IOTA White Paper Sharing

Yuchen Jiang
10/19/2018

Agenda

- **Basic concepts of IOTA**
- Stability of the system
- Possible attack scenarios
- Drawbacks and future

IOTA is not blockchain

- An innovative approach does not incorporate blockchain technology
- Drawbacks of blockchain
  - Transaction fee exists even for micropayments
  - Heterogeneous nature of the system

Tangle

- Tangle is a DAG
  - Xacts issued by nodes constitute the site set of tangle graph, the ledger for storing xacts.
  - The edge set of the tangle is obtained in the way that when a new xact arrives, it must approve two previous xacts.

Basic concepts of tangle

- A approves B:
  - If there is a directed edge between xact A and xact B
- A indirectly approves B:
  - If there is not a directed edge between xact A and xact B, but there is a directed path of length at least two from A to B
- Sites
  - Xacts represented on the tangle
- Node
  - Entities that issue and validate xacts.

Genesis xact

- In the beginning of tangle, there was an address with a balance that contained all of the tokens.
- Genesis xact sent these tokens to several other founder addresses
- All tokens were created in the genesis xact.

Main idea of tangle

- To issue a xact, users must work to approve other xacts.
- Nodes check if the approved xacts are not conflicting.
    - If a node finds that a xact is in conflict with the tangle history, the node will not approve the conflicting xact in either a direct or indirect manner.
- If a large number of nodes follow some reference rule, then for any fixed node it is better to stick to a rule of the same kind.

Node issues a xact

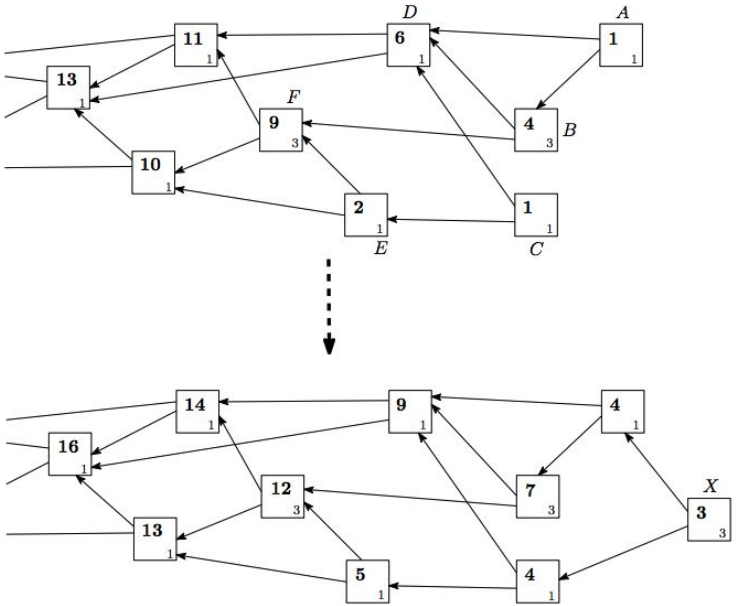
- The node chooses two other transactions to approve according to an algorithm.
- The node checks if the two transactions are not conflicting, and does not approve conflicting transactions.
- The node must solve a cryptographic puzzle similar to those in the Bitcoin blockchain.
    - finding a nonce such that the hash of that nonce concatenated with some data from the approved transaction has a particular form.
    - Much easier than that of bitcoin protocol

Weights

- The weight of xact is proportional to the amount of work that the issuing node invested into it.
- The weight can only be 3^n.
- A xact with a large weight is more important than a xact with a smaller weight.
- It is assumed that no entity can generate an abundance of transactions with “acceptable” weights in a short period of time.

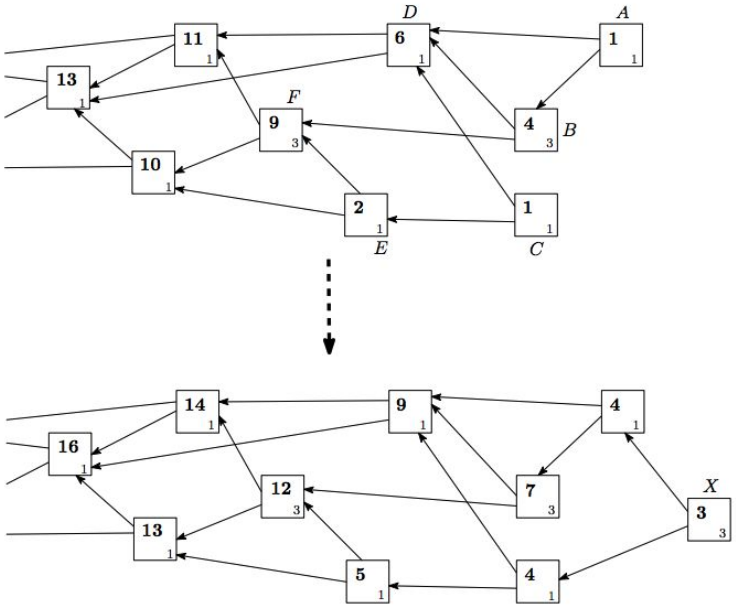
Weights

- Cumulative weight - the own weight of a particular transaction plus the sum of own weights of all transactions that directly or indirectly approve this transaction.
- Tips - Unapproved xacts in the tangle graph.



Weights

- Height - The length of the longest oriented path to the genesis
- Depth - The length of the longest reverse-oriented path to some tip.
- Score - The sum of own weights of all transactions approved by this transaction plus the own weight of the transaction itself.



Finality confidence

- The percentage of tips which directly or indirectly approves your xact.
- Also need to wait long if you want a high confidence
- More flexible in terms of xact latency

Agenda

- Basic concepts of IOTA
- **Stability of the system**
- Possible attack scenarios
- Drawbacks and future

Stability of the system

- L(t) is the total number of tips in the system at time t.
- Assumptions
  - Xacts are issued by a large number of roughly independent entities
  - All devices have approximately the same computing power
  - All nodes behave in the way that to issue a xact, a node choose two tips at random and approves them
  - Any node at the moment when it issues a xact, it observes the state of the tangle h time units ago rather than the actual state
  - The number of tips remains roughly stationary in time
- The expected time for a xact to be approved for the first time is 2h.

Stability of the system

- Cutset - any path from a xact issued at time t’ > t to the genesis must pass through this set
- Use the small cutsets as checkpoints for possible DAG pruning

Stability of the system

- Low load - the typical number of tips is small, and frequently becomes 1
  - A tip gets approved for the first time in O(lambda^-1) time units.
- High load - the typical number of tips is large
  - Depends on tip approval strategy
- Strategy to let xact be approved during high load
  - Issue an empty xact that approves its previous xact together with one of the better tips to increase the prob that empty xact receives approval
  - Based on heights and scores

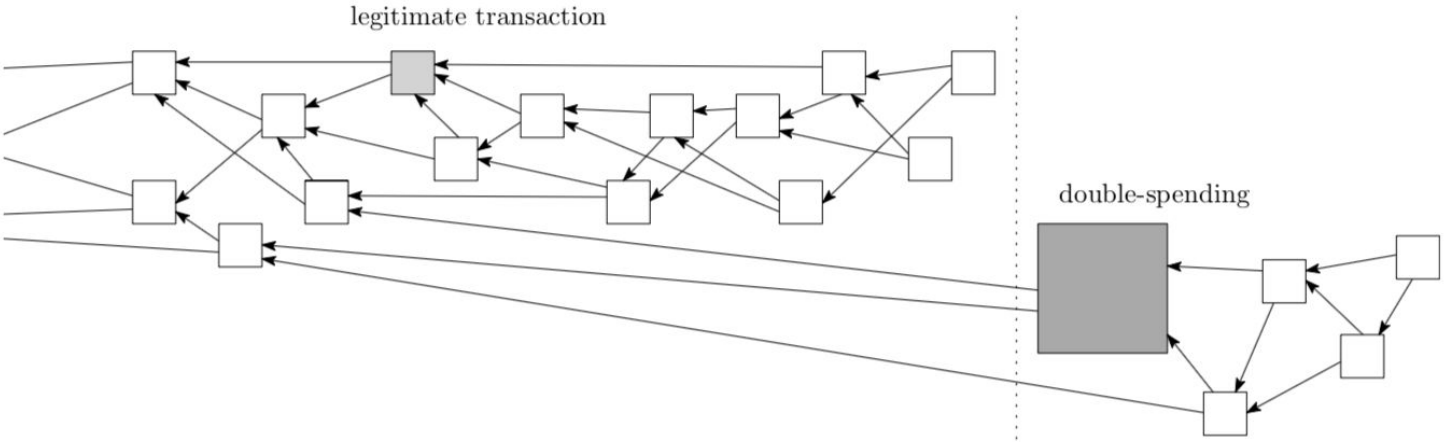
Agenda

- Basic concepts of IOTA
- Stability of the system
- **Possible attack scenarios**
- Drawbacks and future

Possible attack scenarios

- An attacker sends a payment to a merchant and receives the goods after the merchant decides the xact has a large cumulative weight
- Attacker issues a double-spending xact
- Attacker issues many small xacts that approve double-spending xact but not the original xact (or issue a big using all computing power)
- Attacker has a plethora of Sybil
- Attacker hopes dishonest subtangle outpaces the honest subtangle

Possible attack scenarios



Be careful when using cumulative weight as a decision metric to decide which of two conflicting xacts is valid.

Parasite chain attack

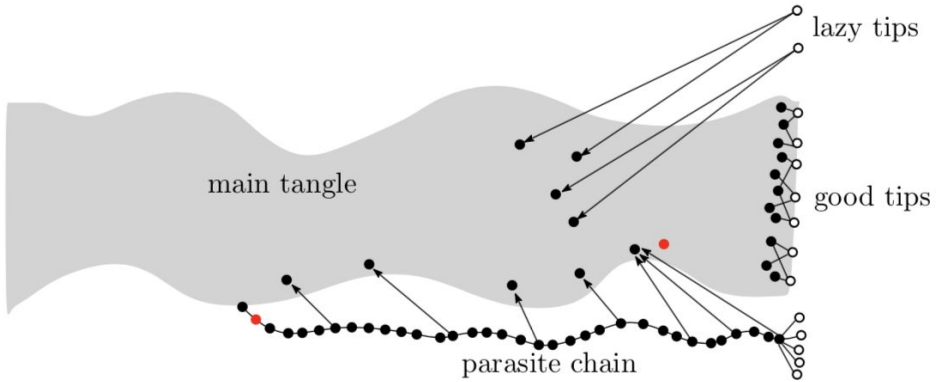
- Attacker secretly builds a subtangle that occasionally references the main tangle to gain a higher score.
- Score of attacker's tips is higher
- Attacker can artificially increase their tip count
- Don't use select strategy that involves a simple choice between available tips

Defend parasite chain attack - MCMC algorithm

- The idea is to place some articles, aka random walkers, on sites of the tangle and let them walk towards the tips in a random way.
  - Consider all sites on interval [W, 2W]
  - independently place N particles on sites in that interval
  - Perform random walks towards the tips if there is an edge
  - The two random walkers that reach the tip set first approve the tips. (discard random walkers that reached the tips too fast due to lazy tips)
  - Transition probability of the walkers are inversely proportional to the difference of cumulative weight

Defend parasite chain attack - MCMC algorithm

- Why this is good?
  - For lazy tips
  - For parasite chain attack



Splitting attack

- In the high-load regime, an attacker try to split the tangle into two branches and maintain the balance between them.
- Allow both branches continue to grow
- Place at least two conflicting xacts at the beginning of the split to prevent an honest node from joining the branches by referencing them both simultaneously
- The attacker would be able to spend the same funds on the two branches

Defend splitting attack

- Use ‘sharp-threshold’ rule that makes it too hard to maintain the balance between the two branches
- For two branches with similar total weight, select the first one with probability much higher than ½
- Make MCMC works this way
  - Choose a very rapidly decaying function f
  - Initiate the random walk at a node with large depth

Resistance to quantum computations

- A sufficiently large quantum computer could be very efficient for handling problems that rely on trial and error to find a solution
- Quantum computer: O(sqrt(N)); classical computer: O(N)

Resistance to quantum computations

- For bitcoin, one must check an average of 2^68 nonces to find a suitable hash that allows a new block to be generated
- In IOTA, the number of nonces that one needs to check in order to find a suitable hash for issuing a xact is not unreasonably large. (3^8)
- The time to find a nonce is not much larger than other necessary tasks

Agenda

- Basic concepts of IOTA
- Stability of the system
- Possible attack scenarios
- **Drawbacks and future**

IOTA Drawbacks

- PoW - work chip on every IOT device
- No smart contracts - not ones that require an order of xacts
- Unproven - not certain a xact can be confirmed after X minutes
- Centralization
  - Coordinator is a close-resource component made by IOTA team
  - Send out a xact (milestone) every minute
  - All the xacts approved by coordinator is 100% confirmed

Thank you!

Yuchen Jiang
10/19/2018