Riassunto: Finanza Decentralizzata e Blockchain

1. Cos’è la Blockchain?

- Definizione: Registro digitale condiviso, decentralizzato e immutabile che memorizza dati in blocchi collegati tramite hash.
- Caratteristiche:
    - Registro: Archivia informazioni in ordine cronologico (blocchi con timestamp).
    - Condiviso: Tutti i nodi della rete hanno una copia identica (rete peer-to-peer).
    - Immutabile: Dati non modificabili dopo la validazione.

---

2. Struttura della Blockchain

- Blocchi: Contengono:
    - Transazioni
    - Hash del blocco precedente
    - Timestamp
    - Nonce (per Proof of Work)
- Merkle Tree: Struttura ad albero per verificare transazioni in modo efficiente (complessità:
- $\log_{f_0}(n)$
- $\log(n)$).
- Hash: Funzioni crittografiche (es. SHA256) che rendono i dati immutabili.

---

3. Tecnologie Fondamentali

- Proof of Work (PoW): Algoritmo di consenso per validare blocchi (es. Bitcoin). Richiede risoluzione di puzzle computazionalmente costosi.
- Mining: Nodi (miner) competono per risolvere PoW e aggiungere blocchi, ottenendo ricompense.
- Crittografia a Chiave Pubblica:
    - Firme Digitali: Chiave privata per firmare, chiave pubblica per verificare.
    - Indirizzi Bitcoin: Derivati da hash di chiavi pubbliche (es. `RIPEMD160(SHA256(pubKey))`).

---

4. Sicurezza e Decentralizzazione

- Double Spending: Prevenuto tramite validazione decentralizzata e immutabilità della blockchain.
- Validazione dei Blocchi:
    - La catena più lunga è considerata valida.
    - Richiede il 51% dei nodi onesti per sicurezza.

---

5. Storia e Contesto

- Origini:
    - Cypherpunk (anni ’80-’90): Movimento per privacy e crittografia.
    - Bitcoin (2008): Prima criptovaluta decentralizzata (Satoshi Nakamoto).
- Pre-Bitcoin: Idee precedenti come Hashcash (PoW) e timestamping digitale (Haber & Stornetta, 1991).

---

6. Bitcoin

- Dati:
    - Supply massimo: 21 milioni di BTC (circa 19,7 milioni in circolazione nel 2024).
    - Transazioni: Pubbliche, semi-anonime (indirizzi non legati a identità).
- Funzionamento:
    - Transazioni validate da miner ogni ~10 minuti.
    - Utilizza ECDSA (curve ellittiche, Secp256k1) per firme.

---

7. Glossario

- Nonce: Valore usato in PoW per generare hash validi.
- Gossip Protocol: Algoritmo P2P per diffondere informazioni nella rete.
- Secp256k1: Curva ellittica usata in Bitcoin.

Fonti

- Whitepaper Bitcoin (Nakamoto, 2008)

- Libri: "Mastering Bitcoin" (Antonopoulos), "Bitcoin and Cryptocurrency Technologies" (Narayanan)

Per approfondimenti: Consultare le slide originali o i testi consigliati nella bibliografia.