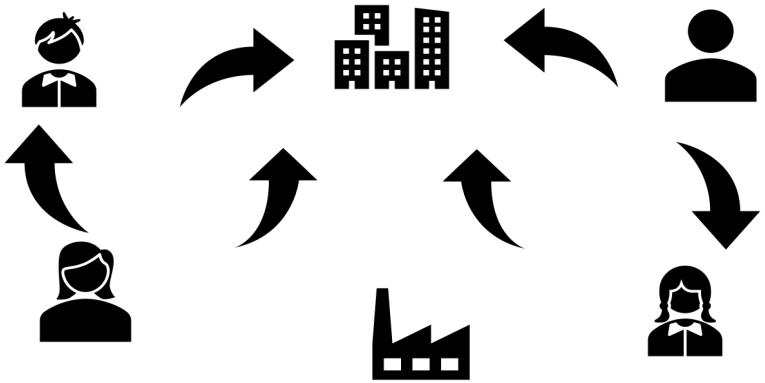
Entità terza scelta dal gruppo

Soluzione centralizzata

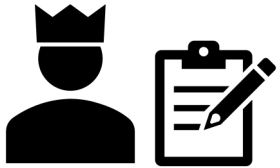
Che cos'è una blockchain e a cosa serve?

- Problema: chi sceglie l'entità terza?
- Problema: ci possiamo fidare?
- Problema: chi garantisce che l'entità terza non modifichi le transazioni a suo favore o a favore di una delle parti?

Soluzione centralizzata



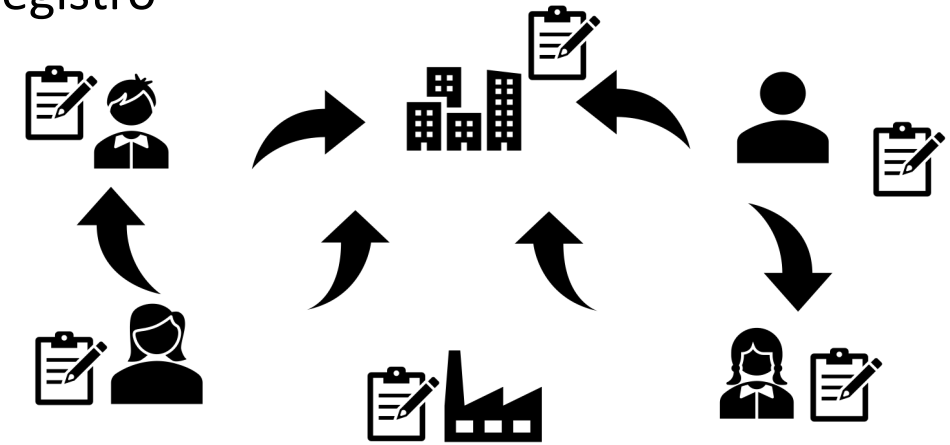
Problema di fiducia



Entità terza scelta dal gruppo

Che cos'è una blockchain e a cosa serve?

- Problema: chi sceglie l'entità terza?
- Problema: ci possiamo fidare?
- Problema: chi garantisce che l'entità terza non modifichi le transazioni a suo favore o a favore di una delle parti?
- Blockchain: ogni membro del consorzio mantiene una propria copia del registro



Soluzione decentralizzata

Che cos'è una blockchain e a cosa serve?

- Blockchain: **consenso decentralizzato**
  - Ogni attore mantiene una copia del registro
- Problema: come garantisco che le copie coincidano?
  - Viene utilizzato un protocollo di consenso decentralizzato
    - Es. Proof-of-Work, Proof-of-Stake
  - Idea: scrivere sul registro ha un costo, se qualcuno "mente" riceve una penalità che rendete tale comportamento non conveniente

Novità

- Blockchain: **immutabilità**
  - Una blockchain è una catena di blocchi
  - Quello che viene scritto non può più essere modificato

Bitcoin e blockchain

- L'innovazione principale della blockchain è la definizione di un protocollo per la costruzione di una rete peer-to-peer (P2P) in grado di raggiungere un consenso circa uno stato globale senza l'intervento di un'entità centrale.

- La tecnologia blockchain è stata utilizzata inizialmente per risolvere il problema del double-spending.
  - Nascita delle criptovalute
  - Bitcoin (2009)

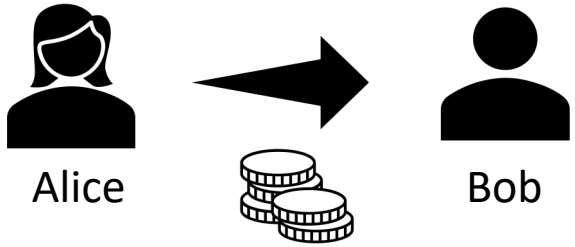
- Prima di Bitcoin c'erano stati molti altri tentativi, ma non sono decollati proprio per la necessità di una entità centrale.

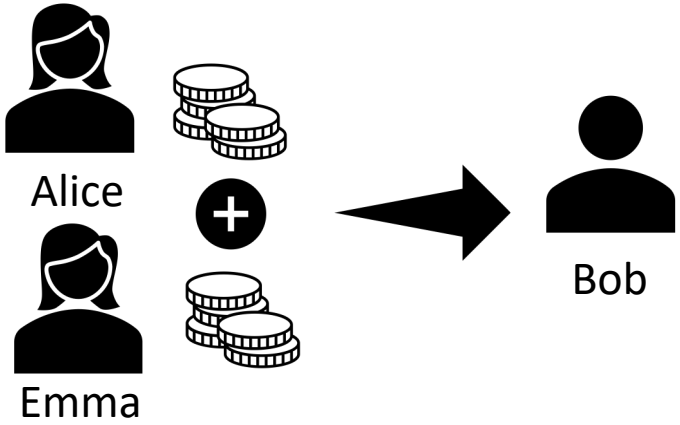
Bitcoin e blockchain

- Perché un'unica entità centrale è un problema?
  - Richiede la fiducia di tutti partecipanti verso l'entità centrale
  - Unico punto debole: per attaccare la rete è sufficiente attaccare l’entità centrale

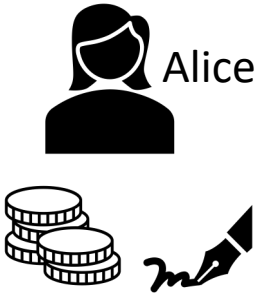
Bitcoin e transazioni

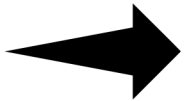
- Una blockchain è una catena di blocchi
- I blocchi contengono informazioni sulle transazioni eseguite
- Una transazione è una struttura dati che racchiude informazioni circa il trasferimento di un certo quantitativo di token da uno o più indirizzi di partenza (input) verso uno o più indirizzi di destinazione (output)

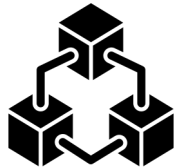




Ciclo di vita di una transazione



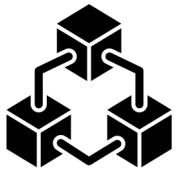




1 Creazione e firma della transazione

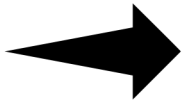
2 Broadcast e validazione della transazione

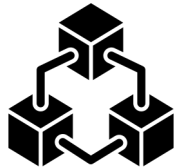
3 Mining o creazione dei blocchi



4 Transazione confermata

Ciclo di vita di una transazione

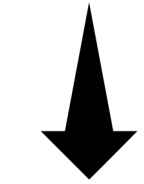


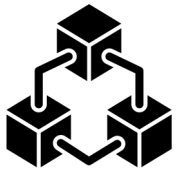


1 Creazione e firma della transazione

2 Broadcast e validazione della transazione

3 Mining o creazione dei blocchi

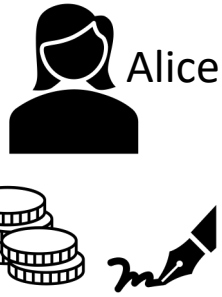


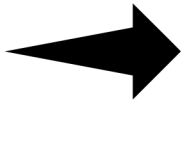


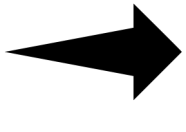
4 Transazione confermata

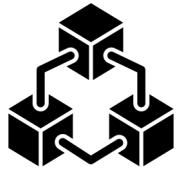
Tramite la firma si prova il possesso dei token e si autorizza a spenderli

Ciclo di vita di una transazione





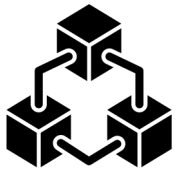




1 Creazione e firma della transazione

2 Broadcast e validazione della transazione

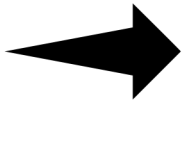
3 Mining o creazione dei blocchi

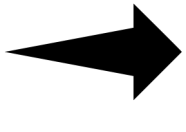


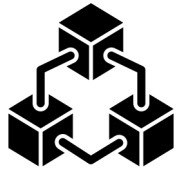
4 Transazione confermata

Ciascun nodo della rete riceve la nuova transazione, la controlla e la passa ai vicini se è valida

Ciclo di vita di una transazione







1 Creazione e firma della transazione

2 Broadcast e validazione della transazione

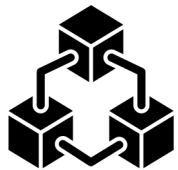
Proof-of-Work

3 Mining o creazione dei blocchi

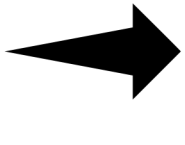
Il mining è il processo attraverso il quale i nodi creano nuovi blocchi a partire da un insieme di transazioni “pendenti”

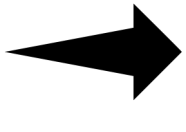
La costruzione di un blocco richiede lavoro (risoluzione problema matematico complesso)

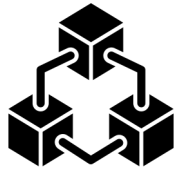
4 Transazione confermata



Ciclo di vita di una transazione





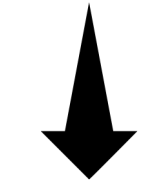


1 Creazione e firma della transazione

2 Broadcast e validazione della transazione

Proof-of-Work

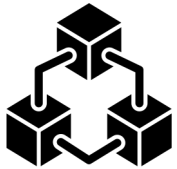
3 Mining o creazione dei blocchi



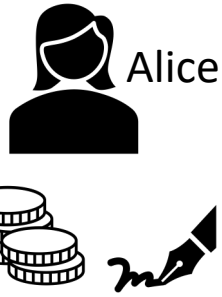
Quando un nodo riesce a costruire un nuovo blocco valido, lo manda a tutti gli altri nodi

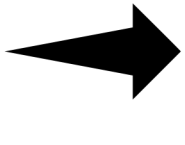
I blocchi validi vengono aggiunti in coda alla catena (blockchain)

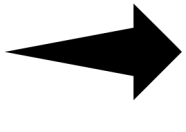
4 Transazione confermata

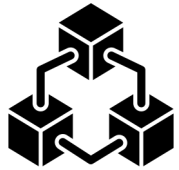


Ciclo di vita di una transazione







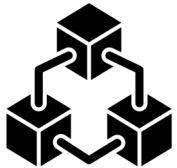


1 Creazione e firma della transazione

2 Broadcast e validazione della transazione

Proof-of-Work

3 Mining o creazione dei blocchi

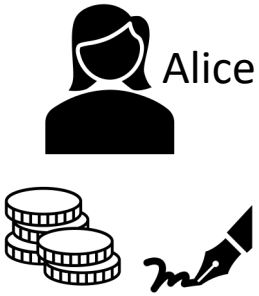


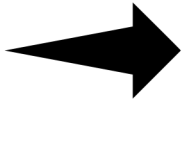
4 Transazione confermata

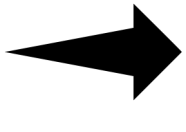
Una blockchain può avere **temporaneamente** più evoluzioni valide (fork)

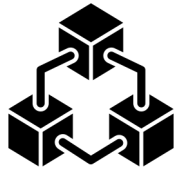
Le diramazioni vengono risolte con la regola della catena più lunga

Ciclo di vita di una transazione





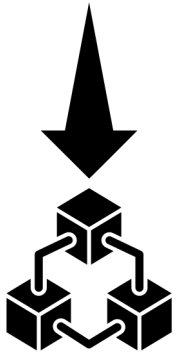




1 Creazione e firma della transazione

2 Broadcast e validazione della transazione

3 Mining o creazione dei blocchi

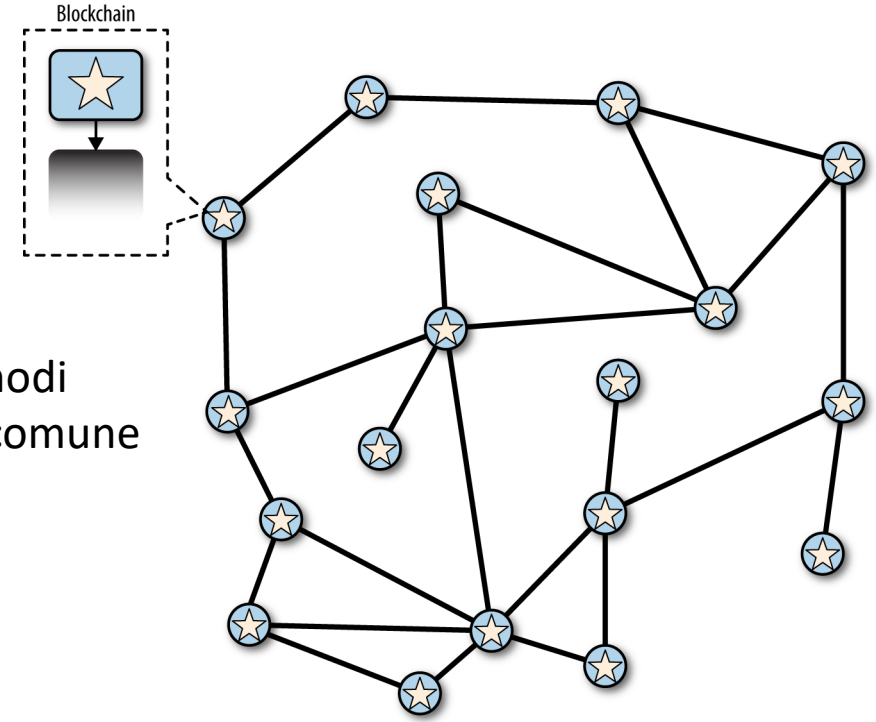


L'esistenza di una lunga catena di blocchi dopo il blocco corrente, rende le transazioni di quest'ultimo immutabili

In Bitcoin una transazione è considerata **immutabile** dopo 6 conferme (dopo 6 blocchi)

4 Transazione confermata

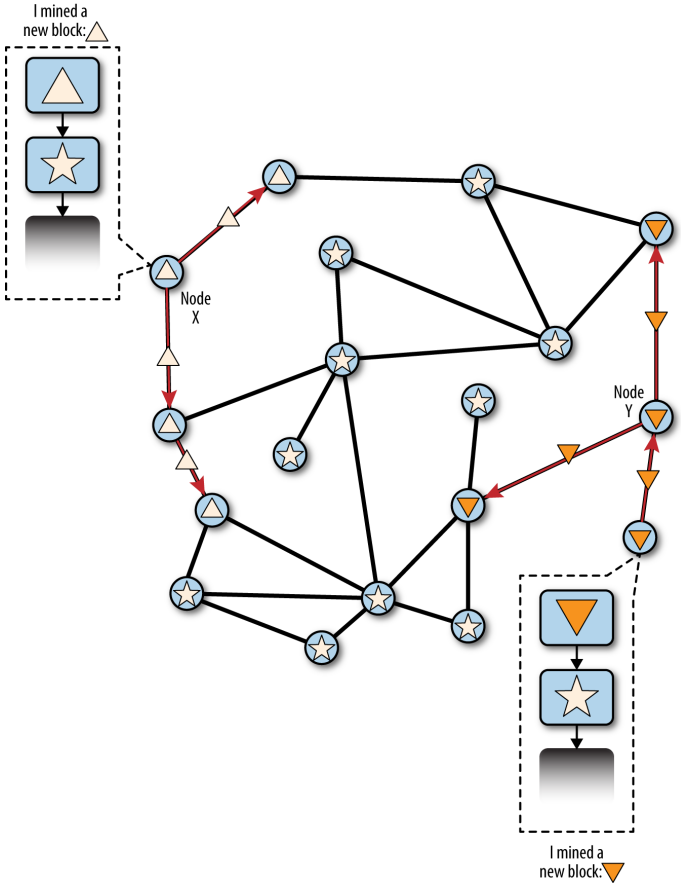
Fork di una blockchain



0 Stato iniziale: tutti nodi hanno una visione comune della rete

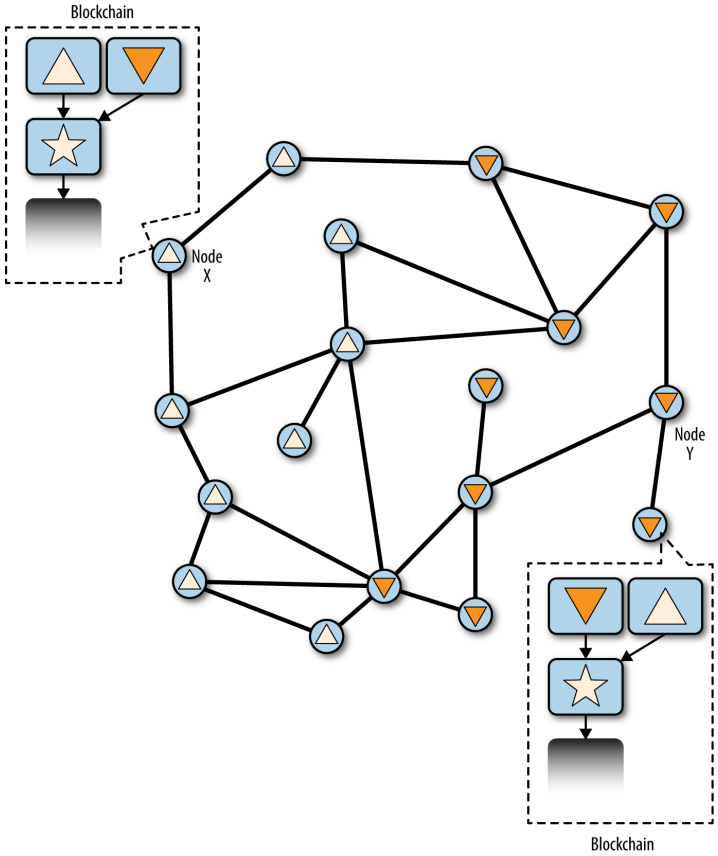
Fork di una blockchain

1 Fork: due nodi espandono la blockchain in modo diverso



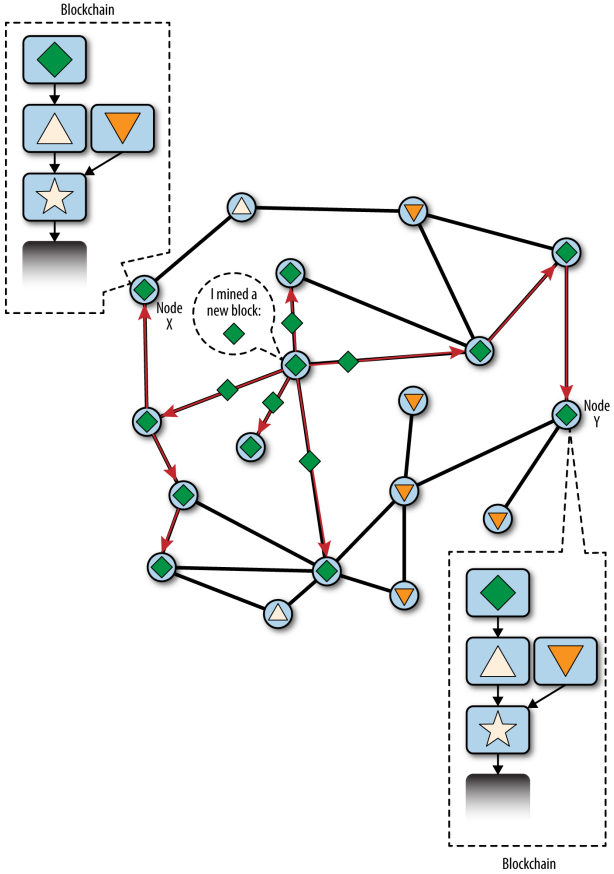
Fork di una blockchain

2 Fork: si verifica uno split della rete



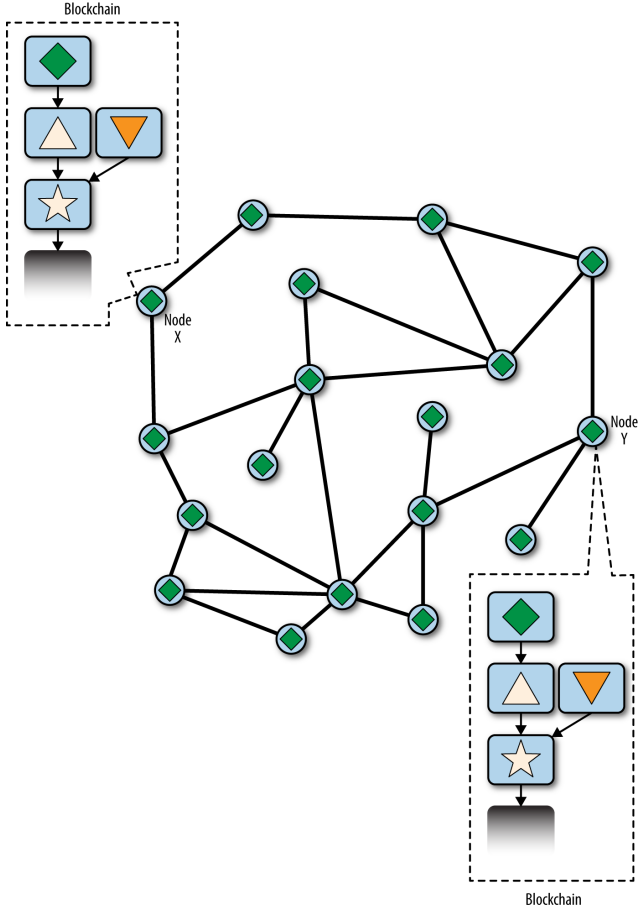
Fork di una blockchain

3 Fork: uno split si espande ulteriormente



Fork di una blockchain

4 Fork: la rete riconverge



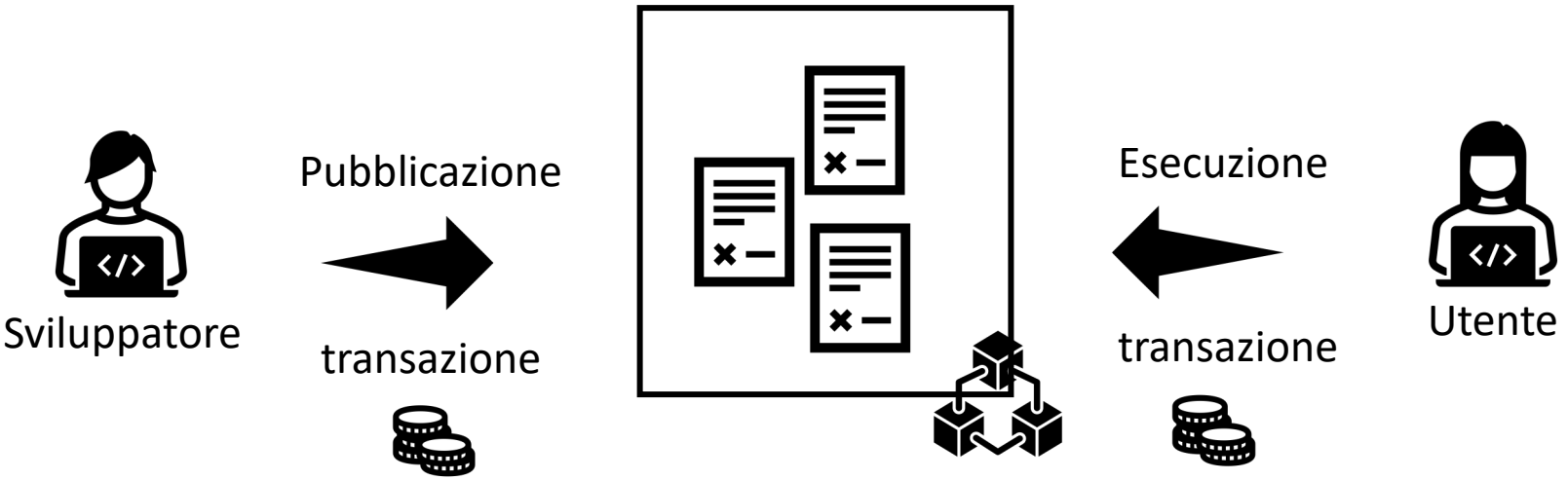
Smart contract

- Uno smart contract è un accordo tra due o più parti, il cui rispetto può essere forzato automaticamente senza il bisogno di un intermediario

- Ethereum è stato il primo progetto che ha implementato il concetto di smart contract in una blockchain

- In Ethereum uno smart contract è un programma memorizzato all'interno della blockchain che viene eseguito automaticamente quando un evento specifico si verifica.
  - Evento = scheduling di una transazione

Smart contract

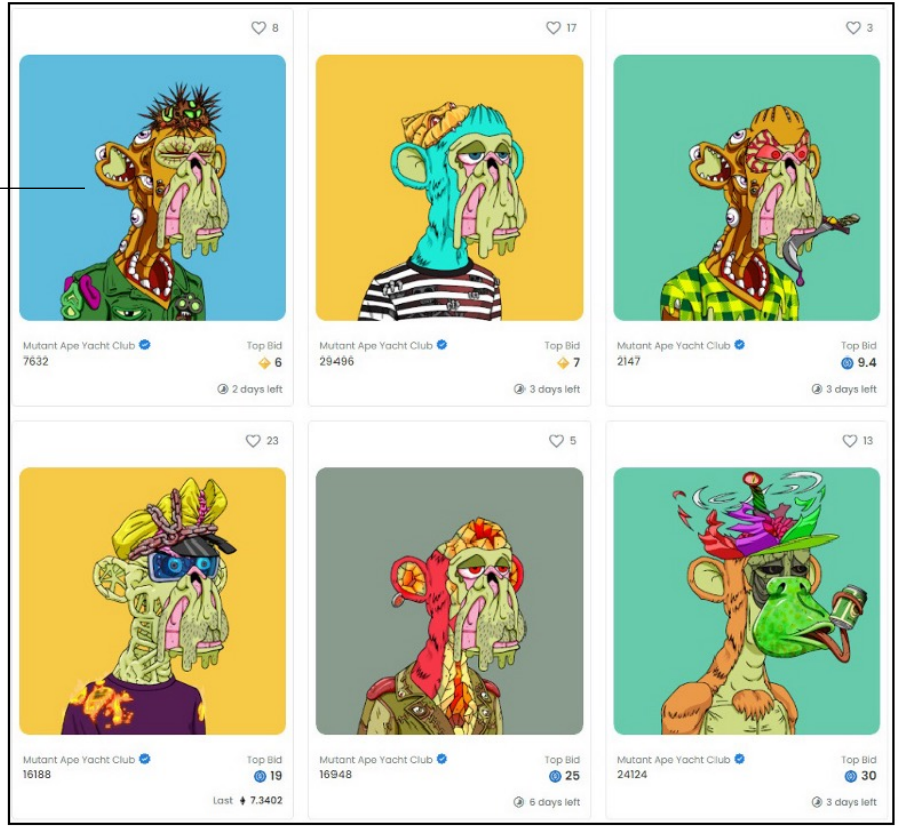


Non-Fungible Token (NFT)

- Tipicamente tutti i token di una stessa blockchain sono intercambiabili tra di loro (Fungible Token) e possono essere divisi in. unità più piccole.
- Un NFT è un identificatore digitale univoco di beni o risorse che prendono la forma di un token digitale che viene memorizzato in maniera permanente nella blockchain.
- Gli NFT non sono intercambiabili tra di loro e non possono essere divisi.
- Gli NFT possono essere usati per verificare e tracciare il possesso e l'accesso a beni o risorse.

What does an NFT represent?

Rappresentazione visual di un token MAYC



Mutant Ape Yacht Club (MAYC) attualmente in vendita su OpenSea

NFT = codice digitale univoco attualmente memorizzato sulla blockchain di Ethereum

- Acquistare un NFT significa diventare il proprietario legittimo del token con ID 7632, che è memorizzato nel contratto con indirizzo 0x60e4d sulla blockchain di Etherem.
- Tutti i trasferimenti di proprietà vengono memorizzati sulla blockchain