Algoritmi di Consenso e Caso Algorand

Oltre PoW e PoS

Negli scorsi anni, la blockchain si è consolidata principalmente su due grandi famiglie di algoritmi di consenso:

1. **Proof-of-Work (PoW)** elevato consumo energetico e finalità probabilistica.

2. **Proof-of-Stake (PoS) "classico"**, in cui i validatori vengono selezionati in base ai token "in stake", riducendo i costi energetici ma introducendo sfide come lo *slashing* e il rischio di concentrazione di token.

Tuttavia, la **ricerca accademica** ha prodotto varie **nuove soluzioni** che cercano di risolvere il "trilemma" (scalabilità, sicurezza, decentralizzazione) attraverso **idee innovative**:

- **Meccanismi ibridi** (Delegated PoS, Avalanche, Ouroboros) con procedure di voto, subcampionamento e finalità rapida.

- **VRF (Verifiable Random Function) + BFT**: protocolli che selezionano validatori o proponenti in modo **crittograficamente casuale**, con un consenso stile BFT capace di finalizzare blocchi in pochi secondi.

Algorand è un esempio di questa nuova generazione: un **Pure PoS** con latenza bassa, finalità forte immediata e meccanismo di estrazione casuale dei validatori (sortition), ideato da **Silvio Micali** per "risolvere" i limiti di sicurezza e scalabilità delle chain precedenti.

Silvio Micali e il Background Crittografico

Silvio Micali è un crittografo di fama mondiale, noto per i contributi fondamentali a protocolli a conoscenza zero, firme digitali, pseudorandomness. Partendo dall'osservazione dei limiti di Bitcoin (PoW lento e energivoro) e di Ethereum (finalità probabilistica, costi di gas), Micali ha proposto un sistema in cui:

1. **Ogni detentore di token** (ALGO) ha la possibilità di partecipare al consenso.

2. La sicurezza non dipende dal "numero di nodi" (come in DPoS) ma dal **peso di stake** e da un meccanismo di **estrazione casuale** che impedisce a un attaccante di sapere in anticipo chi avrà il ruolo di proponente o validatore.

3. Il protocollo deve garantire la **finalità rapida** (stile BFT) in uno scenario permissionless, con potenziali nodi malevoli e un'ampia base di utenti.

Obiettivo Principale: "Pure PoS" con Finalità Istantanea

Algorand si definisce *pure PoS* perché non c'è alcun meccanismo delegato (delegated PoS) o slot leader programmato, né c'è un meccanismo di "Bonding" rigido con penali complesse. La protezione contro i nodi malevoli deriva dal fatto che un attaccante deve controllare almeno 1/3 dello stake per minare la sicurezza BFT. Se la maggior parte dello stake è in mani oneste, l'attacco risulta proibitivo.

Meccanismi di Base: VRF (Verifiable Random Function) e Comitati BFT

VRF: Una “Lotteria Locale e Imprevedibile”

In Algorand, la scelta di “chi produce il blocco” e “chi valida” avviene con un metodo definito **sortition**. Ogni nodo possiede:

- Una **participation key** (che rappresenta il suo stake).
- Una funzione VRF: data una stringa “seed del round r” e la chiave privata, genera un output α pseudocasuale e una proof π.

Se α è inferiore a una soglia correlata alla quantità di stake, il nodo “vince la lotteria” e diventa un potenziale proponente (o validatore del comitato successivo). Importante: **la selezione avviene in locale** e il nodo rivela la “prova π” solo quando propone o vota. Così, un attaccante non può anticipare o censurare i nodi scelti.

Metafora: È come un’**estrazione casuale** in cui ognuno “pesca” un biglietto nel chiuso della propria stanza. Solo chi ottiene il biglietto “vincente” (numero basso) si presenta al pubblico, mostrando la “ricevuta” (proof). Essendo α e π generati localmente, non c’è un broadcast di randomness che un attaccante possa manipolare.

Fasi di Consenso

1. **Fase di Proposta**: più di un nodo può vincere la lotteria “proponente” e produrre un blocco. Ognuno di questi allega la proof π al blocco.

2. **Soft Vote**: un comitato ridotto (di nodi selezionati via VRF) controlla i blocchi proposti. Se c’è un singolo blocco che rispetta le regole e ottiene >2/3 del voto di stake, si passa avanti. Se c’ è conflitto (due blocchi validi?), la rete filtra e si entra in uno step di disambiguazione.

3. **Certify Vote**: un secondo comitato, anch’esso estratto a caso con VRF, finalizza il blocco. Ottenuto un quorum, il blocco diventa “irreversibile.”

Tempi: In condizioni normali, un round di Algorand dura 4-5 secondi. Non c’è un accumulo di “chain tip” come in PoW, ma una finalità BFT quasi istantanea.

Sicurezza di Algorand

- ## Resistenza alla Maggioranza di Stake

Per riscrivere la catena o censurare transazioni, un malintenzionato necessita di controllare ≥1/3 di tutto lo stake. Se la rete è ampiamente distribuita, raggiungere questo scenario è costoso (acquisire i token in open market). Se $\alpha<1/3$, la probabilità che un singolo comitato abbia la maggioranza malevola è esponenzialmente piccola.

Analisi stocastica: Se il comitato ha dimensione **k** (stabilita da un parametro di Algorand) e α è la frazione di stake malevola, la probabilità che la maggioranza >1/2 in un comitato (o >2/3 in certe fasi) finisca malevola decresce in modo esponenziale con **k**.

- ## Attacchi Mirati (Eclipse Attack)

Potrebbe un attacker isolare i nodi che partecipano al consenso? In teoria, se un attaccante sapesse in anticipo chi sarà selezionato, potrebbe lanciare DDoS o manipolare la connettività. Ma in Algorand, l'informazione su chi è selezionato appare **solo dopo** la presentazione del blocco/voto. L'attaccante non ha tempo di isolare i validatori, a meno di avere un enorme controllo topologico in rete.

- ## Riduzione dei Fork

A differenza di PoW, in cui due miner possono scoprire simultaneamente un blocco e generare un "fork momentaneo", Algorand riduce i fork a situazioni eccezionali di proposizione multipla e si risolve in 1-2 passaggi BFT. Non si accumulano catene parallele, e chi riceve la finalità di un blocco può considerare la transazione irreversibile.

Struttura Interna e Smart Contract su Algorand

Account e Participation Key

- **Account**: definito da un address (corrispondente a un hash di una chiave pubblica). Detiene un saldo ALGO e può generare una "participation key" per validare blocchi.
- **Online vs. Offline**: L'utente può decidere di essere "offline" per non partecipare al consenso, delegando ad altri. Se partecipa attivamente, è "online" e può essere selezionato via VRF.

TEAL e dApp

Algorand supporta contratti scritti in **TEAL** (Transaction Execution Approval Language), un linguaggio a basso livello, e in "PyTEAL" (versione high-level in Python). Caratteristiche:

- **Semplicità**: TEAL è uno script stack-based, con istruzioni di base (add, sub, logic operator).
- **Atomic Transfer**: Algorand permette di collegare più transazioni in un gruppo, da eseguire in modo atomico.
- **Applicazioni**: contratti di pagamento condizionale, escrow, token creation (ASA).

Differenza con Ethereum: TEAL è meno flessibile di Solidity, ma più efficiente e "sicuro" per lo scopo di transazioni e contratti "finanziari".

Algorand Standard Assets (ASA)

Si possono creare token fungibili (come stablecoin, reward token, security token) o non fungibili (NFT) con le ASA, definendo parametri come "decimali, freeze, manager, clawback, destroy." L'insieme di tali parametri rende ASA un meccanismo molto utilizzato per DeFi su Algorand.

Dinamiche di Stake e Governance

Ricompense e Staking

All’inizio, Algorand distribuiva ricompense di staking in modo automatico (basta tenere ALGO in un account “online”). Nel tempo, la formula è cambiata, focalizzandosi su un meccanismo di **governance**: i partecipanti bloccano i token per un periodo, votano proposte, e guadagnano reward se non infrangono la regola di lockup.

Governance On-chain

Algorand ha avviato un programma in cui i titolari di ALGO si registrano come “governor”, impegnandosi a mantenere i token “locked” per un intero periodo di governo. Nei referendum, chi vota partecipa a decisioni su parametri di rete, allocazione di fondi per progetti, ecc. In cambio, ottiene una parte delle emissioni di ALGO come ricompensa.

Confronto con Altri Algoritmi Innovativi

Avalanche

Avalanche raggiunge finalità rapida e scalabilità grazie a un meccanismo di sub-sampling e repeated voting. Invece di un comitato VRF, ogni nodo “intervista” un campione casuale di altri nodi per decidere la preferenza di blocco. Man mano che i sondaggi convergono, la rete stabilizza la decisione. Algorand, invece, adopera un comitato definito (anche se random) in ogni round, seguendo un flusso BFT “compatto”.

Ouroboros (Cardano)

Cardano assegna slot leader su base random in epoche: chi possiede stake, con una certa probabilità, diventa produttore di blocchi. Tuttavia, la finalità non è immediata (richiede un certo numero di blocchi e di epoche), salvo alcune versioni BFT-based (Ouroboros BFT, Genesis) che cercano di dare finalità rapida. Algorand, al contrario, fornisce finalità su ogni blocco, perché ha un meccanismo di voto BFT successivo alla proposta.

DPoS

Nei protocolli DPoS (EOS, Tron, Lisk, ecc.), un numero ristretto di delegati produce i blocchi, garantendo TPS elevate ma riducendo la decentralizzazione effettiva a un set di 21 (o 27) “Block Producer.” Algorand vuole che ogni account possa partecipare su base stake, senza “delegare potere” a super-nodi. Ciò teoricamente rende Algorand più democratizzato.

Critiche e Limiti di Algorand

Concentrazione di Stake e Fondazione

Al lancio, la **Algorand Foundation** e i primi investitori possedevano una grande porzione di ALGO. C'è chi critica che in tale scenario, se la fondazione e i top holder si coordinassero, potrebbero superare 1/3 e "catturare" la catena. Dall'altro lato, la Fondazione sostiene di star distribuendo gradualmente i token e promuove una partecipazione larga.

Ecosistema Smart Contract Meno Maturo

TEAL e PyTEAL, pur essendo potenti per contratti finanziari, non dispongono di una community grande come la EVM di Ethereum. Molti progetti DeFi preferiscono Ethereum o catene compatibili (BSC, Polygon, Avalanche subnets). Algorand deve investire in tool, librerie e cross-compatibilità per attirare sviluppatori.

Difficoltà di Onboarding

Partecipare come validatore richiede generare la participation key e mantenere un nodo online. Molti utenti preferiscono lasciare i token in exchange o in portafogli "semplici", riducendo la decentralizzazione reale. Per combattere questo, la Fondazione promuove "self-custody" e delegazione a nodi affidabili, sperando di evitare la centralizzazione in pochi pool.

Osservazioni Sperimentali: Prestazioni, Applicazioni, Partnerships

Prestazioni Reali

In situazioni di test, Algorand dichiara alcune migliaia di TPS con 4-5 secondi di latenza. Nella mainnet, le prestazioni dipendono anche da quante transazioni effettivamente arrivano. Rispetto a Ethereum (15-20 TPS L1, pre-Merge), Algorand può offrire un throughput molto superiore. Non ha i costi di gas esorbitanti di Ethereum, ragione per cui stablecoin e DeFi su Algorand stanno crescendo.

DeFi su Algorand

- **Algofi**, **Folks Finance**, **Tinyman**: esempi di DEX e protocolli di prestito.
- **Yieldly**: lotterie e staking su Algorand.
- In confronto a Ethereum DeFi, la TVL è più piccola, ma i costi di transazione e latenza sono minimi, attirando utenti in cerca di efficienza.

Partnerships con Istituzioni

Algorand spesso citata in progetti di banche centrali o di e-government:

- **Marshall Islands**: Sperimentazione di una moneta digitale su Algorand.
- **Banca d'Italia** rumor su test con Algorand per gestire procedure di reporting.
- Diversi Paesi in via di sviluppo valutano Algorand come infrastruttura di supply chain e identity management.

Conclusioni Generali: Algorand come Emblema di Consenso VRF + PoS BFT

Algorand dimostra come, partendo da un **modello PoS** e integrando idee di **random sortition** (VRF) e BFT, si possono ottenere catene **permissionless** con finalità rapida e overhead computazionale ridotto.

1. **Elevata Sicurezza**: Se <1/3 di stake è malevolo, un attaccante ha probabilità minima di controllare i comitati.
2. **Decentralizzazione Potenziale**: Tutti i token holder possono essere estratti come validatori, senza necessità di un hardware speciale.
3. **Velocità**: Blocco ogni 4-5 secondi, finalità immediata. Adatto a pagamenti real-time e DeFi a bassa latenza.
4. **Sfide**: Distribuzione dello stake, minor ecosistema di dApp rispetto a EVM, e la necessità di partecipation key online per convalidare.

Guardando al futuro, è probabile che Algorand continuerà a evolversi, estendendo il supporto ai contratti più sofisticati e rafforzando la governance on-chain. Se la tokenomics si diffonderà e le integrazioni con bridging cross-chain si consolideranno, Algorand potrebbe guadagnare un ruolo di primo piano come catena efficiente e robusta, posizionandosi come un **algoritmo di consenso** di “nuova generazione” in grado di competere con altre chain ad alta velocità e a convincere attori istituzionali.

Da un punto di vista accademico, Algorand è un riferimento importante nell’evoluzione della “teoria del consenso” e nella combinazione di BFT con PoS e VRF. Comprenderlo permette di vedere come la blockchain possa andare **oltre** le soluzioni “classiche” e spingersi verso un “trilemma” meglio risolto, con un’attenzione costante sia a questioni di sicurezza (Byzantine e località del consenso) sia a questioni di usabilità (tempo di finalità e throughput).