# L'OSSERVATORIO ITALIANO SULLE POLITICHE IN MATERIA DI BLOCKCHAIN

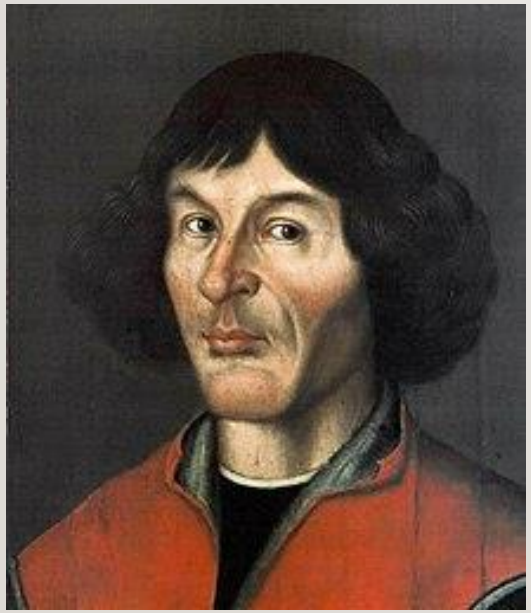
"BLOCKCHAIN, MERCATO DEL LAVORO E  POLITICHE SOCIALI"

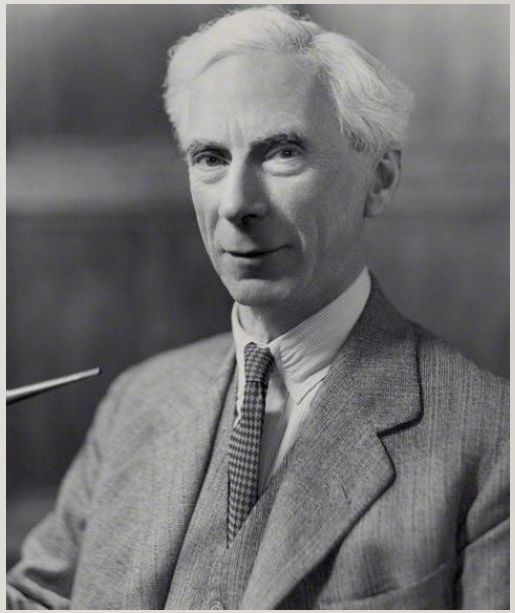
Silvia Ciucciovino, Michele Faioli e Alessandro Toscano

# SOMMARIO

- Programma
  - Forum e Osservatorio Italiano della Blockchain in collegamento con l'EU Blockchain Observatory and Forum (Commissione Europea)
  - Blockchain e politiche attive del lavoro
  - Blockchain e politiche di sostegno al reddito
  - Interventi programmati
  - Gruppi di lavoro
- Blockchain
  - Cos'è
  - Perché

# PERSONAGGI IN ORDINE DI APPARIZIONE





# ARISTORELE

- Aristotele, a quanto si tramanda, giudicava che le stelle si muovessero descrivendo un cerchio, in quanto il cerchio era da lui considerato la curva più perfetta. In assenza di prove in contrario, egli si permise di risolvere un problema di meccanica celeste, di fatto, ricorrendo a considerazioni estetico-morali.
- **In un caso del genere è a tutti noi ora evidente che questo ricorso era ingiustificato.**

# COPERNICO

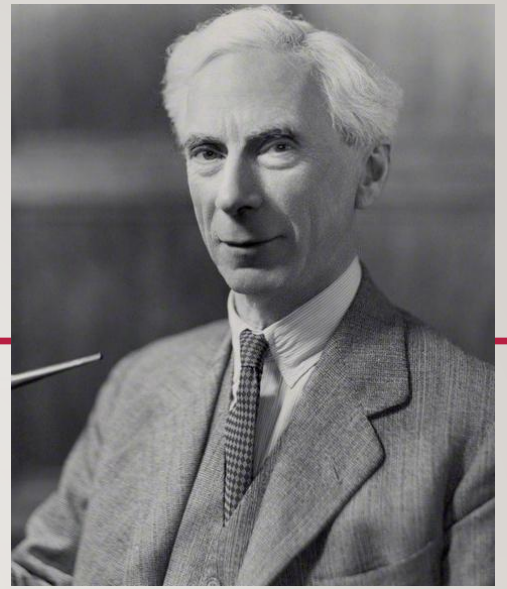
- La sua teoria, che propone il Sole al centro del sistema di orbite dei pianeti componenti il sistema solare, riprende quella greca di Aristarco di Samo dell'eliocentrismo, la teoria opposta al geocentrismo, che voleva invece la Terra al centro del sistema. Quindi non fu il primo a formulare l'idea, già espressa dai greci, ma il primo a dimostrarla rigorosamente tramite procedimenti di carattere matematico.
- **Rivoluzione copernicana.**

# MAXWELL

$$\begin{cases} \nabla \times \boldsymbol{E} = -\dfrac{\partial \boldsymbol{B}}{\partial t} \\ \nabla \times \boldsymbol{H} = \boldsymbol{J} + \dfrac{\partial \boldsymbol{D}}{\partial t} \end{cases}$$

- **La simmetria esiste! Consente di anticipare la verifica sperimentale**
- **Ha reso possibile le comunicazioni via radio e via cavo!**

# RUSSEL



- Aritmetizzazione del pensiero
- Paradosso del barbiere

"In un villaggio vi è un solo barbiere, un uomo ben sbarbato, che rade tutti e solo gli uomini del villaggio che non si radono da soli. Il barbiere può radere se stesso?"

Se, come apparirebbe plausibile, il barbiere si radesse da solo, verrebbe contraddetta la premessa secondo cui il barbiere rade solo gli uomini che non si radono da soli.

Se invece il barbiere non si radesse autonomamente, allora dovrebbe essere rasato dal barbiere, che però è lui stesso: in entrambi i casi si cade in una contraddizione.

**IL SISTEMA FORMALE ASSIOMATICO È INTRINSECAMENTE INCOMPLETO**

# RUSSEL

- Teorema di Goedel o dell'impossibilità di costruire sistemi formali sufficientemente complessi in grado di **sostituirsi completamente al ragionamento informale/non sistematico**.
- Macchina di Turing: è una macchina ideale che manipola i dati contenuti su un nastro di lunghezza potenzialmente infinita, secondo un insieme prefissato di regole ben definite. **Il problema dell'arresto della macchina di Turing è indecidibile**

Più ci si addentra nella realtà e nella logica, più emergono aspetti di **inconoscibilità intrinseca**.

# BLOCKCHAIN

- Definizione di una Blockchain
  - Gli ingredienti
  - Le sette fasi della creazione di una Blockchain
  - Principali caratteristiche di una Blockchain
- Concetti avanzati
  - Smart contracts
- Applicazioni innovative

# BLOCKCHAIN

I **NODI** sono gli attori su cui si basa la blockchain, altri non sono che i **computer** che svolgono le verifiche sulle transazioni. Il loro compito è detenere una copia del registro e finalizzare i blocchi.

I **BLOCCHI** sono gli **elementi base che compongono il registro**, legati l'uno all'altro in una successione che ha avuto inizio con l'inizio della blockchain.

# BLOCKCHAIN

La **TRANSAZIONE** è rappresentata dagli scambi o appunto dalle transazioni tra due o più nodi. Le transazioni vengono poi **registrate in modo immutabile** sulla Blockchain.

Il **LEDGER** è il **registro pubblico** nel quale vengono "annotate" con la massima trasparenza e in modo immutabile tutte le transazioni effettuate in modo ordinato e sequenziale.

# BLOCKCHAIN

La Blockchain si costruisce in sei (più una) fasi

1. Transazione
2. Verifica
3. Strutturazione
4. Validazione
5. Mining
6. Catena
7. Coerenza

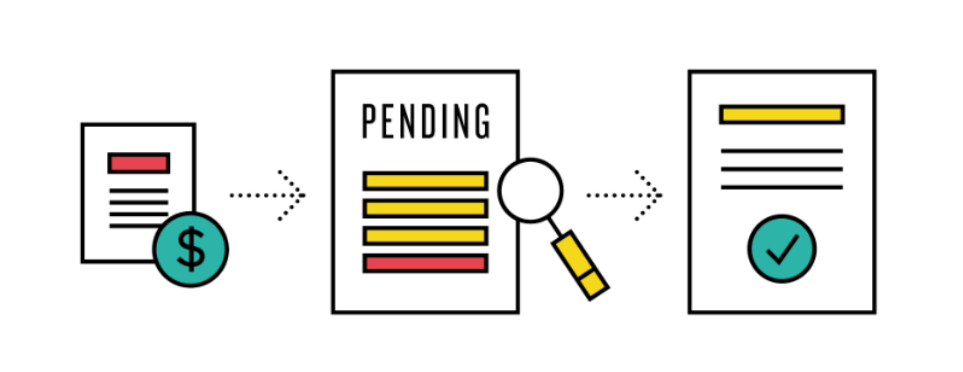
# TRANSAZIONE

Transazione: due parti manifestano l'intenzione di trasferirsi una qualsiasi cosa rappresentabile digitalmente:

- nel caso dei Bitcoin parliamo ovviamente di moneta,
- potrebbe trattarsi di un contratto,
- un bene mobile e immobile

# VERIFICA

VERIFICA: la richiesta di transazione viene inserita in una coda di transazioni. E' in questa fase che la transazione viene verificata dai NODI, che si porranno alcune semplici domande: Chi trasferisce i Bitcoin ha sufficienti disponibilità? Quella quantità di Bitcoin non è già stata trasferita?



# STRUTTURAZIONE

STRUTTURAZIONE: ogni blocco è identificato da un codice, l'hash, creato sulla base delle regole condivise dal network. Ognuno di questi codici è il risultato di un complesso calcolo che viene effettuato a partire dall'hash del blocco precedente e le transazioni contenute nel blocco.

**NON** è possibile modificare il contenuto dei blocchi senza modificare l'hash: questo è l'elemento che rende la catena

**coerente, certa e non modificabile**.

# VALIDAZIONE

VALIDAZIONE: **Il blocco deve essere validato prima di essere aggiunto alla blockchain**.

La forma di validazione nel caso di Bitcoin è il cosiddetto **proof-of-work**, la soluzione ad un complesso puzzle matematico, il complesso calcolo citato nella fase precedente.

# MINING

MINING: il **proof-of-work**, la soluzione al puzzle viene ricompensata in qualche modo.

Tutti i nodi fanno a gara per essere i primi ad arrivare soluzione del puzzle, nessuno sa chi arriverà per primo, questo rende di fatto impossibile ogni tipo di tentativo di manipolazione (con un numero di nodi sufficientemente elevato).

# CATENA O BLOCKCHAIN

CATENA: il blocco è validato e aggiunto alla catena, il nodo che ha risolto il puzzle è ricompensato (il cosiddetto mining).

Il nuovo blocco viene quindi scaricato da tutti partecipanti alla catena.

È possibile che per breve tempo **esistano due o più percorsi diversi** di blockchain, ma i nodi sono programmati per lavorare solo sulla versione più lunga disponibile.

# COERENZA

COERENZA DELLA CATENA: **SE** qualcuno cercasse di inserire dei blocchi alterati nella catena, il loro **hash cambierebbe**, così come cambierebbe quello dei blocchi successivi (ricordate la terza fase?).

I nodi rifiuterebbero il “tarocco” rifiutando la versione corrotta.

Non puoi ingannare la blockchain!

# CARATTERISTICHE DELLA BLOCKCHAIN

**Affidabilità**
Non essendo governata dal centro, ma dando a tutti i partecipanti diretti una parte di controllo dell'intera catena, la Blockchain diventa un sistema meno centralizzato, meno governabile, e allo stesso tempo molto più sicuro e affidabile, ad esempio da attacchi di malintenzionati.

Se infatti soltanto uno dei nodi della catena subisce un attacco e si danneggia, tutti gli altri nodi del database distribuito continueranno comunque a essere attivi e operativi, saldando la catena e non perdendo in questo modo informazioni importanti.

# CARATTERISTICHE DELLA BLOCKCHAIN

**Trasparenza**
le transazioni effettuate attraverso la Blockchain sono visibili a tutti i partecipanti, garantendo così trasparenza nelle operazioni.

**Convenienza**
effettuare transazioni attraverso la Blockchain è conveniente per tutti i partecipanti, in quanto vengono meno interlocutori di terze parti, necessari in tutte le transazioni convenzionali che avvengono tra due o più parti (ovvero le banche e altri enti simili).

# CARATTERISTICHE DELLA BLOCKCHAIN

**Irrevocabilità**
con la Blockchain è possibile effettuare transazioni irrevocabili, e allo stesso tempo più facilmente tracciabili. In questo modo si garantisce che le transazioni siano definitive, senza alcuna possibilità di essere modificate o annullate.

**Digitabilità**
con la Blockchain tutto diventa virtuale. Grazie alla digitalizzazione, gli ambiti applicativi di questa nuova tecnologia diventano tantissimi.

# CARATTERISTICHE DELLA BLOCKCHAIN

**Solidità**
le informazioni già inserite nella Blockchain non possono essere modificate in alcun modo.

In questo modo le informazioni contenute nella Blockchain sono tutte più solide e attendibili, proprio per il fatto che non si possono alterare e quindi restano così come sono state inserite la prima volta.

# SMART CONTRACTS

Uno Smart Contract è la “traduzione” o “trasposizione” in codice di calcolo di un contratto in modo da:

- **verificare** in automatico l’avverarsi di determinate condizioni (controllo di dati di base del contratto) e di

- **autoeseguire** in automatico azioni (o dare disposizione affinché si possano eseguire determinate azioni) nel momento in cui le condizioni determinate tra le parti sono raggiunte e verificate.

# SMART CONTRACTS

**SE gli input sono gli stessi i risultati saranno identici.**

Questo punto è estremamente rilevante perché:

**se da una parte** rappresenta una certezza e una sicurezza in quanto garantisce alle parti una assoluta "**certezza di giudizio oggettivo**" **escludendo qualsiasi forma di interpretazione**,

**dall'altra** sposta sul **codice**, sulla programmazione, sullo sviluppo il peso e la **responsabilità o anche il potere di decidere**.

# SMART CONTRACTS: VANTAGGI

- Intelligenza: Si possono applicare tutte le tecniche di “Machine learning”
- Fiducia: I documenti sono criptati e memorizzati su un registro distribuito
- Sicurezza: I documenti sono criptati e memorizzati su un registro distribuito e, quindi, duplicati molte volte
- Risparmio: Assenza di intermediazione
- Precisione: Esenti da errori che nascono dalla compilazione manuale di di moduli, documenti, etc.

# APPLICAZIONI INNOVATIVE

- Quali sono i limiti delle soluzioni tradizionali?
- Quali i potenziali vantaggi dell'utilizzo della Blockchain?
- Blockchain pubblica o privata?
- Quali transazioni considerare?
- È possibile definire degli "smart contracts"?

# CONCLUSIONI

Grazie!