Tangle - datastructure behind IOTA. Directed grapgh that holds transactions. TX- vertex. Transaction joins - it chooses 2 previous to approve. Unapproved TX - tips. Two tips to approve. Poisson point process - model how transaction arrive. λ - transaction rate. Small λ - chain, huge λ - all to one connected. In the model, we make each transaction invisible for a certain period after it arrives (h). Unweighted random walk - from genesis to tip with equal probability.

Lazy tips - approve old TX, but not new one. To avoid it - cumulative weigh for a random walk. If superwighted graph- some of TX will never be approved. α - how important weight is. Markov Chain Monte Carlo technique, or MCMC - decide alpha each step.

All IOTA was created in genesis block. Approve - verify that the sender has that money. I he aproves bad transaction - his own transaction will never be approved. The approved has a list all the transaction approved by sender's tx. Account do not go below zero. Two txs and not enoght balance for both - double spending solves with weighted graph.

Confirmation confidence. Run the algo 100 times, see how many of 100 tips approve our tx. Every two minutes - milestone tx to have 100% confirmation confidence.

Organizing transaction bundles in DAG. Three main roles: clients, nodes and permanodes.Client interact with network thought the nodes. Low-complexity PoW to prevend spamming and DoS attacks. Nodes does not create a huge computations - no reward. Premanodes - dedicated nodes from IOTA. Nodes store a copy of Tangle. They do not receive bundles txs or participate in consensus protocol. Instead, they receive Tangle updates. Client - tx creator and proposer, nodes - acceptor (validate)m recorder and query responder, permanodes - recorder and query responder. Unlimited bundle size. Tangle and Balances stored in RocksDB. Snapshot data as file. Snapshot purges the db. Node can increase weight during tx send.

IOTA is vulnerable to replay attacks, parasite chain or splitting attack.IOTA allows up to 500 TPS rate, but trade off with storage needs.

Property analysis based on three properties: consistency, ordering and finality. BA (validity, agreement, termination) or NC (persistence and liveness). BA - interactive and deterministic (on agreement), NC - non-interactive and probabilistic. In DAG systems consistency and finality - by consensuses, but Ordering is a new property. Consistency: strict, partial. Ordering: liear, topological(DAG). Finality: deterministics (BA - cannot be reverted), probabilistic(NA). Livenes-tx included, finality - tx can not be reversed. Finality in DAG: Trusted Roles (TRs) like byteball (trusted witnesses), Nano(voting based confirm), vite(snapshot chain created by assigned nodes) or prism (proposal blocks to determine finality)

DAG eliminates fees. IOTA relies on a centralized coordinator. The Coordicide project is focused to remove coordinator. Ideas: probabilistic consensus, approximate consensus. Challenges to remove coordinator : node accountability (use global node ID), autopeering (automates secure peer discovery) and node discovery, rate control(avoid network overload), consensus and voting(voting instead of tip selection) and tip selection(separate from consensus).

Current state - coordinator. Key features of current implementation: manual peering, rate control using PoW, slection using random walk, consensus via milestones, snapshots allows purging of old tangle history. Removing the coordinator requires: software redesign, new consensus, research and testing. Examplespeering, sybil protection, consensus without coordinator, tip selection etc. GoShimmer: experimental

In IOTA without cooringator it is crucial to associate tx with sending nodes to prevent spam and for voting-based consensus (no duble voting). Nodes are identified using public key . The public key is attached to each messages. These are used in communication leayer (cryptograpgy can be updated). Nodes signes tx with private key. But attacker can create a lot of fake identites: vulnerable to Sybil attacks. Sybil protection: Mana - reputation system on tokens. Mana is earned on sending value. Mana is not a token. Mana is used for rate control, autopeering and voting. Pending Mana - rate proportional to the token balance. Mana created then tokens are spent (to recipients), decay mechanism. Mana has maximum.

FPC - Fast Probabilistic consensus- lightweight, randomized voting protocol that enables odes to reach consensus and BT. Key concepts: random voting, low overhead, probabilistic model (not 100%). Nodes query opinions yes or no, based on responses and random threshold nodes update opinion. Random threshold 0.5-1, l round to complete. Three types of Byzanice behaviour: cautios 50%, semi cautios 38% (can skip respining), berserk(send different oinions to diff nodes in one round) 33%. Simulations was made using IVS - cautios mimic minority view or MVS + berserk attackers split nodes. Increas quorum size improves agreement. ManaFPC- FPC with sybil protection. Use mana to weight votes. Greater safety with same communication cost, because mana is stored in system. To detect berserk attack - V-list (list of opinions on previous round), verify, gossip the difference. Randomly with probability request v-lists (not every round). Improvement: check of the whole history of votes and not just the last round.