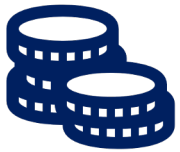
POLITECNICO
MILANO 1863

Blockchain e Credibilità dei Processi Digitali

Francesco Bruschi

Digitalizzare un processo permette di **memorizzare, trasmettere ed elaborare** informazione digitale

costo minore



maggiore velocità

maggiore accessibilità

- Può migliorare anche la «credibilità»?

Digitalizzazione «classica»

La digitalizzazione tramite le tecnologie tradizionali **nasconde la logica** dei processi considerati dietro a back-end opachi

Alcuni esempi:

- Chi assicura che il denaro inviato verrà gestito secondo una certa logica?
- Nel caso di una votazione, che garanzie vengono fornite sulla correttezza del risultato?
- Chi garantisce che il processo non sia stato manipolato esternamente, da un cyberattacco?

La digitalizzazione da sola **non aggiunge credibilità ad un processo, anzi**, in un contesto di suscettibilità ai cyberattacchi, aggiunge vulnerabilità e può inficiare la credibilità

Le piattaforme blockchain possono essere pensate come un **sistema di elaborazione del codice** con le seguenti caratteristiche:

trasparente

immutabile

non interrompibile

Blockchain: caratteristiche principali

Come si ottengono queste caratteristiche?

- La computazione è **pubblica**: chiunque può verificare che, dati gli ingressi (le transazioni degli utenti), il risultato è lo stato corrente
- Chi decide quali transazioni considerare, e in quale ordine?
  - Un sistema decentralizzato di **validatori** che si protegge e regola con dei meccanismi neutrali (il **consenso**)
    - Permissionless: alla validazione può partecipare **chiunque**
      - I validatori vengono puniti o premiati se si comportano bene o male
    - Permissioned: i validatori sono soggetti identificati (esempio: istituzioni di stati membri in EBSI)
- Se un validatore manipola la computazione, **tutti se ne accorgono** e lo penalizzano/cacciano

Storicamente, la prima applicazione è **Bitcoin**, cioè denaro elettronico, inteso come un asset digitale con le seguenti caratteristiche:

- Liberamente scambiabile tra soggetti senza permessi/identificazioni, usando identità crittografiche
- Politica monetaria definita
- Nessun trust nei confronti delle entità coinvolte

In Bitcoin, il programma che gira **è specifico**, un amministratore degli asset, che garantisce che lo scambio avvenga correttamente

Generalizzazione: perché non consentire a chiunque di “caricare” un programma qualsiasi sulla piattaforma, che poi lo esegue fornendo le garanzie sopracitate?

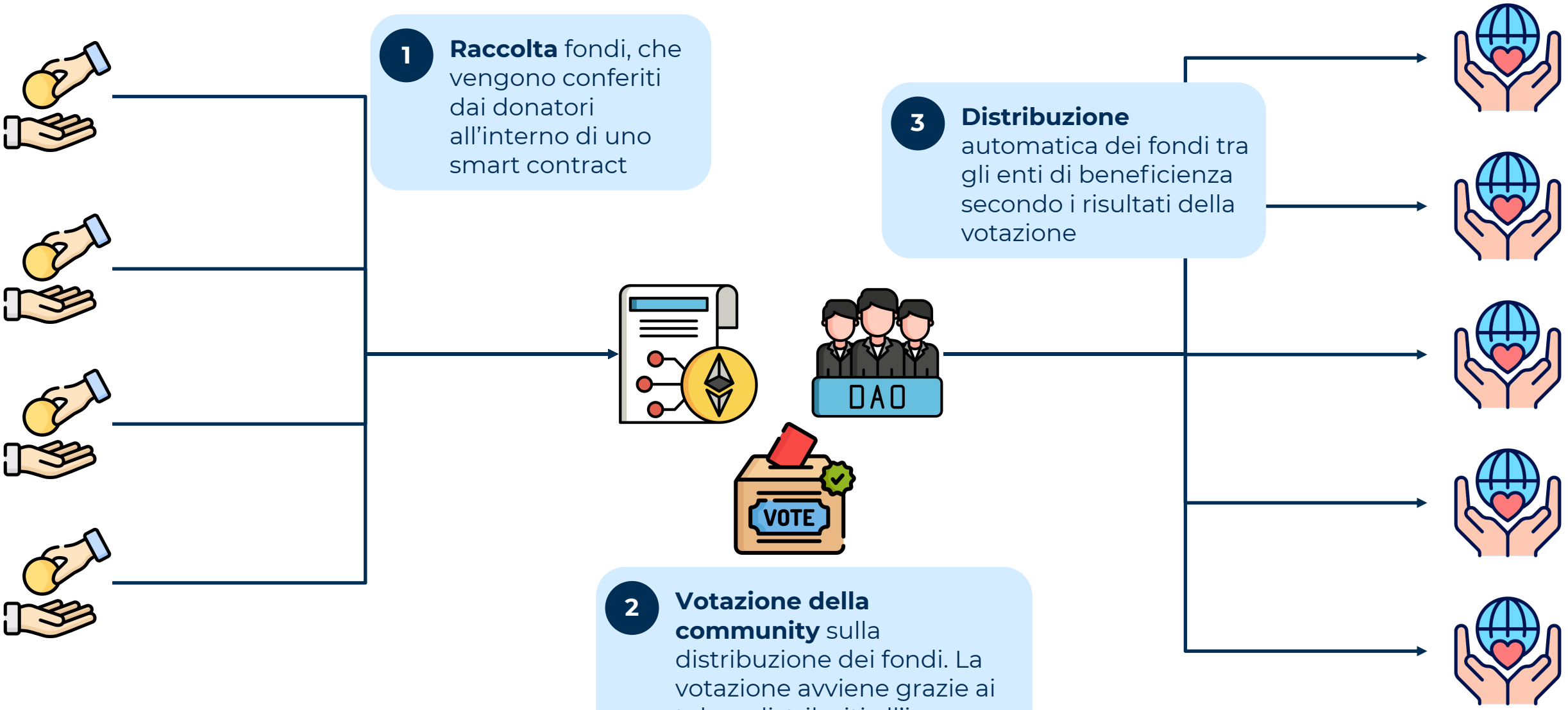
- Ethereum nasce per rispondere a questa esigenza, e permette di digitalizzare un processo rendendolo nel contempo **intrinsecamente credibile**

Possibili applicazioni:

- Definizione di nuovi tipi di asset/token, con proprietà arbitrarie (es: NFT)
- Identità (gestione dei certificati)
- Votazioni e organizzazioni decentralizzate
- Prodotti/meccanismi finanziari
- Assicurazioni
- Compliance intrinseca (sicurezza maggiore di audit!)

ethereum

Cosa farà la DAO



Come ha raccolto i fondi la DAO?

POLITECNICO MILANO 1863

Transactions | ERC-20 Token Txns | Contract | Events | Analytics | Comments

Latest 22 ERC-20 Token Transfer Events

Txn Hash	Age	From		To	Value	Token
0x3ab1304a2b3cd7e0...	9 hrs 30 mins ago	0x6f52c311e6fb1053248...	IN	0x6f5138ac14bae67f15a...	0	USD Coin (Po... (USDC)
0x38557fe6c782c11d0fa...	9 hrs 31 mins ago	0x38a9911d4badd1f22e...	IN	0x6f5138ac14bae67f15a...	300	USD Coin (Po... (USDC)
0xf7e9d7cd1cac310e...	10 hrs 7 mins ago	0x6f52c311e6fb1053248...	IN	0x6f5138ac14bae67f15a...	0	USD Coin (Po... (USDC)
0x3add3597d1d1c8845d...	10 hrs 8 mins ago	0xb6363ab1ffbf58997a6...	IN	0x6f5138ac14bae67f15a...	20	USD Coin (Po... (USDC)
0x2d33befb0b8c5bbd...	13 hrs 13 mins ago	0x6f52c311e6fb1053248...	IN	0x6f5138ac14bae67f15a...	0	USD Coin (Po... (USDC)
0xe63c92fc92c46a2bdbc...	13 hrs 14 mins ago	0xc4d58ac99dd7ba3b5a...	IN	0x6f5138ac14bae67f15a...	500	USD Coin (Po... (USDC)
0x26a1a90f1d71cb3f8...	13 hrs 16 mins ago	0x6f52c311e6fb1053248...	IN	0x6f5138ac14bae67f15a...	0	USD Coin (Po... (USDC)
0xa2362b6d17e367ce84...	13 hrs 17 mins ago	0xe5772c9641b6271f0b...	IN	0x6f5138ac14bae67f15a...	297.84	USD Coin (Po... (USDC)
0xb960ebd56d63aa784a...	14 hrs 18 mins ago	0x691d2f512d0a8dbf2a7...	IN	0x6f5138ac14bae67f15a...	50	USD Coin (Po... (USDC)
0x60d2d6fc5dc31156...	14 hrs 21 mins ago	0x6f52c311e6fb1053248...	IN	0x6f5138ac14bae67f15a...	0	USD Coin (Po... (USDC)
0xcb0118b2019321fdea...	14 hrs 22 mins ago	0x62956c31173dc64ff02...	IN	0x6f5138ac14bae67f15a...	9.5	USD Coin (Po... (USDC)
0x5c0d9a423a17f84e...	14 hrs 37 mins ago	0x6f52c311e6fb1053248...	IN	0x6f5138ac14bae67f15a...	0	USD Coin (Po... (USDC)
0xd489b9832d2ef42b89...	14 hrs 38 mins ago	0xb1898d356804ac77f4...	IN	0x6f5138ac14bae67f15a...	1,086	USD Coin (Po... (USDC)

Accesso ai dati

- Il carattere pubblico dell'esecuzione non comporta che tutti possano accedere a tutti i dati?
- E' possibile controllare l'accesso in lettura ai dati? Se si, in che modo? Questo non inficia i vantaggi introdotti dalla tecnologia e la credibilità del processo?

Alcuni esempi:

- **Votazioni/governance**: si può avere la garanzia dell'esito, tenendo nascosta l'associazione tra votanti e voti?
- **Supply chain**: si può rendere evidente/garantita una caratteristica del prodotto (per esempio che è a km0), senza rivelare tutta l'informazione tracciata?
- **Procurement**: si può garantire che una gara è stata condotta correttamente senza rivelare i dettagli sui partecipanti/sulle offerte?
- **Identità**: si può garantire che i partecipanti ad un processo sono autorizzati/hanno diritto, senza svelare le identità?

- Sono protocolli crittografici che consentono ad un attore (Bob) di dimostrare ad un altro (Alice) di possedere una certa informazione, **senza svelare l'informazione stessa**
  - es. Bob può convincere Alice di conoscere la soluzione di un sudoku, senza fornire alcun indizio sul sudoku stesso

- Questa possibilità è molto generale, e può essere applicata a molti processi

Zero-Knowledge Proofs: alcuni esempi

- **Identità**
  - Minimizzazione (CV anonimo, controllo documenti)
    - Un soggetto può dimostrare di avere certe qualifiche (anzianità, istruzione, etc) senza indicare altro (nome, provenienza etc)
  - KYC
    - Un soggetto può dimostrare di essere autorizzato, o anche solo identificabile, senza rivelare la propria identità
- **Erogazione di crediti**
  - Un soggetto può **dimostrare** di essere un “buon pagatore”, senza entrare nei dettagli (per esempio «provando» di pagare le utenze, senza svelare quali, o gli importi)
- **IoT**
  - un soggetto può dimostrare di aver aggiornato il firmware di una flotta di dispositivi al termine di un processo di revisione e approvazione del codice, senza svelare il contenuto del firmware

ZKP e digitalizzazione

Grazie a questa tecnologia è possibile architettare/progettare/implementare processi che:

- consentono di **controllare l'informazione sensibile**, e allo stesso tempo
- consentono di **provare matematicamente** che l'esito del processo è stato determinato da certe regole (e.g. che il risultato della votazione è stato ottenuto contando correttamente tutti i voti)

Questo apre scenari ampi e notevoli:

- Compliance normativa
- Gestione finanziaria
- Tracciamento/tracciabilità
- Identità
- ...

In generale: le blockchain possono rendere un processo digitale
- **intrinsecamente** credibile
- resistente a manipolazioni ed attacchi in maniera evidente

Alcuni esempi di possibile applicazione:

- **Meccanismi partecipativi/consultazioni**: garanzia matematica che l'esito del conteggio di una consultazione deriva correttamente dai voti espressi dagli aventi diritto (senza svelare le identità)
- **Raccolta dati**: è possibile dare evidenza pubblica di alcune caratteristiche (che i dati provengono dai soggetti incaricati, che i dati sono completi, che sono stati raccolti a certe condizioni etc)
- **Politiche di sostegno al reddito**: si può dare evidenza di:
  - Quanto è stato erogato
  - A chi (non le identità, ma la sussistenza di requisiti)
  - Come è stato speso (anche qui rispettando la privacy)
- **Procurement, gare, concorsi**. E' possibile garantire pubblicamente per esempio:
  - Segretezza offerte
  - Sussistenza condizioni delle offerte
  - Applicazione criteri di valutazione
- **Identità**: soggetti possono dimostrare di possedere requisiti (e.g. patente, isee) senza interpellare ente terzo, in modo **selettivo** (svelando solo informazione utile)
- **Auditability/compliance**: in generale, è possibile raccogliere/fare commitment sui dati di un processo, e poi dimostrare credibilmente una certa proprietà del processo (che si sono usate certe materie prime, o un certo tipo di energia, o un certo tipo di lavoro)

Rischi/punti di attenzione

Non tutte le blockchain sono uguali:

- La configurazione dei validatori garantisce le proprietà di resilienza
- Permissionless: massima resilienza
- Nel caso di permissioned, la credibilità dei validatori (istituzionali?) è fondamentale

E' un paradigma nuovo

- Dal punto di vista della gestione dell'informazione (e.g. privacy garantita dalla crittografia)
- Dal punto di vista software ingegneristico (e.g. perché il codice è sistematicamente pubblico)
- Dal punto di vista del design dei processi (e.g. perché riconfigura e redistribuisce le responsabilità in modo nuovo)

⇒ Necessarie cultura e formazione