IOTA FOUNDATION

A ledger for the Internet of Things

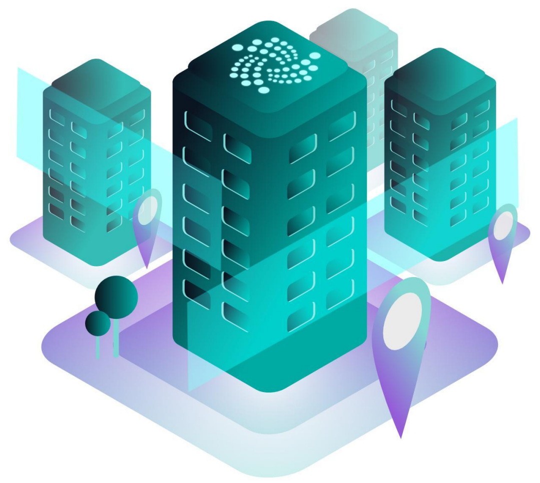
Who am I?

Michele Nati
Lead Architect, IOTA Foundation
michele@iota.org

IOTA Foundation
www.iota.org
@michelenati
@iotatoken

The IOTA Foundation

IOTA FOUNDATION

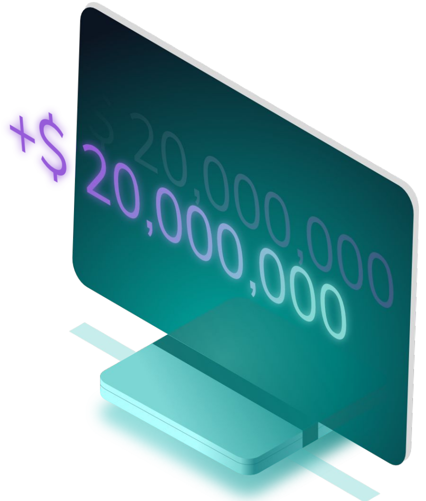


Hubs in Berlin, Tel Aviv, Oslo, Taipei

More than **90 employees** around the globe

Donations of **$100M+** to date

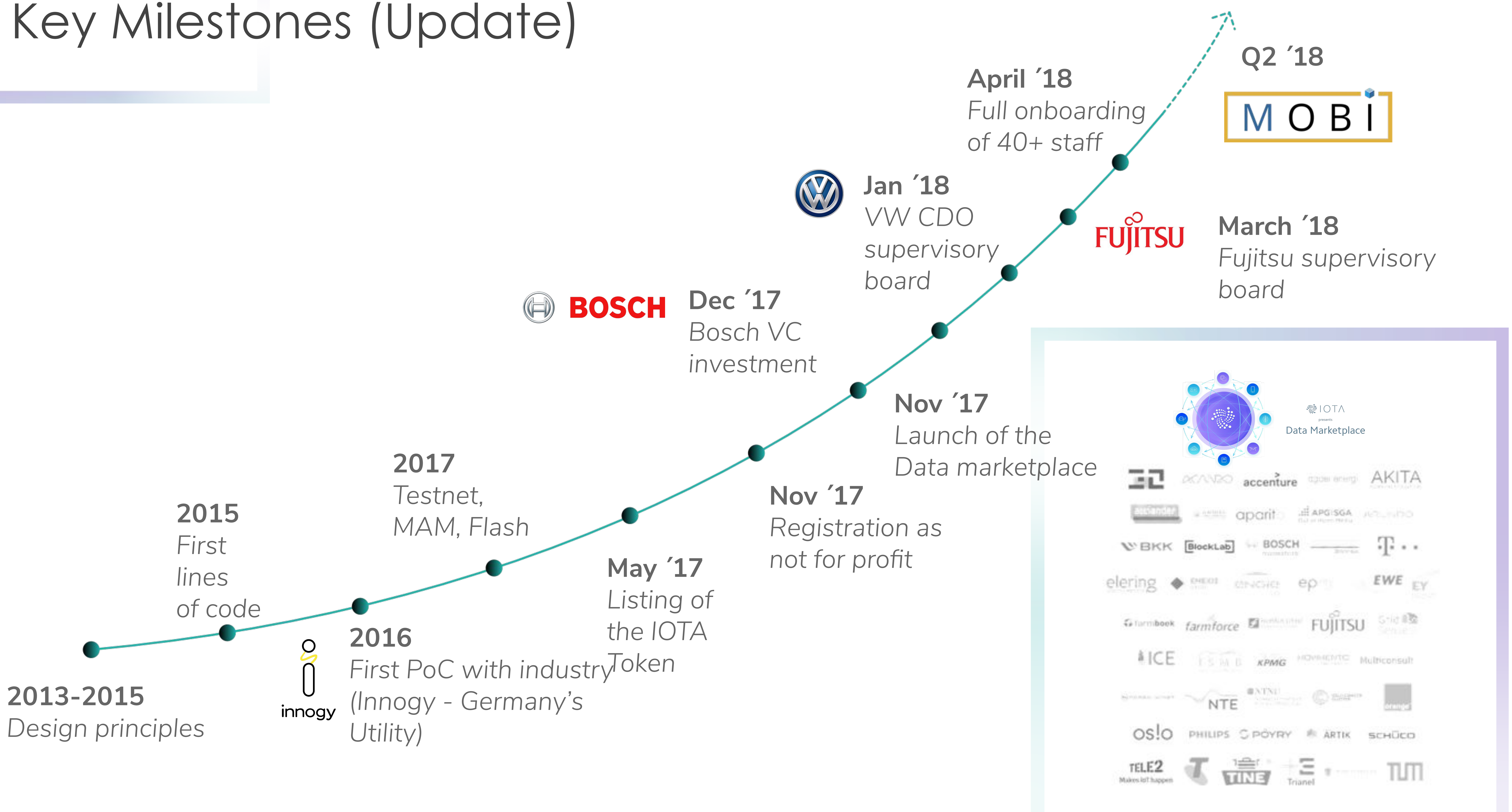
> 70k active community members
> 120k content followers



Ecosystem Development Fund
$13M+ in funding
over $150k awarded to date

Ecosystem of more than **100 entities**

Key Milestones (Update)



2013-2015
Design principles

2015
First lines of code

2016
First PoC with industry (Innogy - Germany's Utility)

2017
Testnet, MAM, Flash

May ´17
Listing of the IOTA Token

Nov ´17
Registration as not for profit

Nov ´17
Launch of the Data marketplace

Dec ´17
Bosch VC investment

Jan ´18
VW CDO supervisory board

March ´18
Fujitsu supervisory board

April ´18
Full onboarding of 40+ staff

Q2 ´18

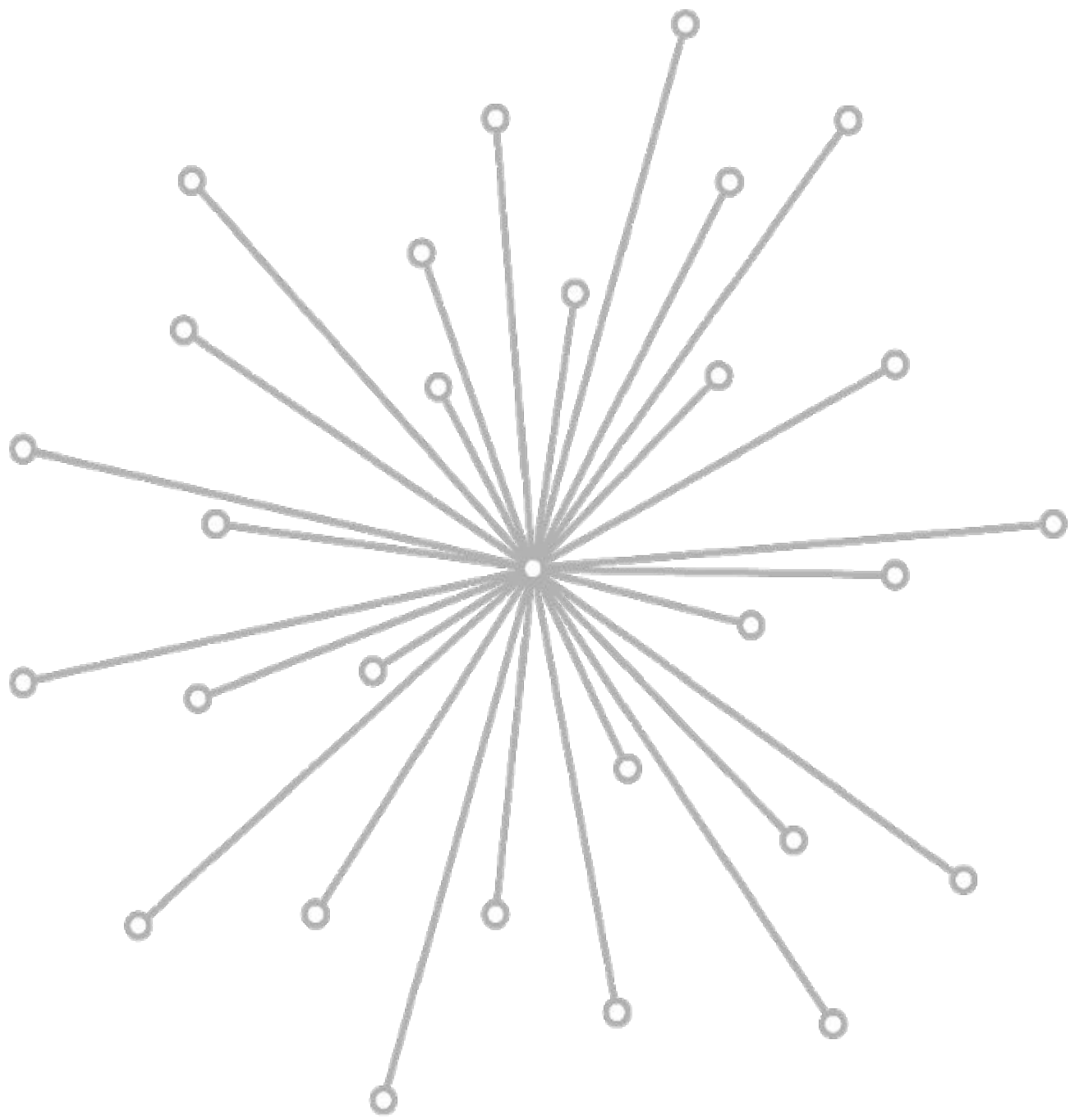
Table of Contents

1. What DLTs are?
2. Why IOTA?
3. IOTA vs Blockchain
4. Deep dive into ‘The Tangle’
5. Tangle Research
6. The IOTA Network
7. IOTA and IoT
8. IOTA Applications (some)
9. IOTA Ecosystem (building with IOTA)

What DLTs are?

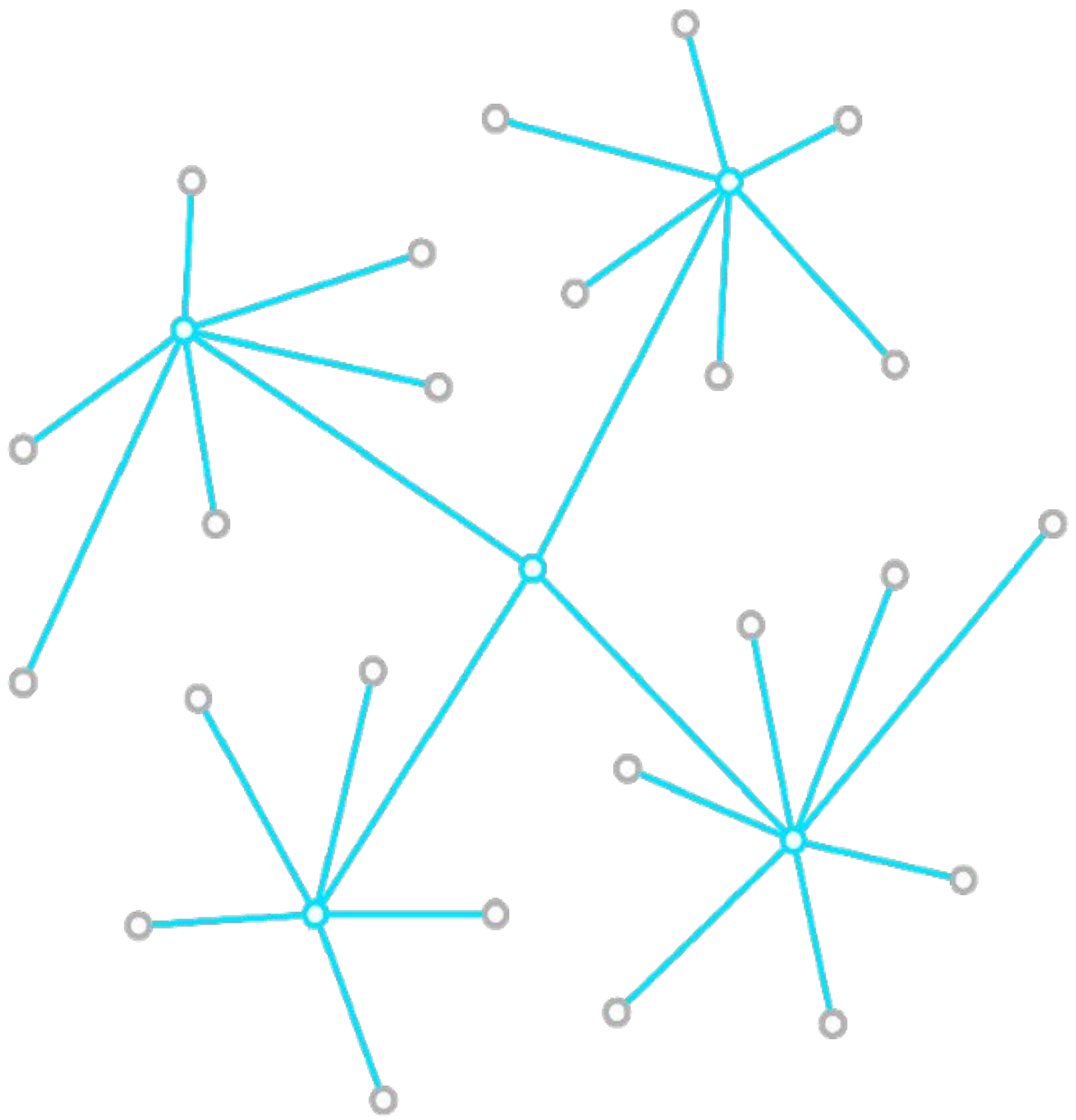
Network Decentralization

Centralized



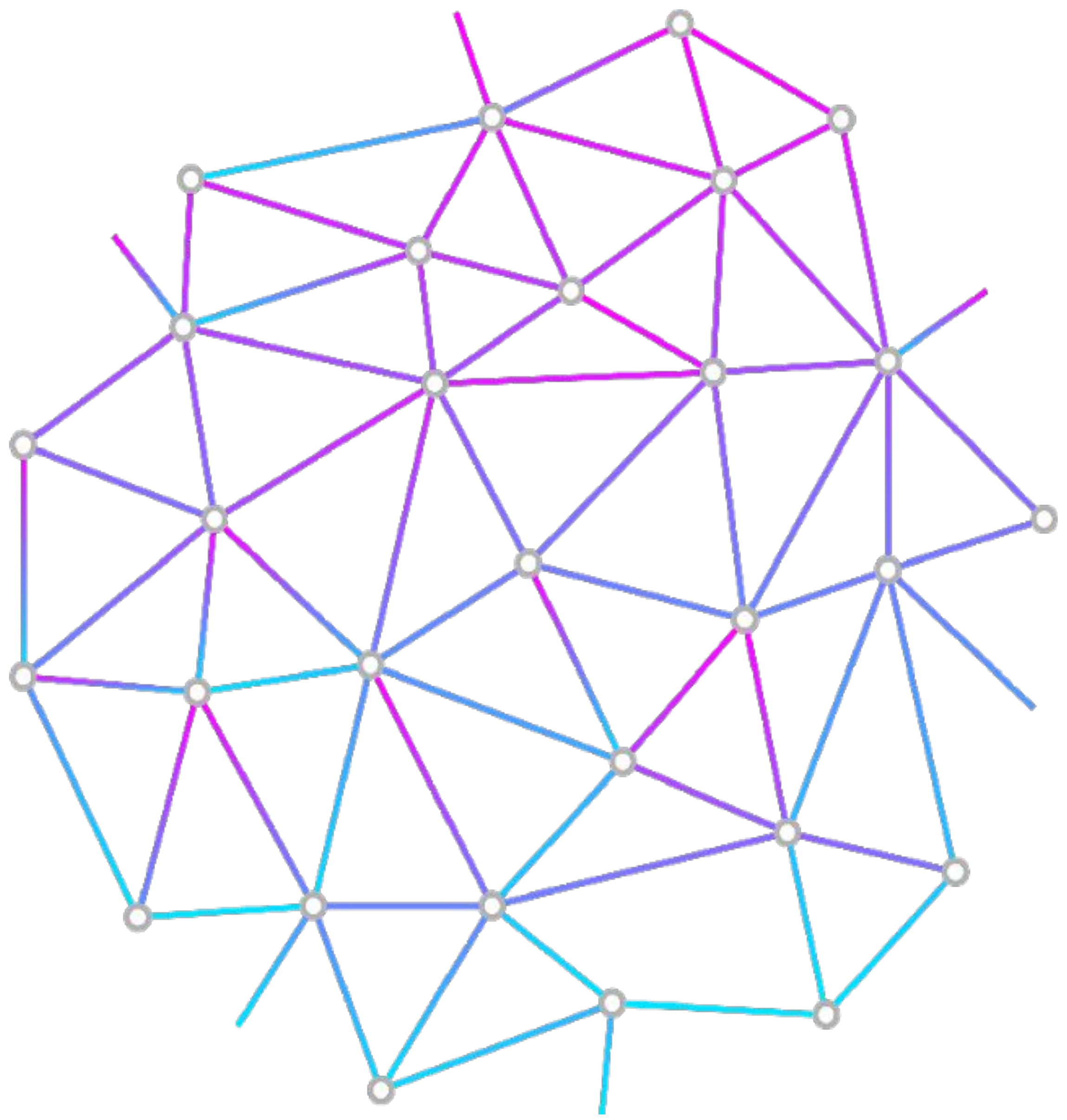
- Single Point of Access to “Truth”
- Single Source of “Truth”
- Single Point of Failure

Distributed



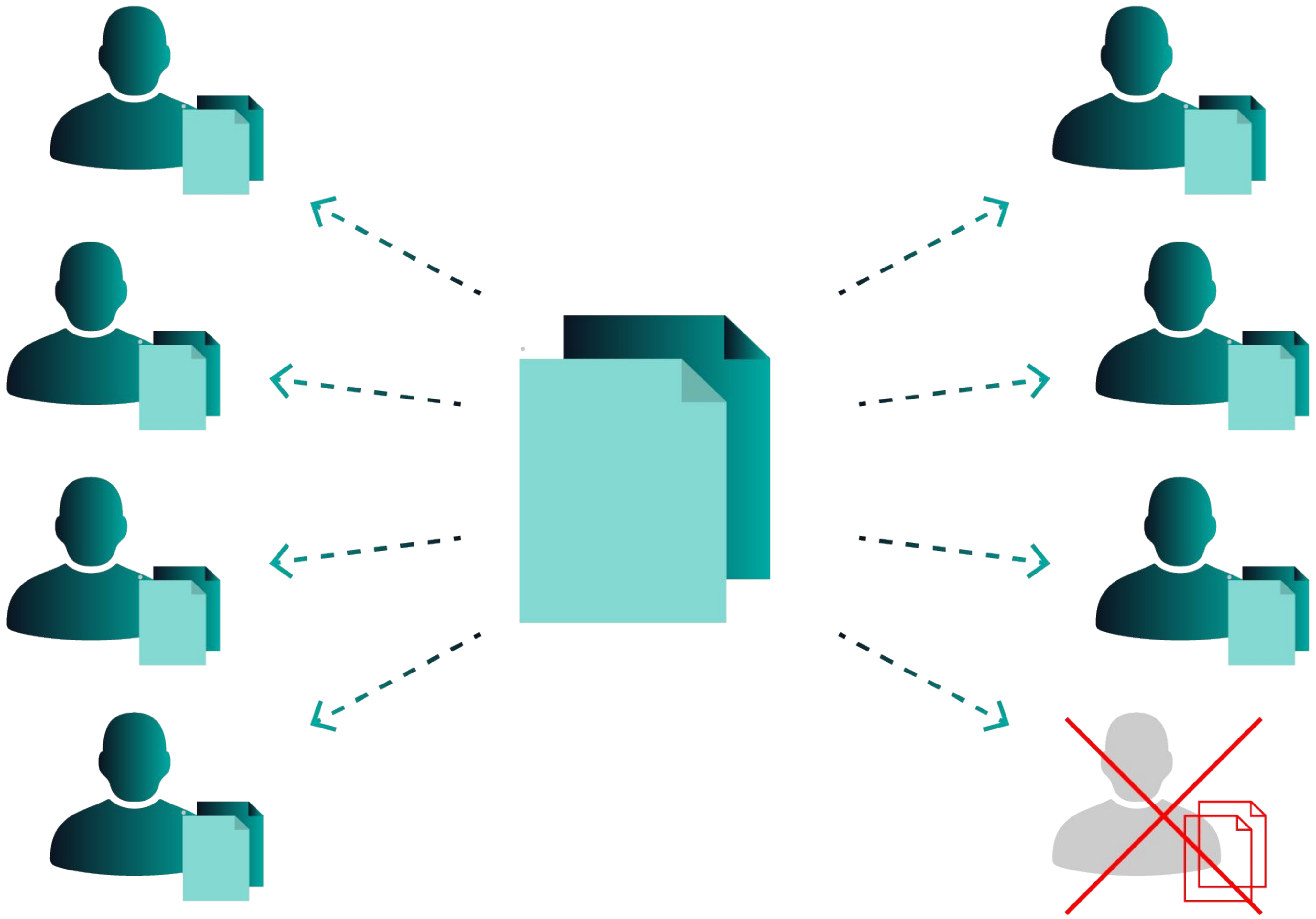
- Multiple Points of Access to “Truth”
- Single Source of “Truth”
- Single Point of Failure

Decentralized



- Multiple Points of Access to “Truth”
- Democratized Source of “Truth”
- No Single Point of Failure

Core Innovation



Data is **replicated** in a distributed network. Through **consensus**, the network comes to an agreement which data to store.

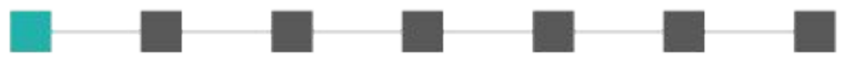
Through this, Blockchain's are a:

- Single Source of Truth
- Immutable and verifiable record of data

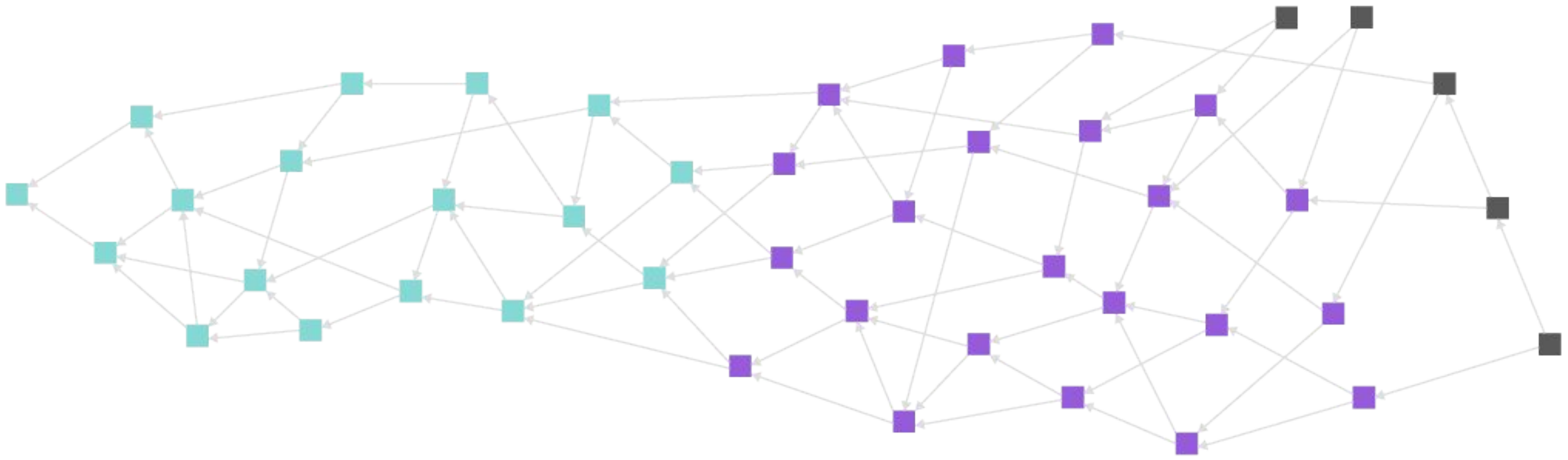
Trustless solution to Double Spends

Ledgers without a trusted authority where you have consensus on user accounts and double spend resolution

Distributed Ledger Technologies



Blockchain



Tangle

(DAG - Directed Acyclic Graph)

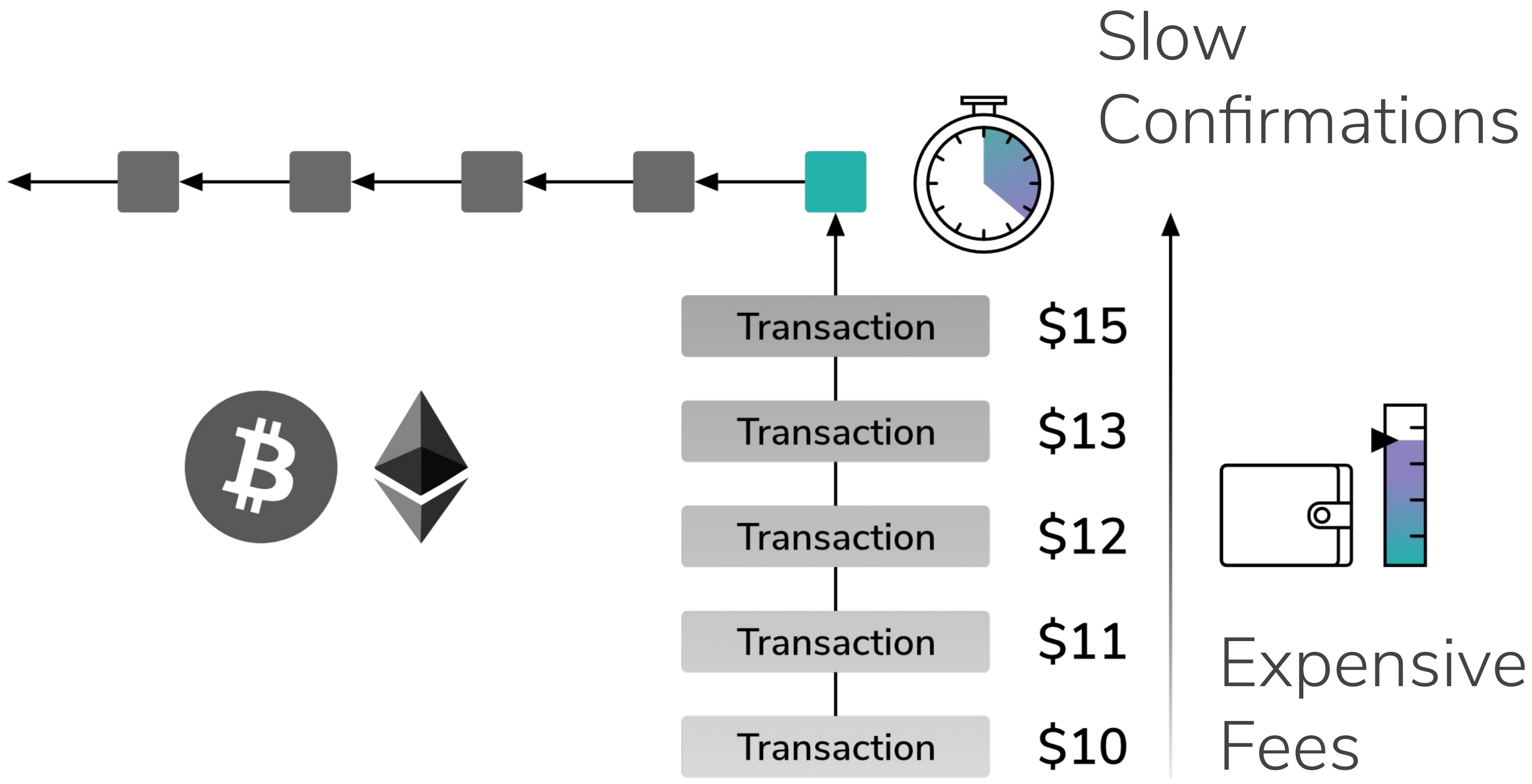
Why IOTA?

In 2015, the IOTA Founders saw the limits of Blockchain scalability fast approaching.

One of the founders, Dr. Popov, proposed a novel architecture that had better scaling properties. This set out a new way to handle the inherent speed limitations of the blockchain.

This novel architecture is called the Tangle.

What they saw was a classic bottleneck



Slow Confirmations

Transaction $15

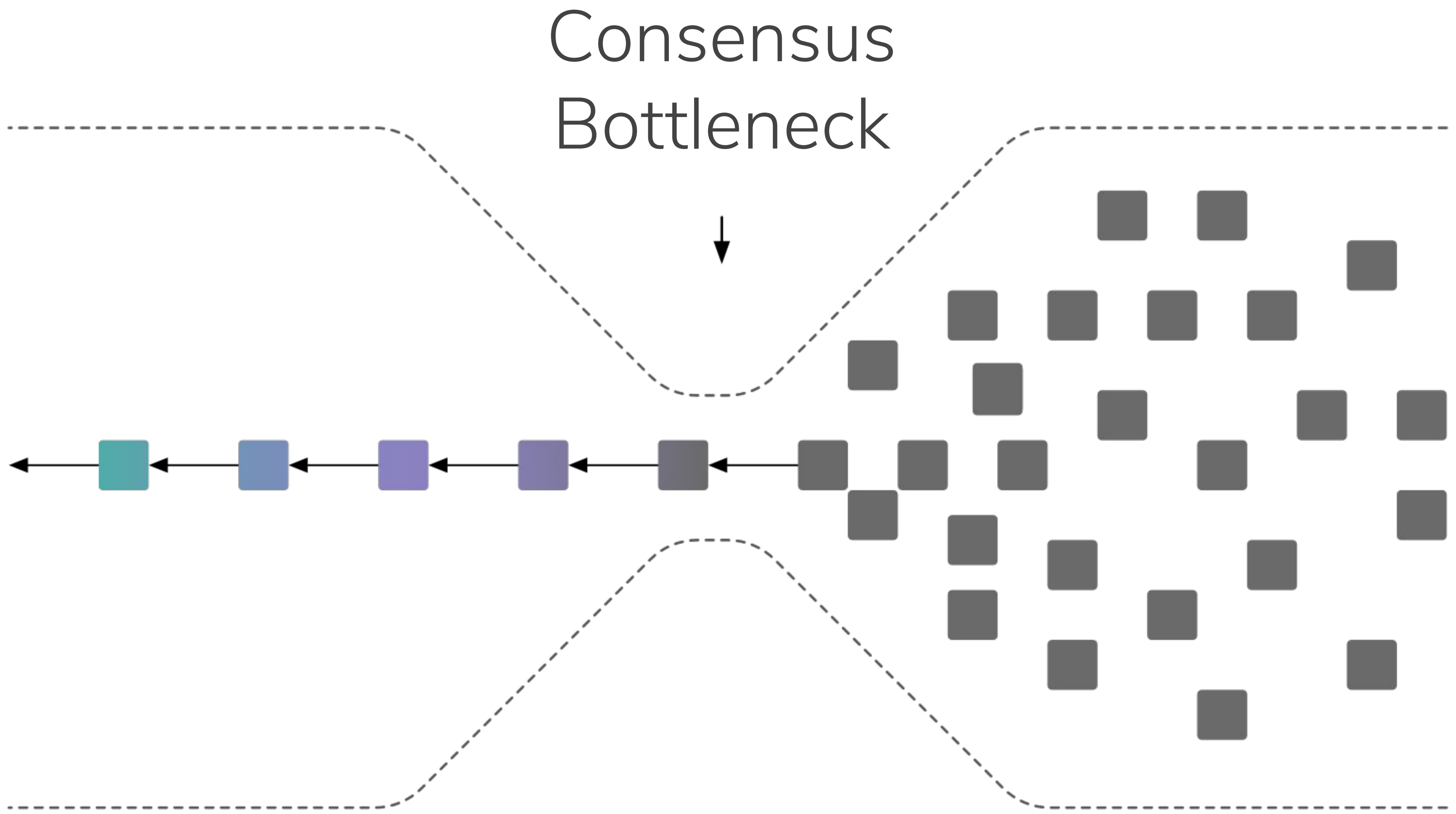
Transaction $13

Transaction $12

Transaction $11

Transaction $10

Expensive Fees



Consensus Bottleneck

Blockchain was designed for small scale

Blockchains have a built in scalability limitation: you cannot send blocks too quickly.

- In Bitcoin, blocks are 1 megabyte in size and arrive every 10 minutes.
- This implies a maximum global capacity of about 7 transactions per second.

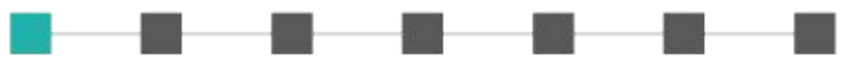
This cannot be fixed by simply increasing the size or frequency of block: **if blocks are too big or frequent, we will have many forks.**

- Blockchains can’t reconcile forks easily
- Instead the next block chooses which block is orphaned.

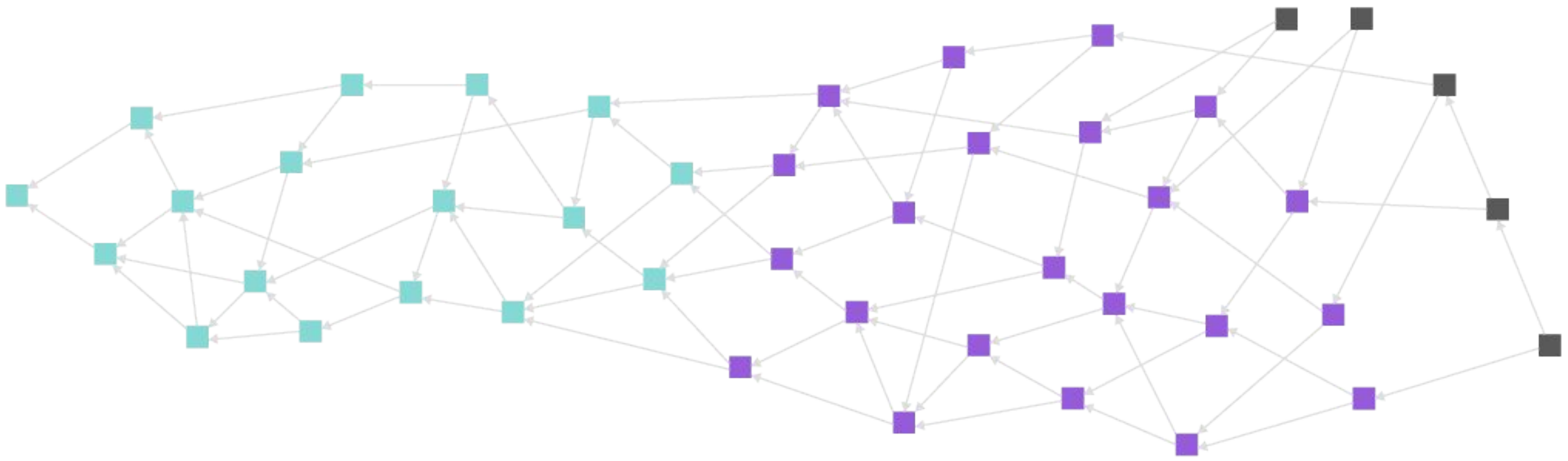
BEYOND THE BLOCKCHAIN

IOTA

Blockchain Vs Tangle graph structure



Blockchain

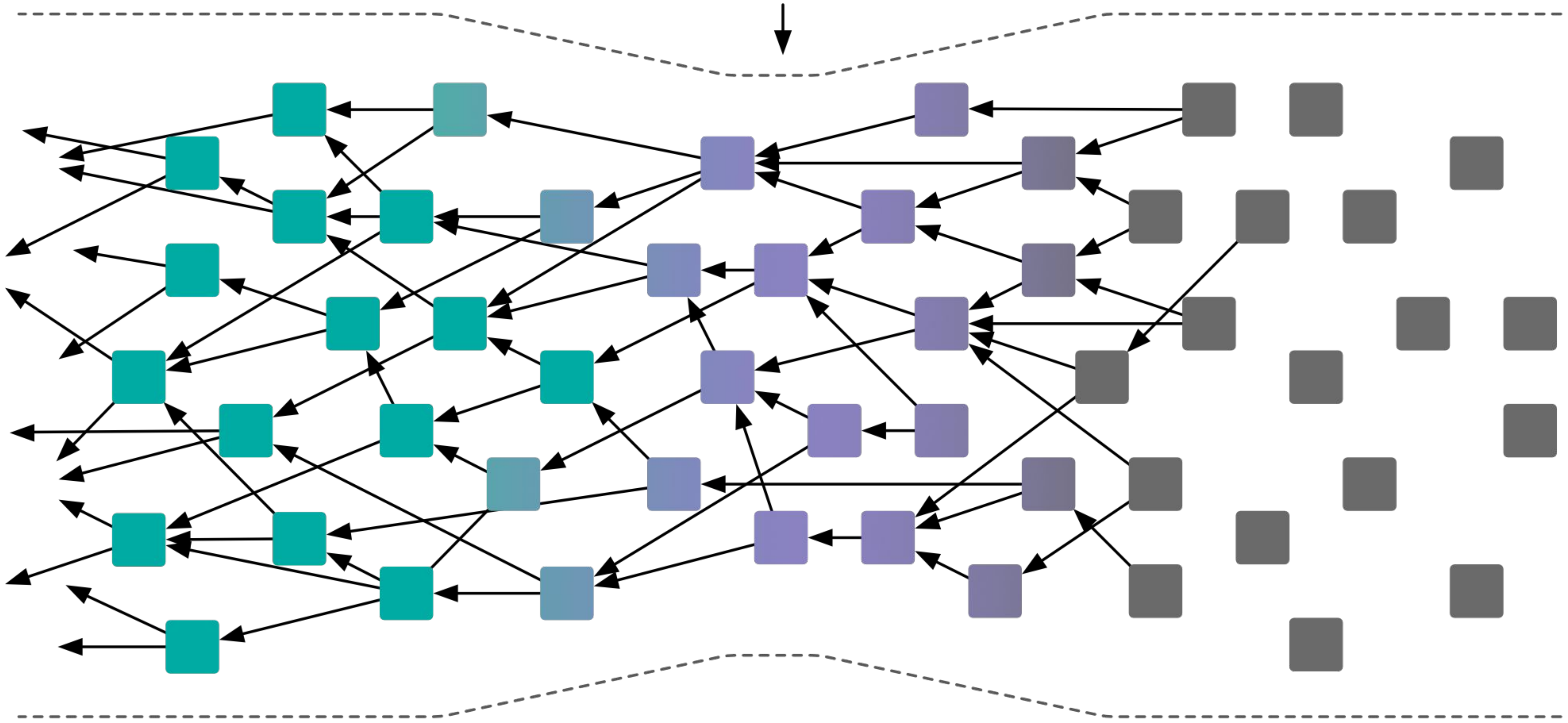


Tangle

(DAG - Directed Acyclic Graph)

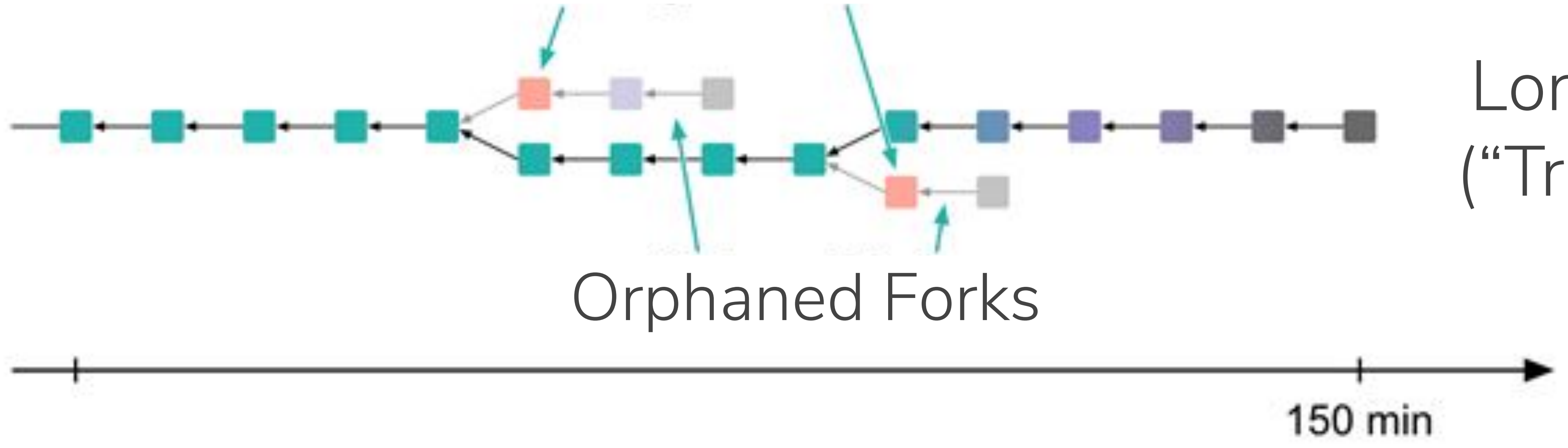
The Tangle

More activity
=
More validation



Consensus in IOTA vs. Blockchain

Blockchain

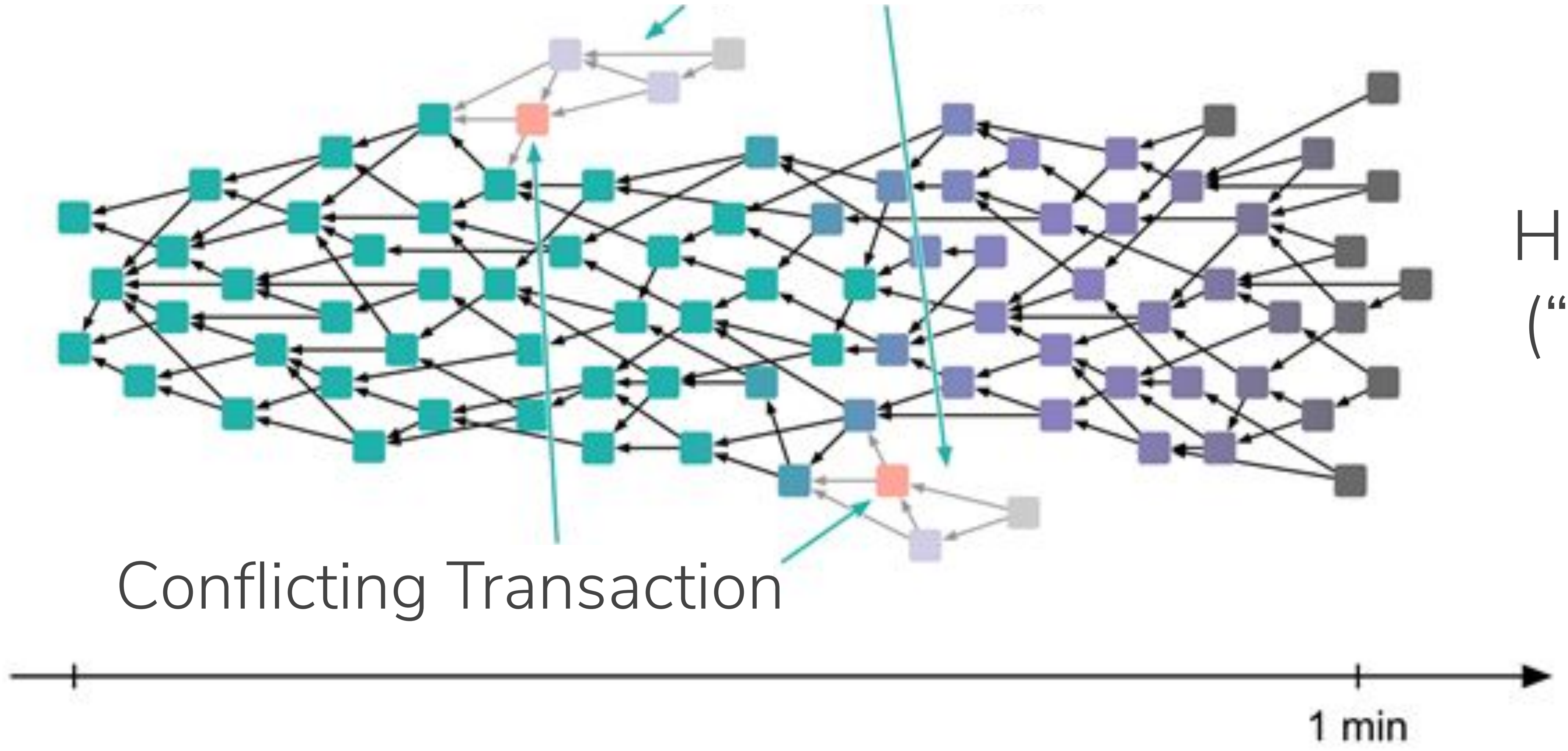


Conflicting Transaction

Orphaned Forks

Longest Chain
("True History")

IOTA Tangle

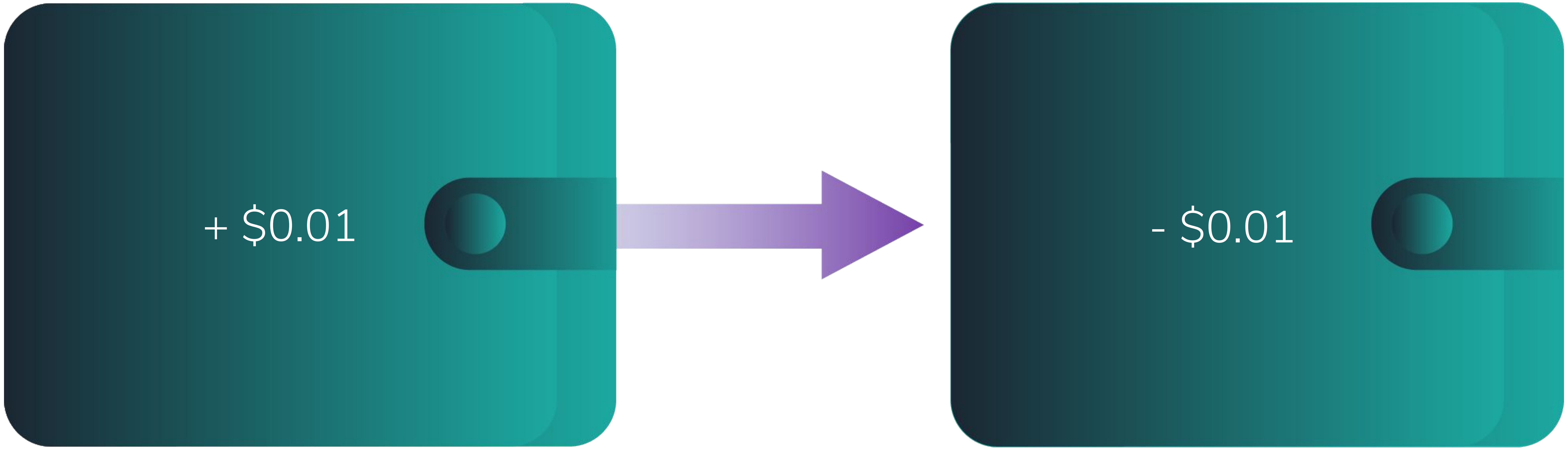


Orphaned Sub-Tangles

Conflicting Transaction

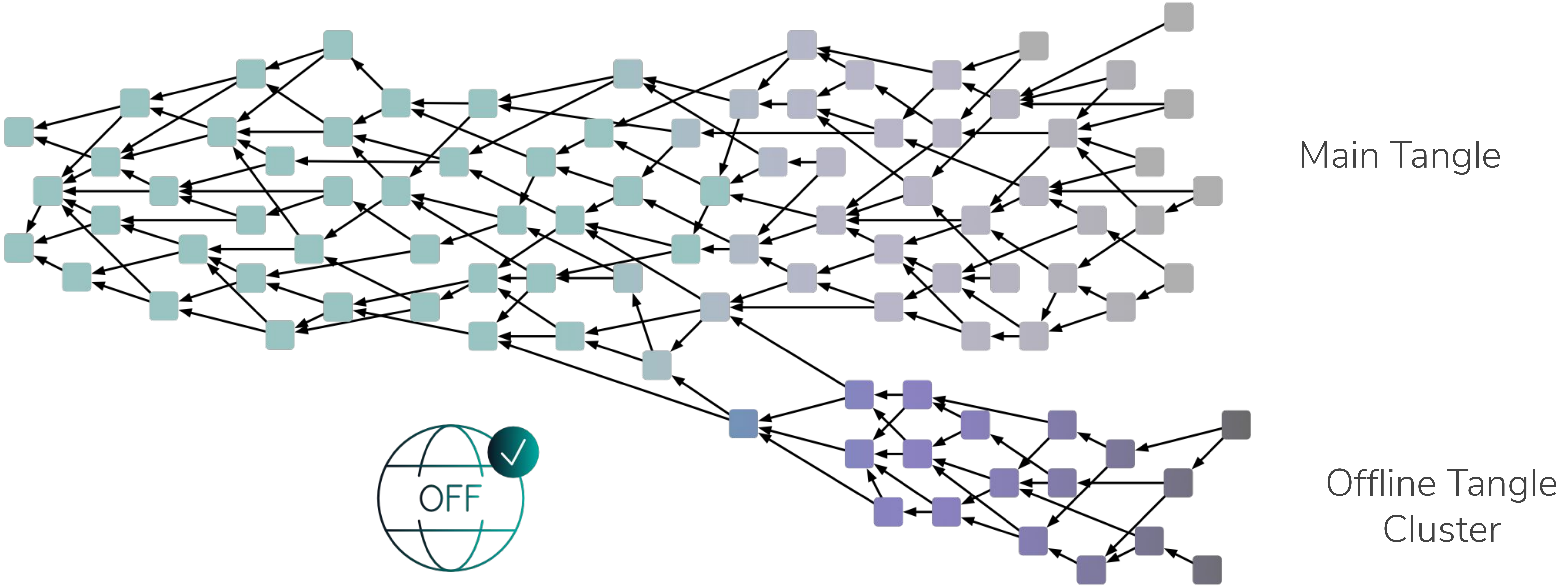
Heaviest Tangle
("True History")

No Miners = No Fees

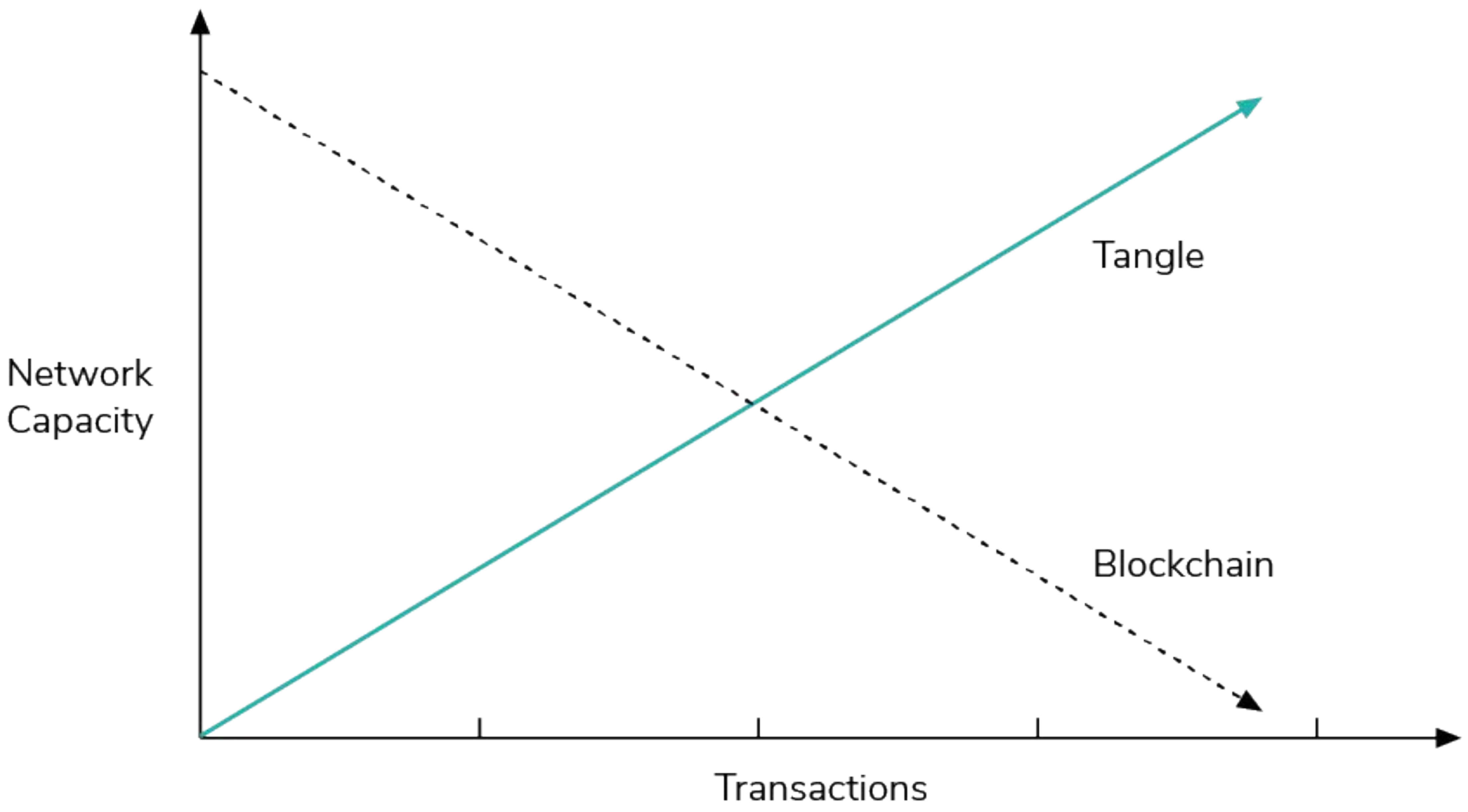


IOTA makes fee-less micro-transactions possible

Offline Transactions



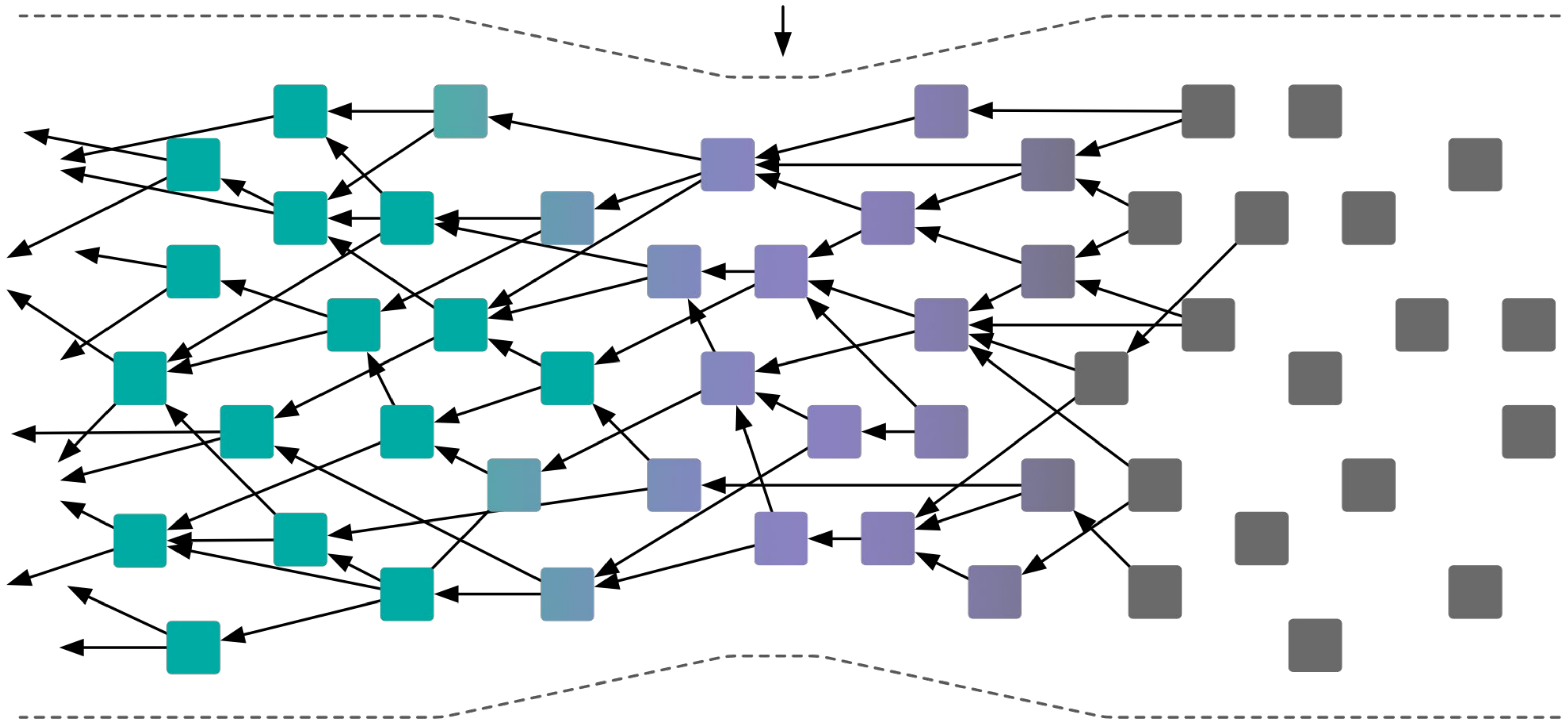
A Technology for the Era of Trust



- No Transaction Fees
- Secure and Decentralized
- Scalable
- Interoperable

Deep dive into ‘The Tangle’

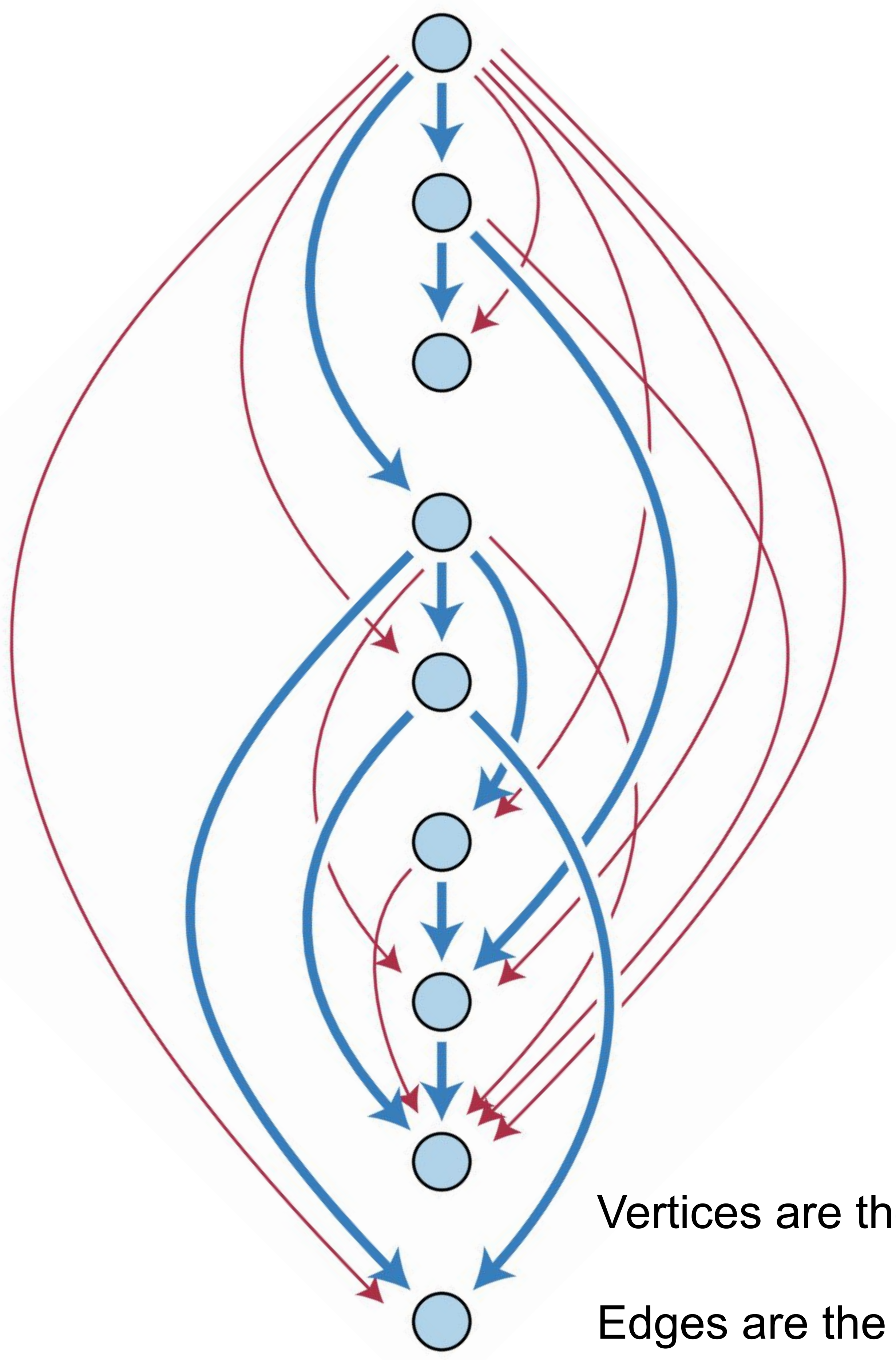
The Tangle



… The main feature of this novel cryptocurrency is the tangle, a directed acyclic graph (DAG) for storing transactions. The tangle naturally succeeds the blockchain as its next evolutionary step, and offers features that are required to establish a machine-to-machine micropayment system…

The Tangle, 2015 - Prof. Serguei Popov

What is a Directed Acyclic Graph

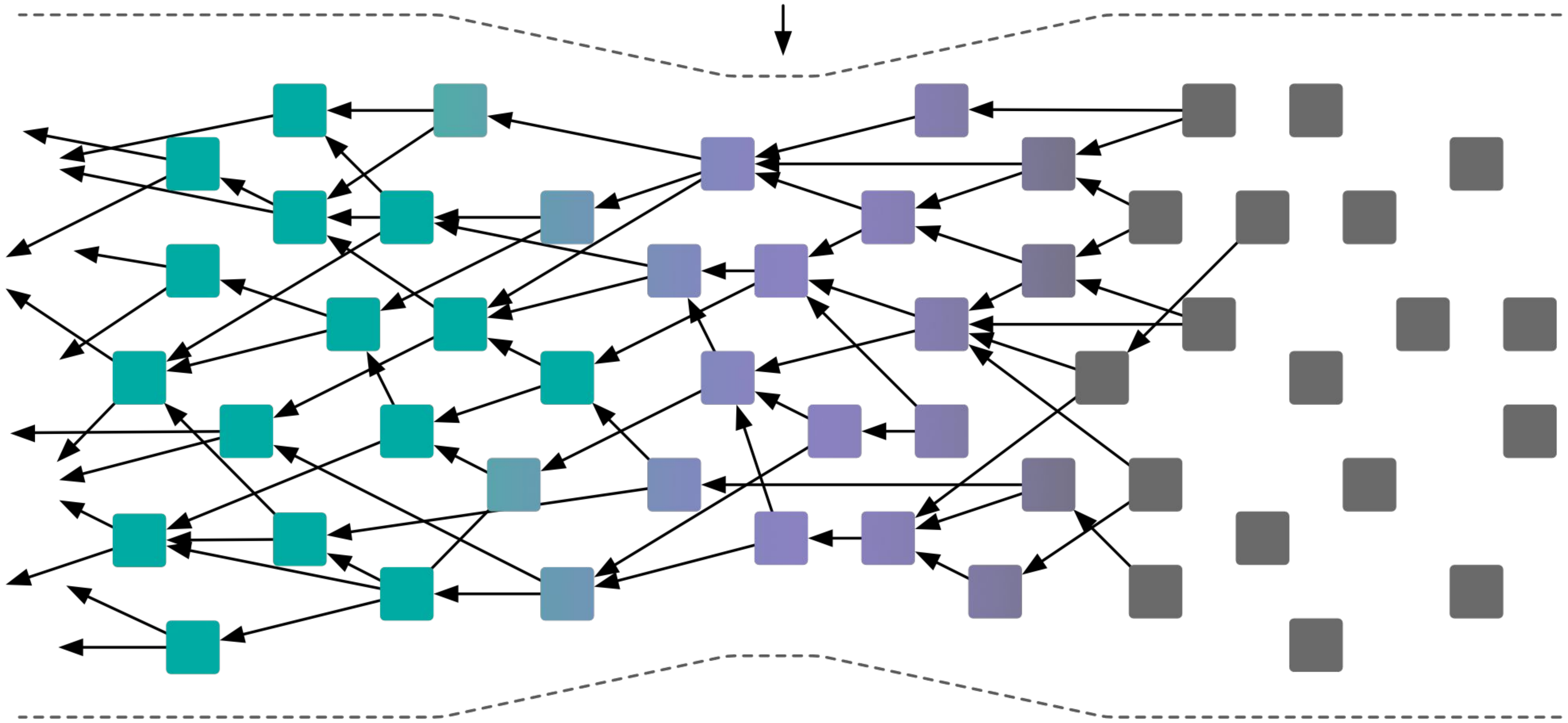


Vertices are the Circles

Edges are the lines

- A **DAG** is a finite **directed graph** with **no directed cycles**
  - Directed: *Vertices* connected by *edges*: edges have a direction
  - No Cycles: *Vertices* unable to be connected in a closed chain
- Topological ordered
  - *Vertices* organised such that every *edge* is directed from earlier to later in the sequence

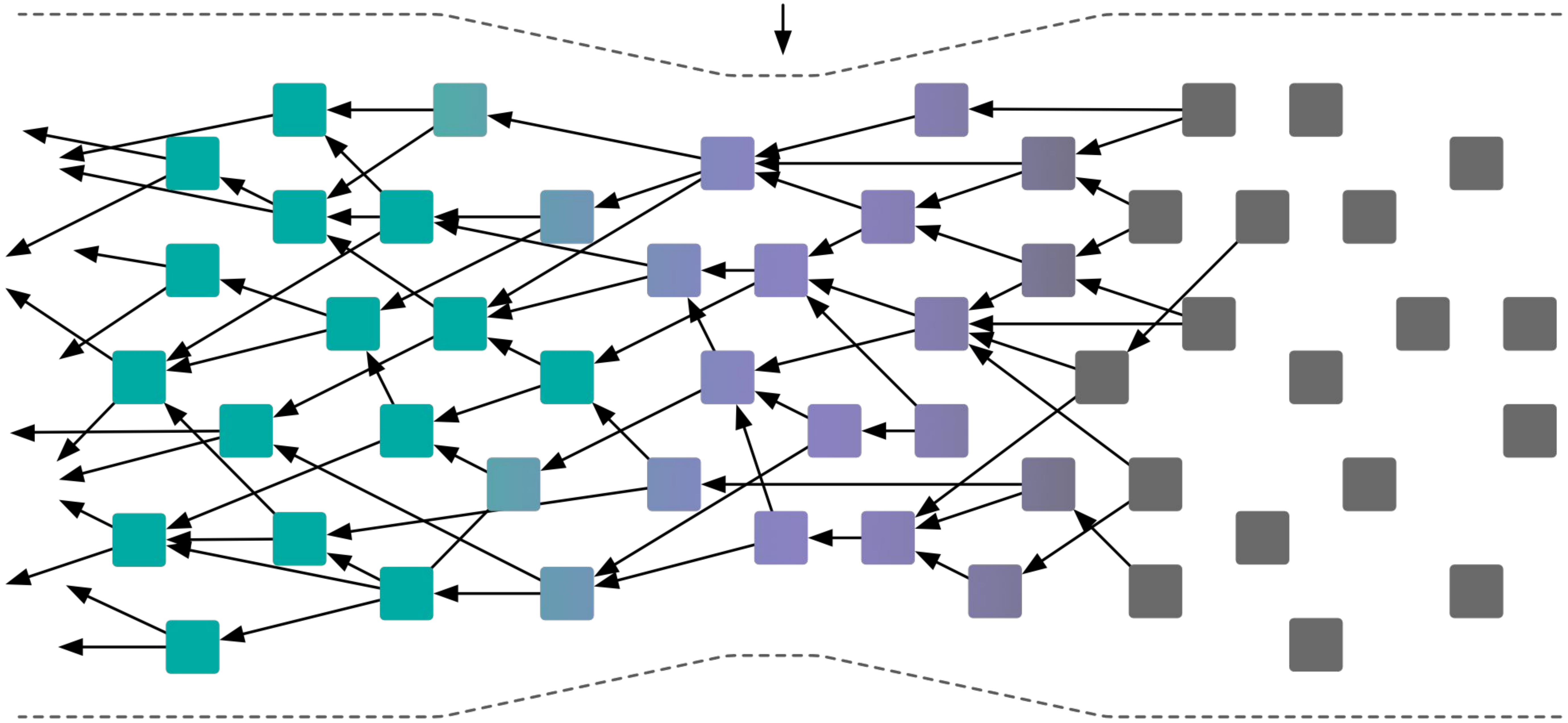
IOTA’s DAG Structure



Each **Vertex** represents a <u>transaction</u> (Squares)

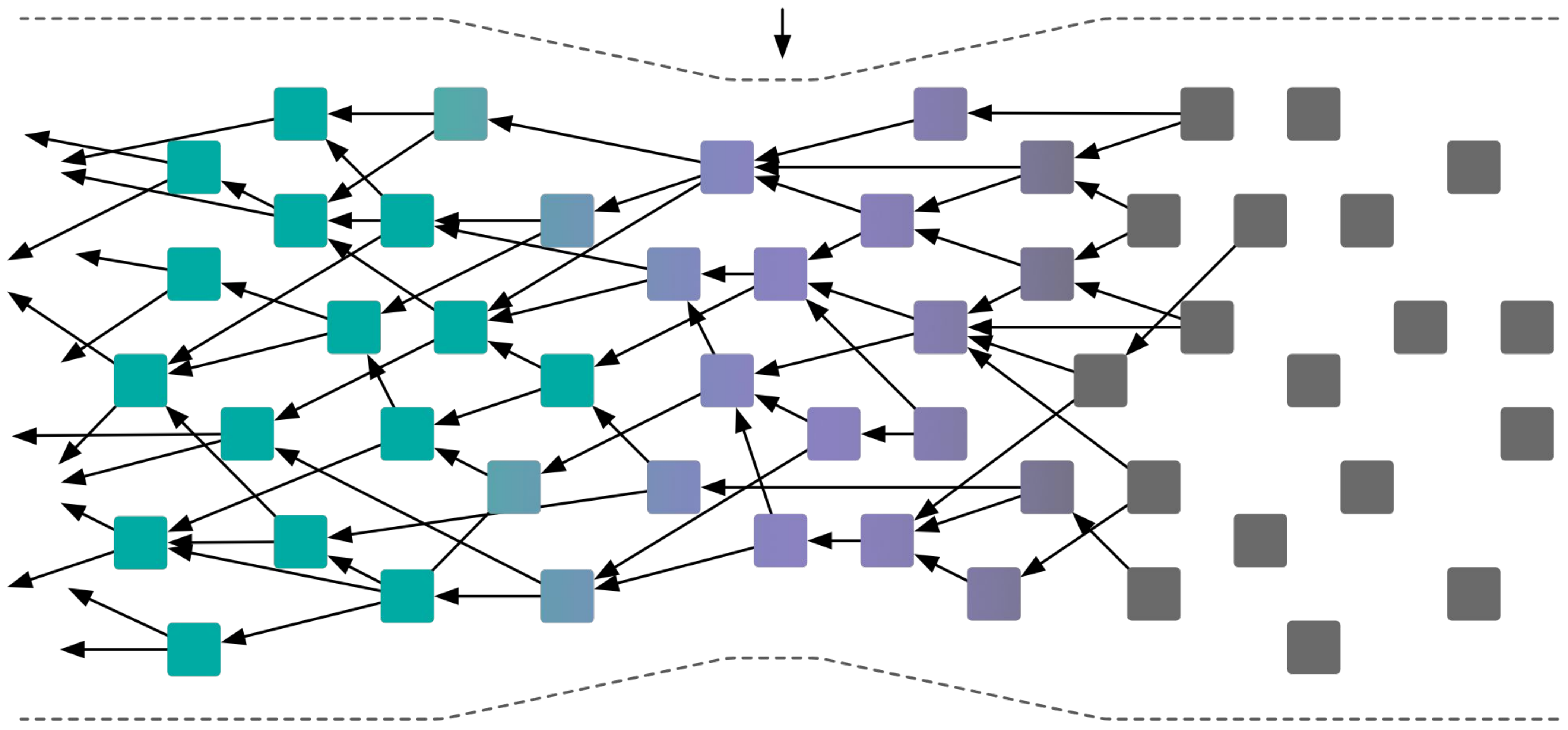
Each **Edge** represents an <u>approval</u> (Lines)

Transaction States



🟩 High Confidence 🟪 Low Confidence ⬛ Tip (unreferenced)

Adding a Transaction to the Tangle



■ Tip (unreferenced) ←

- To add a Transaction to the network your TX **must** reference **two** Tips (unreferenced vertices).

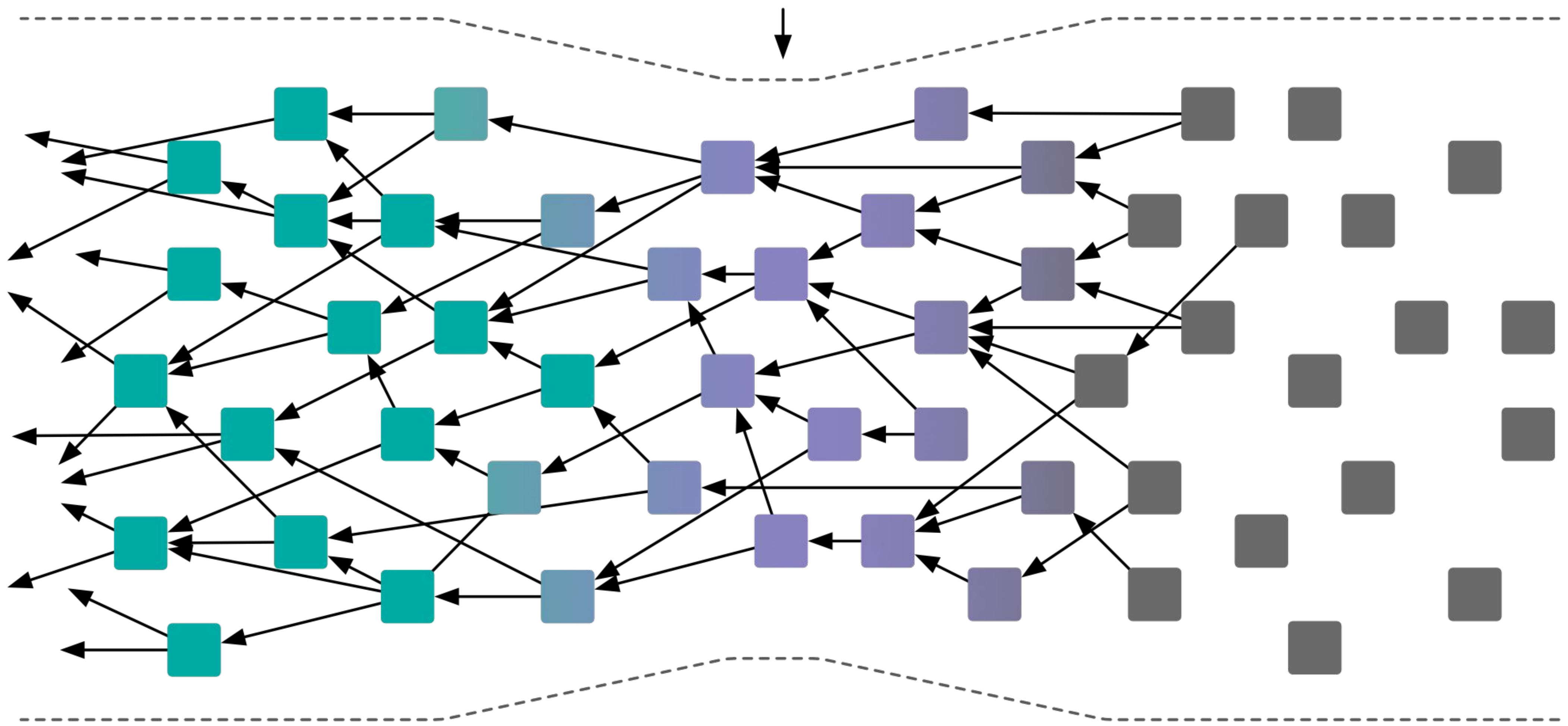
- When you reference a TX (vertice) you are directly & indirectly <u>approving</u> all TX’s back to the latest epoch

- Reference a TX that breaks consensus, namely transaction resulting in a negative balance or conflicts with another TX, will cause you Tip not to be referenced.

Rules

- Vertices have exactly **two** Edges
- Edges **can** reference already referenced Vertices

Picking Tips to Approve



■ Tip (unreferenced) ←

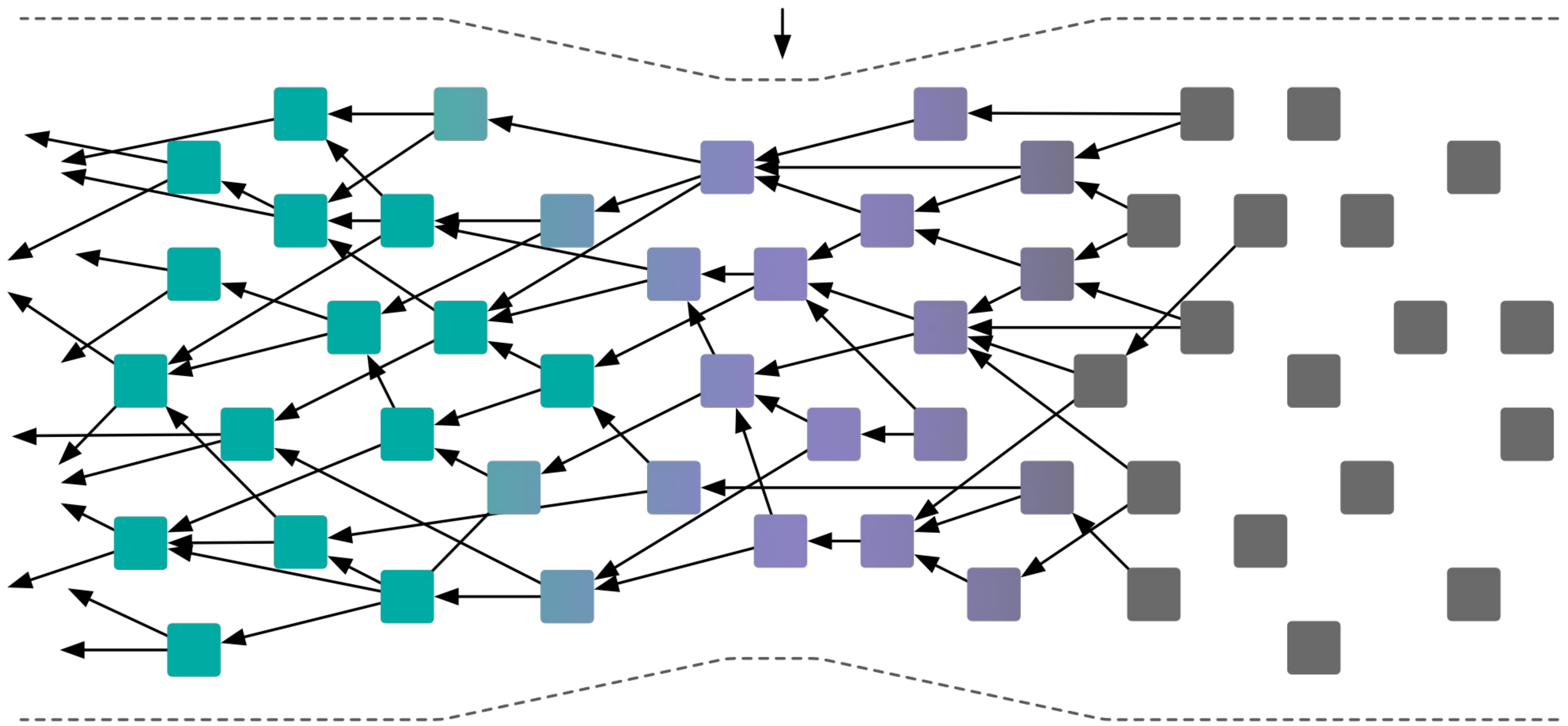
Tip selection in The Tangle is done by performing a Weighted Random Walk (WRW) from the genesis finishing at the Tips.

- The WRW is performed **twice**, to get the two required tips.

The WRW is **biased** towards transactions with more **cumulative weight**, or more **transactions referencing** them.

- Incentive to approve new TXs rather than old ones.
- WRW causes large branches (sub-tangles) to grow and small branches to get abandoned.

Consensus in The Tangle

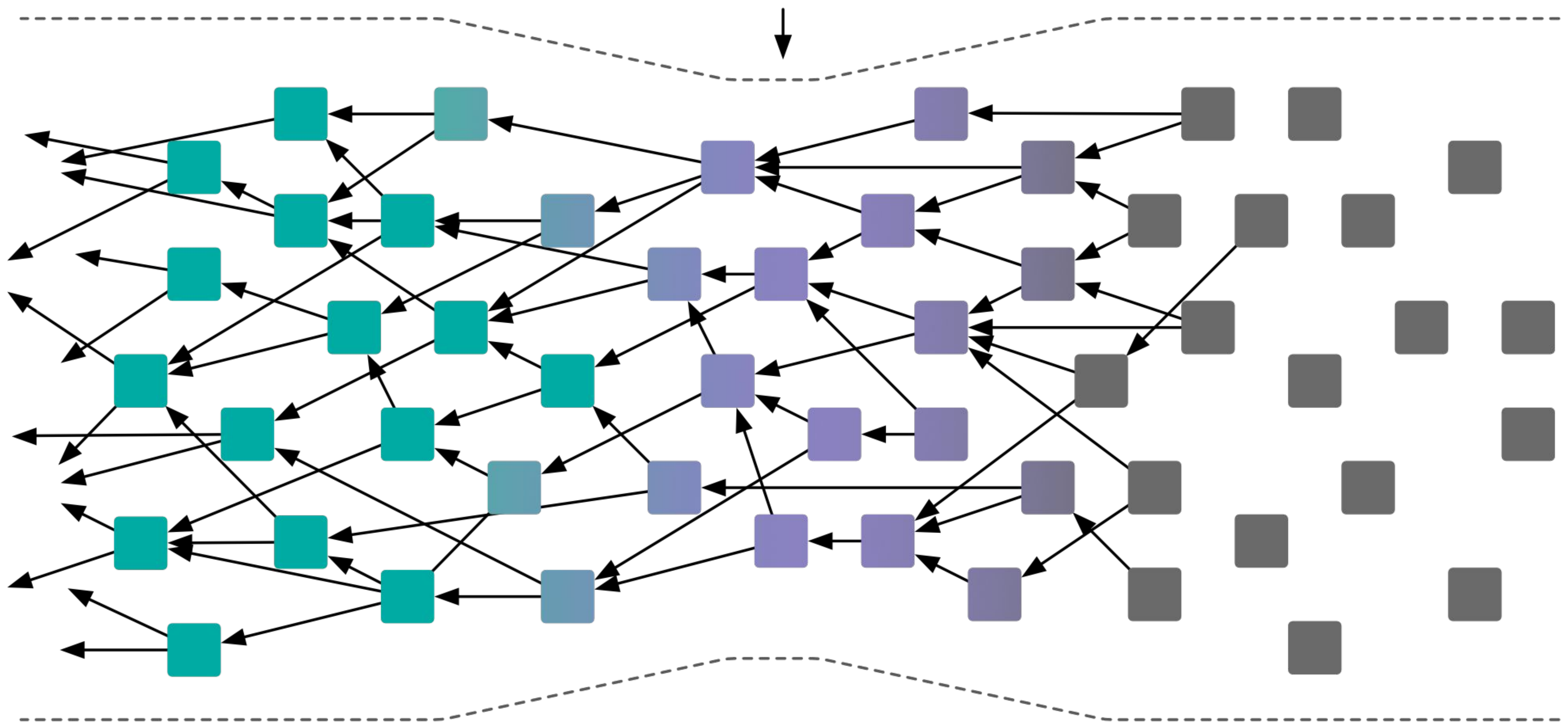


🟩 High Confidence ← 🟪 Low Confidence

- Similar to Bitcoin and other DLTs, a transaction has a **confirmation confidence**, which is an indication of its acceptance level.

- **Confirmation confidence** is derived by sampling the Tangle's Tips. Then the percentage of those Tips which reference a transaction is calculated. If 80% reference that TX then the TX is 80% confirmed.

Incentive to participate



🟩 High Confidence ← 🟪 Low Confidence

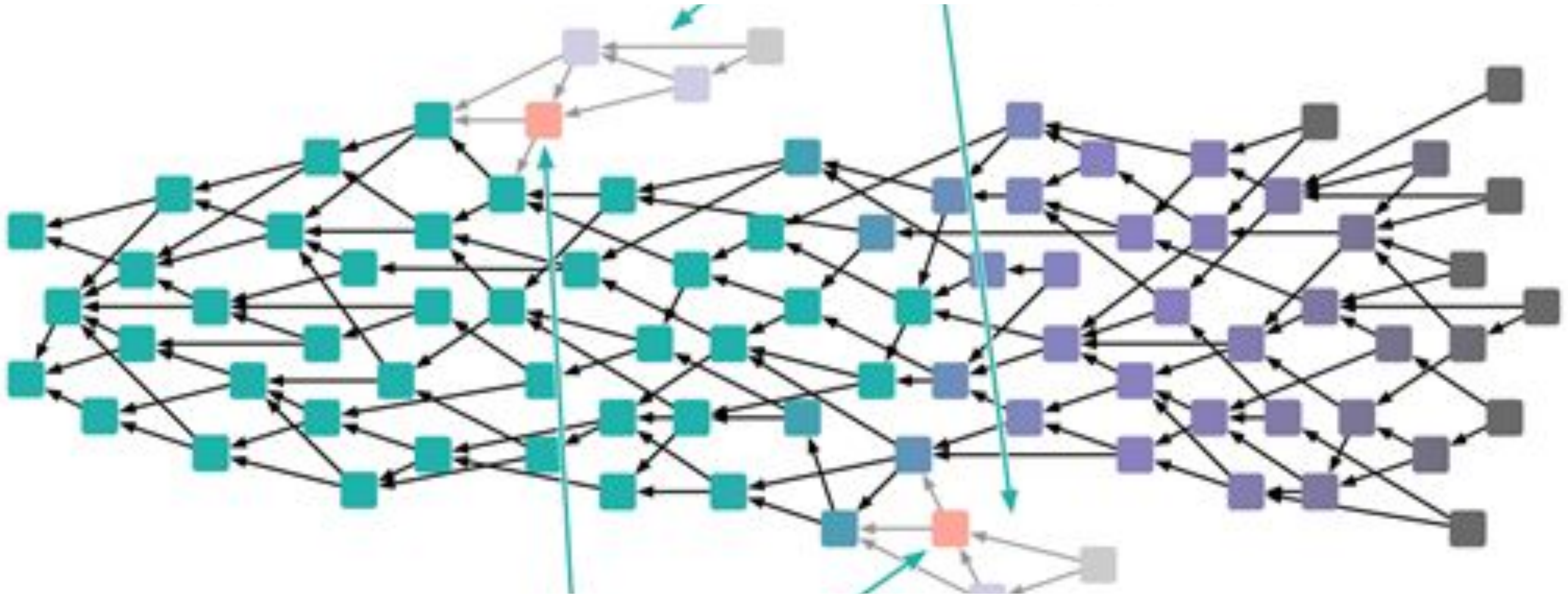
- Your aim when adding a transaction to the Tangle is to reach the highest **confirmation confidence**.

- To achieve 100% **confirmation confidence**, the TX should be referenced by all of the Tips of the network.

- To have the best chance of getting referenced, pick the two tips with the **heaviest cumulative weight / references.**

- This will incentivise other TXs using WRW to reference the TX.

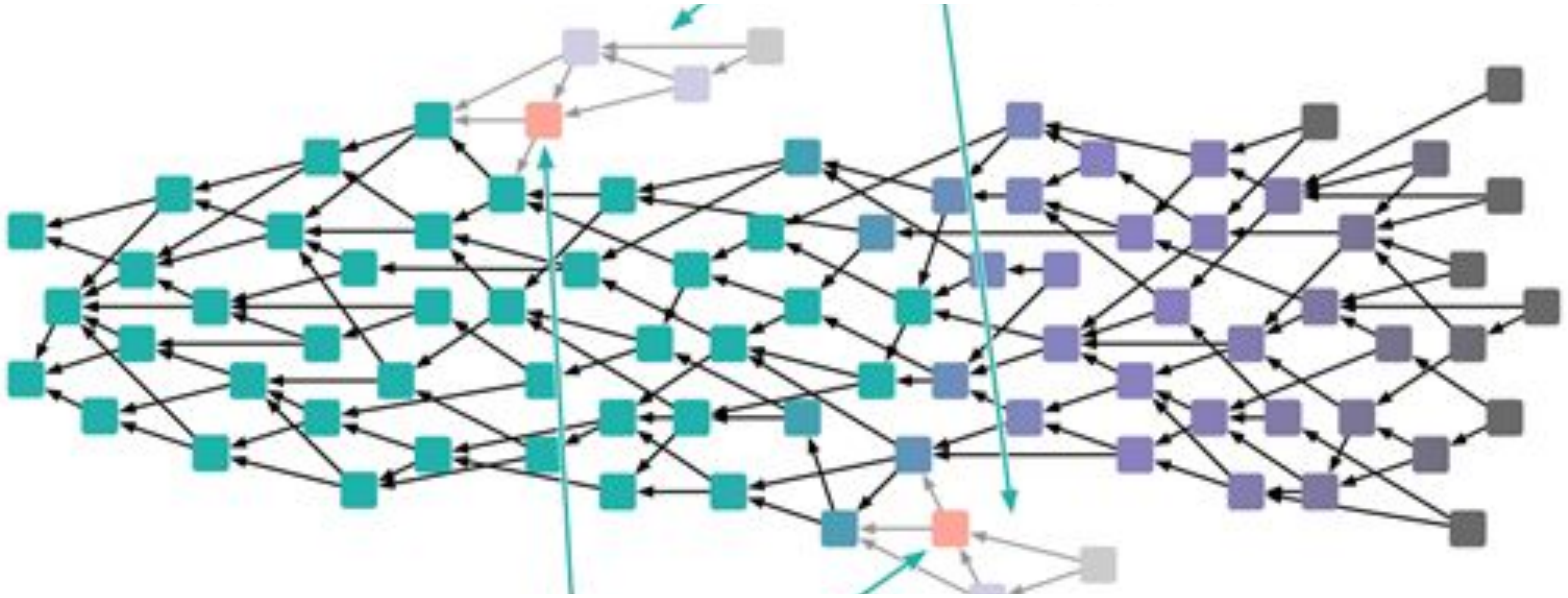
Unique Outcomes



- **Single participant class**
  - No dichotomy between Miners and Users
  - **Users** validate the network which enables them to publish TXs without paying a fee.
    - Note: Validation of the Ledger is not free and requires CPU cycles.

- **Networking as the TPS limit**
  - Removing *'Blocktime'* and *'Blocksize'* in favour of a blockless DAG offers scalability.
    - Blockchains will require soft-forks or 2nd layer solutions to keep up with adoption
  - Scalability towards the limit of the communication medium.

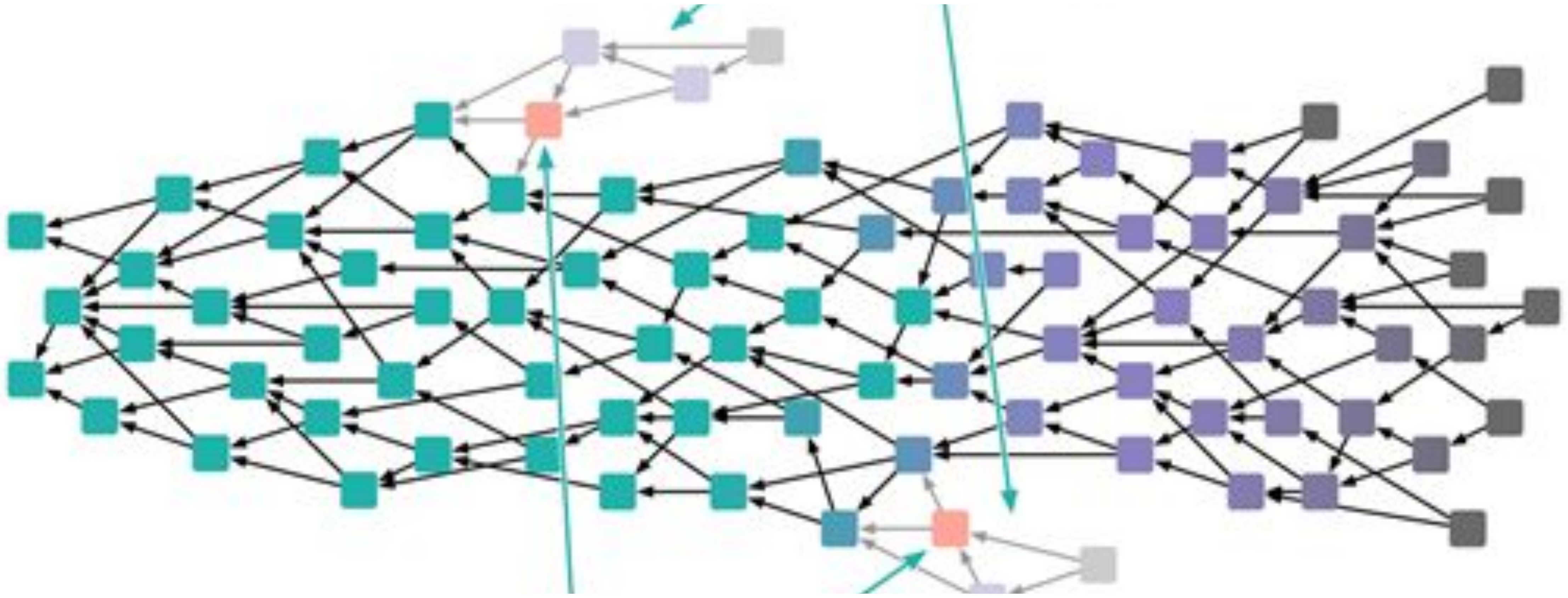
Unique Outcomes



- **Micro Transaction Economics**
  - With no payable fee, there is no minimum payment size. *1i sent is 1i received.*
  - Provides the access to new business models that traditional infrastructure can’t support.

- **Partition Tolerance**
  - Sub-Tangles can split off & merge later due to the Tangles architecture
  - Considers real-world networking events and maintains functionality through them.

Unique Challenges

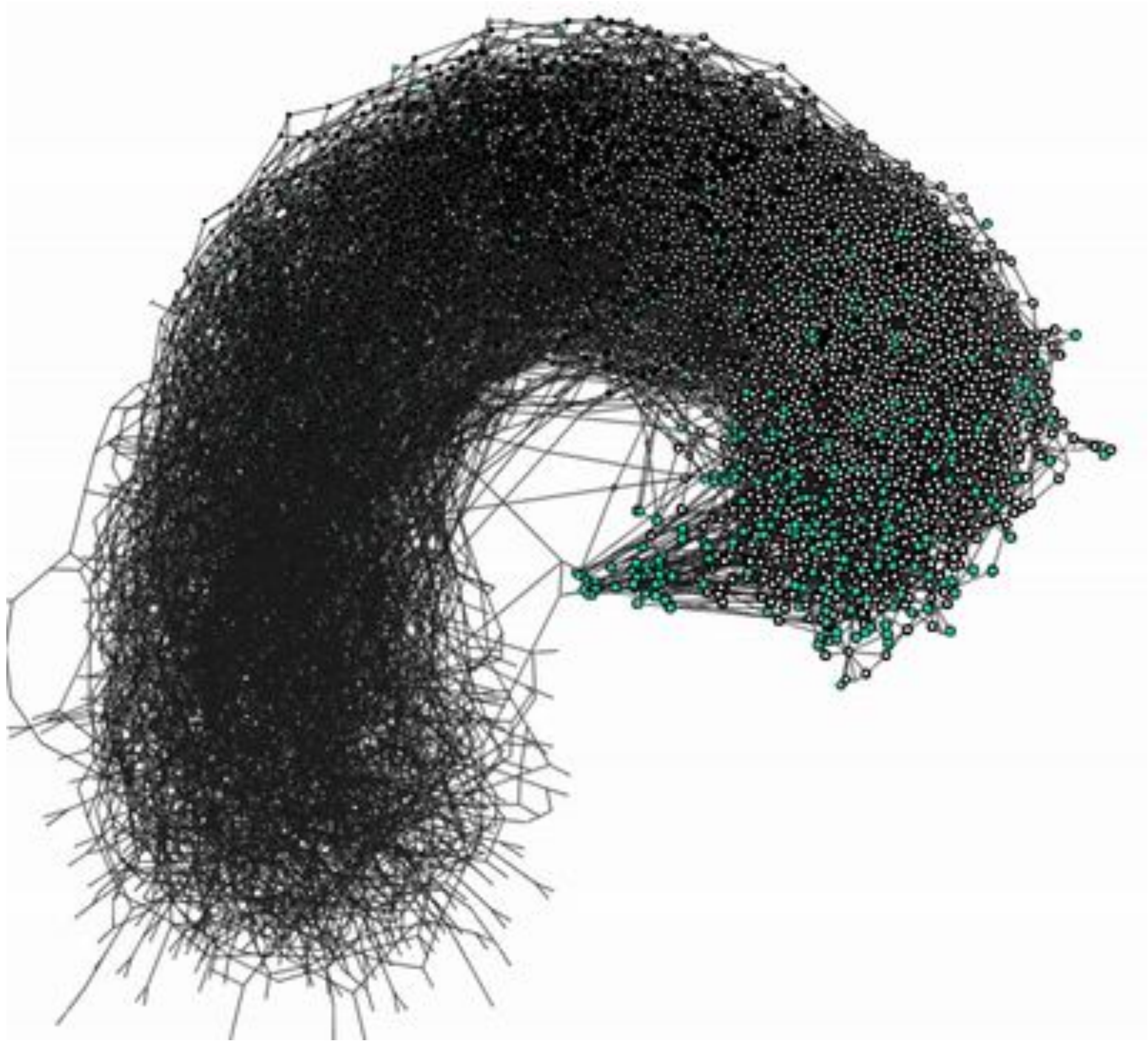


- **Probabilistic Confirmation**
  - Tip selection isn’t deterministic which can lead to unselected TXs. Thus unconfirmed TXs
  - Requires extra Promotion or Reattachment transaction to rectify

- **Open Research Questions**
  - The Tangle is a new concept in the DLT world.
  - There are a few areas of active research relating to throughput, stability and security.

Tangle Research

IOTA’s Tangle

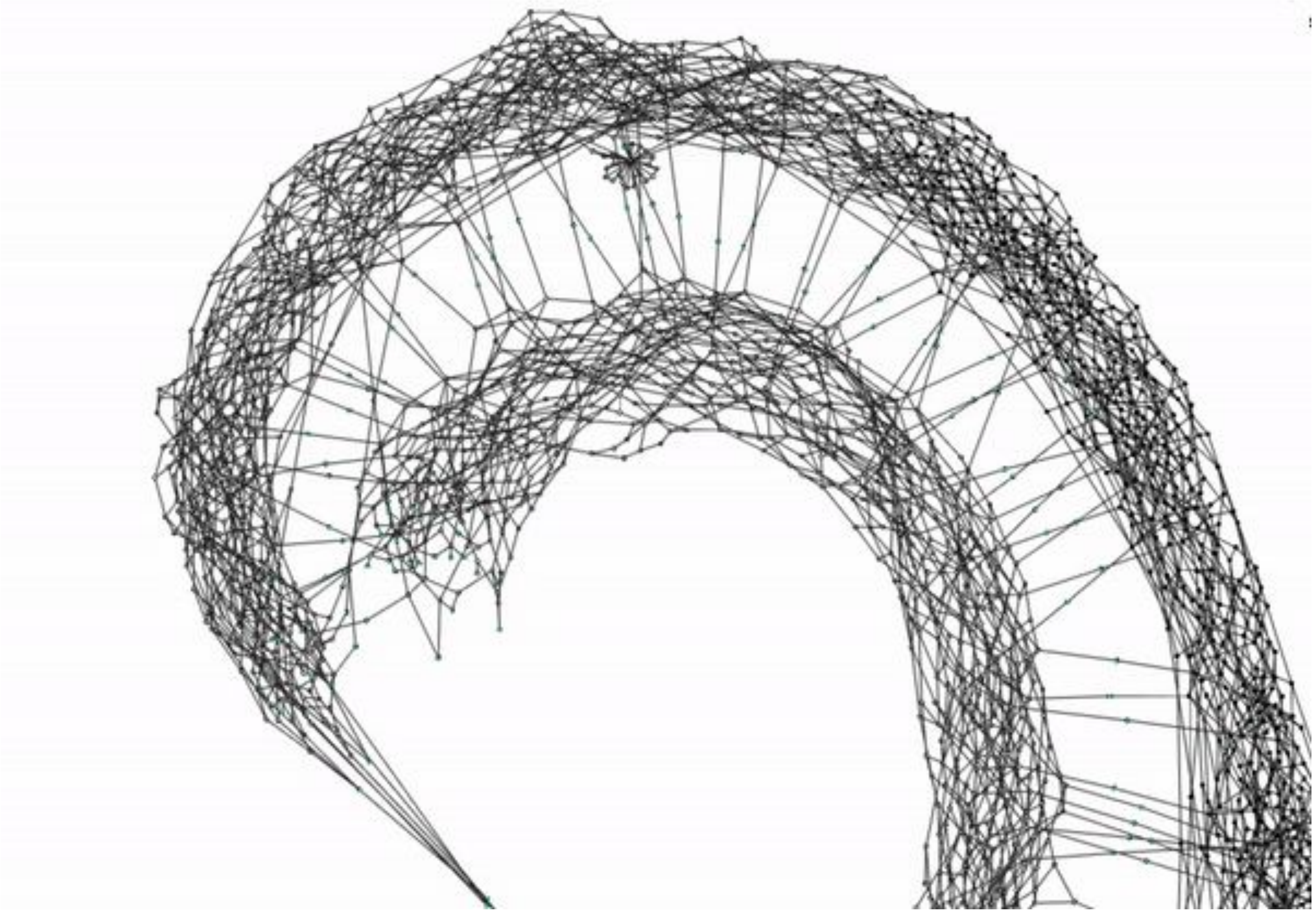


The IOTA Tangle (know as the ‘Mainnet’) has been operational since 2016.

The current Tangle slightly differs from the protocol outlined in ‘The Tangle’ whitepaper due to a need ‘bootstrap’ the network during the initial adoption phase.

We are working towards building a stable tangle that represents the protocol outlined initial whitepaper.

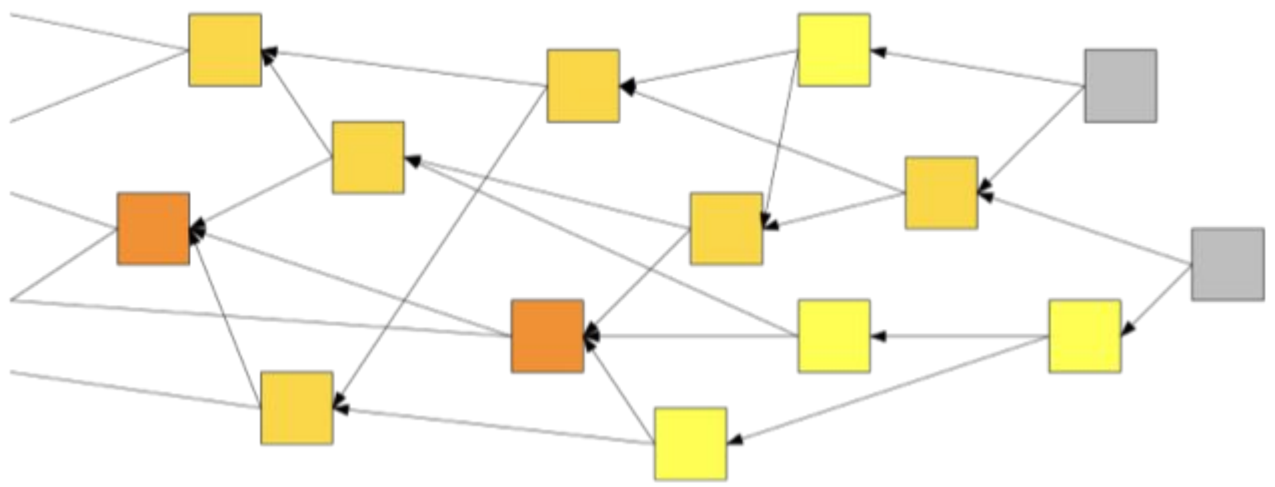
Attacks on the Tangle



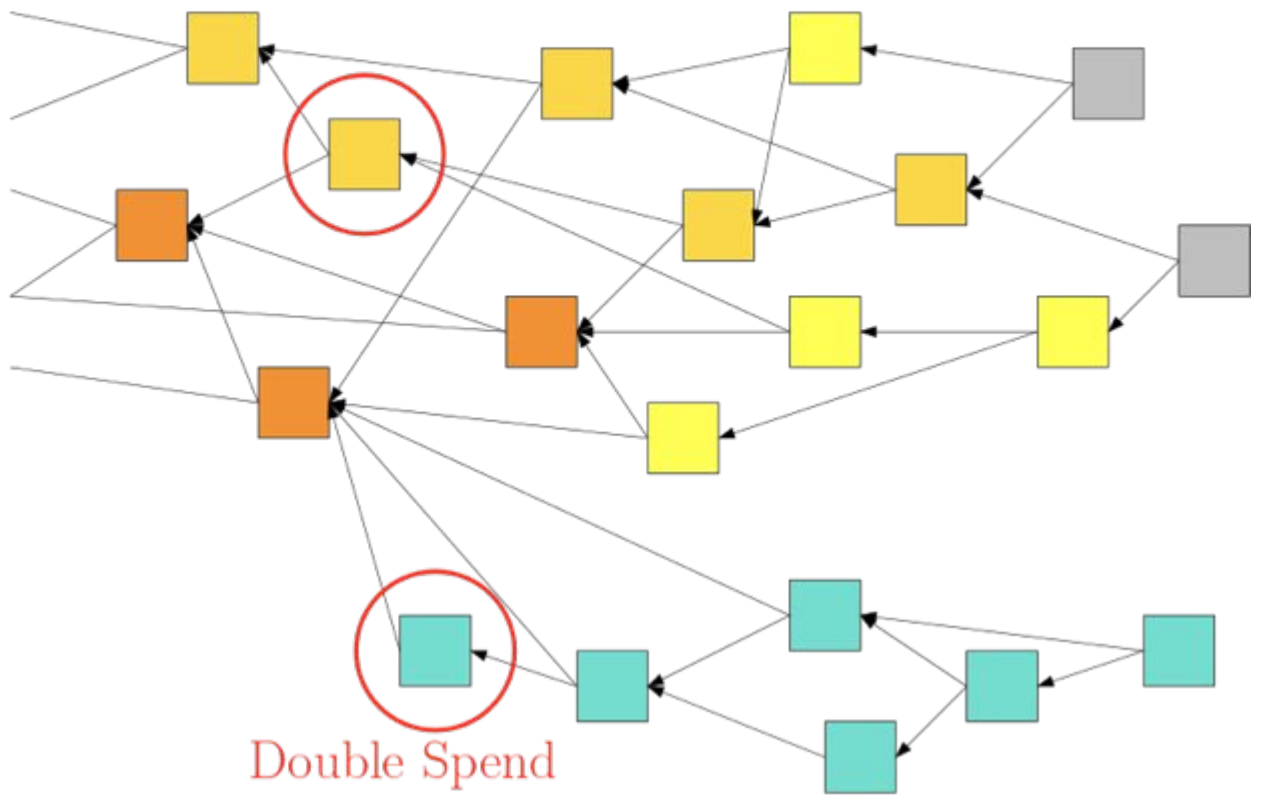
Parasite Chain Attack

An adversary secretly builds a sub-tangle, which is called **parasite chain (PC)**. At some point the adversary issues a transaction in the main tangle, as well as issuing a conflicting transaction on the still hidden PC, thereby creating a double spend. For a while the attacker continues to issue hidden transactions to the PC, until the transaction in the honest part of the Tangle is accepted. He then reveals the PC and hopes to exploit the tip selection algorithm to make most of the incoming transactions approve the double-spend transaction on the PC, thereby reverting the ledger history.

Before Parasite Chain is revealed



After Parasite Chain is revealed



How to counteract

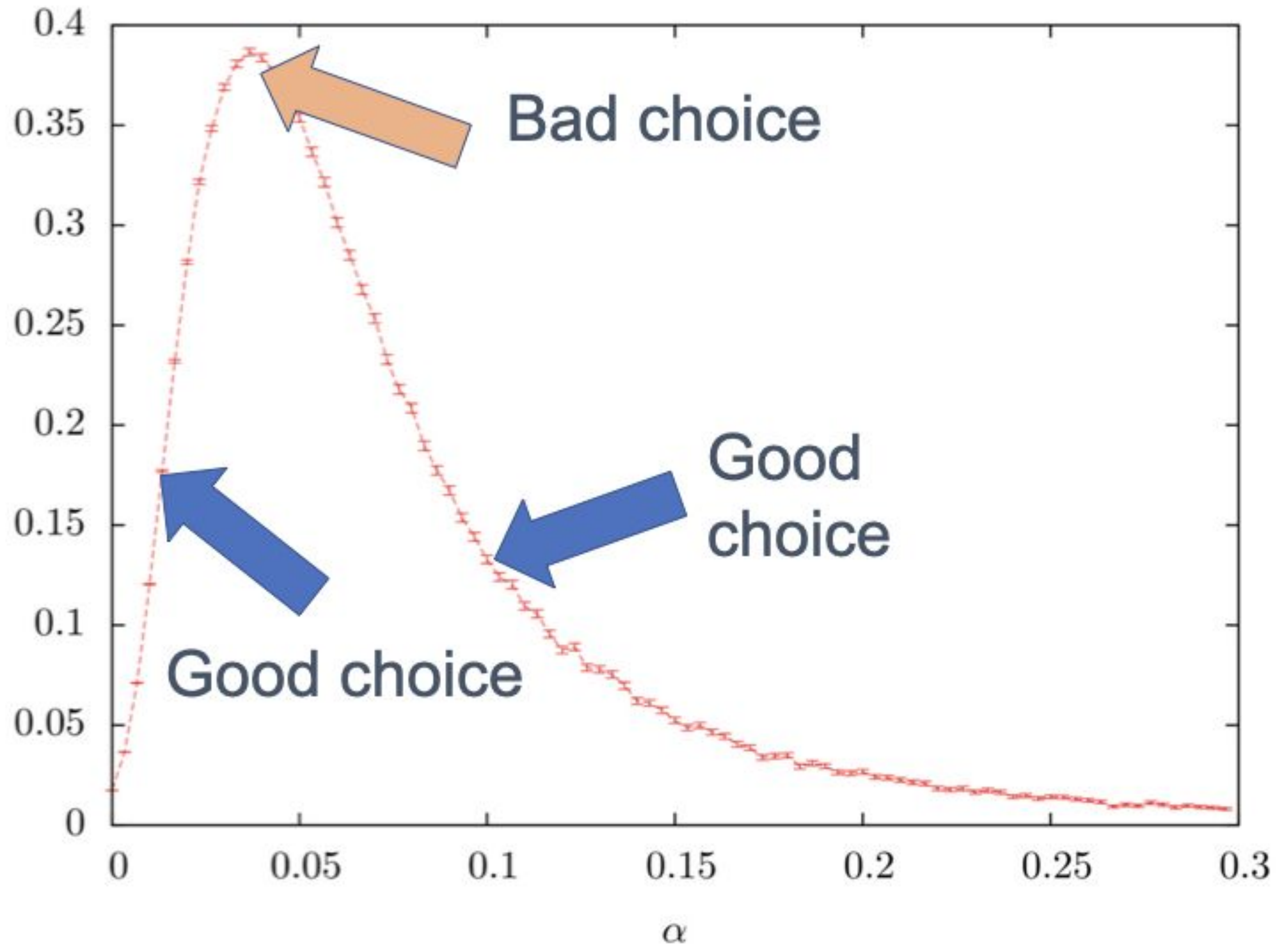
- ts - suggested waiting time before accepting payment (analogous to Bitcoin 6 blocks rule)

Parameters of random walk:

- α parameter
- Local modifiers (β parameter)
- q - backtrack probability
- Different tip selection mechanisms

Problem:

A high value of α increases security, but increases the probability of becoming orphan because random walkers will, with high probability, walk over heaviest txs



Probability of Random Walk ending on Parasite Chain

TSA models

Biased Random Walk

Pro

- Prevents Lazy tips
- Nash equilibrium

Cons

- Computationally demanding
- Security relies on high participation / honest tx rate
- Growing complexity to prevent attacks

Known attacks:

- Parasite chain
- Splitting
- Multiple Spend

Uniform Random (URTS)

Randomly select 2 tips

Pro

- Computationally efficient
- No tx left behind

Cons

- Lazy tips
- Time does not necessarily add to security of tx

Known attacks:
Similar to Biased Random Walk

Secure and swipe

1. Trunk tip = Security step (α↑)
   Ensure honest tips get selected
2. Branch tip = Swipe step (α↓,URTS)
   No orphans

Pro

- No tx left behind
- Similar tip number to URTS

Cons

- 2 classes of txs?
  (Security txs and Swipe txs)
- Similar attacks still possible?
- Confirmation time for Swipe txs increase?

The IOTA Network

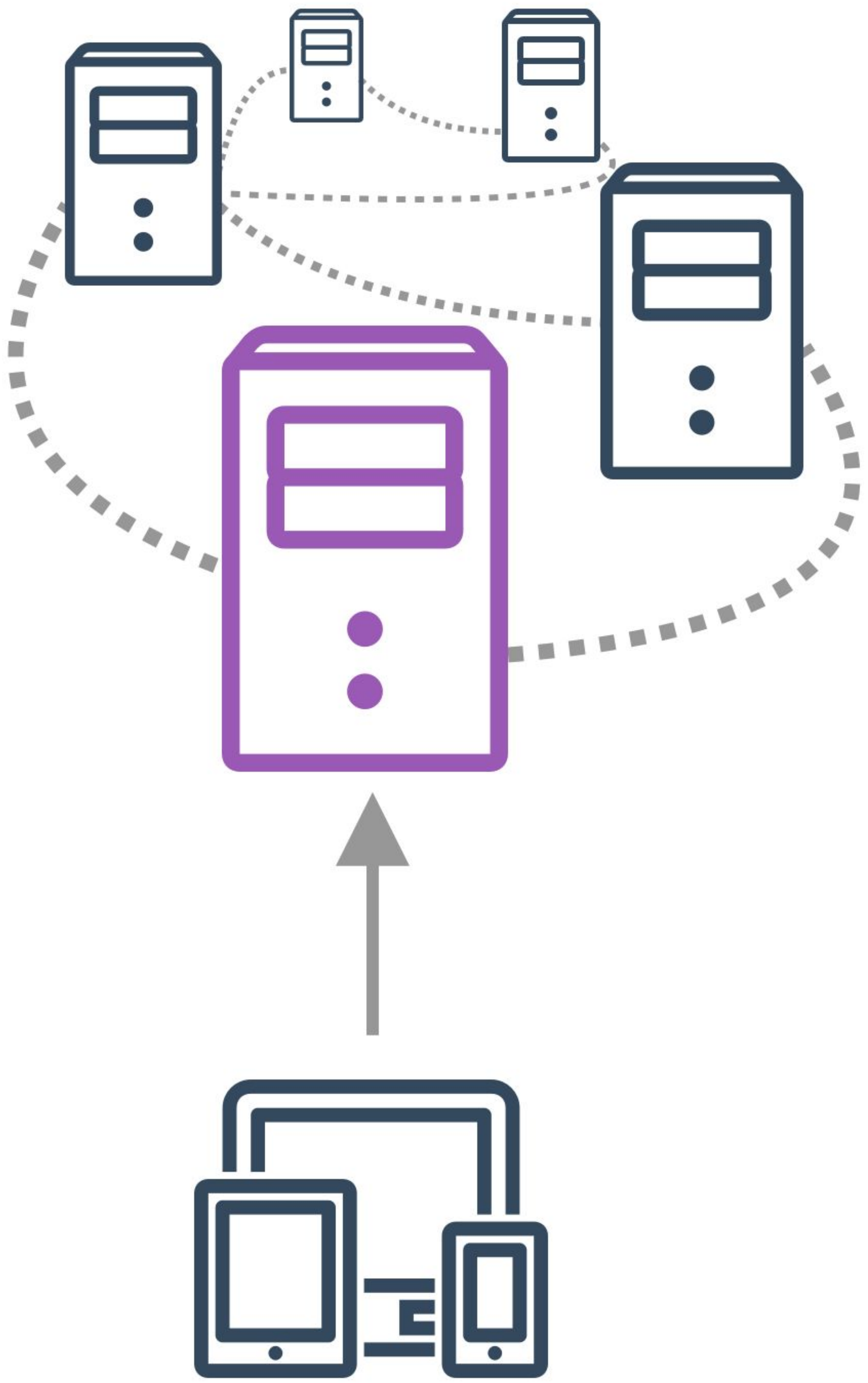
The Tangle Network

The IOTA Tangle is hosted by a collection of computers known as ‘Nodes’.

Nodes maintain a realtime database of the distributed ledger. Node receive new transactions from clients and share them with their neighbours.

Currently, the majority of the network runs the **IOTA Reference Implementation** (IRI) which is developed by the IOTA Foundation.

IOTA Reference Implementation

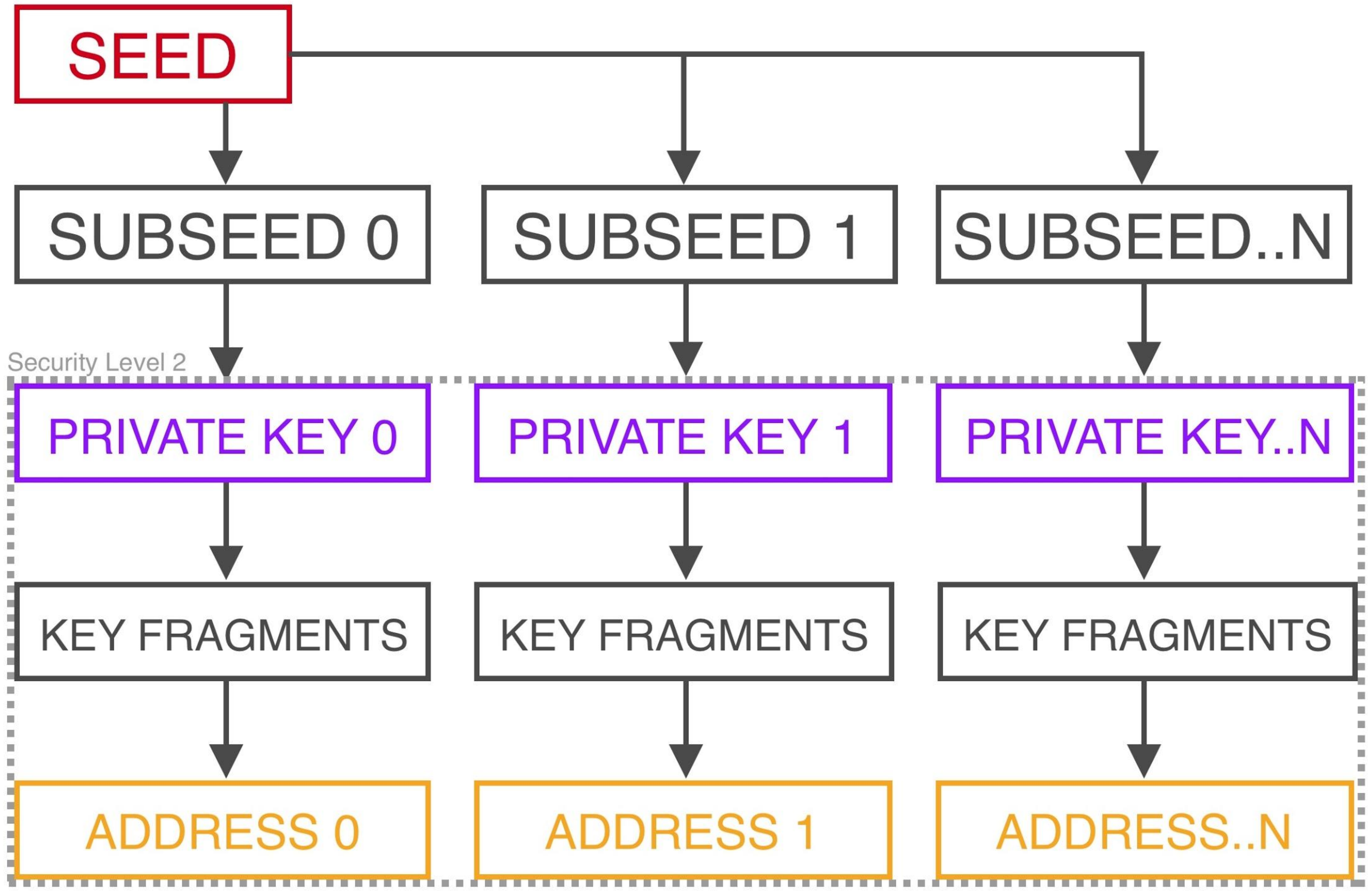


The **IOTA Reference Implementation** (IRI) is the current standard for Node software on the network. It is actively maintained by the IOTA Foundation and has frequent releases.

Its main function is to maintain the ledger state, execute the tip selection algorithm, and propagate information amongst its peers.

There are other implementations of the Node software being produced by third parties which are target at different platforms.

Seeds, Private Keys & Addresses



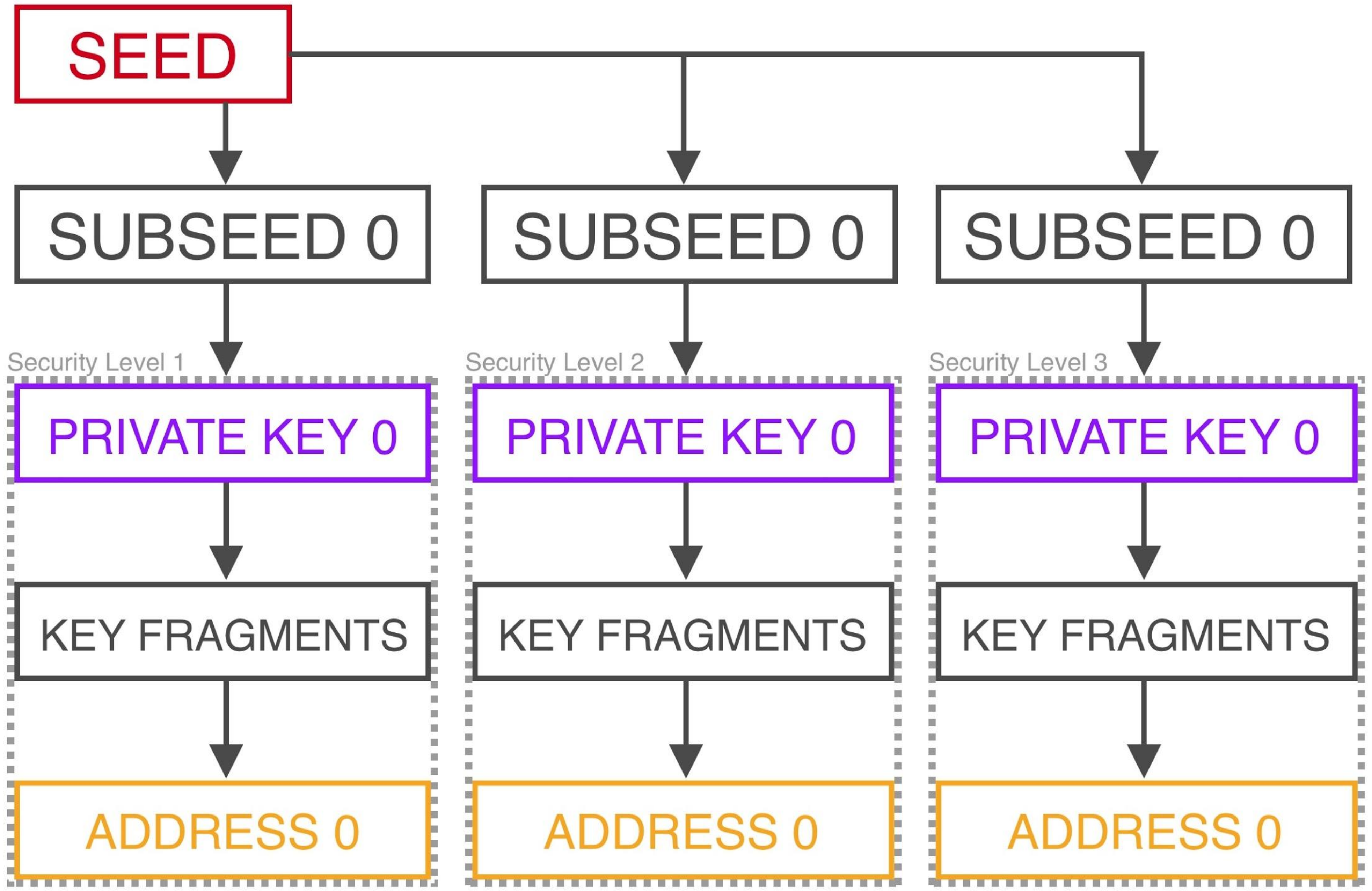
The Seed is starting point for creating an ‘account’ or ‘wallet’. This is the **secret** that controls the addresses that hold tokens.

- It is used derive the secret **Private Keys** and their corresponding public **Addresses.**
- A seed has a practically limitless number of **Addresses.**

A few important notes:

- Knowing a Seed is **Proof of Ownership**. If you can control an address this means you own the tokens at it.
- A Seed is comprised of 81 Trytes.

Hashing & Security



When generating new Addresses and Private keys it is possible to specify one of **3 Security Levels.** The security level specifies the number of rounds of hashing to derive the **Private Keys**.

- Resulting in 81, 162, 243 trit keys respectively
- More hashing rounds are more difficult to brute force but take longer to generate addresses and sign transactions.

Each security level generates **totally independent** pool of addresses. This enables one Seed to have 3 ‘different’ wallet spaces. However, most applications stick to **Level 2.**

A note on Trinary

Trit:

Analogous to **one bit** in binary,

Trits have **3** states

[1, 0, -1] are three states

Tryte:

Analogous to **one byte** in binary

Trytes consist of 3 Trits giving them 27 states

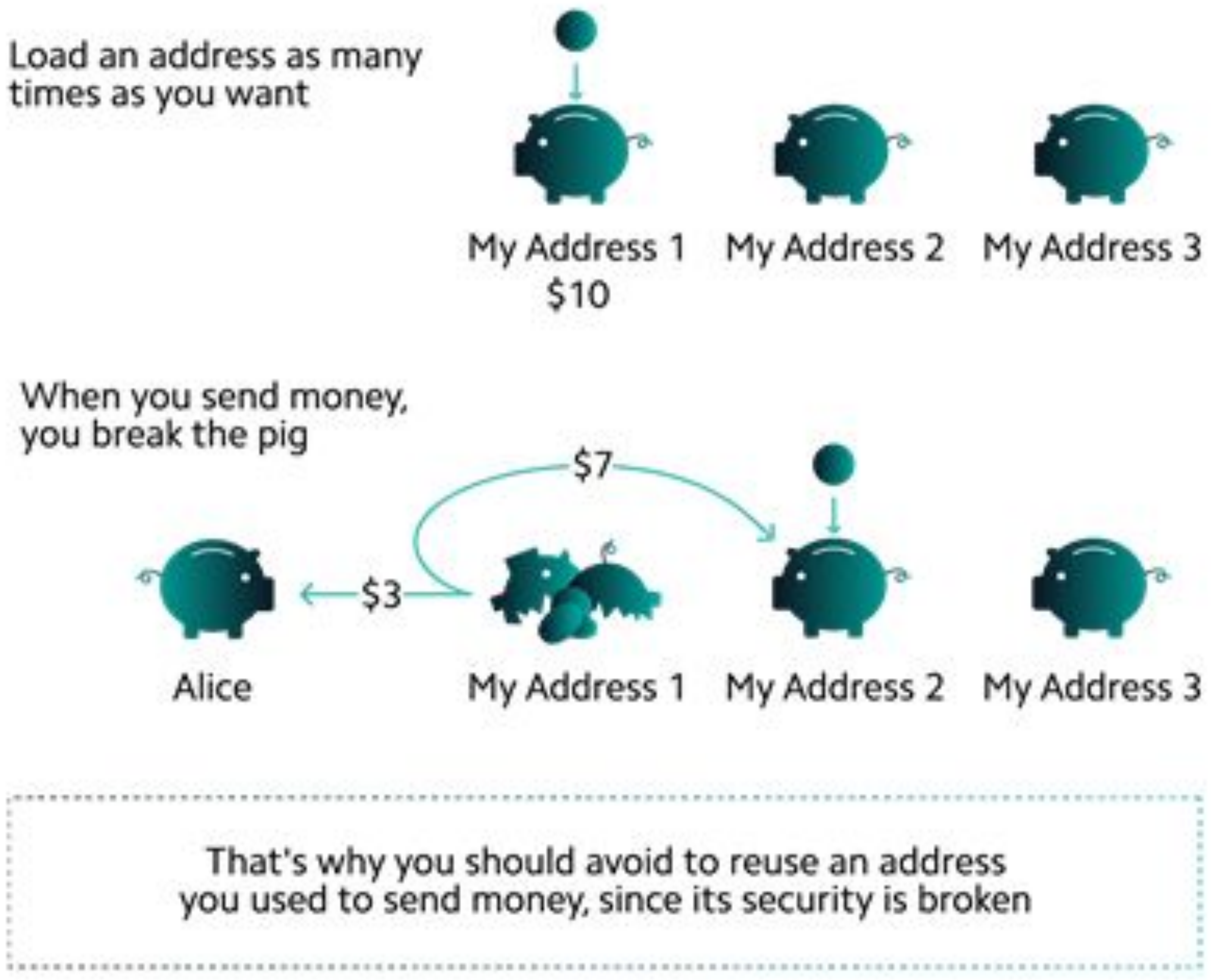
IOTA uses Trinary instead of Binary:

- Transaction and information transmitted through the network is sent in Trinary
- Client libraries allow for the conversion of data to & from Trytes.

Trytes are represented as the characters ‘A-Z + 9’

- Valid Tryte string: **BAKDHA9K**
- Invalid Tryte string: **BAjjsak82D**

Winternitz OTS



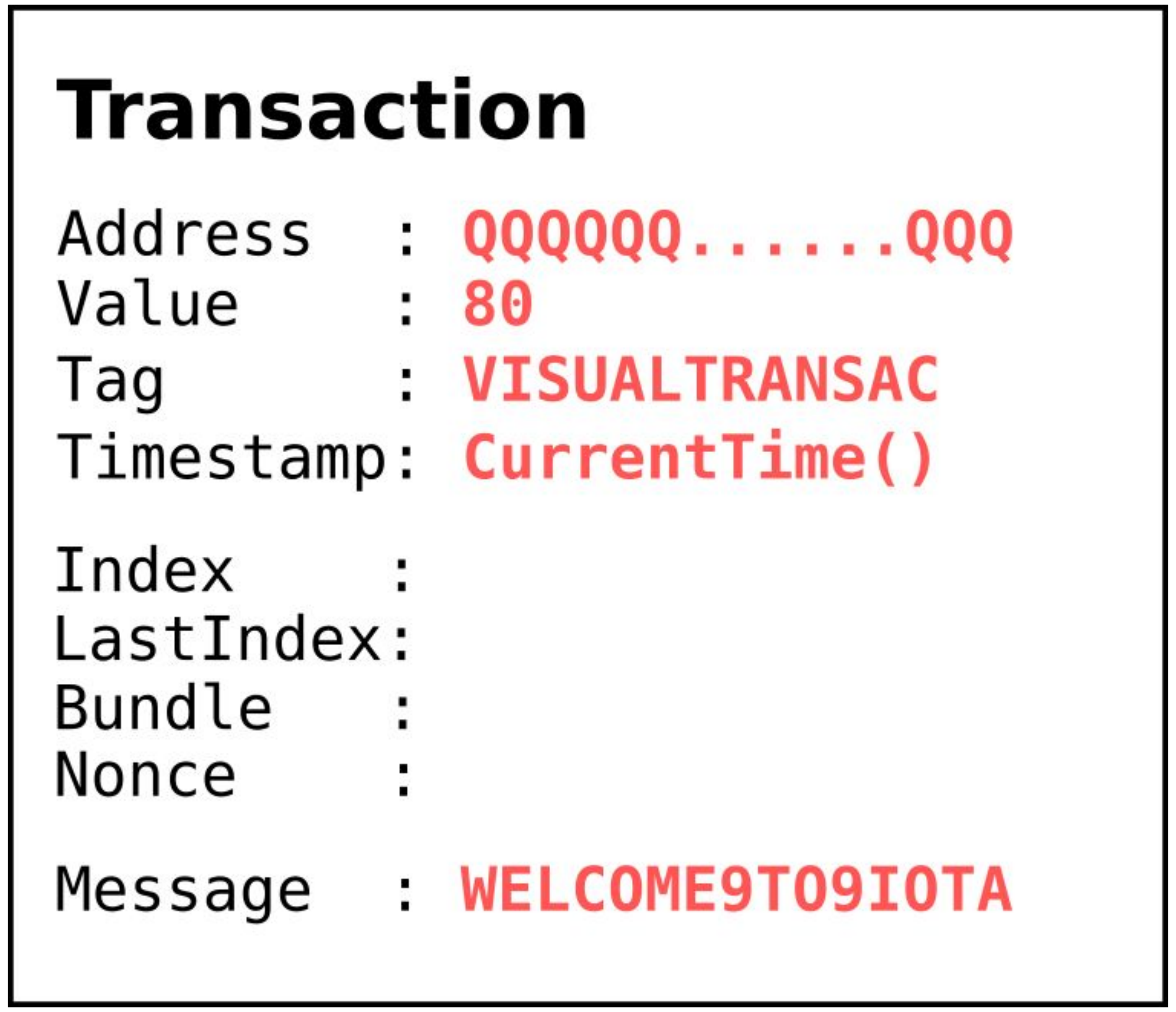
Load an address as many times as you want
My Address 1
$10
My Address 2
My Address 3
When you send money, you break the pig
$7
$3
Alice
My Address 1
My Address 2
My Address 3
That's why you should avoid to reuse an address you used to send money, since its security is broken

IOTA uses Winternetz One Time Signatures (**OTS**) which is a Hash-based signature scheme. This is used to authorise spending IOTA tokens from an address. This scheme was chosen due to its superior Quantum Resistance over ECC schemes.

As per the name: Signatures can only be used **once**

- Due to its one-time nature, the security of funds in an address decreases rapidly if you sign multiple transactions using the same key.
- IOTA you **never re-use an address** that has been spent from (as one signature has already been shared with the network).

Transaction Anatomy



Transaction

```
Address  : QQQQQQ......QQQ
Value    : 80
Tag      : VISUALTRANSAC
Timestamp: CurrentTime()

Index    :
LastIndex:
Bundle   :
Nonce    :

Message  : WELCOME9TO9IOTA
```

In order to send tokens or data on the IOTA ledger you must construct a valid transaction to attach to the Tangle.

Address: The relevant address for the operation the transaction is performing.

Value: Positive/Negative number of tokens to send

Message: 2187 Tryte field that can be filled with information.

Tag: 27 Tryte field that can be used to search for the transaction.

Other fields are computed internally.

Typical Bundle Construction

```
Transaction

Address  : QQQQQQ......QQQ
Value    : 80
Tag      : VISUALTRANSAC
Timestamp: CurrentTime()

Index    : 0
LastIndex: 4
Bundle   :
Nonce    :

Message  : WELCOME9TO9IOTA
```

Output

- Address directed to recipient
- Value is positive
- Message field is able to be used
- There can be **multiple outputs**

```
Transaction
```

```
Transaction

Address  : AAAAAA......AAA
Value    : -100
Tag      : VISUALTRANSAC
Timestamp: CurrentTime()

Index    : 1
LastIndex: 4
Bundle   :
Nonce    :

Message  :
```

Input

- Address is where the tokens are taken from
- Value is negative and equal to total balance
- Message field is taken up by **Signature**
- There can be **multiple inputs**

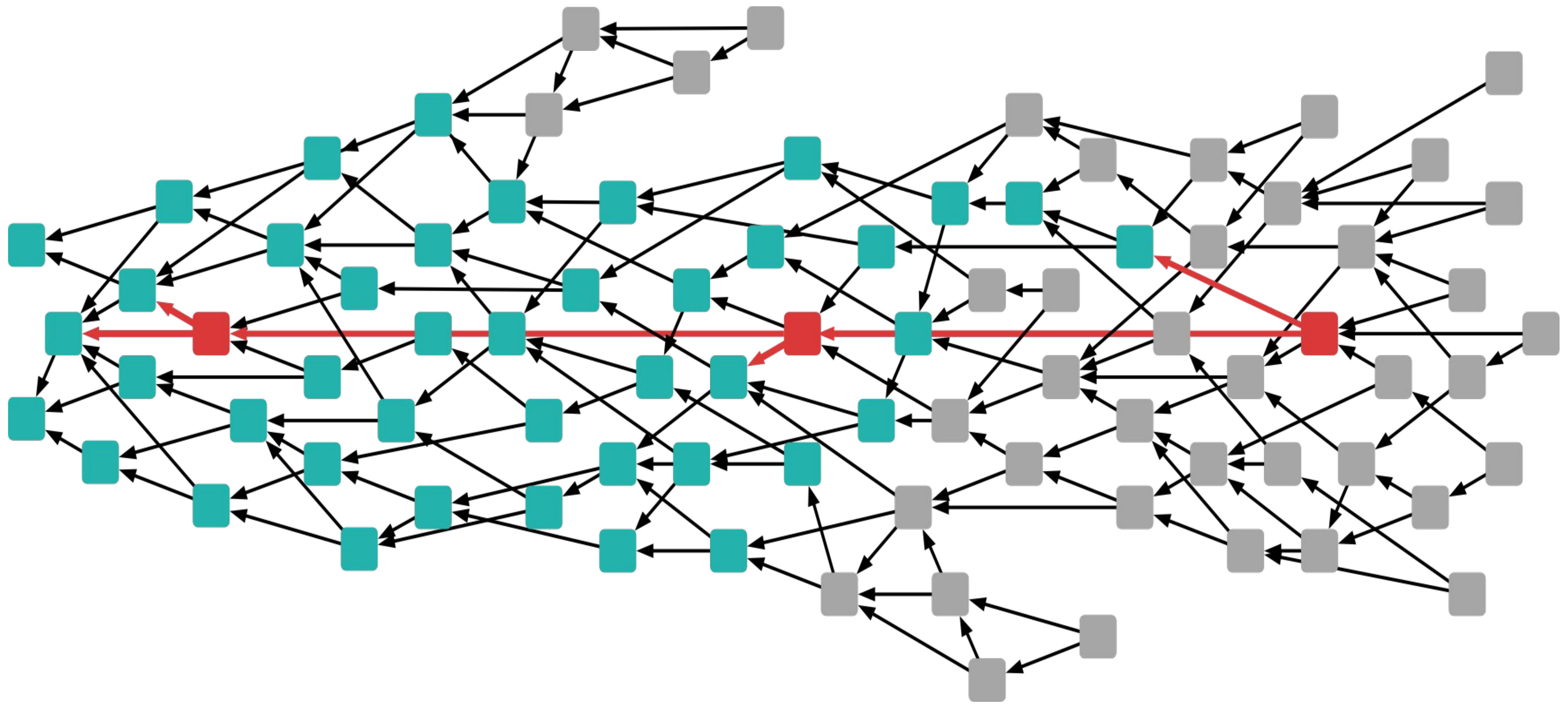
Note: There are two transactions above due to the imaginary address having a security level of 2.

```
Transaction

Address  : EEEEEE......EEE
Value    : 20
Tag      : VISUALTRANSAC
Timestamp: CurrentTime()

Index    : 4
LastIndex: 4
Bundle   :
Nonce    :

Message  :
```

Remainder

- Address directed to Seed controlled address
- Value is equal to '**Input - Output**'
- This is usually generated by the client software.
- If no remainder is found, this transaction wont be created.

Coordinator & Consensus



In the current IOTA Mainnet there is a service running call the **Coordinator (COO)**. The COO helps protect the network from 51% Double Spend attacks.

The COO achieves this by publishing transactions with its signature, these transaction are call Milestones. Other clients see this signature and count the transactions indirectly referenced by it as confirmed.

The COO is needed in the beginning stages of any Tangle network when there is a comparatively small amount of hashpower on the network.

It is the intention that the Coordinator is removed in the future. We are actively researching the implications and timing of this event. We call it 'Coordicide'

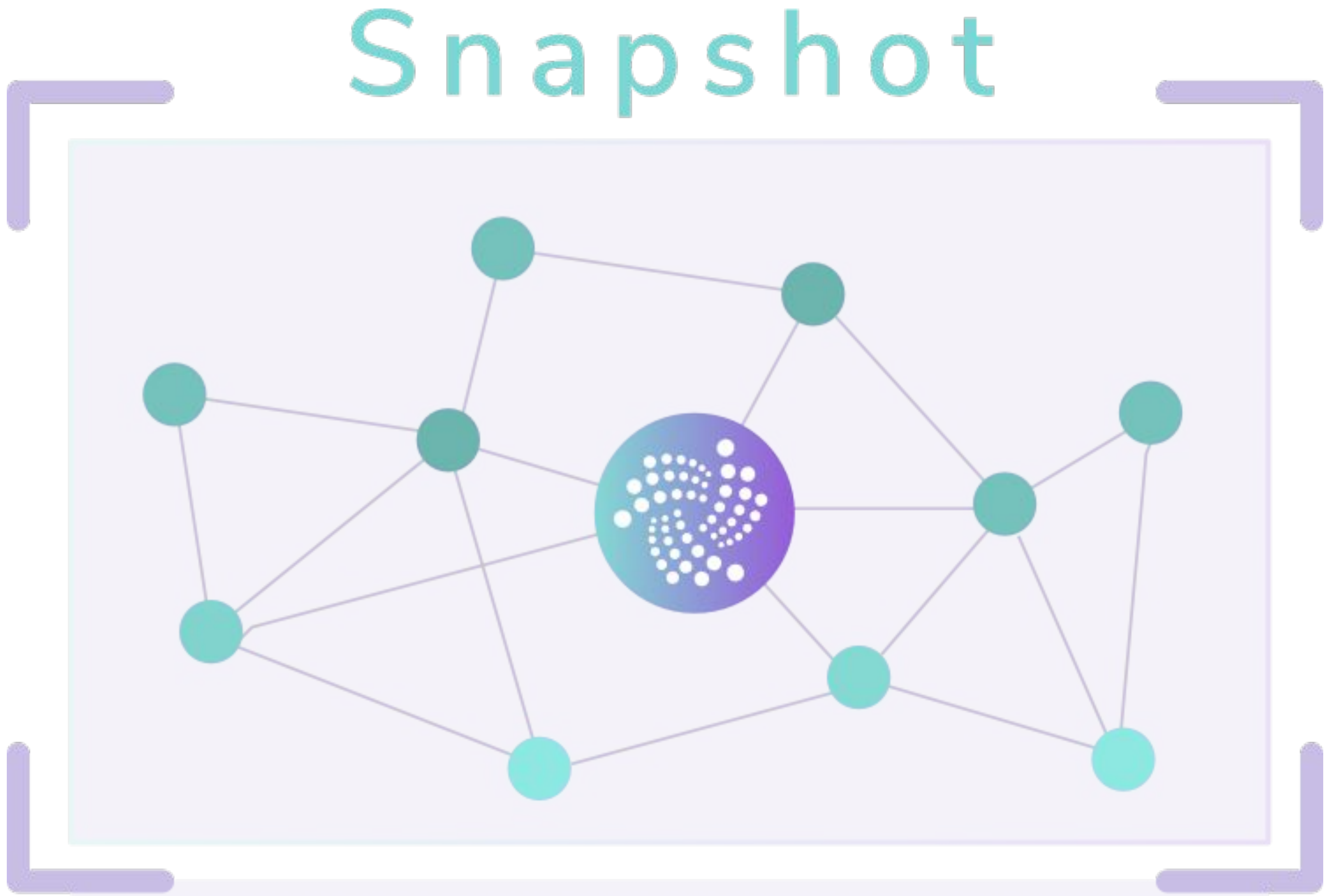
Transaction Lifecycle

	Proof of Work Blockchain	IOTA
LOCAL	Create Transaction	Create Transaction
	Sign transaction	Sign transaction
	Send transaction to a node	Send transaction to a node
NETWORK		Select TWO network tips
	Tx get propagated amongst nodes	Solve PoW for the TWO tips
	Mining pool picks up Tx (if fee is high enough)	**Tx get propagated amongst nodes**
	Miner solves the block and broadcast	Other transactions select Tx as tip.
ADAPTATION	Wait for 6 confirmations	Wait for milestone to reference Tx (IOTA with the coordinator)
	Confirmed	Confirmed

IOTA FOUNDATION

IOTA and IoT

Snapshots



‘Pruning of the ledger’

From Global

1. Synchronous
2. Consensus need to be achieved
3. Switch is not automatic

to Local Snapshots

4. Permanodes

Permanodes

Do not take part to Local Snapshots

Store the entire Tangle history

Useful for auditing purpose

Make it available for an incentive

Benefits vs risks

A. Cost and freedom vs trust

Step 3: 2nd Layer

MASKED AUTHENTICATED MESSAGING

FLASH CHANNELS

The base IOTA protocol was build to be as flexible and minimal as possible to enable developers to create a number of different **2nd Layer** technologies that augment and extend the functionality of IOTA.

These 2nd Layer solutions can take many forms and have different focuses. Two examples of libraries which do this are **Masked Authenticated Messaging** & **Flash Channels**. Both of these libraries utilise the IOTA protocol in interesting ways to extend the capabilities of the network.

These 2nd Layer libraries do not require protocol changes or hardforks, they can be built and supported by anyone to ensure that IOTA fits their needs.

Encrypted Messaging Streams

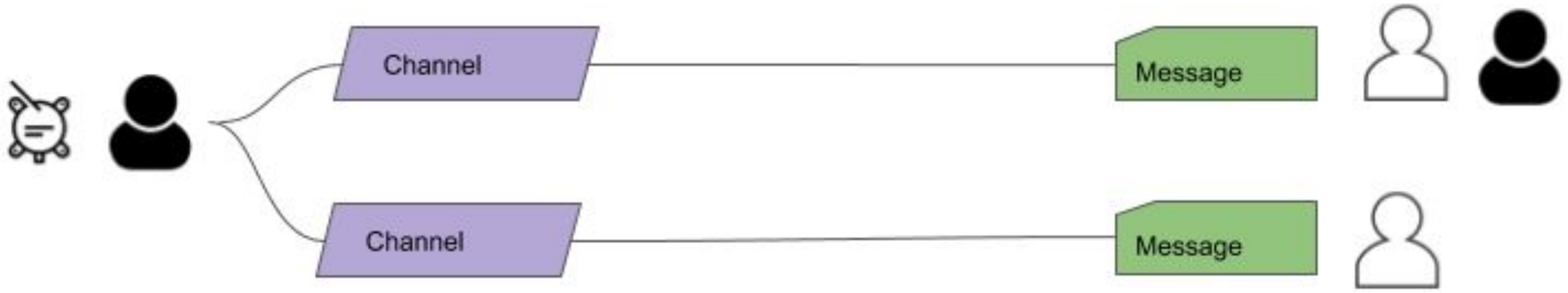
Emit and access a forward-secret and encrypted data stream over the Tangle.

Masked Authenticated Messaging

Masked Authenticated Messaging (MAM) allow for public or encrypted messaging streams to be published to the Tangle.

These streams can be read back by anyone who has access to the Ledger, and anyone who has the encryption key. These message streams are signed so you are also able to attest to the authenticity of the data.

Current MAM is written in **RUST** with bindings for **Javascript** and **Java**.



Offline State Channels

Flash Channels enable off-tangle token transactions in a safe environment.

Perfect for token streaming application such as EV Charging or Video Streaming.

Flash Channels

Flash Channels are a protocol centered around a multisignature wallet and key reuse. Flash lets two or more participants open a state channel, commit funds into it and then sign bundles back and forth transferring value instantaneously off Tangle.

Once the channel is opened you are able to communicate the transfers through any medium.

Currently the implementation of the Flash Channel protocol is in **Javascript**.