IOTA

Structure and Validation Method

2018.10.
JY

Agenda

- Blockchain vs IOTA
  - ➢ Blockchain
  - ➢ IOTA
- Key Factors
  - ➢ Directed Acyclic Graph
  - ➢ Markov Chain Monte Carlo Algorithm
- IOTA Structure - Tangle
  - ➢ Directed Acyclic Graph
  - ➢ Tip, Height, Depth
  - ➢ Approvals
  - ➢ Own Weight
  - ➢ Cumulative Weight
  - ➢ Minimum Weight Magnitude
  - ➢ Transaction Confirmation (Coordinator and MCMC)
  - ➢ How a Transaction is Created
- Pros and Cons
  - ➢ Pros and Cons of IOTA
- Reference
  - ➢ Reference

Blockchain vs IOTA

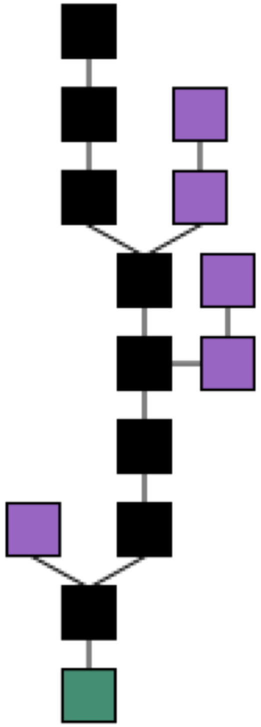
Blockchain

Definition

- A **blockchain** is a growing list of records, called *blocks*, which are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree root hash).

Block Structure

- A sequential chain of blocks where each block references its chronological predecessor.



IOTA

IOTA is a revolutionary new transaction settlement and data transfer layer for the Internet of Things (IoT).

- Introduces a new way of reaching consensus in a decentralized peer-to-peer system.
- Features
  - ➢ Scalability
    1. Increase in the number of transactions → Networks become stronger.
    2. Creates more IOTA transaction → The confirmation rates get better.
  - ➢ Decentralization
    1. No miners.
    2. Every transaction maker = Transaction validator.
    3. Every transaction makers actively participates in the consensus.
    4. In Bitcoin network, most hashing power are concentrated in few mining pools.
  - ➢ No transaction fees
    1. No transaction fees → Can be used for micropayments (able to send 1 IOTA to an address with no fee).
  - ➢ Quantum computing protection
    1. Quantum computing is in the early stages of development → Estimated that it will arrive between 2030 and 2050.
    2. Quantum computers will be able to "crack" current data encryption methods such faster than current classical computers.
    3. IOTA uses the Winternitz One-Time Signature which is a quantum resistant algorithm.

Key Factors

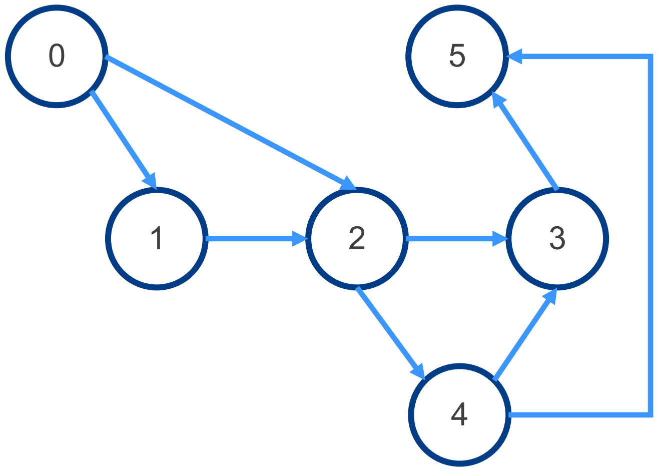
Directed Acyclic Graph (DAG)

Definition

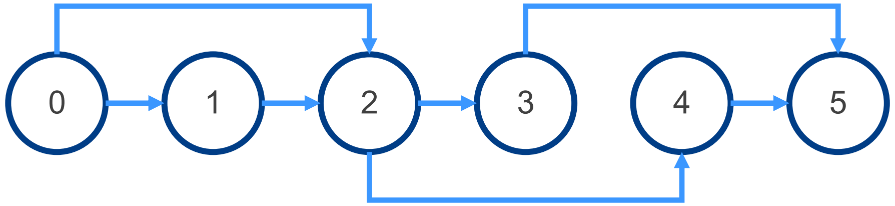
- A graph is acyclic if it has no cycles.
- A tree is a connected acyclic graph.
- Any graph without cycles is a forest, thus the components of a forest are trees.
- Directed Acyclic Graph is finite directed graph with no directed cycles.
  - ➢ Finite vertices and edges.

DAG structure allows transaction to be issued

- Simultaneously.
- Asynchronously.
- Continuously.



Directed Acyclic Graph (DAG)



Topological ordering

Markov Chain Monte Carlo (MCMC) Algorithm

Goal : To generate fair samples from some difficult distribution

Used in two ways:

1. Choose two other unconfirmed transactions (tips) when creating a transaction.
2. Determine if a transaction is confirmed.

Monte Carlo

- Sample from a distribution
  - ➢ To Estimate the distribution.
  - ➢ To compute max, mean.

Markov Chain Monte Carlo

- Sampling using “local information”
  - ➢ Generic “problem solving technique”.
  - ➢ Decision / optimization / value problems.

IOTA Structure

(Tangle)

Tangle - Directed Acyclic Graph

Directed Acyclic Graph (DAG) based transaction settlement and data integrity layer focused on the Internet-of-Things (IoT).

- No miners.
- Two distinct types of participants.
  - ➢ One who issue transactions.
  - ➢ One who approve transactions.
- Key difference from other blockchain networks.
  - ➢ “Blockless” blockchain.
  - ➢ Rather than transactions created by users being incorporated into blocks by miners, users function as both the miners and the creators of transactions.
- Essentially a string of individual transactions that are interlinked to each other.
- Stored through a decentralized network of node participants.
- Transactional settlement (especially feeless and fast micropayments).
- Data integrity.

IOTA Tangle Visualization

Tangle - Tip, Height, Depth

Tip

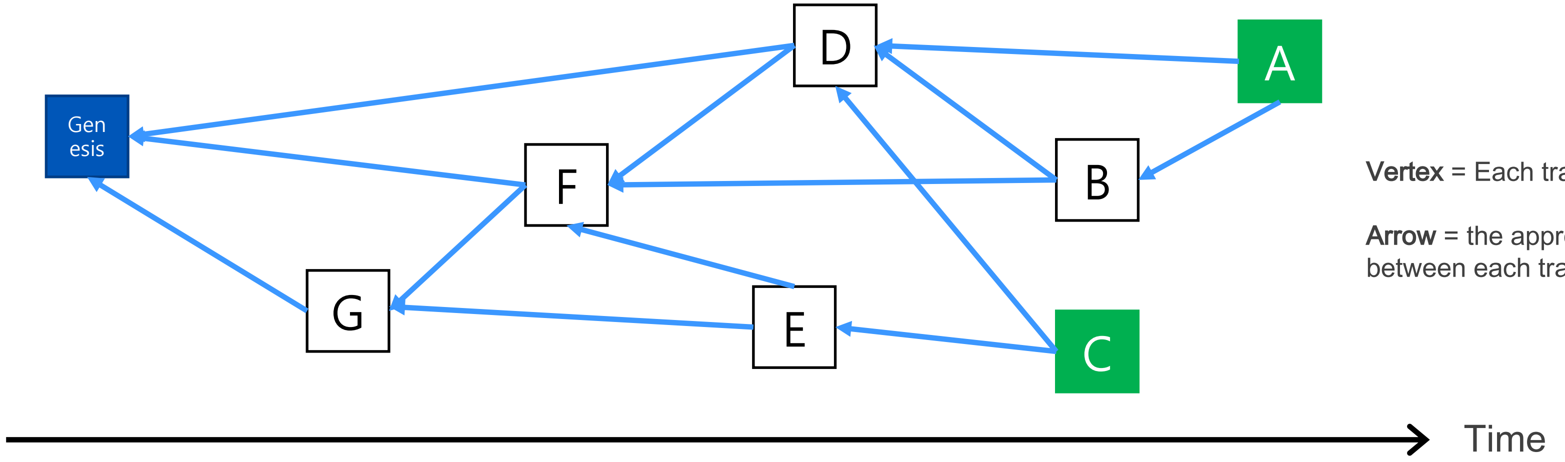
- Unconfirmed transactions.
- They are transactions which have no other transactions references them but they should each reference two previous transactions.

Height

- The length of the longest oriented path to the genesis.
- e.g. Transaction G has a height of 1.
  Transaction D has a height of 3.

Depth

- The length of the longest reverse-oriented path to some tip.
- e.g. Transaction G has a depth of 4.
  Transaction D has a depth of 2.



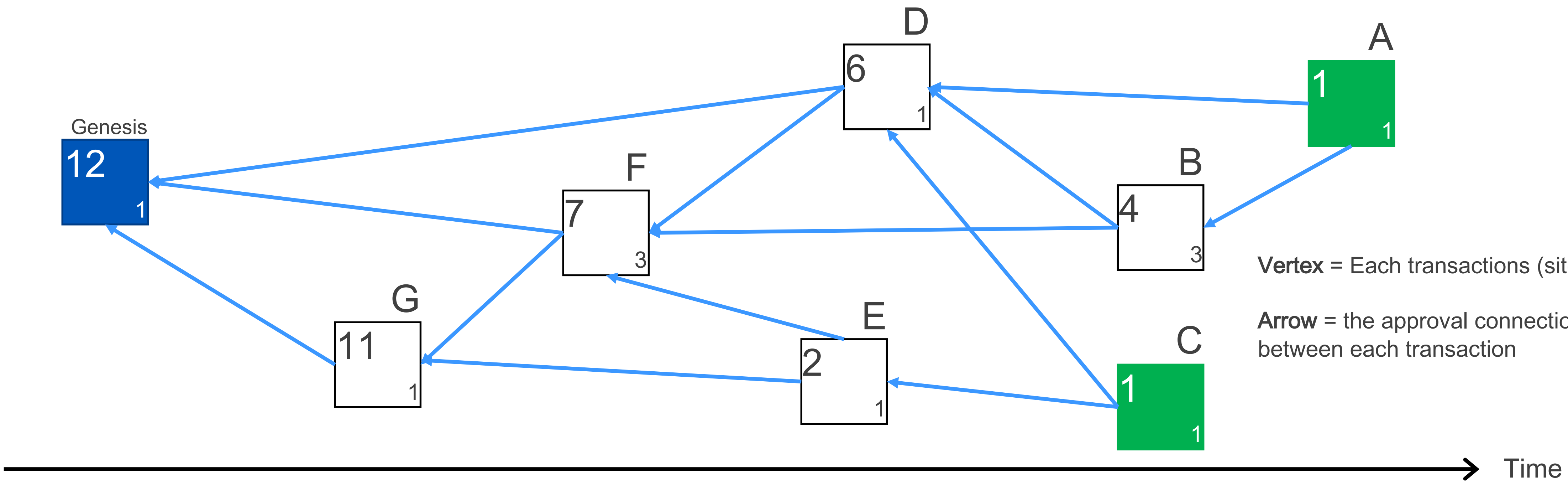
Vertex = Each transactions (sites)

Arrow = the approval connections between each transaction

Tangle - Approvals

Each incoming transaction needs to approve two previous transaction in order to become validated, and as a result, the edges (arrows) represent the connection of each transaction to previous ones.

- Direct approvals → Transaction B approves Transaction D and Transaction F.
- Indirect approvals → Transaction B approves Transaction G.
- Genesis contains all the MIOTA (IOTA coin) that will ever be created. Transaction A is referred to as a transaction tip because it is an unapproved transaction, which you will see it is important in the transaction structure.



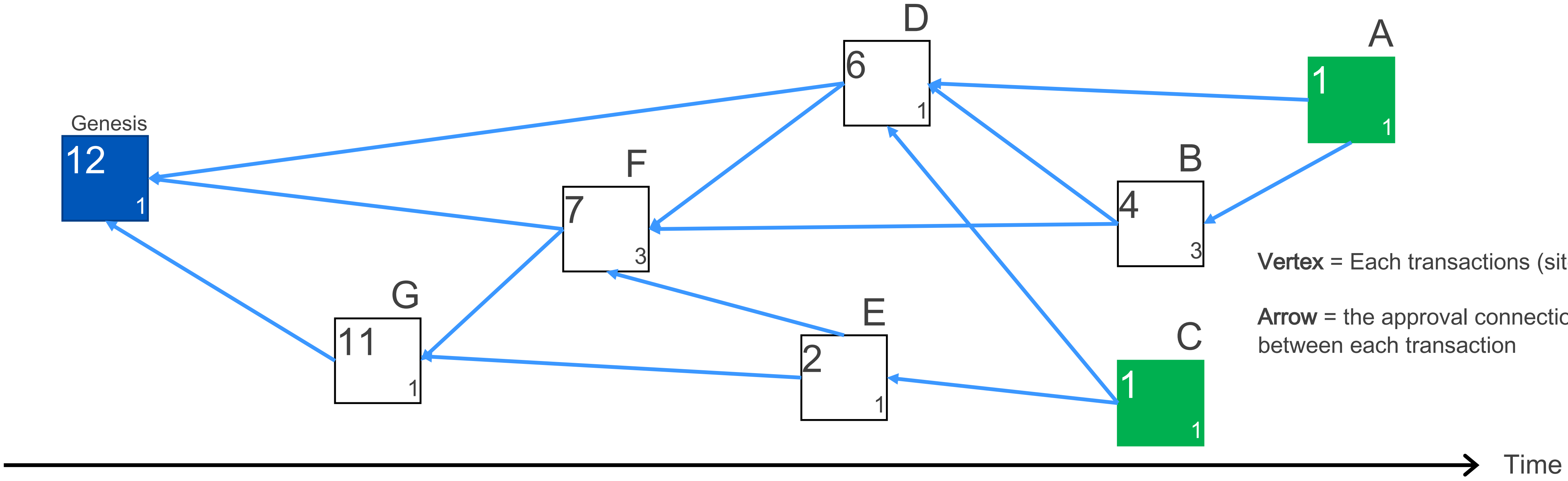
Vertex = Each transactions (sites)

Arrow = the approval connections between each transaction

Tangle - Own Weight

Own Weight

- Every transactions has an initial weight called the own weight (1, 3, 9, etc. → 3^n, where $n \leq 0$).
  - Current initial own weights are all 1's.
- The own weight is determined by the effort put by its issuing node.



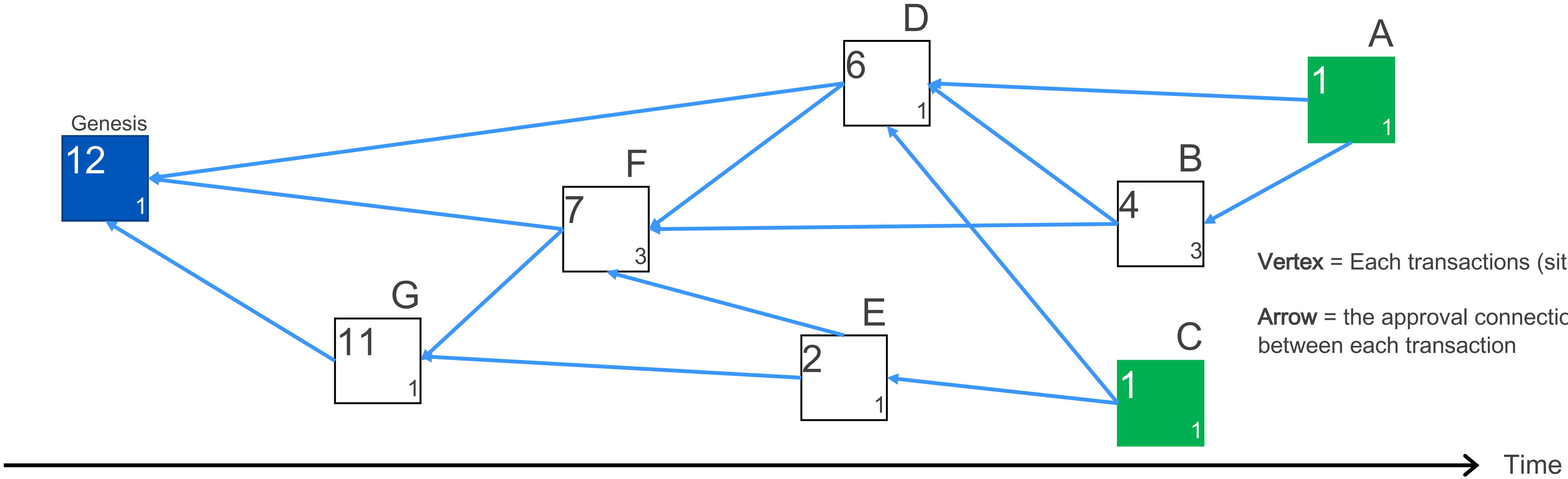
Vertex = Each transactions (sites)

Arrow = the approval connections between each transaction

Tangle - Cumulative Weight

Cumulative Weight

- $Cumulative\ weight = Own\ Weight + \sum Weights\ of\ all\ transaction\ that\ directly\ or\ indirectly\ approve\ this\ transaction$
  - ➢ A very important metric for transactions on its way to network approval.
  - ➢ A transaction with a larger cumulative weight is more “important” than a smaller one.
- Each new transaction added to the tangle increases the ancestors cumulative weight by the weight of that transaction.
  - ➢ Older transactions grows in importance over time.
- It avoids spamming and other attack styles.



Vertex = Each transactions (sites)

Arrow = the approval connections between each transaction

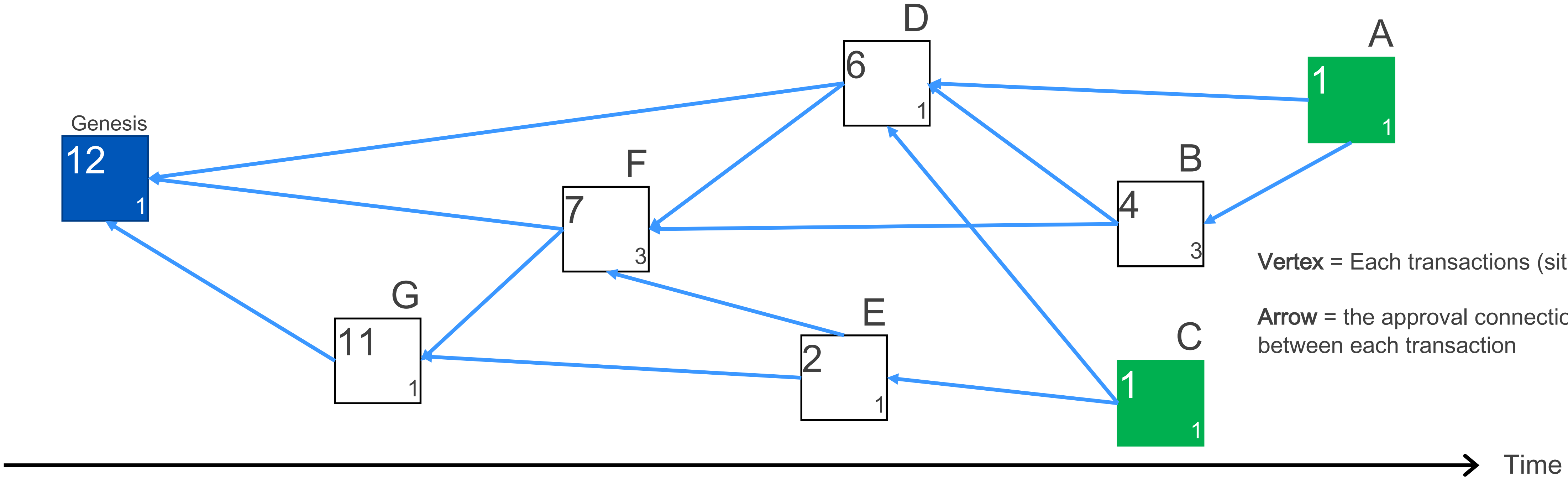
Tangle - Minimum Weight Magnitude

Minimum Weight Magnitude (MWM)

- The difficulty of Proof-of-Work (PoW).
- IOTA’s PoW algorithm is similar to Hashcash.
- The MWM is the number of trailing zeros.

e.g. Assume MWM = 4.

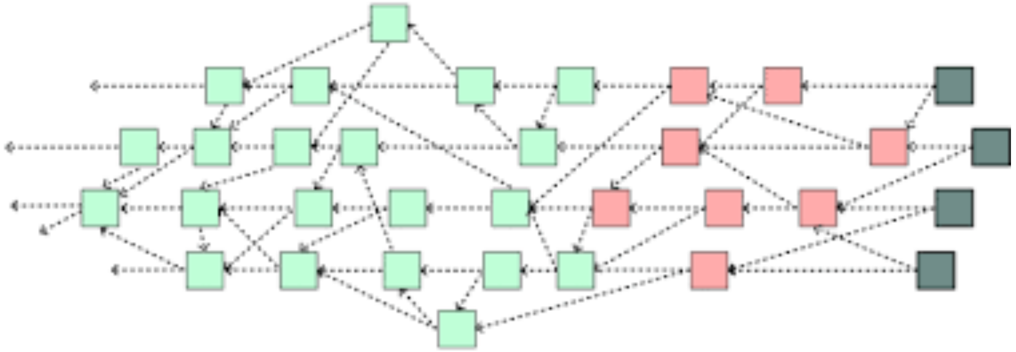
- hash(transaction data + counter) = …9f86d081884c7d659 (PoW not ok).
- hash(transaction data + counter) = …884633bce1d660000 (PoW ok).



Vertex = Each transactions (sites)

Arrow = the approval connections between each transaction

Tangle - Transaction Confirmation (Coordinator and MCMC)



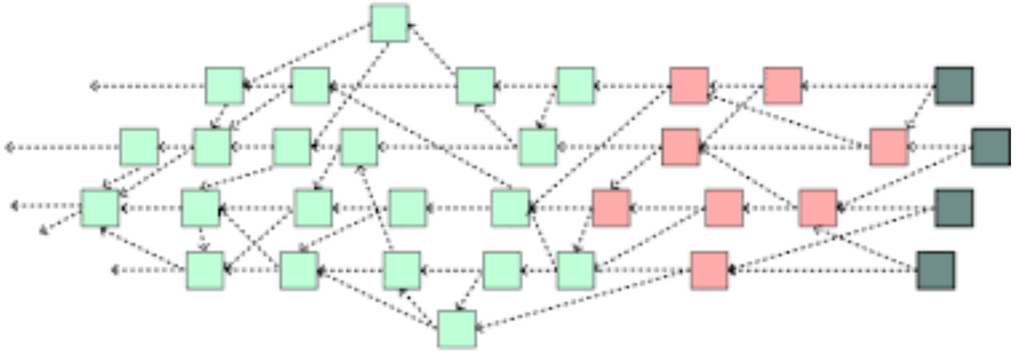
https://coincentral.com/what-is-iota-cryptocurrency-coin/

Green : achieved consensus a.k.a confirmed transactions.
Red : uncertain on their full acceptance.
Grey : tips.

Goal : Make all the transactions to green.

- Green blocks are indirectly approved by ALL the grey blocks. For every green blocks, a path leading from a tip exists.
- In order to determine the confirmation level of the transaction, calculate the depth and execute the Markov Chain Monte Carlo algorithm N times. Therefore, the probability of the transaction being accepted is M of N, where M is the number of times you land on a tip that has a path to the transaction.

Tangle - Transaction Confirmation (Coordinator and MCMC)

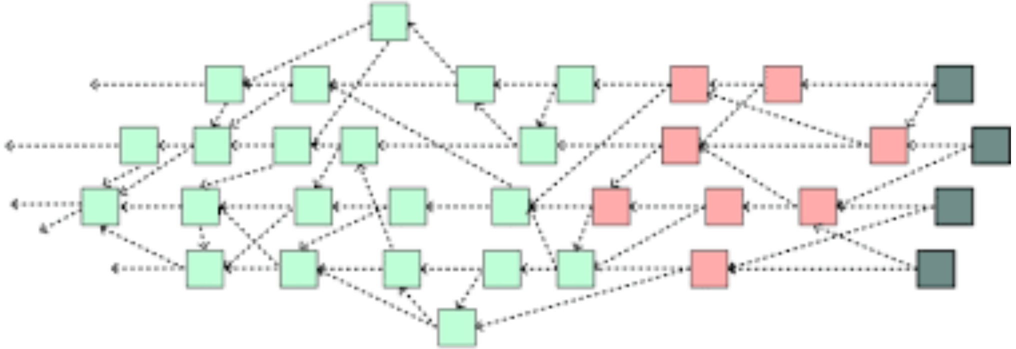


https://coincentral.com/what-is-iota-cryptocurrency-coin/

e.g. Assume we executed RWMC 100 times and number of tips are 70.

- The transaction is 70% confirmed.
- The merchant decides whether or not to accept the transaction and exchange good.
  - ➢ This is same as Bitcoin where you wait for at least 6 blocks for high value transactions.
- Transactions with bigger depths takes longer to be validated.

Tangle - Transaction Confirmation (Coordinator and MCMC)



https://coincentral.com/what-is-iota-cryptocurrency-coin/

Tangle whitepaper p.19

From the above discussion it is important to recognize that the inequality λ > μ should be true for the system to be secure. In other words, the input flow of "honest" transactions should be large compared to the attacker's computational power. Otherwise, the estimate (12) would be useless. This indicates the need for additional security measures, such as checkpoints, during the early days of a Tangle-based system.

Tangle - How a Transaction is Created

3 Step Process:

Step 1. Signing

- Node (computer / mobile) constructs the bundle
  - ➢ Bundle consists multiple transactions containing credits to the receiving address (output) and debits from the spending addresses (inputs).
  - ➢ Bundle represents a transfer of value.
- Sign the transaction inputs with personal private key.
  - ➢ A transaction is an object containing several fields: address, signature, value and tag.
- There are two types of transactions.
  - ➢ One where you transfer value and thus, have to sign inputs.
  - ➢ One where you simply send a transaction to and address with no value transfer (e.g. message).

Tangle - How a Transaction is Created

3 Step Process:

Step 2. Tip Selection

- Node chooses two other unconfirmed transactions (tips) using Markov Chain Monte Carlo (MCMC) algorithm.
- The tip selection is a process whereby you traverse the tangle in a random walk to randomly choose two transactions which will be validated by your transaction.
  - ➢ Your transactions checks for example if the descendants of that transaction is valid.
  - ➢ If these transactions are valid they will be added to your bundle construct.
    - ➢ branchTransaction and trunkTransaction.

Tangle - How a Transaction is Created

3 Step Process:

Step 3. Proof-of-Work (PoW)

- Node checks if the two transactions are not conflicting.
- The node must do some Proof-of-Work by solving a cryptographic puzzle (hashcash).
- Hashcash works by repeatedly hashing the same data with a tiny variation until a hash is found with a certain number of leading zero bits.
- The PoW is to prevent spam and Sybil attacks.
  - ➢ A Sybil attack is based on the assumption, that half of all hash power is coming from malicious nodes.
- Once the bundle is contructed, signed and the tips are added to the bundle.
- When the PoW is done, the nonce of the transaction object should be updated. The transaction can now be broadcasted to the tangle network and wait for it to be approved by someone else.

Pros and Cons

Pros and Cons of IOTA

Pros

- Billions of transactions per second at scale.
- Every transactions need to confirm 2 transaction at first → Instant at scale.
- Transaction fees.
- Scalability.
- Lightweight.
- Quantum-secure (Quantum-proof).

Cons

- No mining.
- New technology.
- Not blockchain technology.

Reference

Reference

IOTA
https://docs.iota.org/introduction
https://www.iota.org/getting-started/faqs

Cornell, Introduction to Markov Chain Monte Carlo
http://www.cs.cornell.edu/selman/cs475/lectures/intro-mcmc-lukas.pdf

Duke, Intro to Markov Chain Monte Carlo
http://www2.stat.duke.edu/~rcs46/lecturesModernBayes/601-module6-markov/markov-chain-monte-carlo.pdf

BLOCKONOMI, What is The Tangle? Complete Guide to IOTA’s Directed Acyclic Graph (DAG)
https://blockonomi.com/iota-tangle/

Thank you