Enegiota: A scalable and feeless decentralized billing system on Tangle

Shikhar Mahajan
Supervisor: Prof. Sandeep Shukla

Indian Institute of Technology, Kanpur
Undergraduate Project Presentation

smahajan@iitk.ac.in

April 20, 2018

Overview

Introduction

Introduction

One of most actively pursued current Blockchain-related use case has been the Internet of Things. The three prominent reasons being: M2M Payments, Securing Identity of Things and inferably automating the execution of processes. But the reality is Blockchain & IoT arent ready to be in production yet mainly because of two limitations in current models: scalability and transaction fees.

Introduction

IOTA is based on Directed Acyclic Graphs and relates scalability in direct proportion to number of transactions in the network without having any provision of incentivised mining and subsequently transaction fees.
Tangle is the newly introduced distributed ledger architecture underlying the IOTA network.

Tangle

- Same underlying principles of P2P network and decentralization as that of a Blockchain
- Blockchain without the blocks and without the chains
- The genesis transaction created the maximum amount of IOTA tokens that can ever be circulated in the network
- All transactions in the Tangle are called sites which are also the nodes of the DAG
- The sites which are unconfirmed at given point of time are called tips

Tangle

- Each transaction or a site has an associated weight with it which is proportional to the amount of computation or work that the validating node has invested into it
- The proof of work linked with IOTA is similar to Hashcash but has much less complexity
- IOTA does not support smart contracts because it is primarily meant for lightweight IoT devices which are very resource and infrastructure constrained
- Is interoperable with other platforms like Ethereum that support Smart Contracts.

Tangle V/s Blockchains

- **Centralization** in terms of resources
- **Discrimination of participants** on the network on the basis of intensions
- **Consensus** is no longer decoupled but rather is an intrinsic part of the whole system in IOTA

Tangle V/s Blockchains

- **Scalability**
- **Quantum resistance** using a trinary hash function Curl and Winternitz one-time signatures.
- Ability to conduct **Micropayments**

The IOTA Network

Network

- Neighbours and mutual tethering
- Each node stores the entire state
- When a node issues a transaction or hears about one from its neighbors it sends it to all of its neighbors, so transactions eventually propagate through the network
- The data stored in IoT devices is governed by CAP (Consistency, Availability, Partition Tolerant) theorem

Transactions

- Every transaction in the Tangle references to two past unconfirmed transactions.
- Directly attests two transactions and indirectly a subsection of the Tangle

Basically a 3 step process:

1. Signing with private keys
2. Tip Selection via MCMC (Markov Chain Monte Carlo Box)
3. Proof Of Work

Assumptions

- Assume the rate of transactions to be λ
- λ is too small $\implies$ Blockchain
  λ is too large $\implies$ tangle with each site referencing the genesis transaction
- Assume the delay involved with the visibility (the time between preparation and propagation) of a transaction be 1 unit

Tip Selection Algorithms

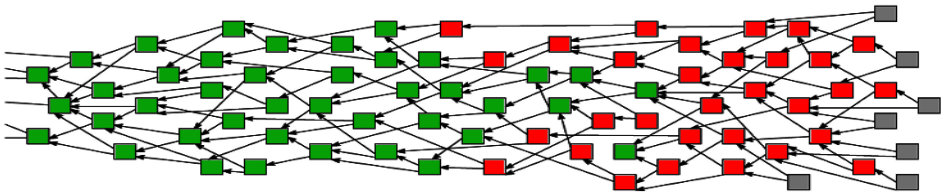
- **Unweighted Random Walk:** Put a walker on the genesis transaction, and have it start walking towards the tips. On each step it jumps to one of the transactions which directly approves the one we are currently on. We choose which transaction to jump to with equal probability, which is where the term unweighted comes from.

Tip Selection Algorithms

- **Weighted Random Walk:**
  - Built-in incentives against Lazy Tips i.e. tips that approves old transactions rather than recent ones.
  - Cumulative weight: 1+ approvers(direct+indirect) of a transaction. We are more likely to walk towards a heavy transaction than a light one.
  - Parameter α sets how important a transaction's cumulative weight is.
  - α is 0 $\implies$ Unweighted Walk
    α is too high $\implies$ super-weighted walk.
  - This method of setting a rule for deciding the probability of each step in a random walk is called a Markov Chain Monte Carlo technique, or MCMC.

Visit: `https://public-qnbiiqwyqj.now.sh/`[1]

Consensus


[2]

- Green blocks: Transactions on which consensus was achieved
  Red blocks: Transactions still uncertain on full acceptance
  Grey blocks: tips (unconfirmed transactions)
- For every confirmed transaction, there is a direct path leading to it from a tip
- Deciding transaction finality subject to users.

The double spending problem

The double spending problem

- The most well-known attack vector is the 51% attack. Research shows that actually only 34% of the network hashing power is needed to carry out the attack [3]
- IOTA mesh net: Each full node only sees one tiny part of the Tangle through their handful of neighbors. No one has a list of all IPs of all nodes.
- Because blockchains are not in mesh nets, Percentage of network hash rate is the only variable in the block chain 34% attack.

The double spending problem

However in IOTA, there are three variables involved:

1. X percentage of network hash rate
2. Omnipresence: Seeing the entire network topology at once
3. Y percentage of omnipotence: Neighboring with a sufficiently large portion of the network (Y% omnipotence)

The combination of X and Y will determine what percentage of edge nodes are taken down in the attack, and thus the effectiveness of the attack.
The edge nodes of compromised nodes would be overwhelmed with the attack and restart or just blacklist the attacker to become functional again.

The Coordinator

COO

- IOTA is in 'transition period'
- The Coo controls the transaction status of all the transactions presently
- Issues a new transaction called 'Milestone' which indicates all the full nodes to change tangles states in regular periods of times
- A transaction directly or indirectly referenced to by a milestone, will have the status of a confirmed transaction

Why Coo is in existence?

- Possibility that that the node in your neighbour is malicious and is trying to trick you into verifying its transactions
- The only role of Coo is to protect the network against the hash rate attack in its infancy stage
- In fact, its quite easy to change the Coo logic with a Random Walk Monte Carlo logic in its own private testnet

What if Coo is malicious?

- Each node looks at the information it gets from its neighbours and only propagates other neighbours about transactions that are valid
- The Coo is also no exception, if it starts issuing bad Milestones, full operational nodes will just reject them
- Decentralization still pertains

Downsides

- All its internal trinary notation have to be encapsulated in binary, leading into significant overhead in storage and computation
- Derivably, there is also a small but compulsory need of additional ASIC of IOTA in each IoT device to communicate with the network
- Violates the Rule 1 of Cryptography: "Dont roll your own Crypto"

Demonstration:
EnergIOTA

Thank You
Questions?

References


Alon Gal.
IOTA Tangle Visualisation.
https://public-qnbiiqwyqj.now.sh/.


Scott J.
IOTA Masterclass.
https://forum.iota.org/t/iota-consensus-masterclass/1193.


Eclipse Attacks.
https://eprint.iacr.org/2015/263.pdf.