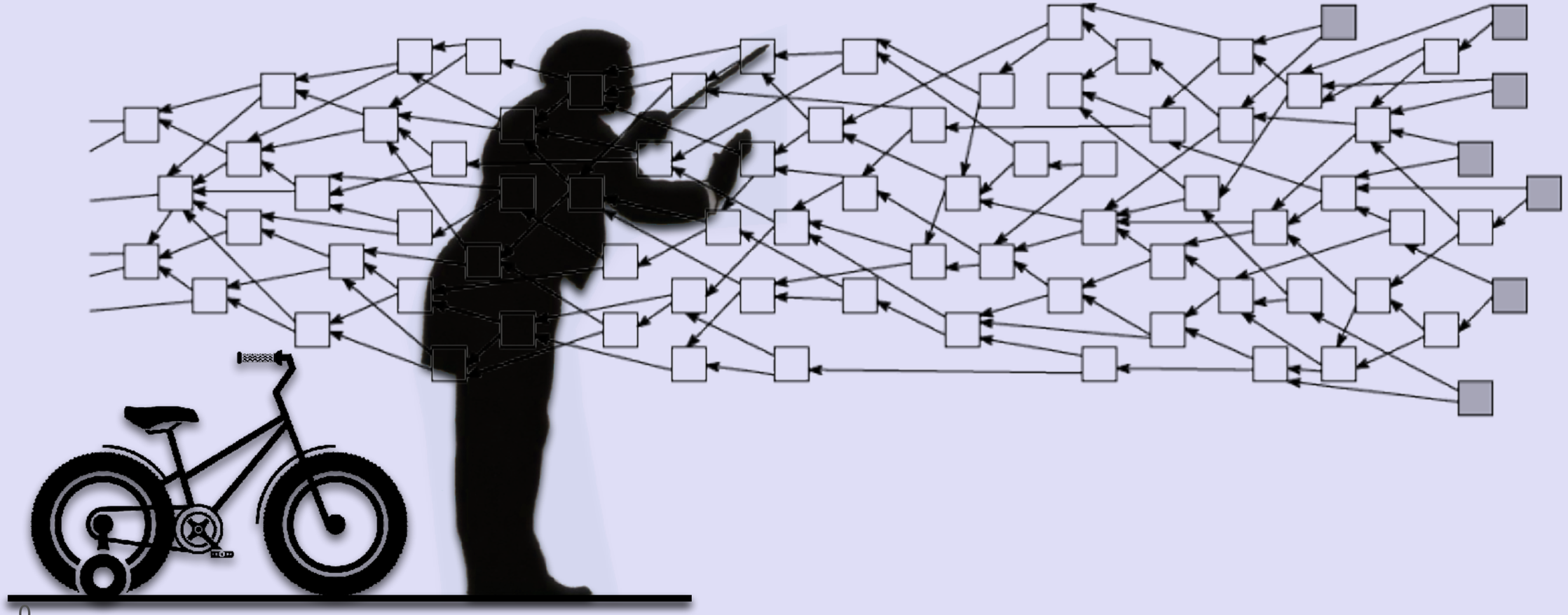
IOTA TUTORIAL I2

Coordinator



INTRO

- In this video I will explain what the Coordinator is.

COORDINATOR

- In a Tangle network transactions are validated by selecting transactions many times by using the Random Walk Monte Carlo (RWMC) method. This is already explained in IOTA Tutorial I, but here is a short explanation how a transaction is validated:
  - Using the RWMC method, select 100 new transactions (tips).
  - Calculate how many tips directly or indirectly will reach the transaction.
  - If it is less than 50% the transaction is not yet validated.
  - If it is more than 50% the transaction has a fair chance to be validated.
  - If it is 99% the transaction is considered validated (aka confirmed).

COORDINATOR

- In its infancy stage the Tangle network has a small number of nodes. An attacker can relatively easily create many nodes on the network and thus creating many malicious transactions.

- In this situation, if we were to use the Random Walk Monte Carlo method, there is a big chance that malicious transactions are selected.

- To protect the Tangle network against 34% attacks in its infancy stage a temporary protection mechanism is used called the Coordinator or COO for short.

- The Coordinator is a special node run by IOTA Foundation and this node is used to directly or indirectly validate the transactions.

COORDINATOR

- The Coordinator location and source code are not publicly available.

- Using the Coordinator does not mean that the network is centralised, the network is still 100% decentralised because every node on the network verifies that the Coordinator is not breaking consensus rules by creating IOTAs out of thin air or approving double-spendings.

- The Coordinator will be shut down as soon as the network reaches a certain number of confirmed transactions per second (ctps). When this number is reached many people are confirming transactions all the time.

- What this number is, is not known at the moment and when it will be reached is also unknown as no one knows how fast the IOTA adoption will be.

COORDINATOR

- The Coordinator address is hardcoded into the IOTA Reference Implementation (IRI). https://github.com/iotaledger/iri/blob/master/src/main/java/com/iota/iri/Iota.java

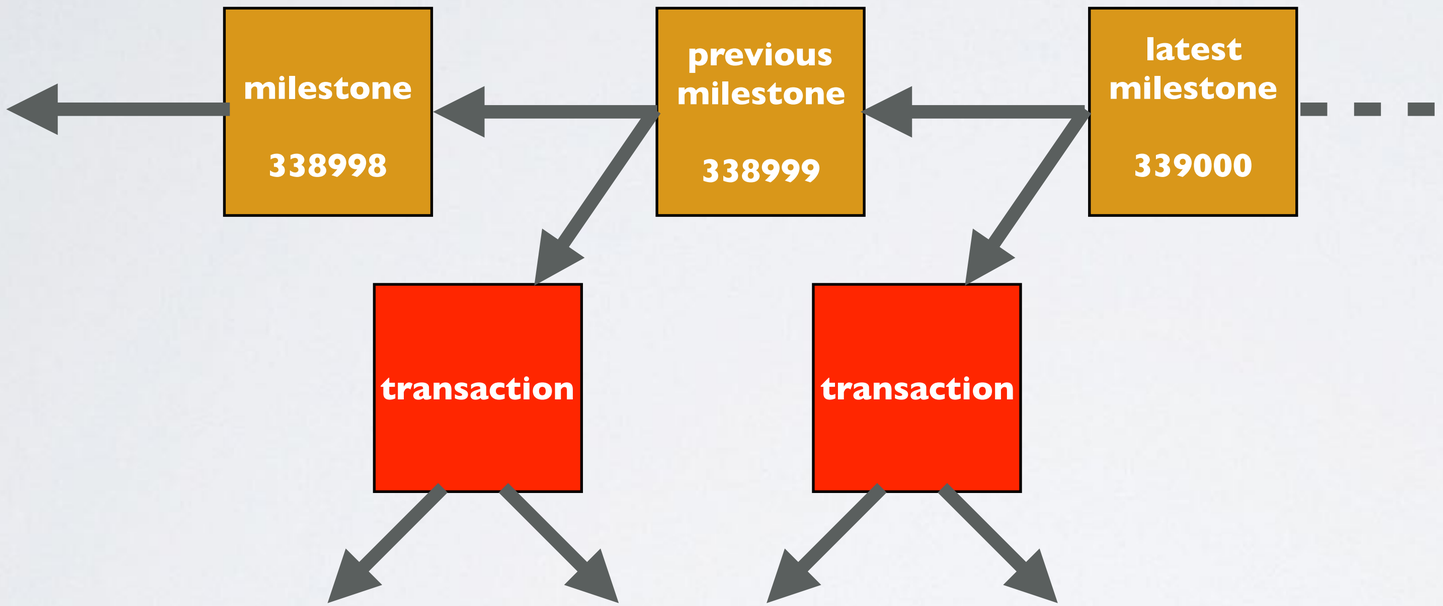
- The Coordinator creates approximately every minute, a zero value transaction from address (Mainnet):
  KPWCHICGJZXKE9GSUDXZYUAPLHAKAHYHDXNPHENTE
  RYMMBQOPSQIDENXKLKCEYCPVTZQLEEJVYJZV9BWU
  The transaction is signed and has no inputs.

- These Coordinator created transactions are called milestones and each milestone has a unique index number, for example: 339000

- Example: https://www.mobilefish.com/download/iota/iota_coordinator_milestones.txt

COORDINATOR

- Based on: https://www.mobilefish.com/download/iota/iota_coordinator_milestones.txt

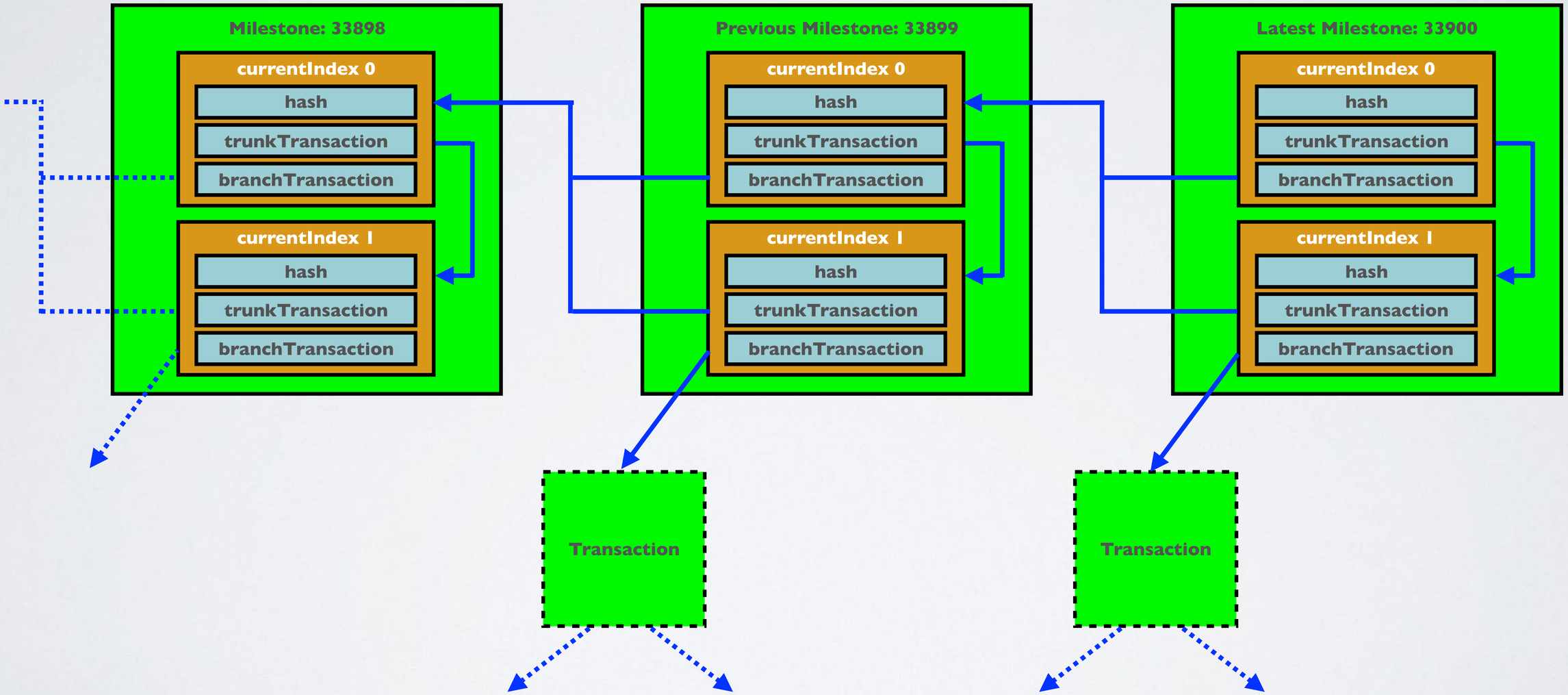


Coordinator creates milestones approx. every 1 minute

- Every transaction, including milestones, verifies two other transactions.

COORDINATOR

- Based on: https://www.mobilefish.com/download/iota/iota_coordinator_milestones.txt



COORDINATOR

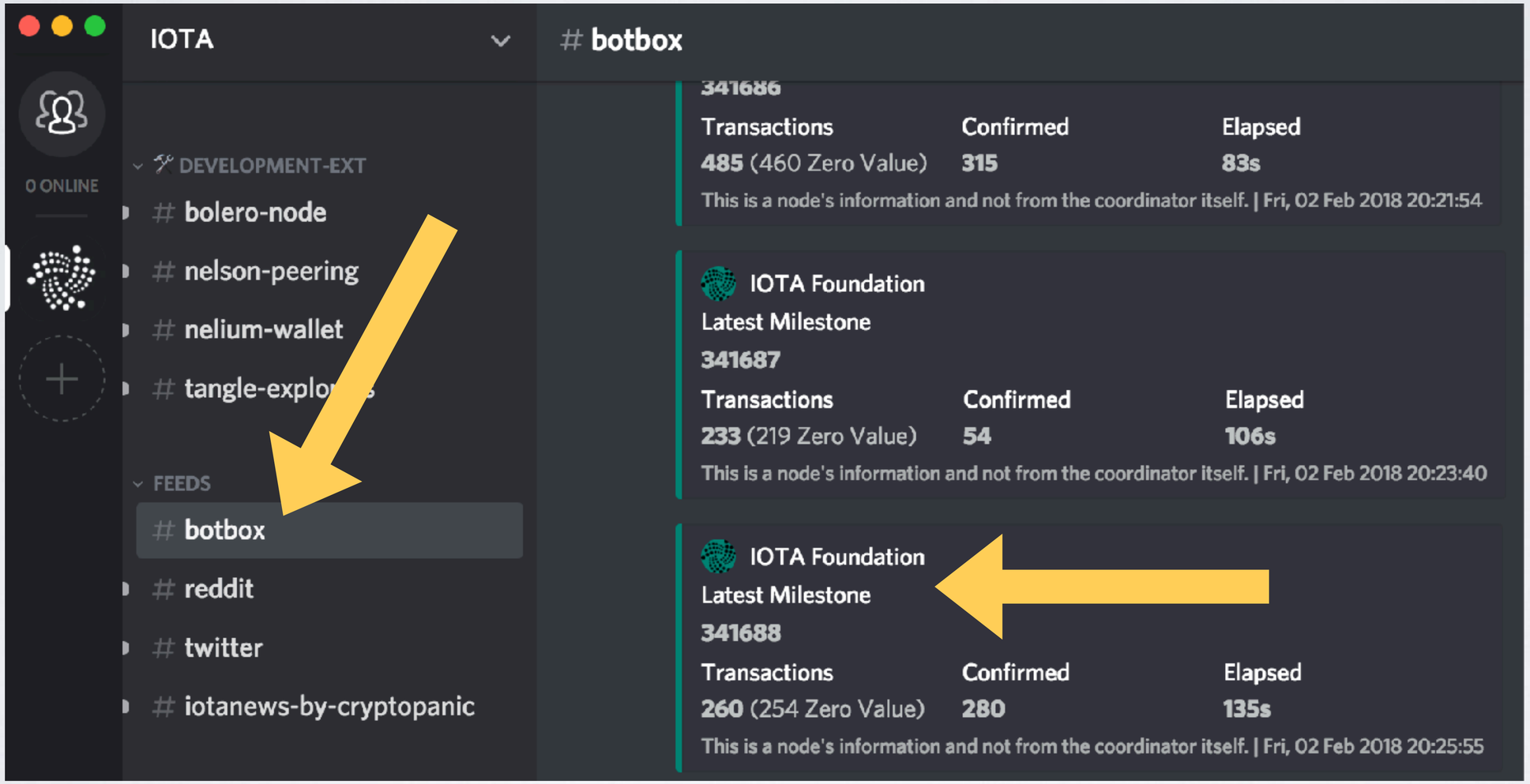
- Milestones set the general direction for the Tangle growth.

- The latest milestone can be found in:
  - The Discord app: https://discordapp.com/invite/7Gu2mG5 (#botbox channel)
  - or https://milestone.iotatangle.space/

- Transactions are considered confirmed if it is directly or indirectly referenced by a milestone. Milestones can not be faked because they are signed by the Coordinator.

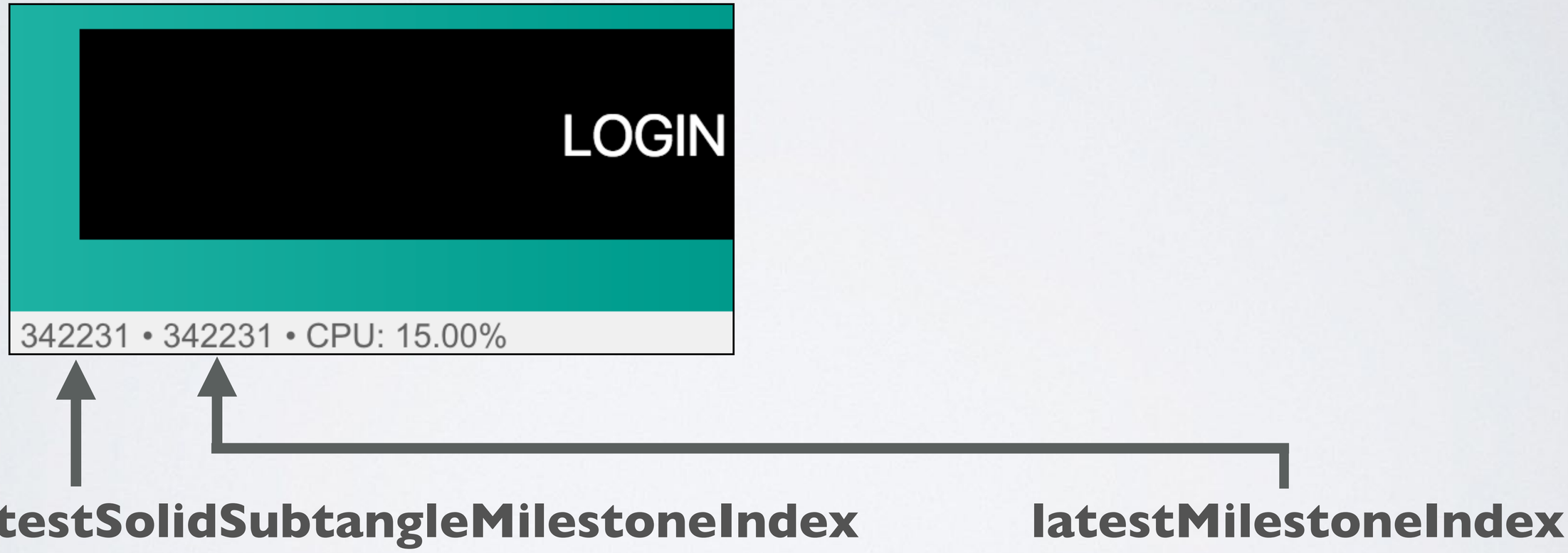
COORDINATOR

- #botbox channel on Discord.



COORDINATOR

- When the IOTA Light wallet is started the latestSolidSubtangleMilestone and latestMilestone appears in the status bar.
  The wallet gets this information from the node it is connected to.



COORDINATOR

- If you query a node with the getNodeInfo API call, it will return a JSON object similar to the following:


```
"appName": "IRI Testnet",
"appVersion": "1.4.1.3",
"jreAvailableProcessors": 8,
"jreFreeMemory": 508995728,
"jreVersion": "1.8.0_151",
"jreMaxMemory": 6442450944,
"jreTotalMemory": 6442450944,
```

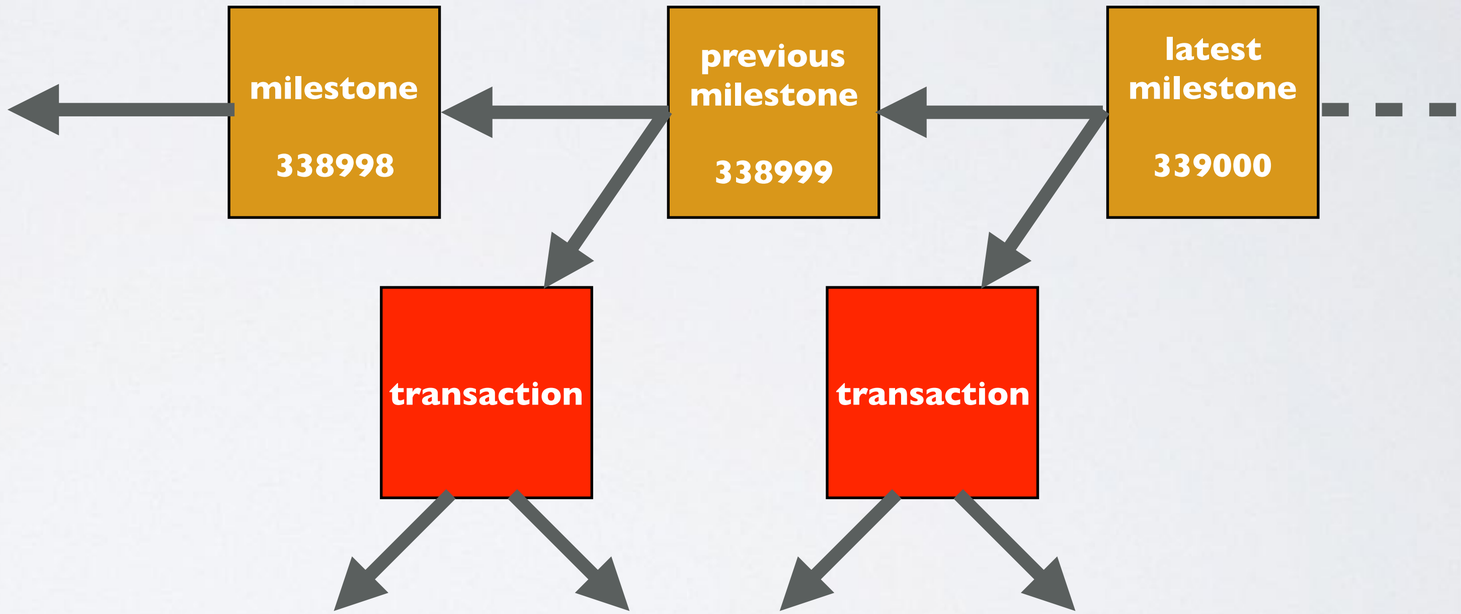
COORDINATOR


```
"latestMilestone": “FIQJBZDNS……DFVGSDI999”,
“latestMilestoneIndex": 273160,
"latestSolidSubtangleMilestone": “FIQJBZDNSKBJ…VGSDI999”,
"latestSolidSubtangleMilestoneIndex": 273160,
"neighbors": 10,
"packetsQueueSize": 0,
"time": 1516898751009,
"tips": 5183,
"transactionsToRequest": 177,
"duration": 0
```

COORDINATOR

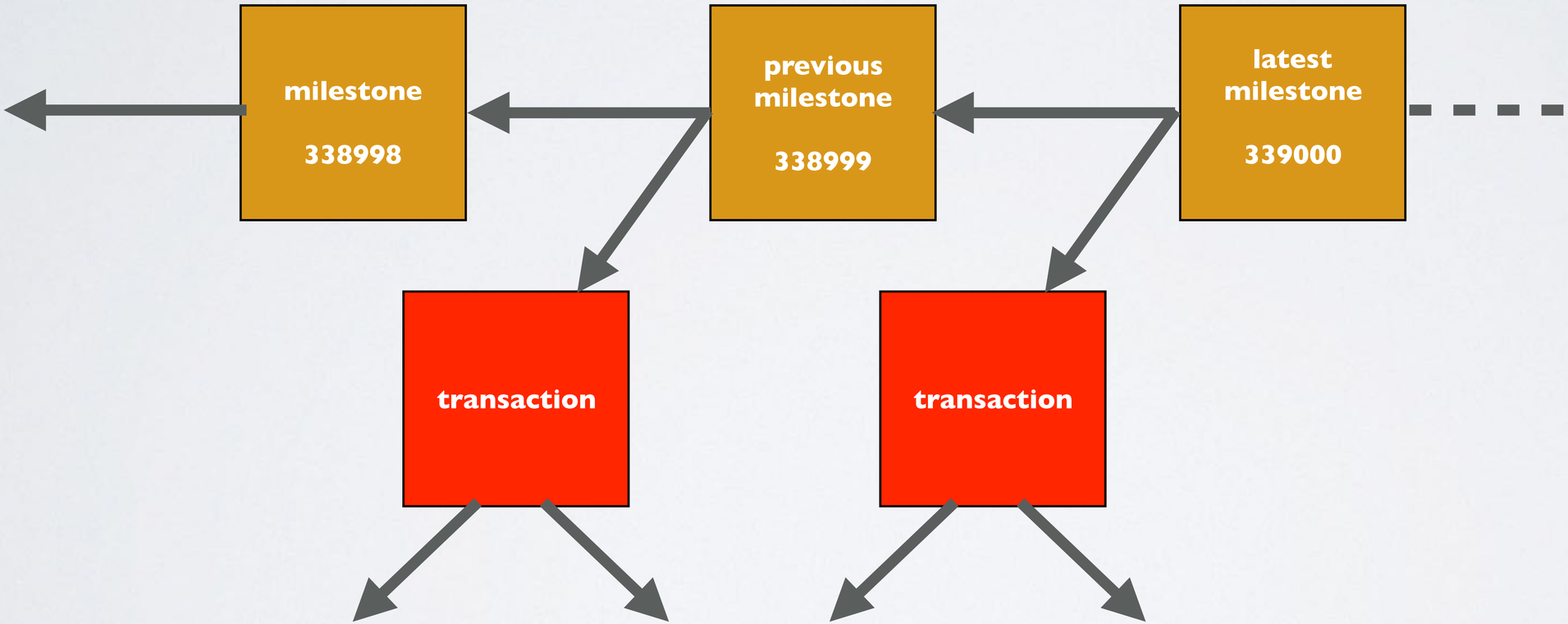
- **latestMilestone**
  The latest milestone is created by the Coordinator.
  The latestMilestone value is the latest transaction hash the node received from the Coordinator.

- **latestMilestoneIndex**
  Index of the latest milestone.



COORDINATOR

- **latestSolidSubtangleMilestone**
  When the Coordinator creates milestones, each milestone references a subtangle of Coordinator approved transactions.



COORDINATOR

- **latestSolidSubtangleMilestone**
  For a node this milestone becomes “solid" if the node has ALL the approved transactions that are directly or indirectly referenced by this subtangle.

  If some of these approved transactions are missing, the milestone is not solid and the node is not synced.

  The latestSolidSubtangleMilestone is used to send transactions. If an outdated solid milestone is used, the transaction might not be approved.

- **latestSolidSubtangleMilestoneIndex**
  Index of the latest solid subtangle milestone.

COORDINATOR

- A full node is synchronised with the Tangle if the following conditions are met:
  - The latestMilestoneIndex is updated to the actual last milestone index validated by the Coordinator,
  - The latestSolidSubtangleMilestoneIndex is the same as the latestMilestoneIndex.