IOTA: A Scalable and Feeless Distributed Ledger

1. Introduction to IOTA and the Tangle

IOTA is a permissionless distributed ledger technology designed for the Internet of Things (IoT). Unlike Bitcoin or Ethereum, which group transactions into blocks, IOTA organizes its transactions into **bundles** and stores them in a **Directed Acyclic Graph (DAG)** called the **Tangle**. Each new transaction must validate two previous transactions, eliminating the need for miners and enabling **feeless, scalable** transactions.

2. Core Components

- **Clients**: External users or applications issuing transactions.
- **Nodes**: Core participants validating transactions, solving lightweight cryptographic puzzles (proof-of-work) to deter spam.
- **Permanodes**: Specialized nodes storing the entire Tangle history, optimized for complex queries, not transaction issuance.

3. Transaction Lifecycle in IOTA

To issue a transaction, a node follows these steps:

1. **Bundle Creation**: Group inputs and outputs into a bundle.
2. **Weight Assignment**: Define the bundle's weight to influence its validation speed.
3. **Proof-of-Work**: Solve a puzzle proportional to the bundle's weight.
4. **Tip Selection**: Choose two "tips" (unconfirmed transactions) to approve using a random walk from the genesis.
5. **Validation**: Check for integrity and detect double-spending.
6. **Propagation**: Share the bundle and its approved tips over the network.
7. **Monitoring**: Reattach if not confirmed within time, influenced by cumulative weight of bundles.
8. **Consensus**: Achieved through probabilistic tip approval and confirmation confidence metrics.

The **Tangle** grows as transactions validate each other. Over time, snapshots remove old transaction data to reduce storage overhead.

---

4. Coordicide: Eliminating the Coordinator for Full Decentralization

The original IOTA network used a **Coordinator** to provide finality and security through periodic "milestone" transactions. While effective for early-stage security, this introduced centralization and hindered full decentralization.

Coordicide is the name of IOTA's ambitious project to remove the Coordinator and replace it with a **modular, decentralized architecture**. It involves the development and integration of several key components:

4.1. Goals of Coordicide

- Achieve **full decentralization** and censorship-resistance.
- Preserve IOTA's core benefits: **feeless transactions** and **high scalability**.
- Provide strong **security guarantees** against Sybil and double-spending attacks.
- Ensure network **robustness** under diverse and dynamic conditions.

4.2. Key Components of Coordicide

- **Global Identity Layer (Node IDs)**: Every node receives a verifiable cryptographic ID, establishing accountability in consensus and communication.
- **Auto-Peering**: Instead of manually setting neighbors, nodes use Mana and verifiable identities to **automatically and securely discover peers**. This ensures a dynamic and fair network topology.
- **Mana (Reputation System)**: Nodes earn **Mana** by issuing transactions. This decaying metric:
    - Secures auto-peering and consensus participation.
    - Defends against Sybil attacks by limiting resource access.
    - Prioritizes honest, active nodes.
- **Rate Control**: Transaction throughput is regulated based on each node's Mana, preventing spam and overload while fairly allocating network bandwidth.
- **Fast Probabilistic Consensus (FPC)**: A lightweight, voting-based consensus where nodes randomly sample each other's opinions.
  In FPC, decisions are probabilistic and converge quickly, even under adversarial conditions.
  it Incorporates random tie-breaking (via verifiable random functions) to avoid deadlock.
- **Modular Tip Selection**: Tip selection (choosing unconfirmed transactions to approve) is decoupled from consensus. Nodes use efficient, attack-resistant algorithms, improving speed and resilience.

4.3. Anti-Malicious Behavior and Security

- **Berserk Detection**: FPC includes mechanisms to detect **malicious nodes** who send inconsistent votes to peers. These nodes are exposed by comparing voting lists (v-lists) and sharing them with signed proofs.

- **Verifiable Random Functions (VRF)**: Ensures randomness and unpredictability in voting while remaining deterministic and verifiable.

4.4. Implementation Strategy

Coordicide is designed with **modularity and adaptability** in mind. Each component (peering, consensus, rate control, etc.) can evolve independently and be replaced without disrupting the network.

Prototype networks (e.g., GoShimmer) have tested Coordicide features in isolation and in combination. These testbeds help validate the design under real-world conditions before mainnet deployment.

5. Mana and Sybil Protection

Mana is a central mechanism in Coordicide. It provides Sybil protection without requiring resource-intensive mining or fees

Nodes receives mana for they contribution to the consensus, the nodes with more mana have a higher weight

6. Fast Probabilistic Consensus (FPC)

FPC is IOTA's consensus protocol post-Coordicide. Its main strengths:

- **Efficiency**: Suitable for IoT devices with limited resources.

- **Security**: Resilient to Byzantine and Sybil attacks, especially with Mana-based quorum selection.

- **Convergence**: Rapid consensus on valid transactions via probabilistic majority voting.

The protocol cycles through **multiple voting rounds**, during which:

- Each node samples a quorum of peers.

- The node updates its opinion based on the sampled average and a random threshold.

- The process repeats until all nodes converge to the same decision or reach a fallback rule.

This decentralized, opinion-based model enables IOTA to finalize transactions quickly and securely, without blocks or a leader.