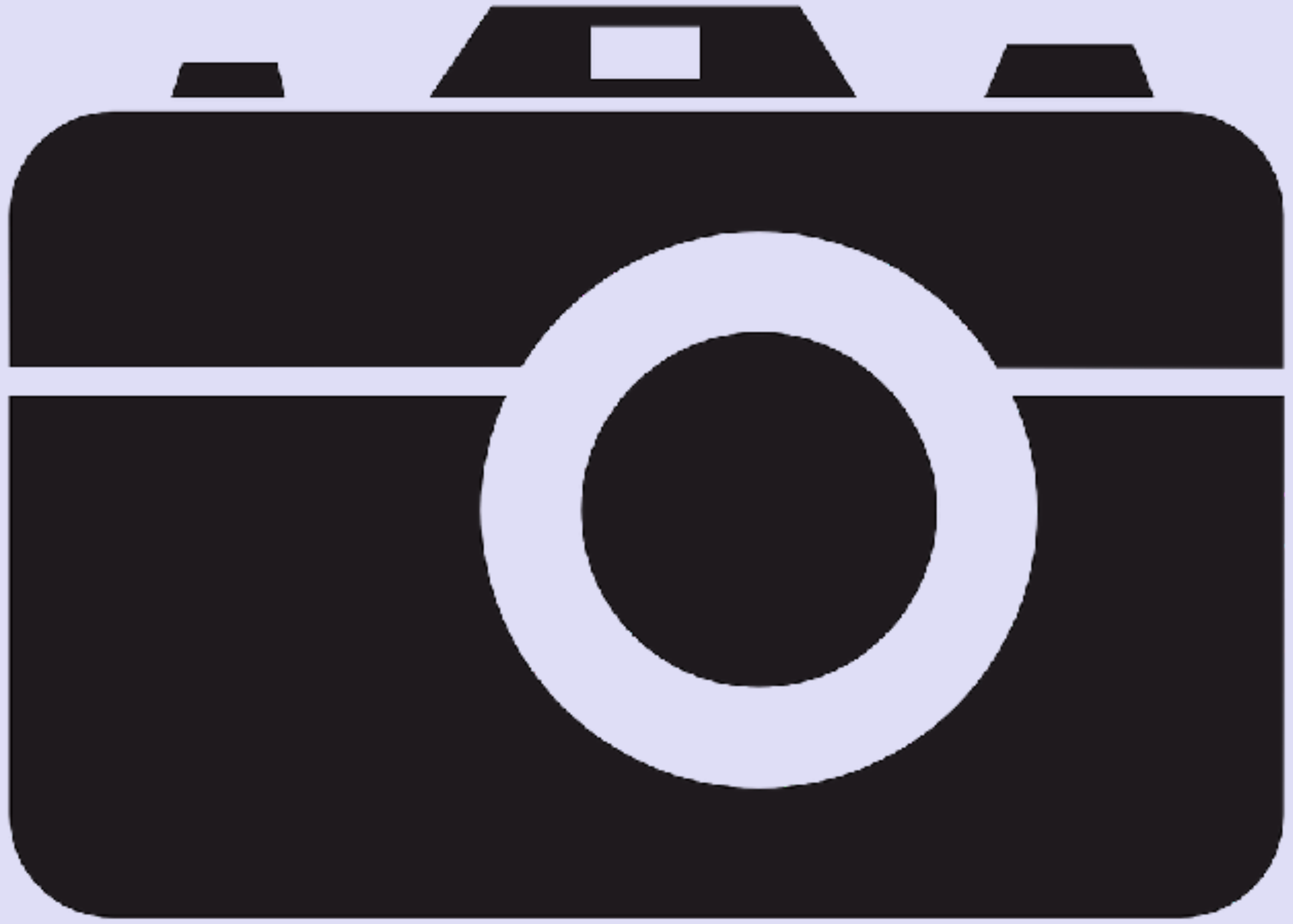
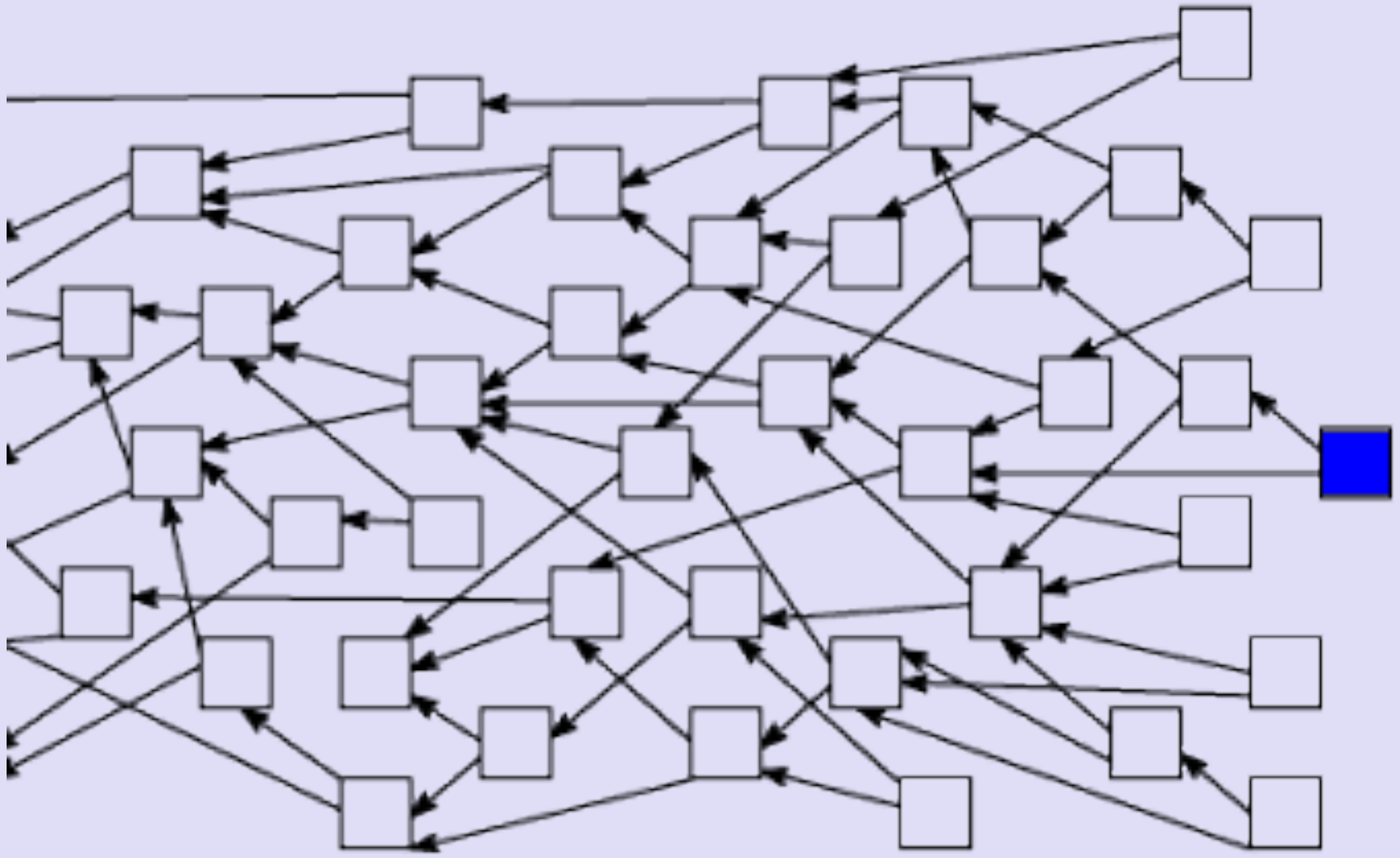
# IOTA TUTORIAL 5

## Snapshot & Attach to tangle





v1.0.0

# INTRO

- In this video I will explain what a snapshot is and why it is needed.

- And I will explain what attach to tangle means and why you need to attach addresses to the tangle.

# SNAPSHOT

- A snapshot is a method to reduce the size of the Tangle database by removing all transactions from the Tangle, leaving only a record of addresses with corresponding balances. Addresses with zero balance are also removed from this record.

- A snapshot is simply a list of every address with corresponding non zero balance. This list can be found in the IOTA Reference Implementation (IRI).
https://github.com/iotaledger/iri/blob/dev/src/main/resources/Snapshot.txt

- These addresses with balances acts like a genesis address.

# SNAPSHOT

- Once the snapshot is successfully performed it is **possible** you may need to claim your tokens.

- Claiming means, that you need to transfer your tokens from the old Tangle database (before the snapshot) into the new Tangle database (after the snapshot). If you forget to claim your tokens you will never be able to get access to your tokens again.

- Example of a previous snapshot announcement and claim instructions:
  https://blog.iota.org/upgrades-updates-d12145e381eb
  https://iotasupport.com/claimingyouriota.shtml

- The claiming process is only needed when there are major design changes in the IOTA protocol and please note that IOTA is still in the development phase. So claiming your tokens after a snapshot may still occur.

# SNAPSHOT

- The IOTA Foundation announces when snapshots are made.
  It is your duty to be kept informed. See the following links for IOTA announcements:
  https://forum.helloiota.com/Technology/General-Discussion/Announcements/IOTA-Announcements
  https://iotatangle.slack.com/messages/C1MB9CZ41

- Right now, the IOTA community agrees that snapshots are to be conducted by the IOTA Foundation, but in the future there will be local auto-snapshotting capability for each node.

# DETERMINISTIC WALLET

- An IOTA wallet is a deterministic wallet, meaning when a new address is generated it is calculated from the combination of the seed and address index, where the address index can be any positive integer.

- The wallet starts from address index 0, and asks the node it is connected to, for a list of transactions that incorporate that address.

- If there are no transactions found referencing that address the wallet concludes that it has not used the address yet. The wallet will not increase the address index and shows the total balance of all the addresses found.

# DETERMINISTIC WALLET

- If there are transactions found referencing that address, the wallet will increase the address index which in turn creates a new address. The wallet again searches the Tangle for transactions referencing that new address.

- The wallet will skip any address index where it sees that the corresponding address has already been attached to the Tangle.

# ATTACH TO THE TANGLE

- When you attach an address to the Tangle it creates:
  - a zero-value transaction referencing that address,
  - choosing and validating two transactions from the Tangle,
  - and then does the Proof-of-Work.
- In the wallet an attached address is shown in the history tab, as a transfer of 0 funds.

# ATTACH ADDRESS TO THE TANGLE

- It is not necessary to attach an address, IOTAs can be successfully sent to a non-attached address.
- **HOWEVER IT IS RECOMMENDED THAT YOU ALWAYS ATTACH AN ADDRESS BEFORE USING IT.**
- By attaching an address to the Tangle you inform the wallet that it should not reuse that address.
- Reusing an address, especially for **outgoing** transactions, can have huge security implications.

# DO NOT REUSE ADDRESS FOR OUTGOING TX

- In IOTA, the security of a transaction decreases when you send tokens more than once from the same address.

- This is because IOTA uses the Winternitz one-time signatures which degrade security exponentially after each address reuse for outgoing transactions.

- Once you have sent a transaction with a specific address as input, you should never use it again because a part of the private key of that specific address is revealed.

- The more outgoing transactions you make from the same address, the easier it will be for attackers to steal that address's balance by brute force the private key.

- Attackers uses a Tangle explorer to see if addresses are reused and try to steal funds from these reused addresses.

# DO NOT REUSE ADDRESS FOR OUTGOING TX

- You can reuse an address for receiving as long as you have not used it for any outgoing transaction.

- An additional security issue is after a snapshot, when the wallet forgets all of its history, people reuses addresses again.

- To avoid this, create a new wallet and transfer all your funds from the old wallet to the first address on this new wallet before the snapshot. This step ensures that all addresses in this new wallet (except the first) have never been used before.