IOTA TUTORIAL 1

What is IOTA and some terminology explained

IOTA

- IOTA is not an acronym for Internet of Things, (IoT) but it just mean something very small.

- David Sønstebø, Sergey Ivancheglo, Dominik Schiener and Serguei Popov founded IOTA in 2015.

- In Nov and Dec, 2015 IOTA hosted an Initial Coin Offering (ICO). In Dec 22, 2015 they raised 1337 BTC (approx. USD$0.5M) for project development.

- All tokens were sold to the ICO investors.

IOTA

- The IOTA team has setup the IOTA Foundation, a non profit foundation registered and headquartered in Berlin (Germany) focused on developing and standardising new distributed ledger based technologies.

- IOTA main focus is Internet of Things and the Machine Economy but this technology is well suited for payments between humans as well.

- The mainnet was online since July 11, 2016.

- The IOTA white paper can be found at: https://iota.org/IOTA_Whitepaper.pdf

IOTA

- All IOTA's which will ever exist have already been created.
  There will be no mining involved. The total IOTA supply is:
  $(3^{33}-1) / 2 =$ **2,779,530,283,277,761** IOTAs = ~2.8 Peta IOTA's.

- In contrast in October 8th, 2140 there will be a maximum of **20,999,999.9769** Bitcoins (~21 million BTC) mined. In Nov 11, 2017 there are already **16,675,488** Bitcoins mined, approx 79% of its total.

- The maximum number of available Bitcoins converted into its smallest unit is:
  2,099,999,997,690,000 Satoshis = ~2.1 Peta Satoshi's.

- Which means there will be ~32% more IOTA's compared to Bitcoins in October 8th, 2140.

IOTA FEATURES

- Scalability
- Decentralisation
- No transaction fees
- Quantum computing protection

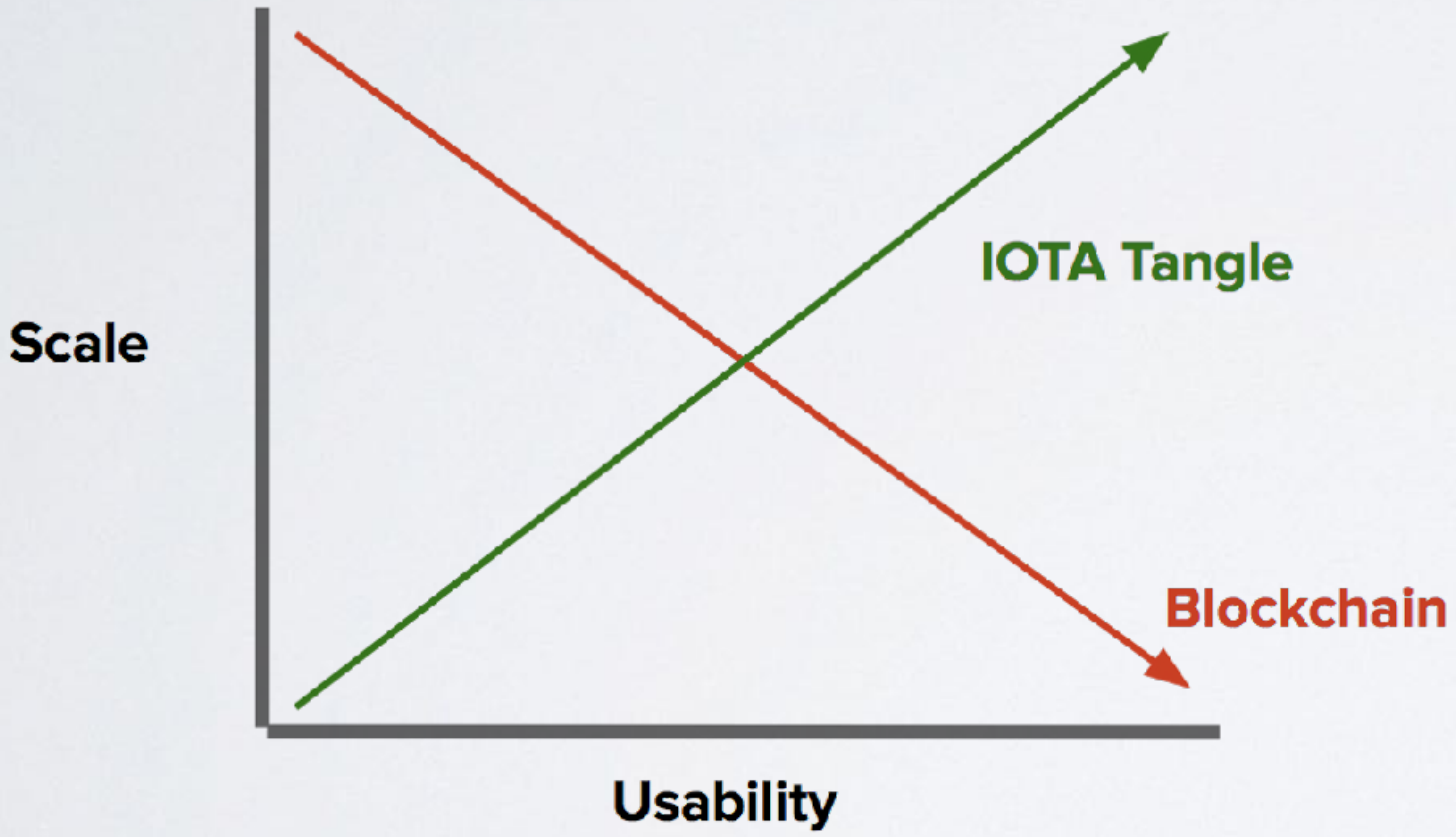
IOTA FEATURES: SCALABILITY

- The network becomes stronger when the number of transactions increases.

- A stress test conducted in April 2017 already shows 112 confirmed transactions per second in a small network of 250 nodes.

IOTA FEATURES: SCALABILITY

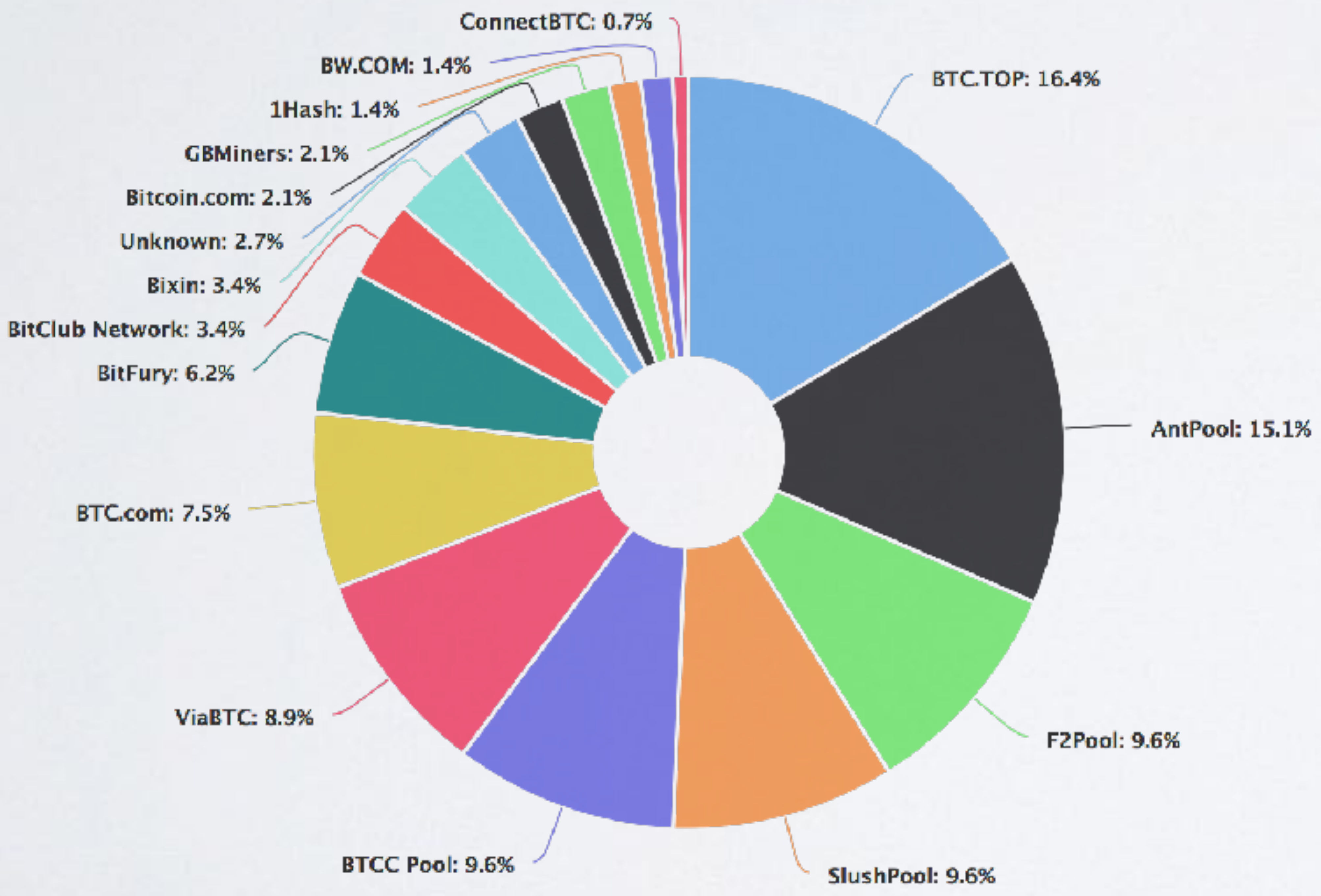
- IOTA can achieve high transaction throughput.
  If more IOTA transactions are created, the confirmation rates are getting better.



IOTA FEATURES: DECENTRALISATION

- IOTA has no miners. Every transaction maker is also a transaction validator which means every transaction maker actively participates in the consensus.

- If we look at the Bitcoin network most hashing power are concentrated in a few mining pools.



https://blockchain.info/pools
Graph: Oct 30, 2017

IOTA FEATURES: NO TRANSACTION FEES

- IOTA has no transaction fees which means IOTA can be used for micropayments.
- You can send 1 IOTA to an address with no fees charged.
- An IOTA is the smallest unit which is the same as 1 Satoshi (Bitcoin) or 1 Wei (Ethereum).
- Making micropayments in the Bitcoin network makes no sense if the fees are higher than the transaction value.

IOTA FEATURES: QUANTUM COMPUTING PROTECTION

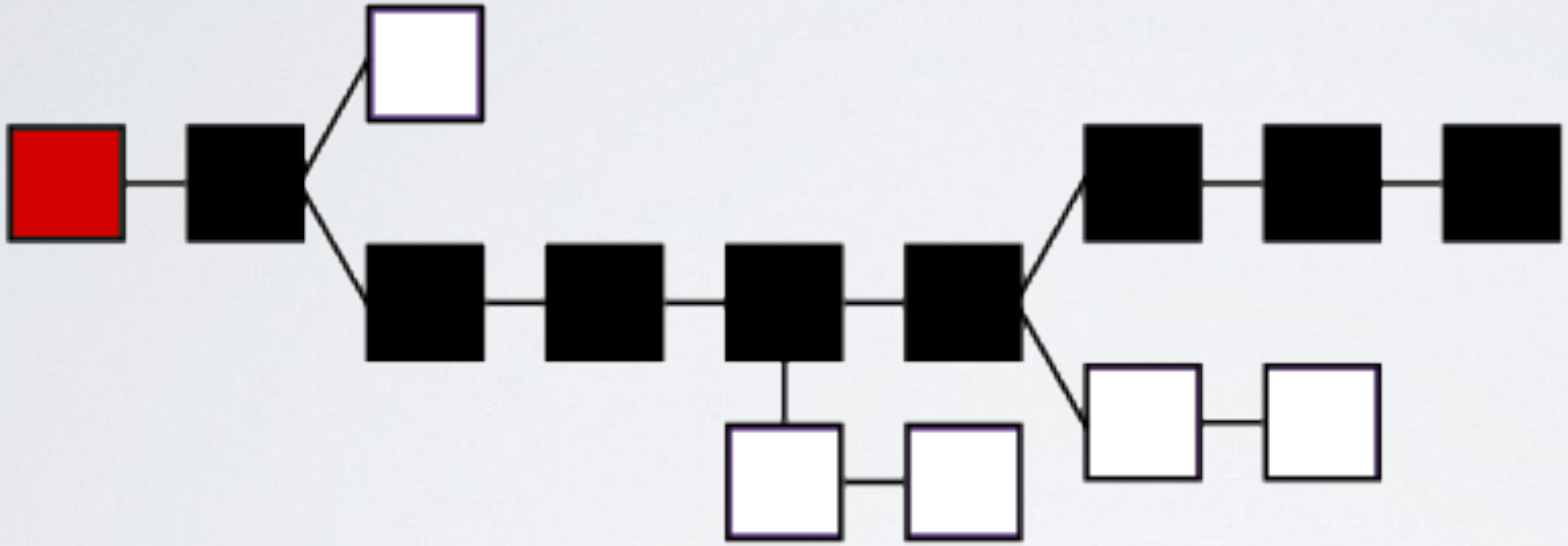
- Quantum computing is still in the early stages of development but it is estimated that this technology will arrive between 2030 and 2050.

- Quantum computers will be able to "crack" current data encryption methods much faster than current classical computers.

- IOTA uses the Winternitz One-Time Signature Scheme which is a quantum-resistant algorithm. See: https://eprint.iacr.org/2011/191.pdf

BLOCKCHAIN VS TANGLE

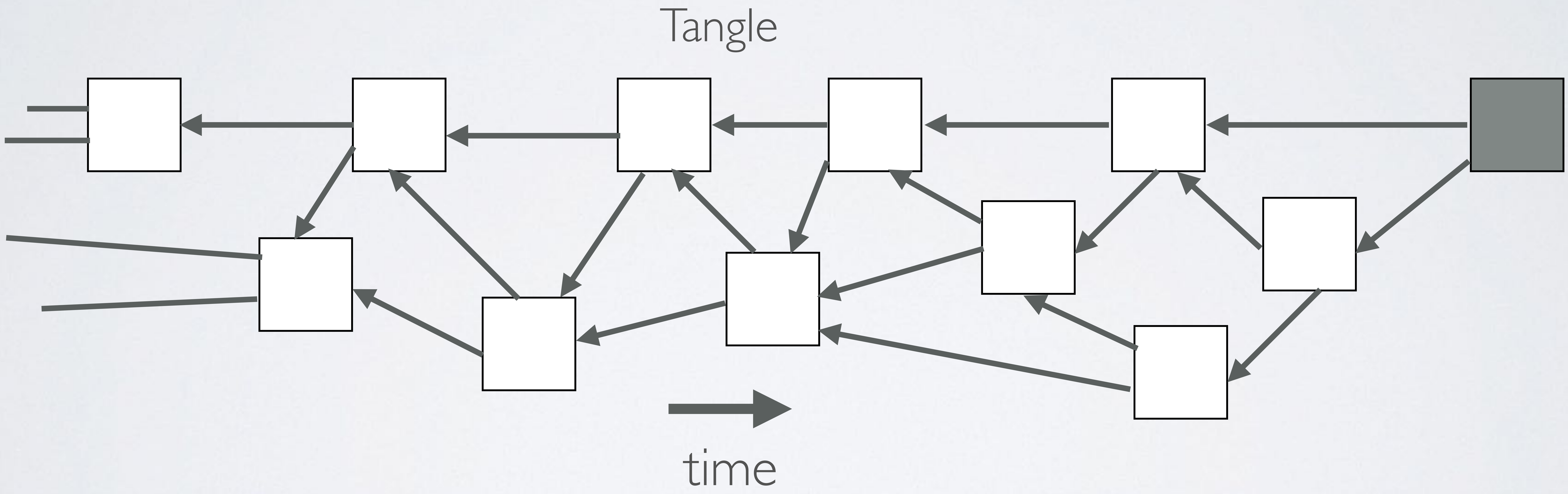
- In a Blockchain network (for example Bitcoin) multiple transactions are stored in blocks and the blocks are sequentially connected to each other ("chained").



- IOTA is the 3rd generation public permissionless distributed ledger, based on a Directed Acyclic Graph (DAG). IOTA called this DAG the tangle.
  The tangle is **NOT** the same as the Blockchain.

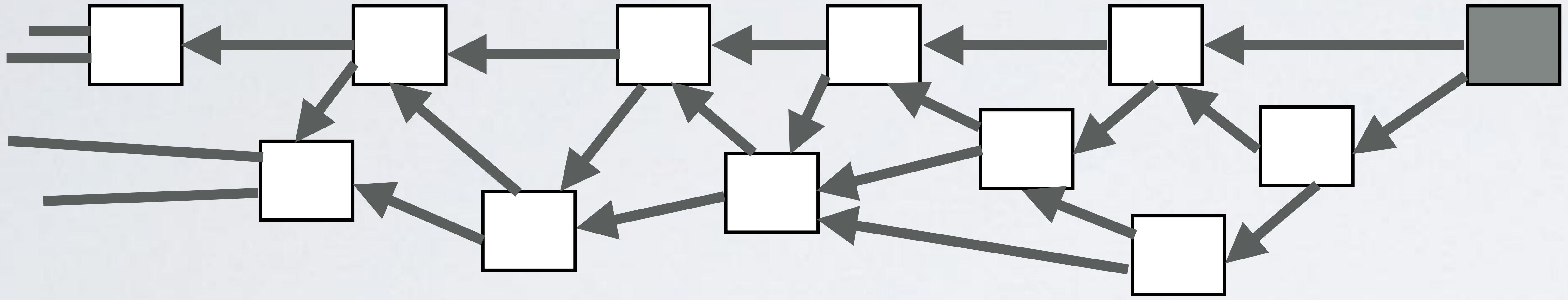
TANGLE

- A tangle is a data structure based on Directed Acyclic Graph (DAG). Each square represents a **single transaction**. Each transaction always validates 2 previous non validated transactions.

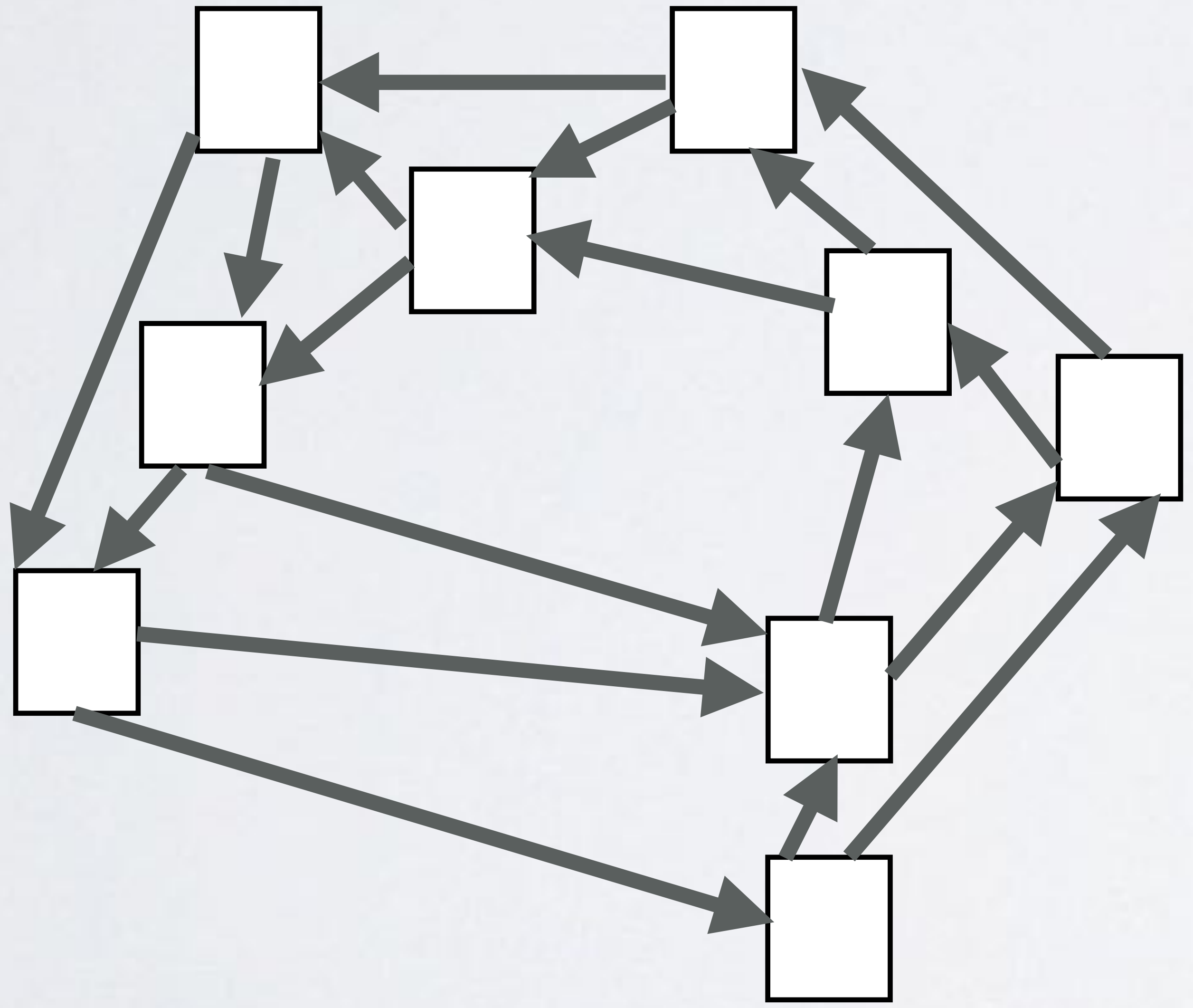


DIRECTED ACYCLIC GRAPH

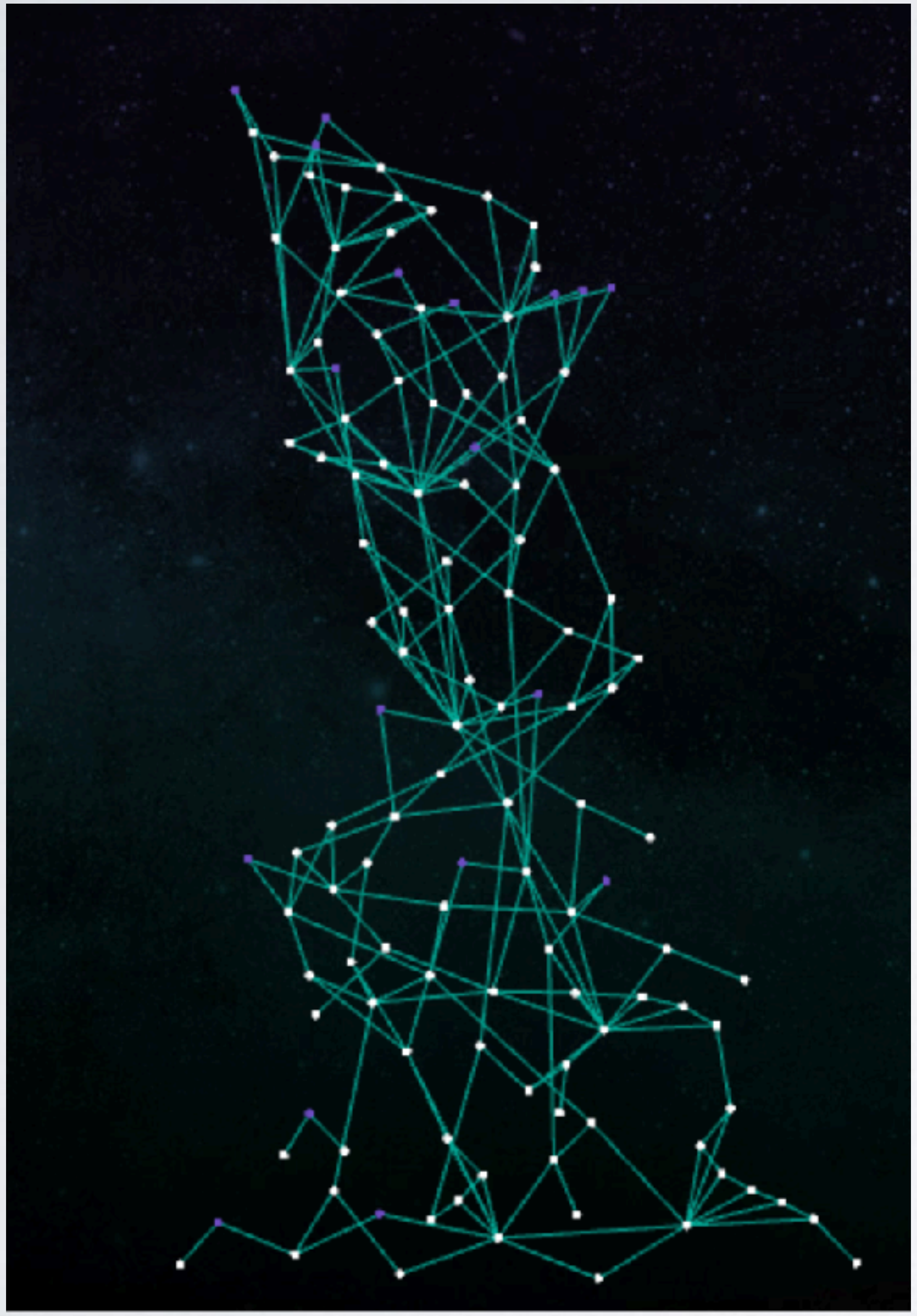
- Directed means the graph is pointing to one direction.



- Acyclic means the graph is non circular. This will not happen:



TANGLE

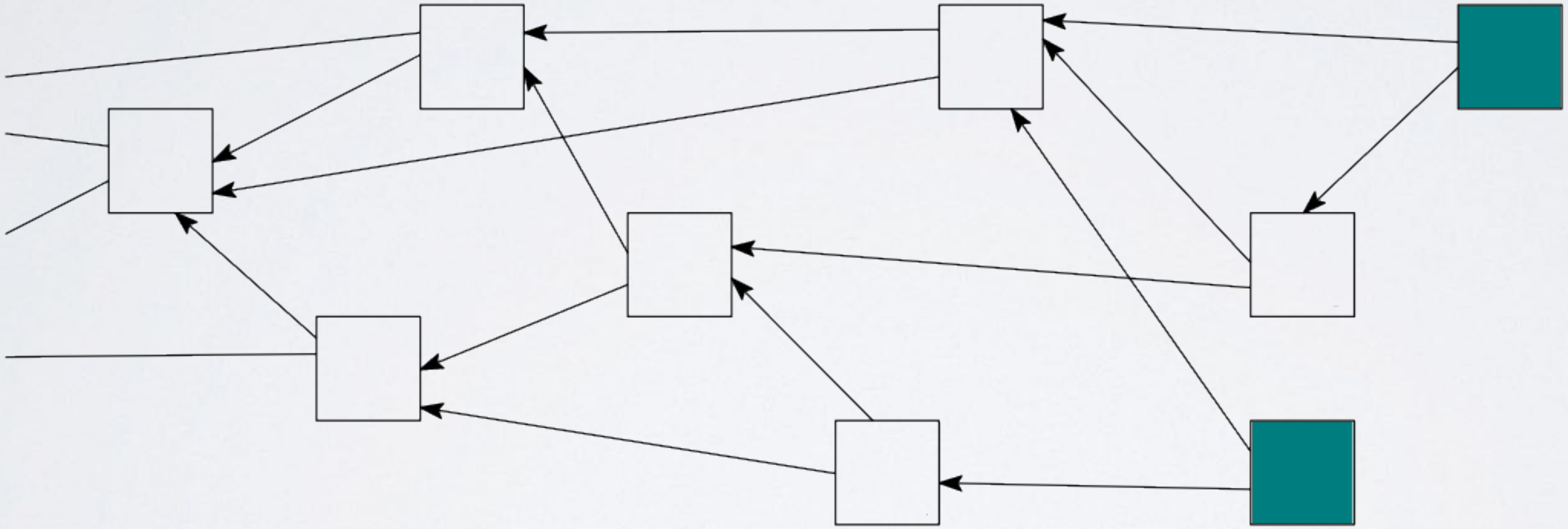


Tangle visualisation:

http://iota.dance/live/
https://tangle.blox.pm/

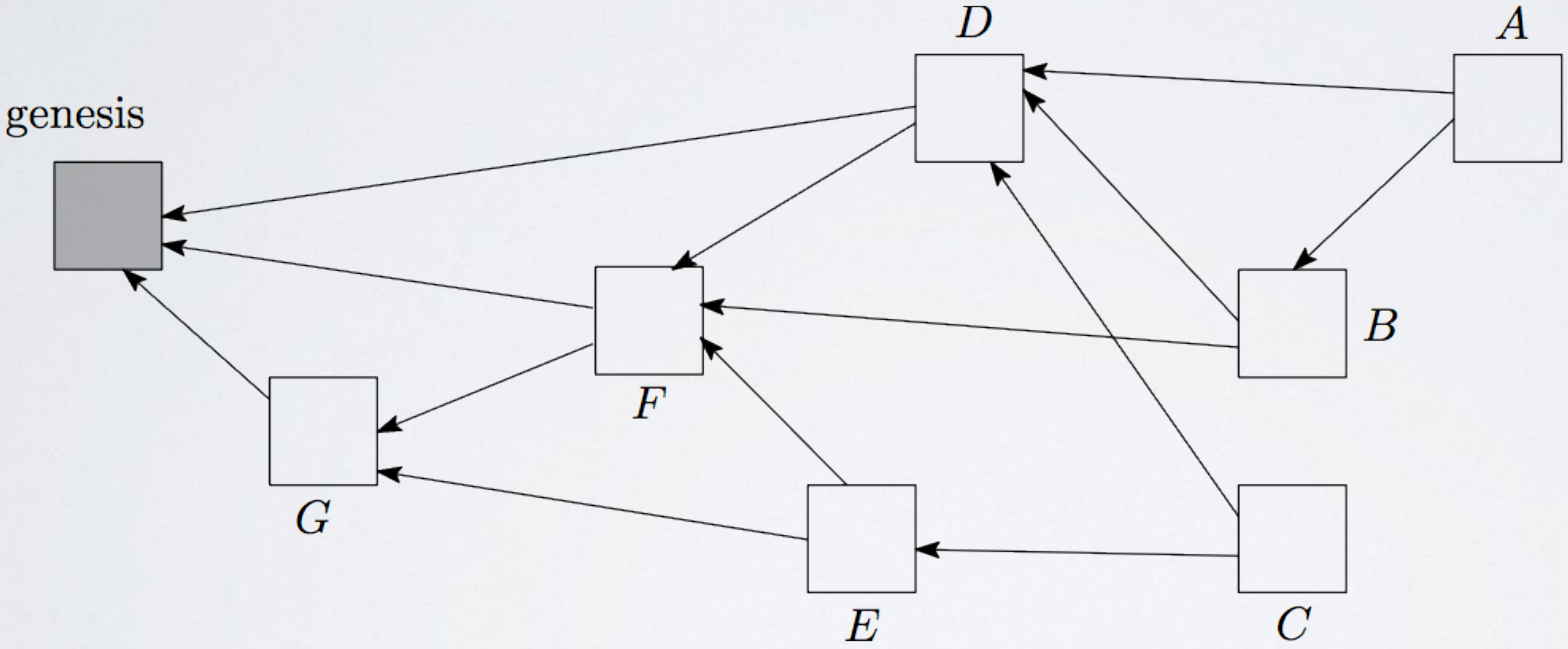
TIPS

- Tips are the unconfirmed transactions in the tangle graph. They are transactions which have no other transactions references them but they should each reference two previous transactions.



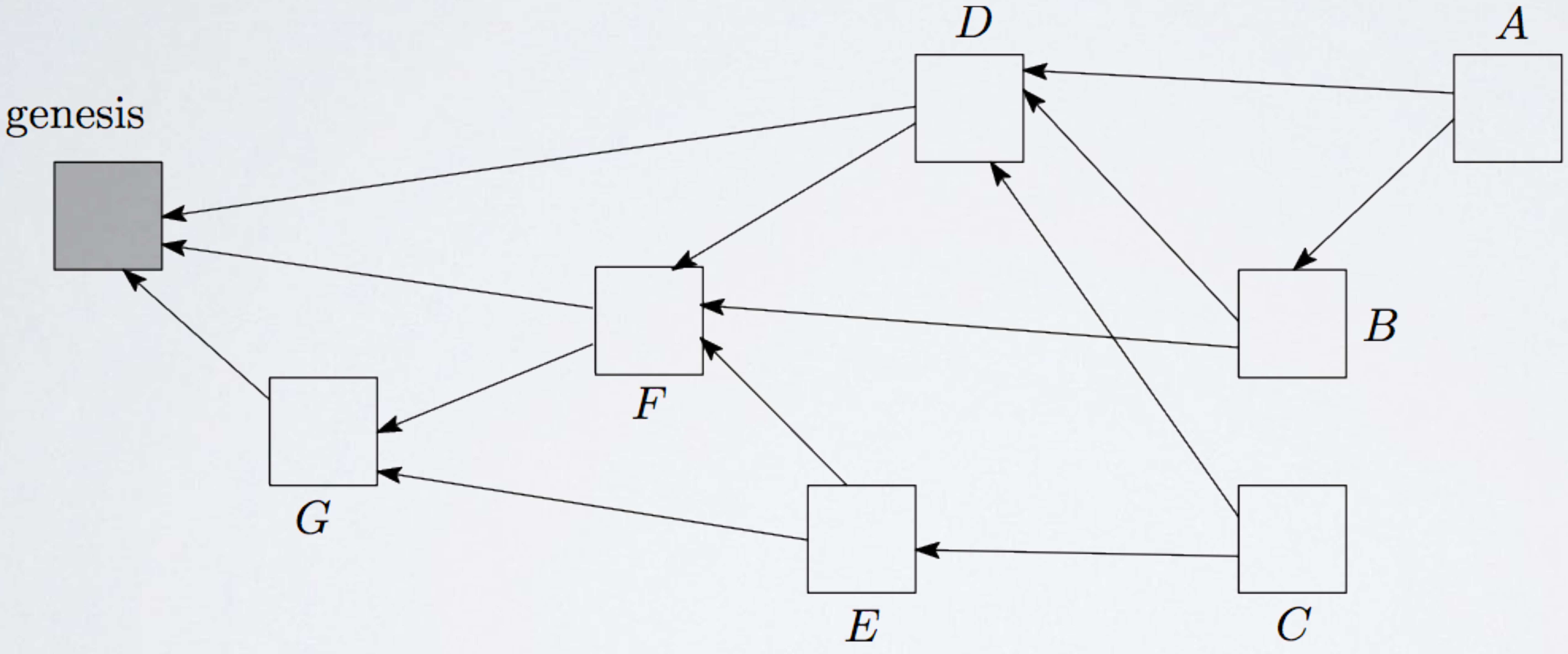
HEIGHT

- Height is the length of the **longest** oriented path to the genesis.
- For example: G has a height of 1. D has a height of 3.



DEPTH

- Depth is the length of the **longest** reverse-oriented path to some tip.
- For example: G has a depth of 4 to Tip A. Path = F, D, B and A.



HOW A TRANSACTION IS CREATED

- Making a transaction is a 3 step process:
  - **Signing:** Your node (computer / mobile) creates a transaction and sign it with your private key.
  - **Tip Selection**: Your node chooses two other unconfirmed transactions (tips) using the Random Walk Monte Carlo (RWMC) algorithm.
  - **Proof of Work**: Your node checks if the two transactions are not conflicting. Next, the node must do some Proof of Work (PoW) 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. This 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.

RANDOM WALK MONTE CARLO (RWMC) ALGORITHM

- The goal of the Random Walk Monte Carlo algorithm is to generate fair samples from some difficult distribution.

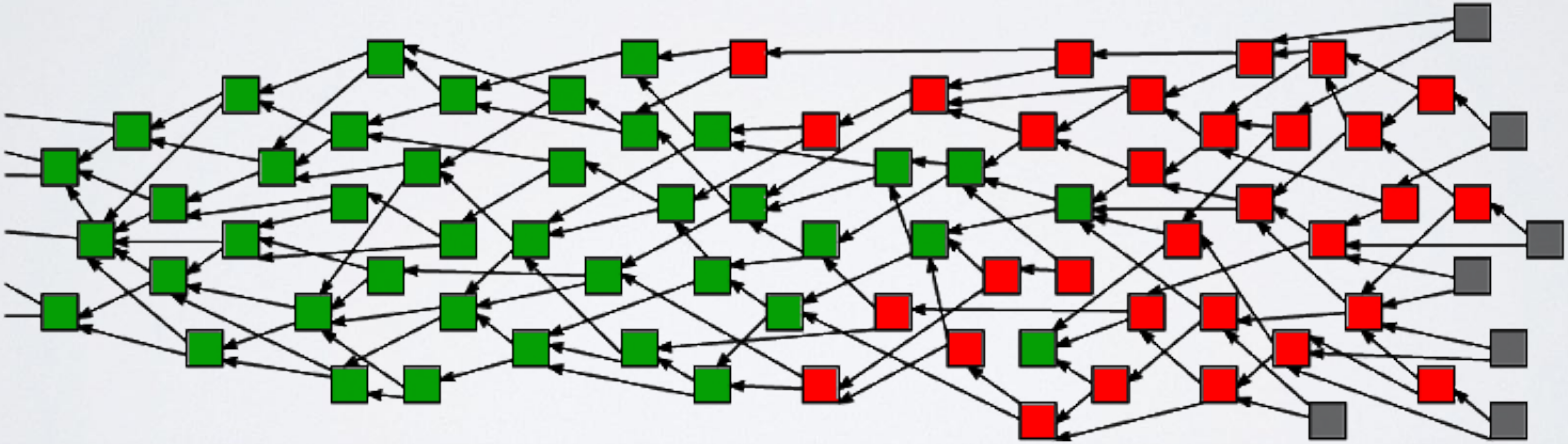
- The Random Walk Monte Carlo (RWMC) algorithm is used in two ways:

  - To choose two other unconfirmed transactions (tips) when creating a transaction.

  - And to determine if a transaction is confirmed.

TRANSACTION CONFIRMATION

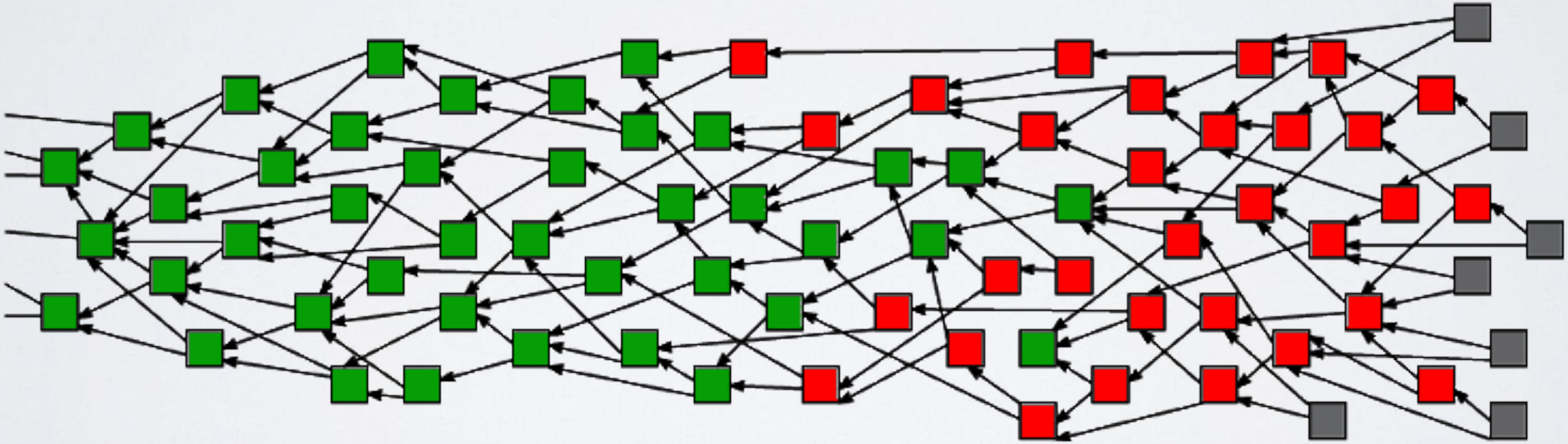
- Green blocks: transactions on which consensus was achieved a.k.a confirmed transactions.
  Red blocks: transactions where we are still uncertain on their full acceptance.
  Grey blocks: unconfirmed transactions (tips).



TRANSACTION CONFIRMATION

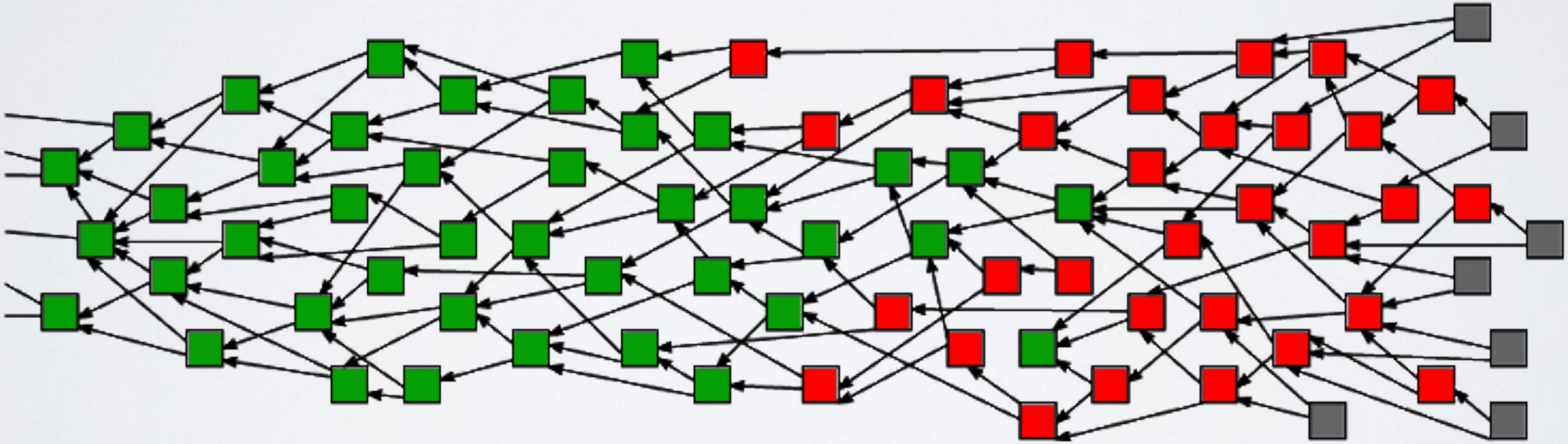
- The goal of any transaction is to be green.
  But how do you go from grey, to red, to green?

- Green blocks are indirectly referenced by **ALL** the grey blocks.
  For every confirmed transaction, there is a path leading to it from a tip.



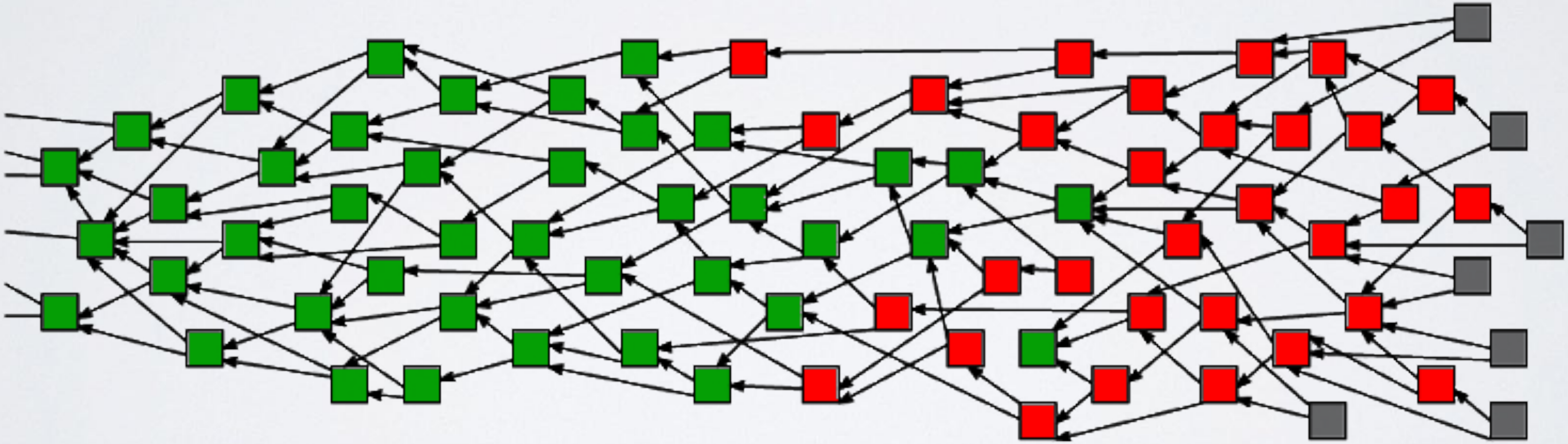
TRANSACTION CONFIRMATION

- To determine the confirmation level of your transaction we need the depth to start from and we execute the Random Walk Monte Carlo algorithm N times, the probability of your transaction being accepted is therefore M of N. M being the number of times you land on a tip that has a path to your transaction.



TRANSACTION CONFIRMATION

- If you execute RWMC 100 times, and 60 tips has a path to your transaction, than your transaction is 60% confirmed. It is up the the merchant to decide to accept the transaction and exchange goods. It is the same as Bitcoins where you want to wait for at least 6 blocks for high value transactions. Transactions with bigger depths takes longer to be validated.



IOTA GITHUB

- An IOTA Reference Implementation (IRI), wallet and libraries are available at: https://github.com/iotaledger
- The IOTA Reference Implementation is written in Java.
- As of Nov 2017 this implementation is not production ready.
- The IOTA libraries are available in different programming languages such as JavaScript, Python and Go.

FULL NODE

- To setup a full node you need to tether with neighbours by exchanging your ip address with theirs.

- It is recommended only to share you IP address with only the neighbours you are tethering with and no one else.

- Previously peer-discovery was included in the IOTA Reference Implementation but peer discovery was causing more problems. Peer discovery is now removed and manual node sharing is used instead to optimise IOTA and to make it more suitable for the IoT.

IOTA ADDRESS USAGE

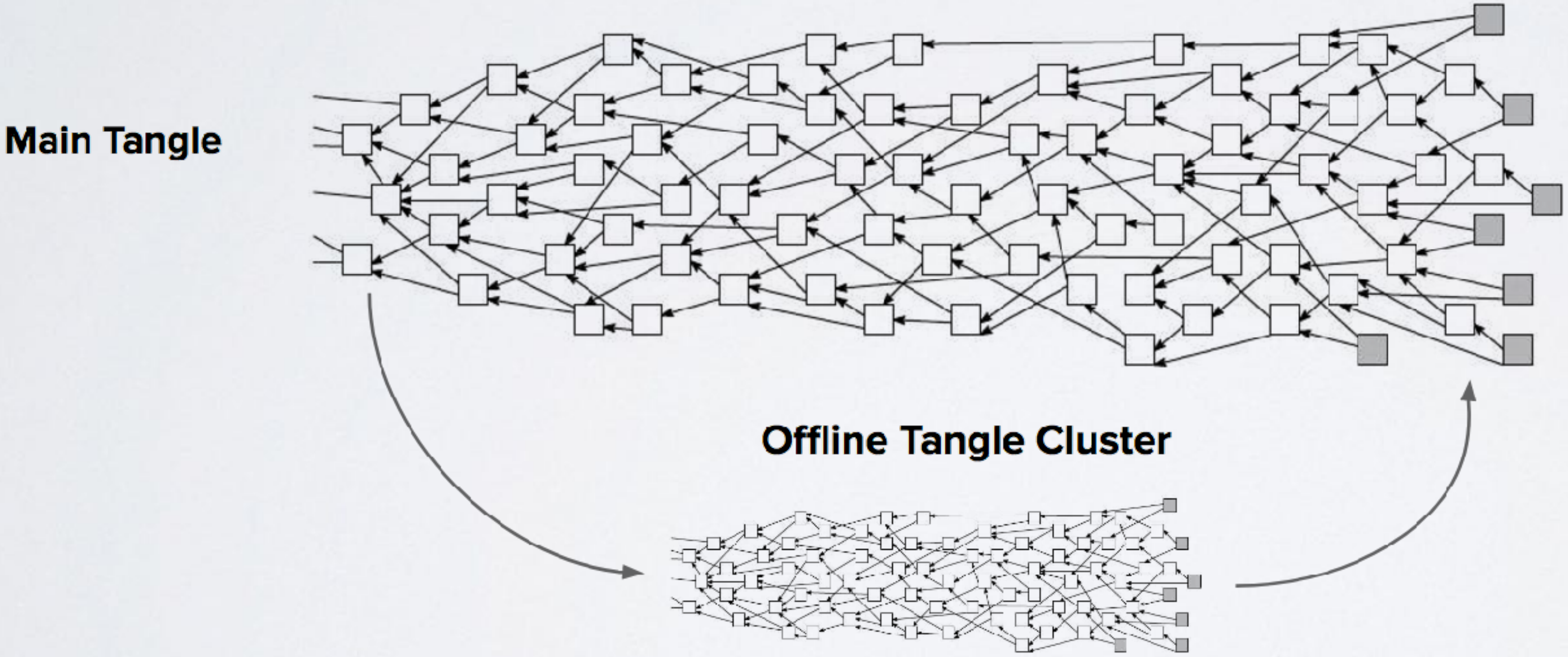
- Once you have sent a transaction from an address, you should never use this address again. Each time you sent a transaction from an address a part of the private key is revealed. IOTA uses the Winternitz one-time signature. This makes it easier for attackers to steal that address's balance via brute force.

- You can receive as many transactions you want to an address, but once you make a transaction from this address you should **NOT** reuse this address again for receiving OR sending transactions.

- The seed is not compromised if you receive funds at an address that has already been spent from. But the funds at that address is.

TANGLE

- A tangle can get branch off and back into the network. This is called partitioning. For example sensors on containers on a freighter ship losses connectivity with the main tangle when the ship travel across the ocean. The sensors can create an offline tangle cluster.



COORDINATOR

- The Coordinator or 'Coo' for short, are several full nodes scattered across the world run by the IOTA Foundation. It creates zero value transactions called milestones which full nodes reference to.

- Its main purpose is to temporary protect the network in its infancy stage to sustain against a large scale attack from those who own GPUs. The Coordinator sets the general direction for the tangle growth and do some kind of checkpointing.

- The network is considered decentralised because every node verifies that the Coordinator is not breaking consensus rules by creating iotas out of thin air or approving double-spendings.

- When the amount of organic activity on the IOTA ledger is sufficient to where it can evolve unassisted, the Coordinator is permanently shut off.

SNAPSHOT

- A snapshot is a method which keeps the ledger database that devices has to keep very small in size.
- Snapshotting groups several transfers to the same address into 1 record, saves only non zero balances and removes transaction history.
- The addresses with balances acts like new genesis addresses, but no previous history or data will be attached.
- Currently making snapshots are done manually but in the future it will be done automatically.
- There will be permanodes which stores the entire tangle history and data permanently and securely.

KECCAK-384 / KERL

- IOTA created their own hash function called Curl based on SHA-3/Keccak.

- Researchers from the Boston University and Massachusetts Institute of Technology reported on a vulnerability in Curl in July 14, 2017.
  See: https://github.com/mit-dci/tangled-curl/blob/master/vuln-iota.md
  The Curl produced collisions (when different inputs, hash to the same output).

- On August 7th, 2017 the IOTA team implemented a patch by replacing Curl with the Keccak-384 hash function. This hash function is used for generating addresses and signing transactions. The Keccak-384 hash function is wrapped and named "Kerl" as a tongue-in-cheek homage to what it was replacing. See: https://github.com/iotaledger/iri/commit/539e413352a77b1db2042f46887e41d558f575e5