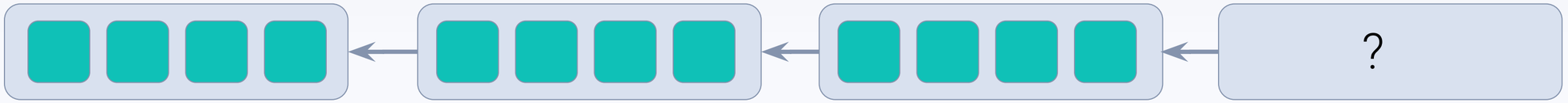
4th Scientific School on Blockchain & DLTs

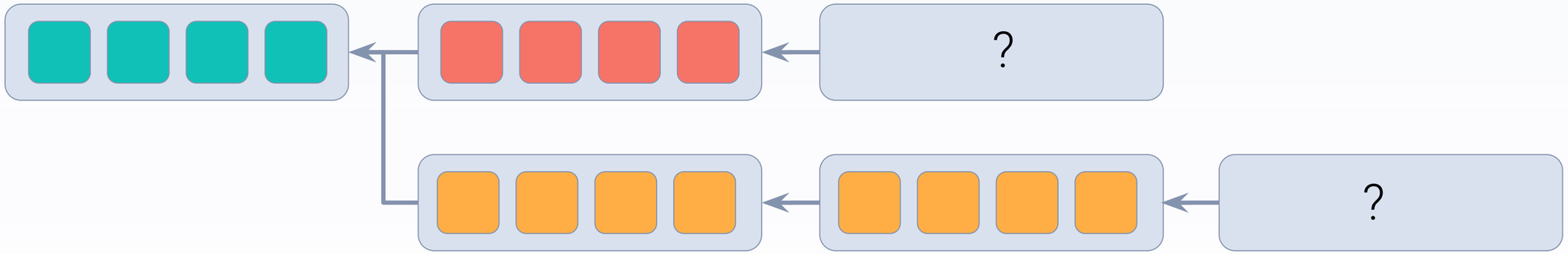
Introduction to IOTA

Can Umut Ileri
Research Scientist
IOTA Foundation

Comparison to Blockchains



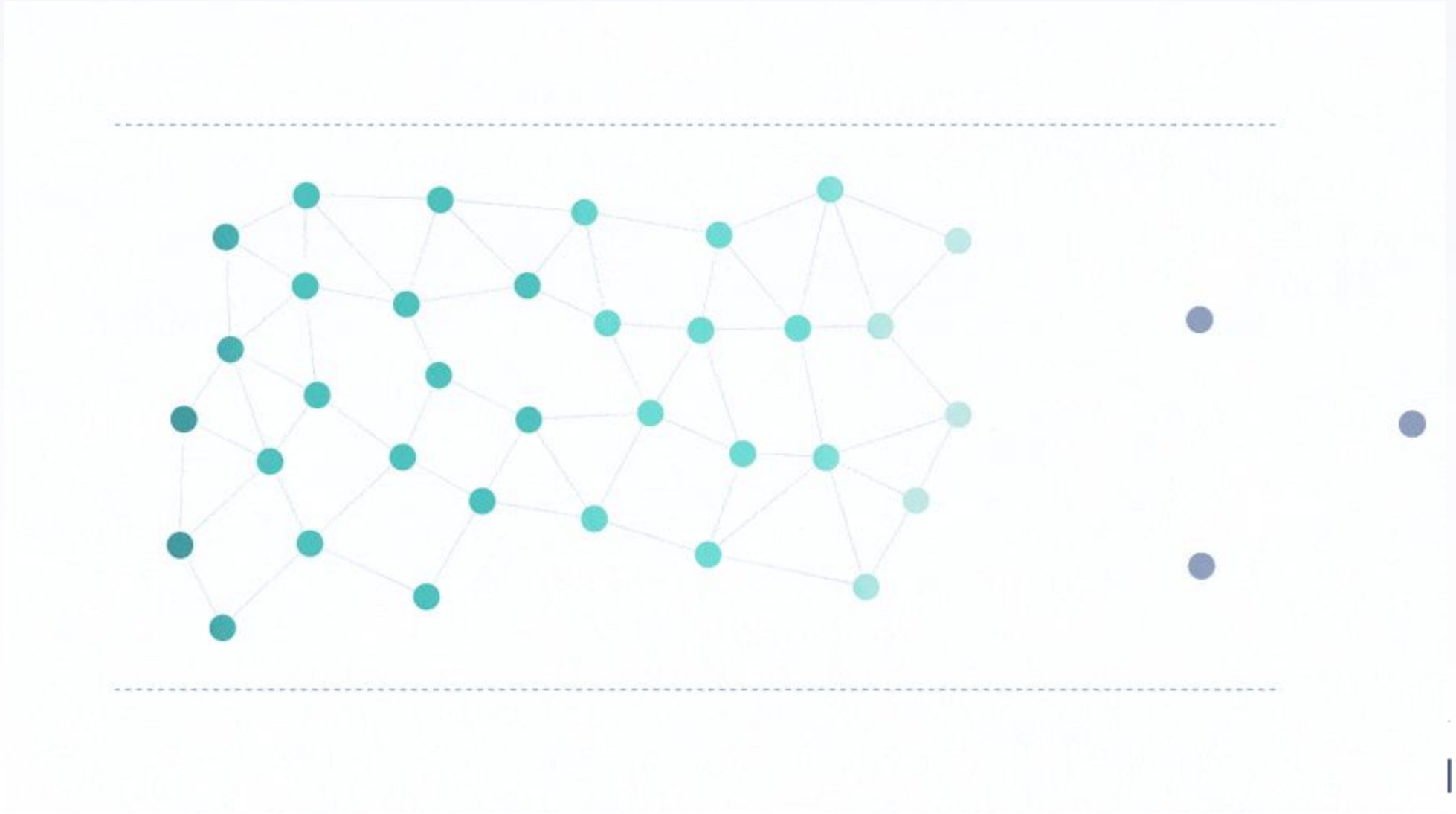
Block creation some node is *elected/chosen* to add new block (PoW puzzle, PoS,...)



Tip Selection blockchain is a DAG (network latency, attacker, ...): new block produced has to choose a *tip*. For example, PoW chooses longest chain; PoS may continue on all *branches*.

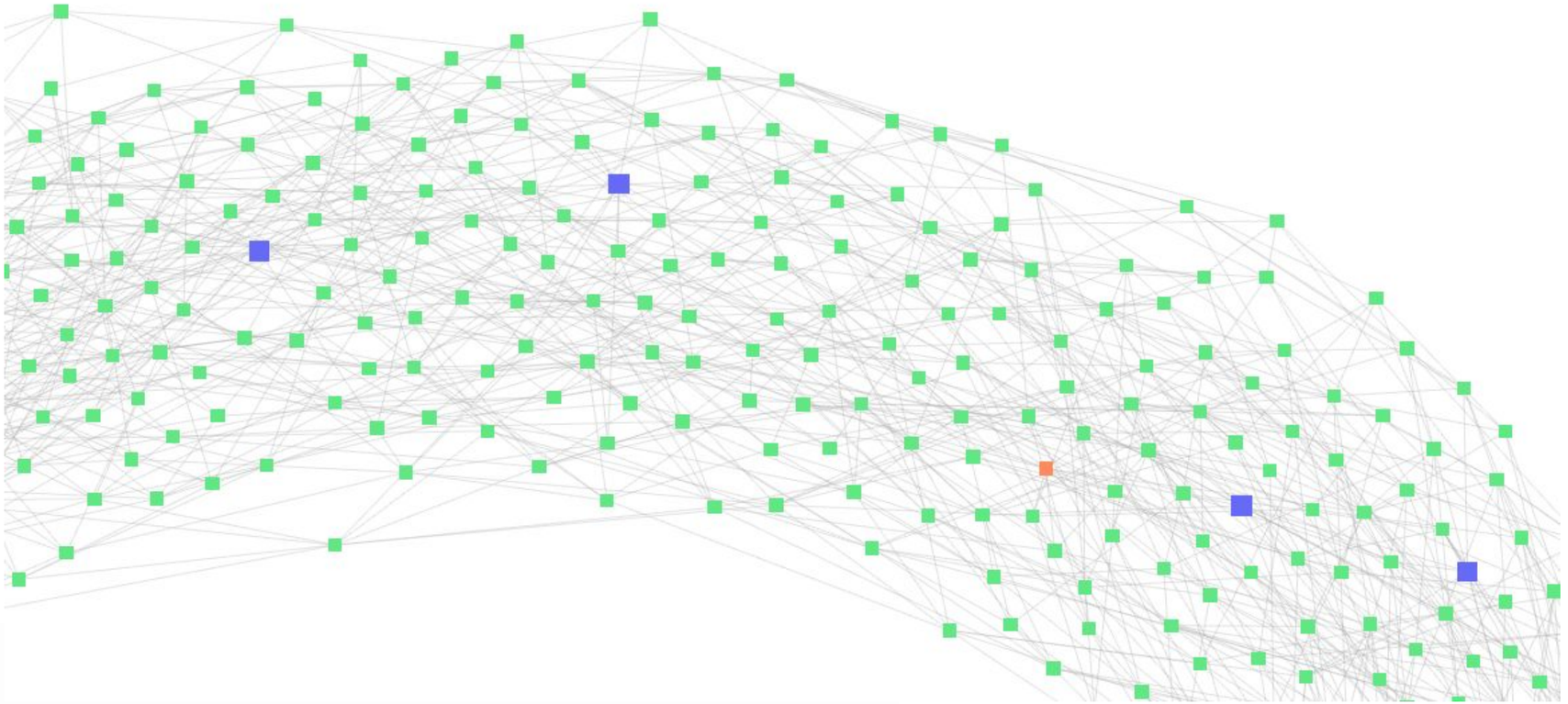
IOTA

The Tangle



IOTA

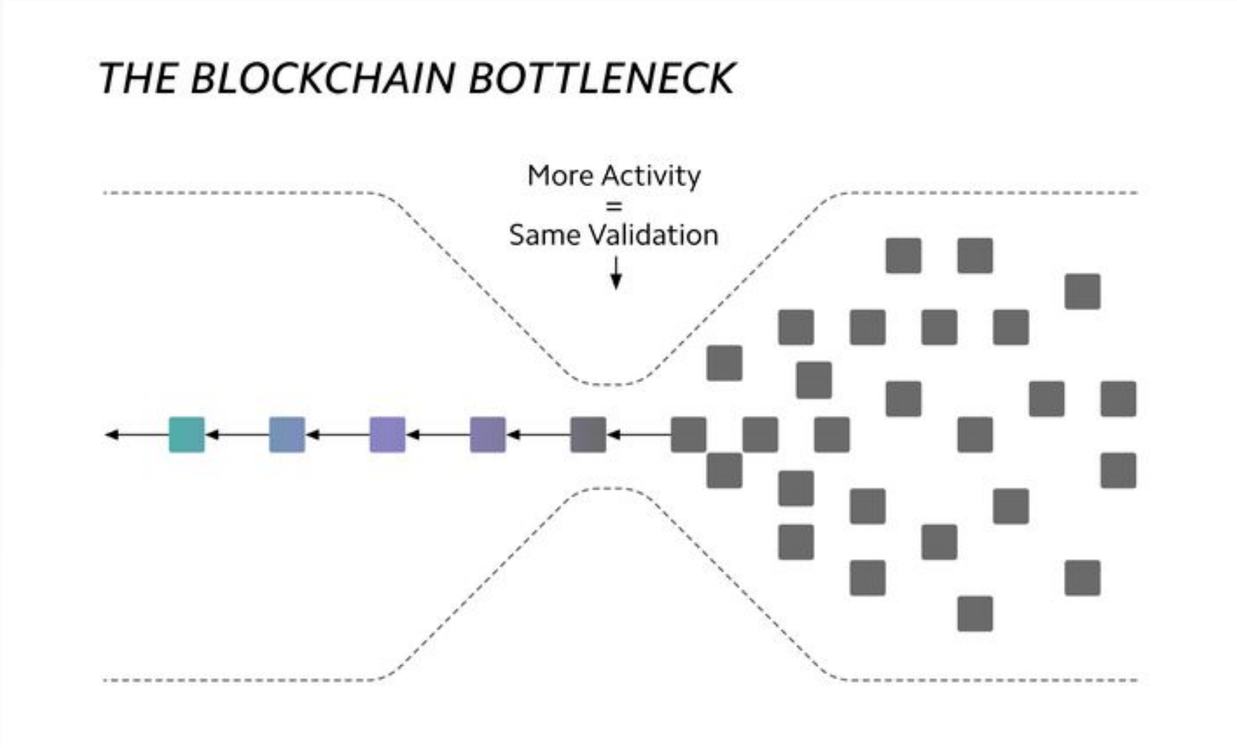
Tangle Explorer

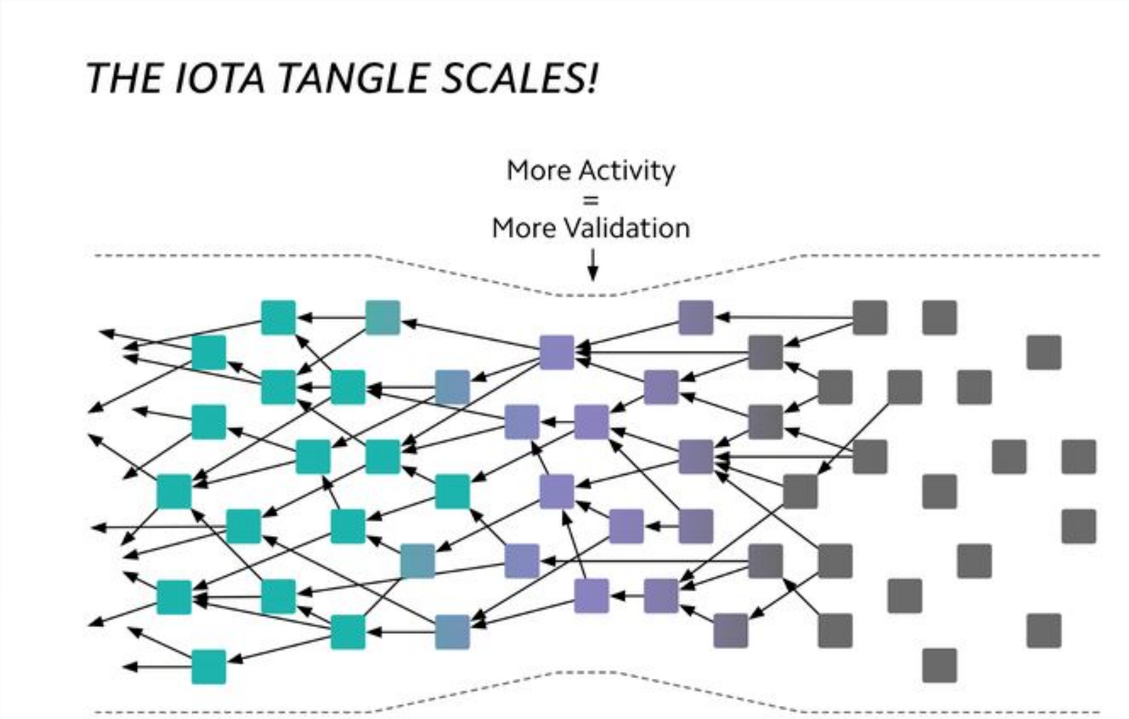


https://explorer.iota.org/mainnet/visualizer/

IOTA

Why DAG?


THE BLOCKCHAIN BOTTLENECK
More Activity
=
Same Validation


THE IOTA TANGLE SCALES!
More Activity
=
More Validation

IOTA

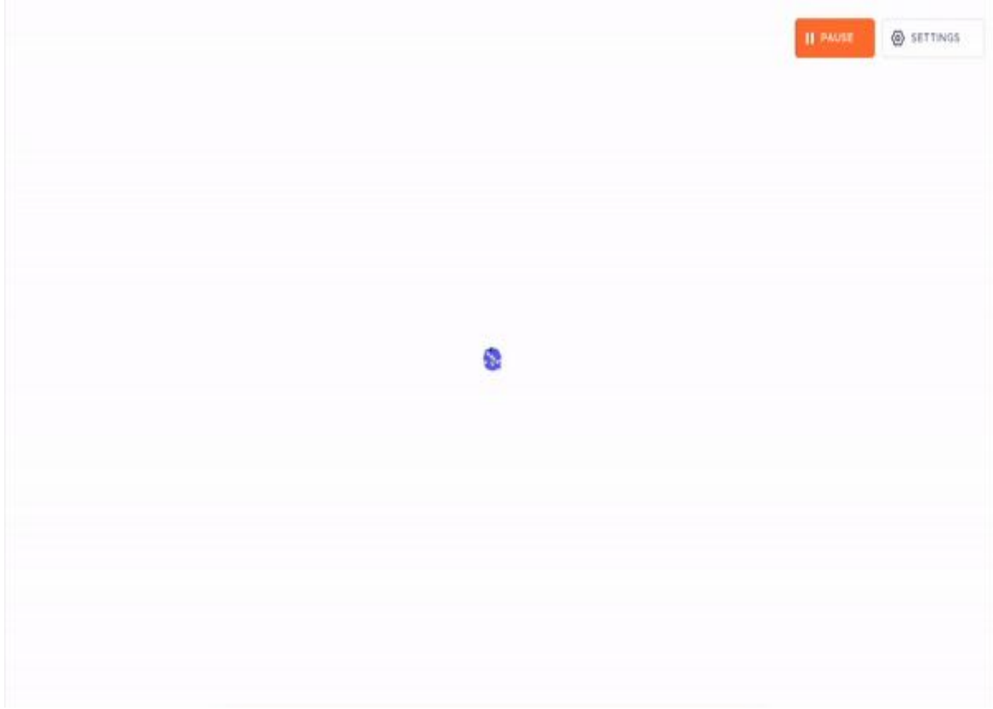
Challenges of the Tangle

Non-linearity only partial ordering

Asynchronous / Local Tangles there is no such thing as *THE Tangle*

Finality find practicable and secure rule for fast confirmation

Sybil protection



Realities ledger state

Managing the Tangle

Blocks - vertices of the Tangle

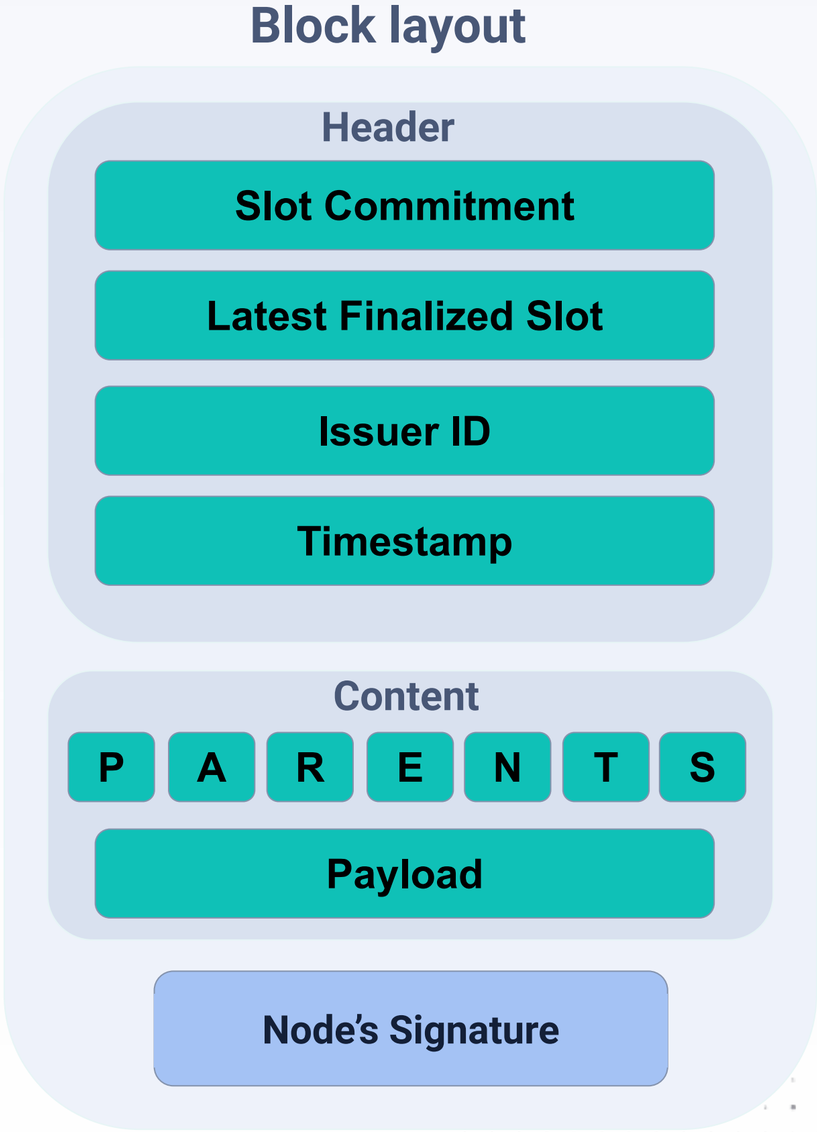
Parents reference some previous blocks, constitute the edges of the Tangle

Issuer ID identifies the node that issued the block

Timestamp records issuing time of block, has to be higher than the one of the parents

Payload contains the actual content of the block

Signature proves that Issuer issued the above elements



IOTA

UTXO - value transfer

UTXO

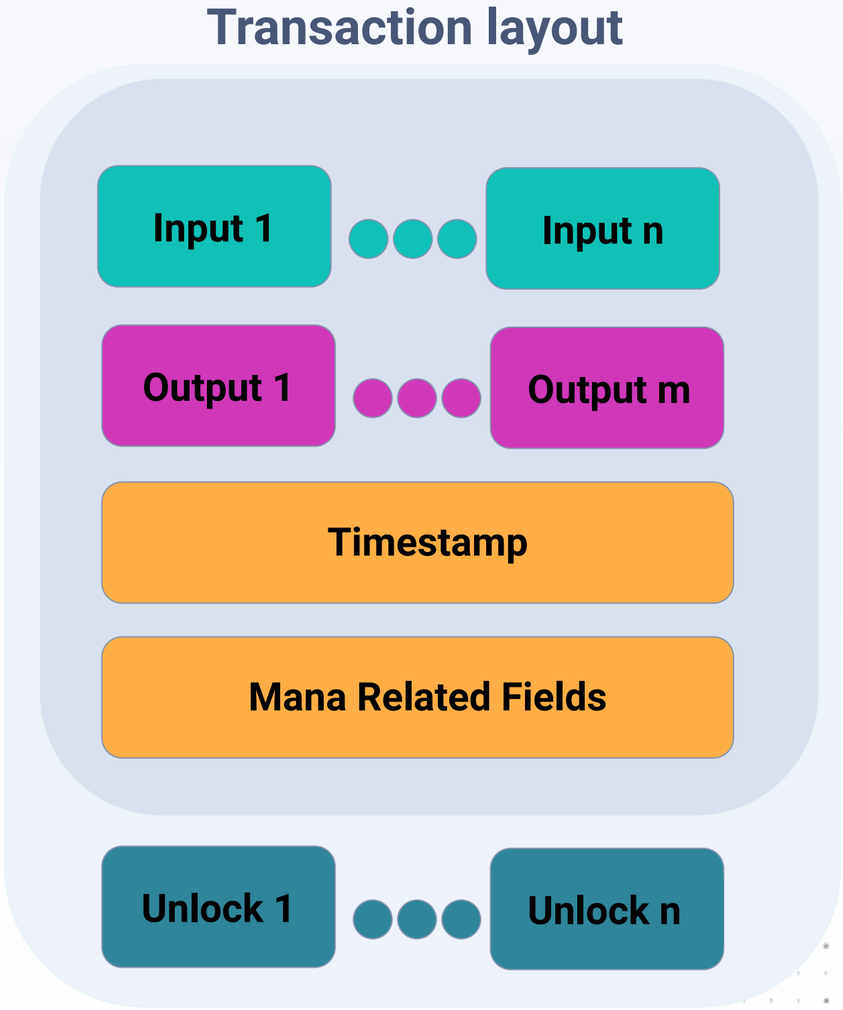
UTXO (unspent transaction output) can be spent once. Total balance of Inputs must equals total balance of outputs.

Inputs referencing unspent outputs to collect funds, contains also input types

Outputs creating new outputs, contains also output types

Timestamp issuing time of transaction; must be higher than the one of *transporting* block

Unlocking signatures for each Input

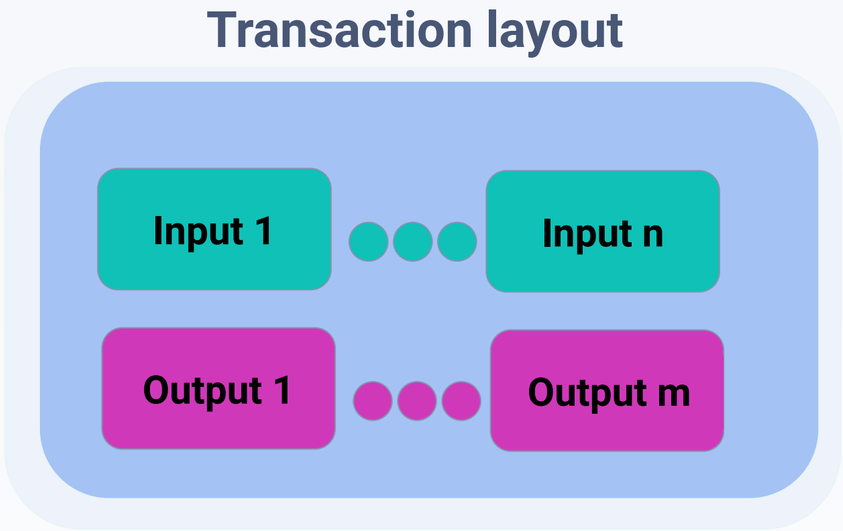


IOTA

UTXO - value transfer

UTXO

UTXO (unspent transaction output) can be spent once. Total balance of Inputs must equals total balance of outputs.

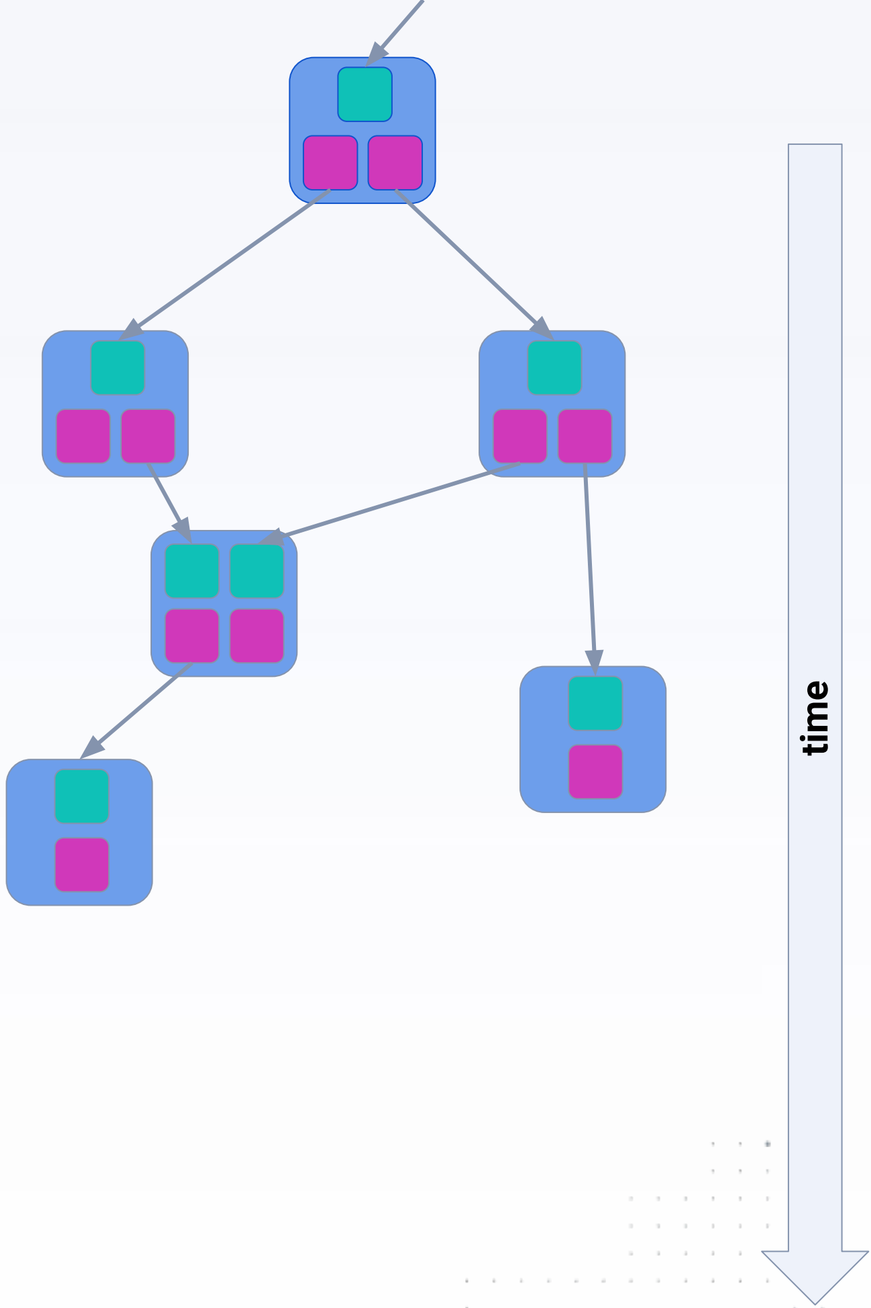


IOTA

UTXO DAG

UTXO (unspent transaction output) can be

1) spent once
2) merged
3) split



No conflict

=

UTXO has at most **one child edge**

IOTA

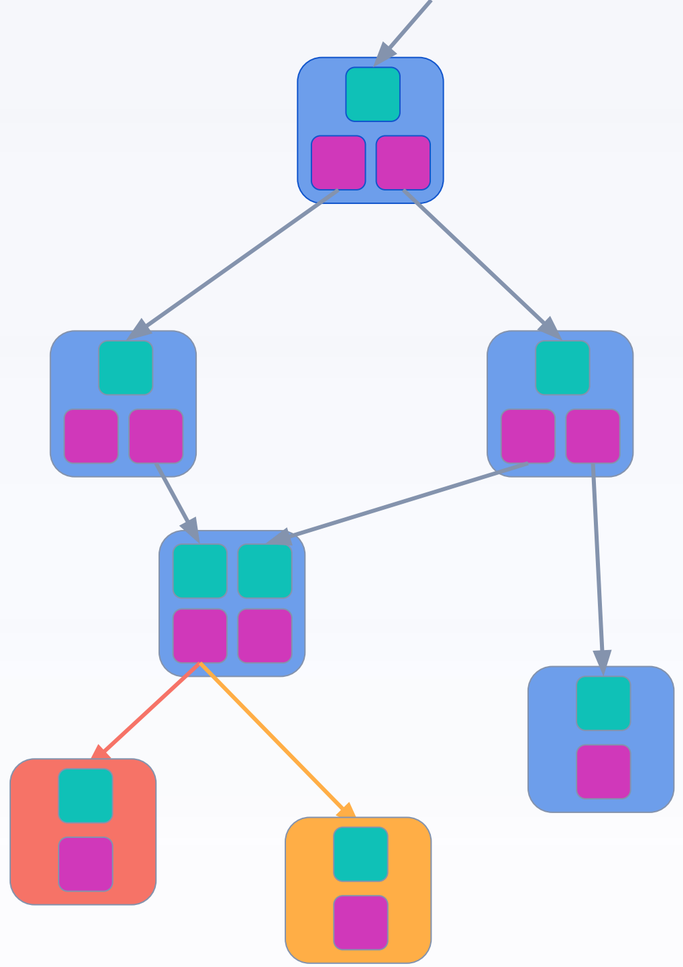
UTXO DAG

UTXO (unspent transaction output) can be

1) spent once
2) merged
3) split

Double spend output spent multiple times

Conflict
=
UTXO has **more** than **one child edge**

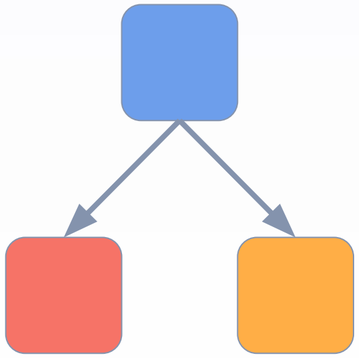


Branch DAG

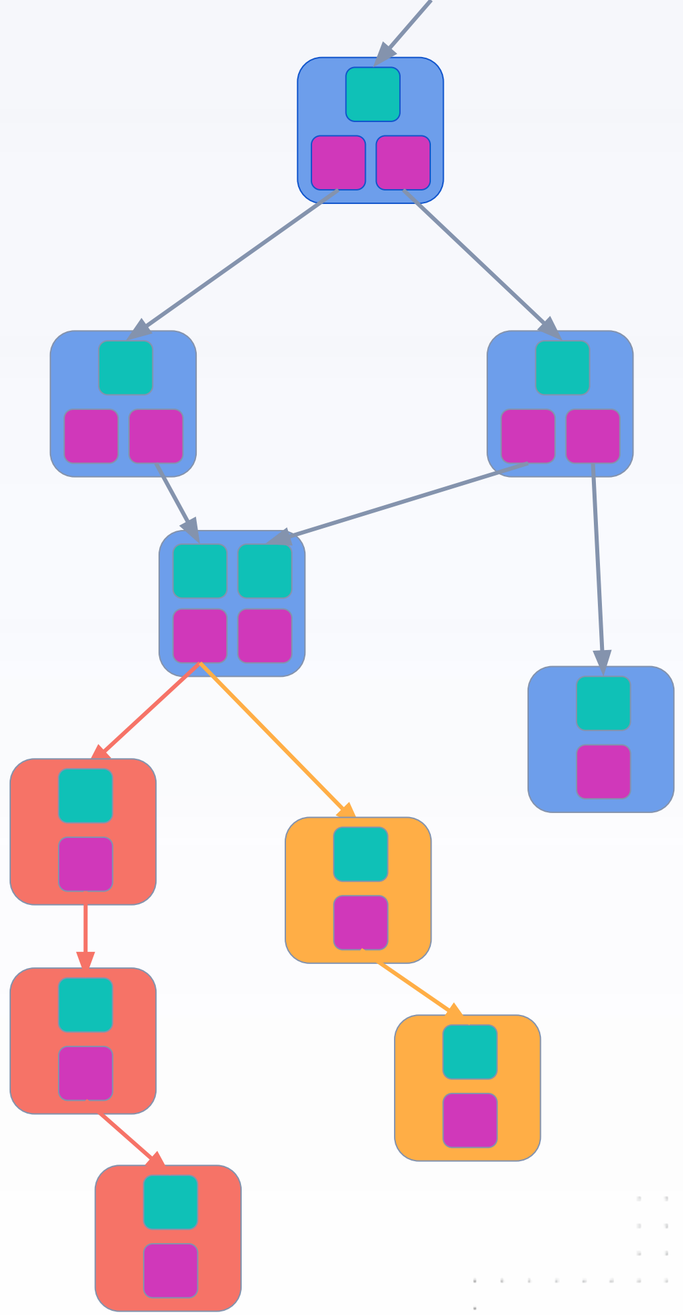
Double spend output spent multiple times

Conflict set double spending transactions get an entry in a conflict set

Branch a transaction that is in a conflict set is linked to a branch



Branch DAG



UTXO DAG

IOTA

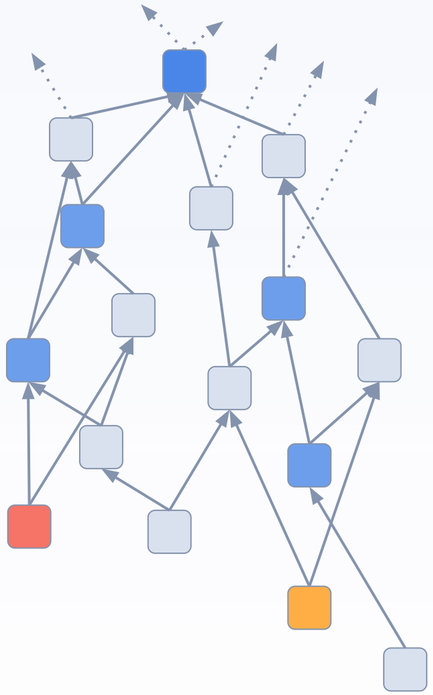
Tangle DAG

UTXO DAG

Branch DAG

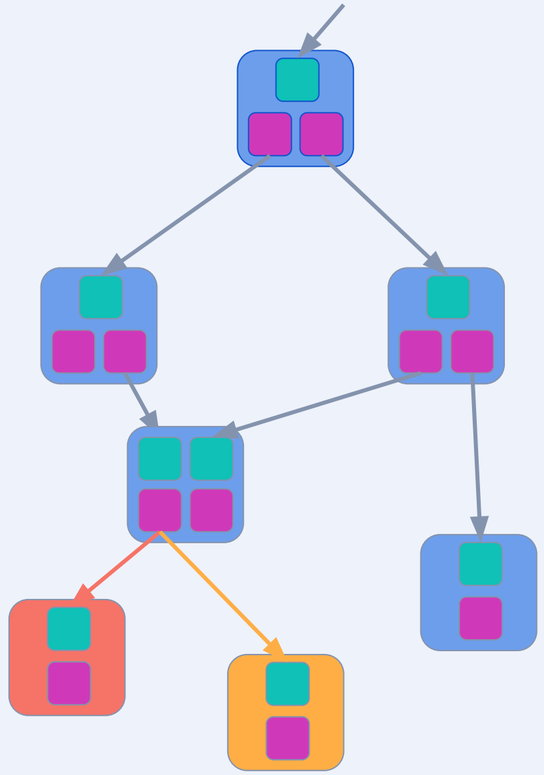
time

Blocks



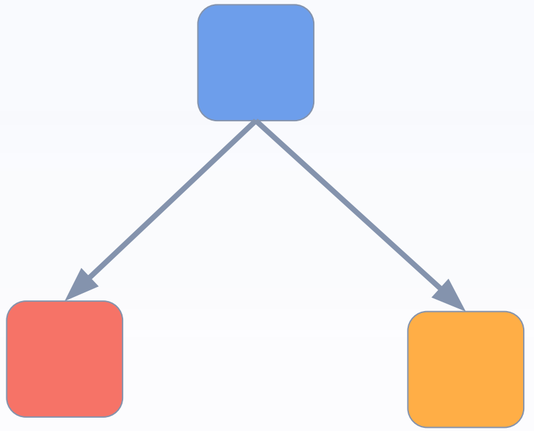
Data structure
Virtual votes propagation

Transactions



History of value transfers

Possible outcomes



History of conflicts

IOTA

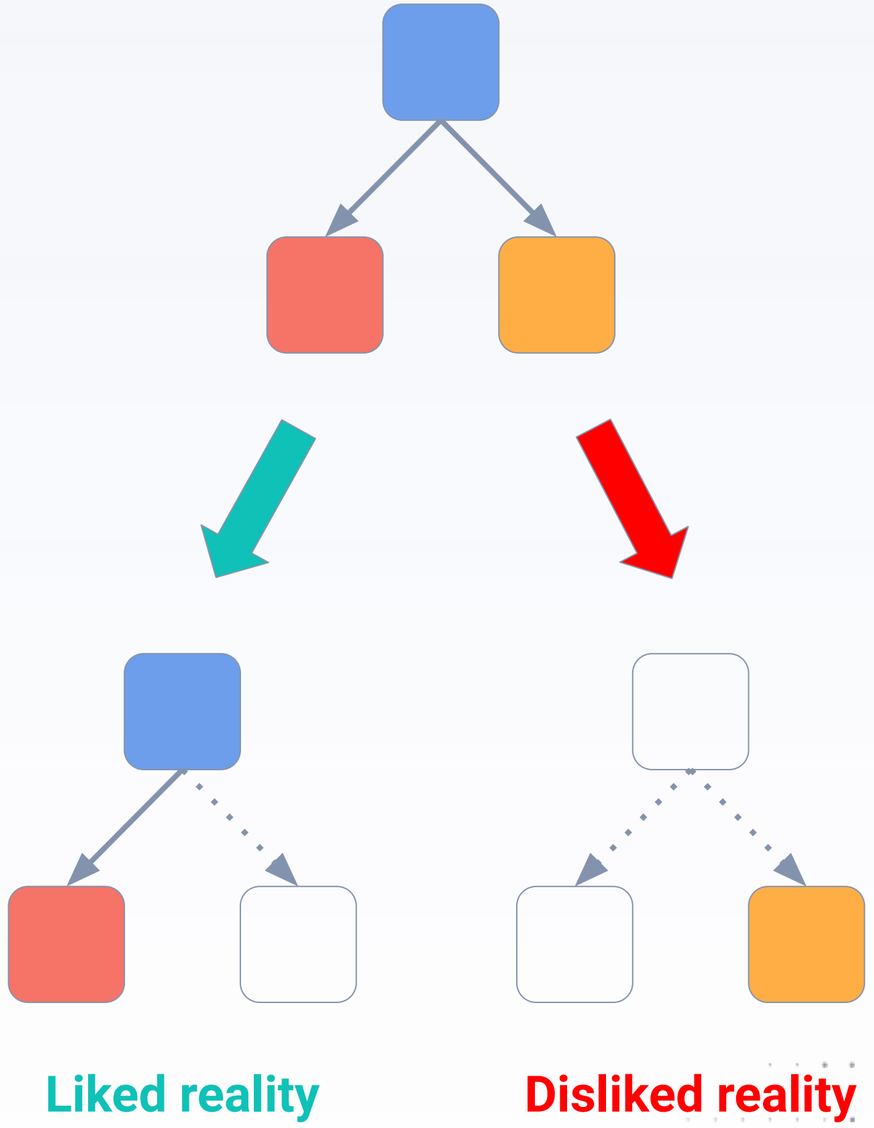
Branches and Realities

Liked branch a winning branch

Disliked branch a losing branch

Liked reality collection of non-conflicting liked branches

Disliked reality collection of disliked branches



Branch DAG

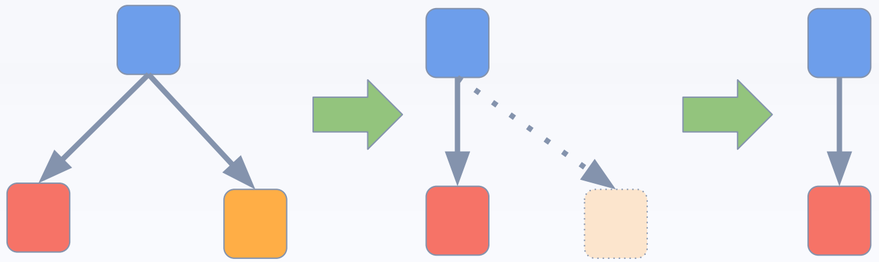
IOTA

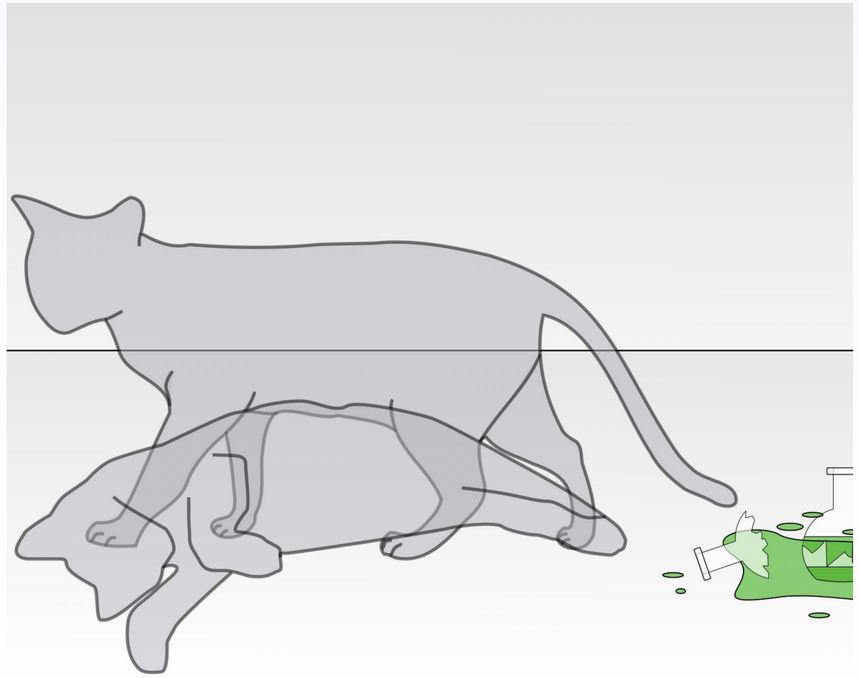
Collapse of Realities

Branch DAG superpositions give an intuition about what happens on the Branch DAG

UTXO DAG not affected

Tangle DAG some messages and transaction need to be picked up to guarantee liveness





IOTA

Availability - Finality

What does a user expect from a distributed ledger?

1.

Assurance that the submitted data will eventually find a place on the ledger

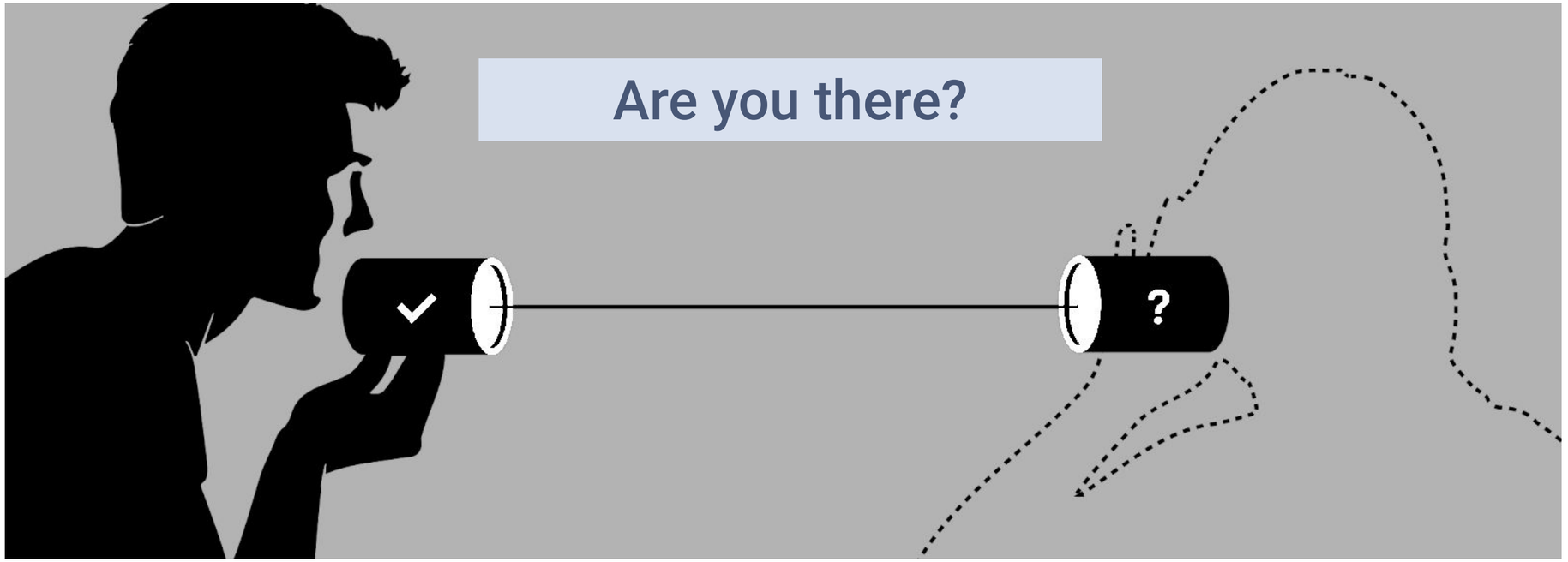
2.

Assurance that, once included, the fate of your data will be definitively determined.

No distributed ledger can simultaneously satisfy both expectations.

IOTA

Unreliability of Networks



IOTA

Ensuring finality: Voting-based consensus protocols

Assumptions:

- Each node participating in the consensus protocol has knowledge of the total number of nodes in the protocol.
- There is an upper bound on the number of adversarial nodes, which is known to all participants. (Note: It has been theoretically proven that consensus is not achievable when more than one-third of the nodes are adversarial .)

Ensuring availability: Proof-based consensus protocols

- Nakamoto consensus: inception of the blockchain revolution.
- Participants don’t have to know how many miners exist in the network.
- Protocol continues even if there is only one miner.
- Longest chain wins.

ethereum

PoW

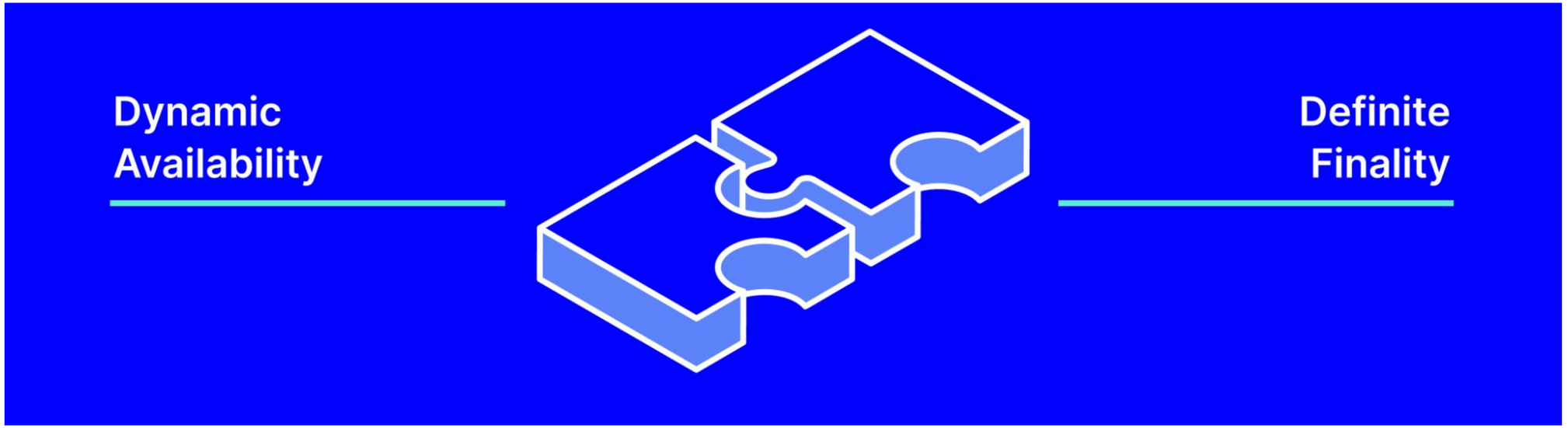
How can you be sure whether what you know is the longest?

Probabilistic Finality

A transaction in a Bitcoin block that is six rounds older than the newest block may be successfully reverted with a probability between 0.11% and 0.16% by an adversary controlling 10% of the mining power.

Gaži, Ren, and Russell. Practical Settlement Bounds for Proof-of-Work Blockchains (2022)

Flexible Consensus: Picking The Best of Both Worlds



IOTA

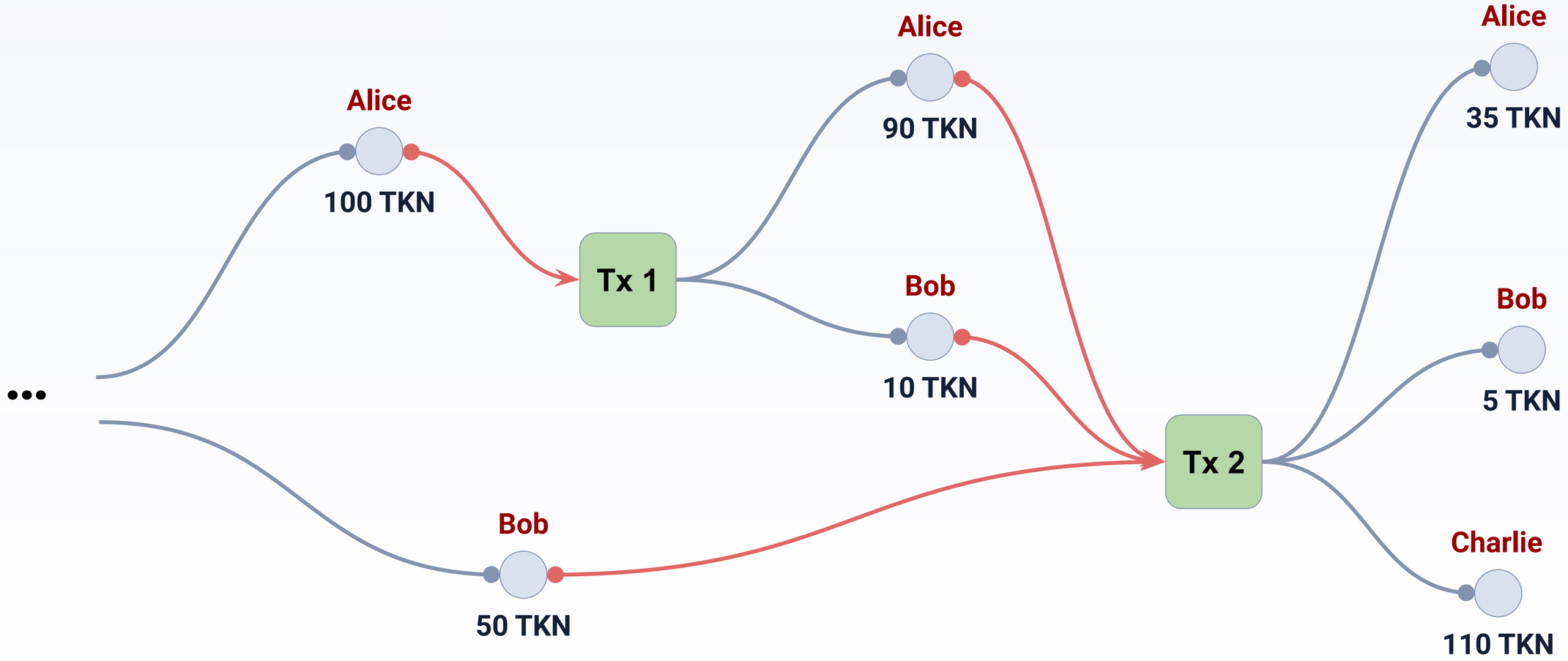
Level of Safety and Caution

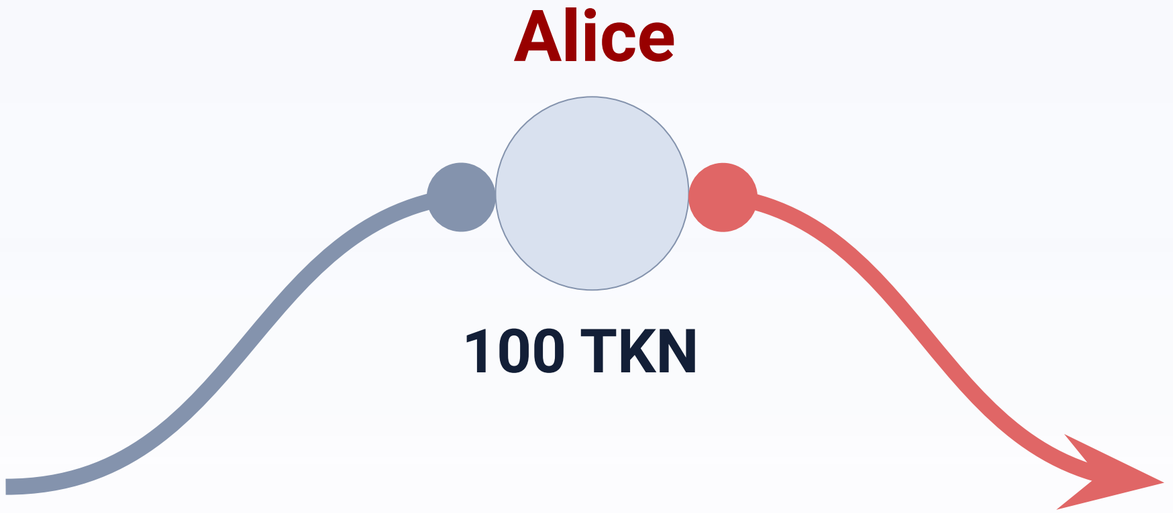
IOTA

Revisiting the Tangle Explorer

https://explorer.iota.org/mainnet/visualizer/

Programmability

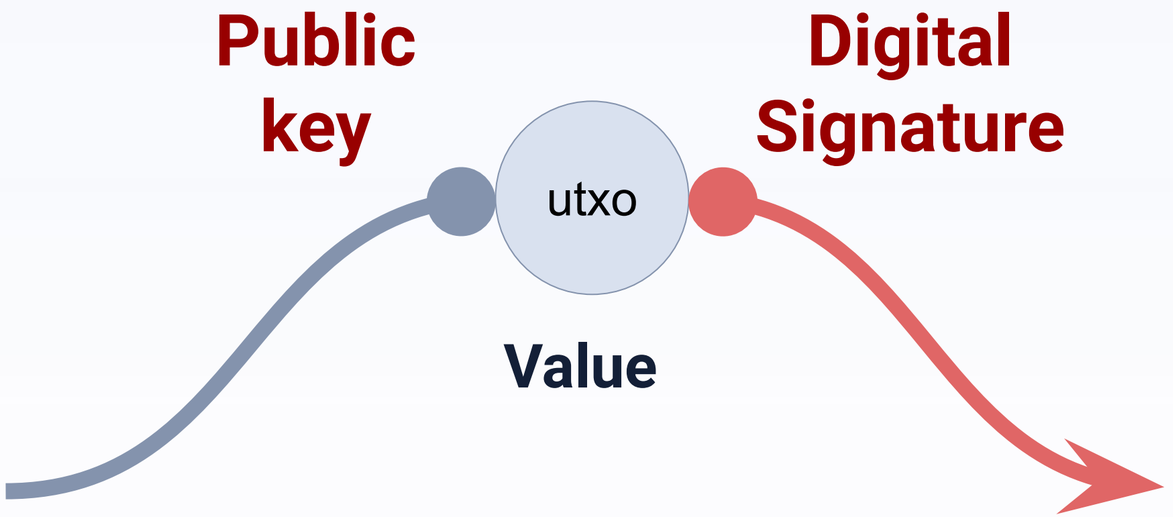

Alice
100 TKN
Tx 1
Alice
90 TKN
Bob
10 TKN
Bob
50 TKN
Tx 2
Alice
35 TKN
Bob
5 TKN
Charlie
110 TKN



Can only be spent if Alice permits

IOTA

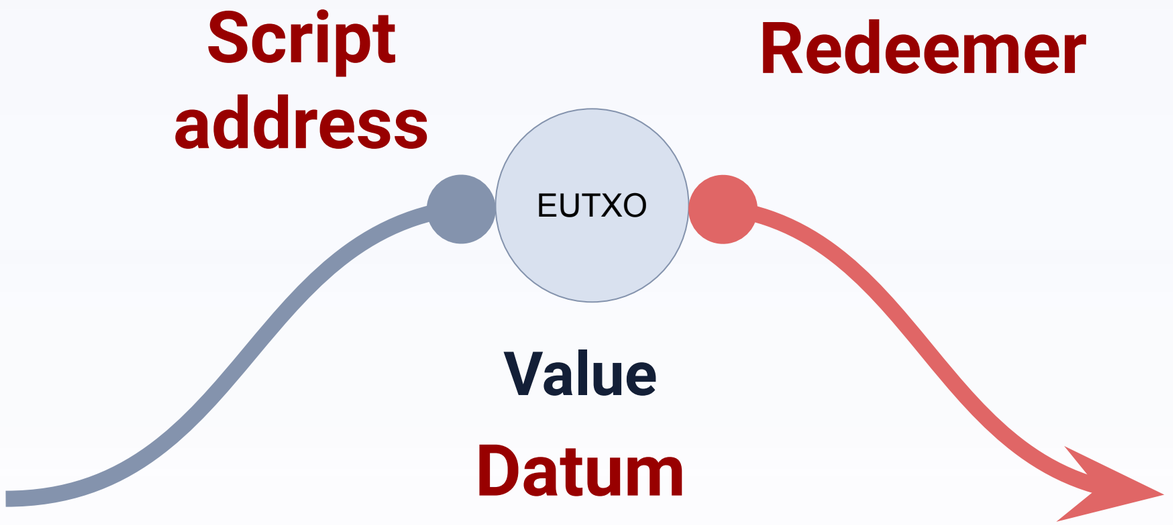
Basic UTxO



Extended UTxO

Script Address = Hash(Binary Output (Plutus SC))

User specific arguments



- Arbitrary user data
- Can be used as a **local script state**
- Using its full potential is up to developers
- Only hash of the datum is provided by the locker

validator(Datum, Redeemer, ScriptContext) → {True, False}

validator(LockerInput, UnlockerInput, ScriptContext) → {True, False}

IOTA

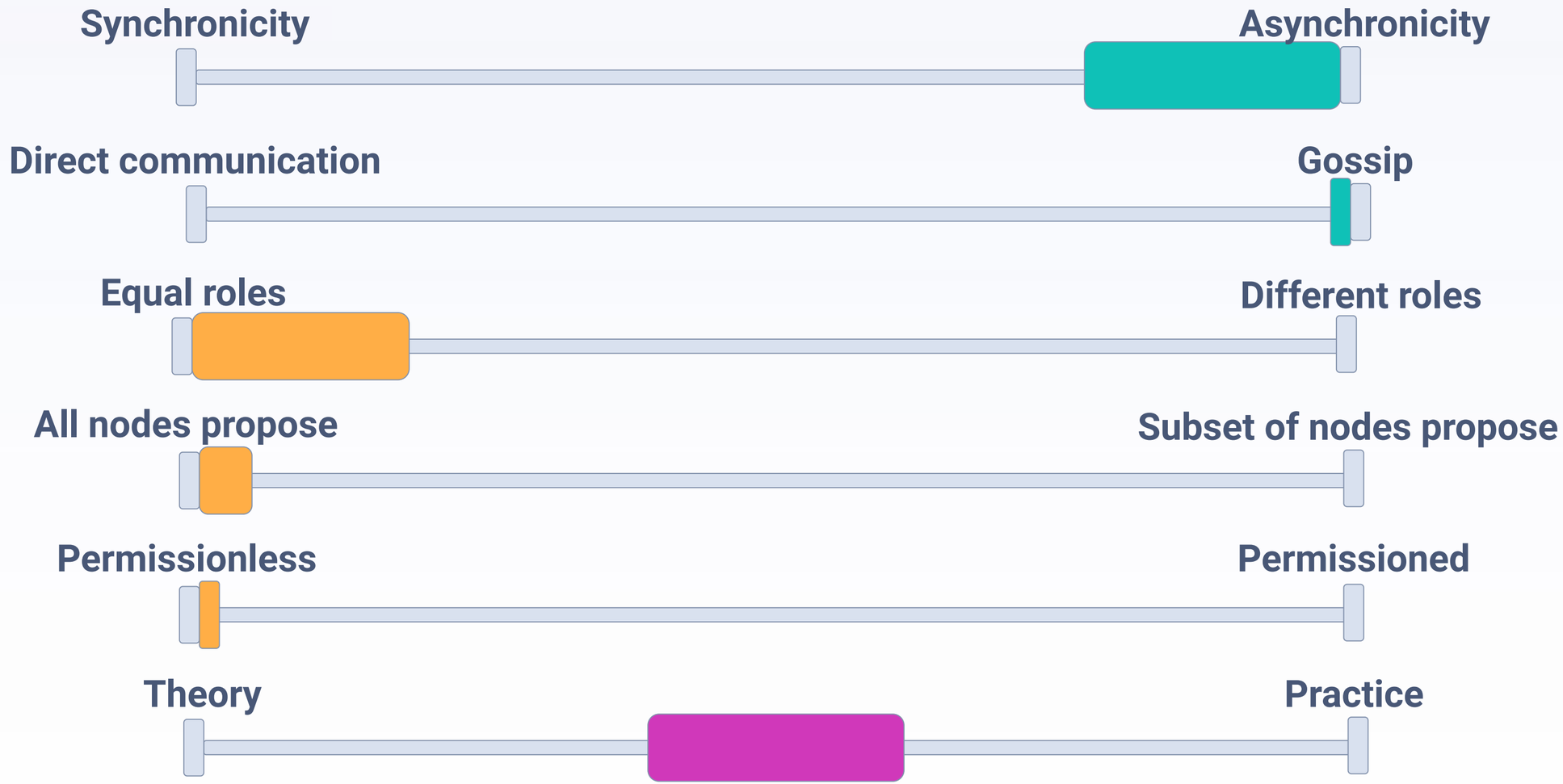
IOTA L2 Smart Contracts

- A platform that brings scalable and flexible smart contracts into the IOTA ecosystem. It
- Allows anyone to spin up a smart contract blockchain and **anchor** it to the IOTA Tangle.
- Supports EVM and WASM (Experimental)

IOTA

Conclusion

Classification



IOTA

References

Popov, Buchanan, **FPC-BI: Fast Probabilistic Consensus within Byzantine Infrastructures**, *Journal of Parallel and Distributed Computing, Volume 147, January 2021, pages 77-86.*

Capossele, Müller, Penzkofer, **Robustness and efficiency of leaderless probabilistic consensus protocols within Byzantine infrastructures**, *Blockchain: Research and Applications Volume 2, Issue 1, April 2021*

Müller, Penzkofer, Kuśmierz, Camargo, Buchanan, **Fast Probabilistic Consensus with Weighted Votes**, *Proceedings of the Future Technologies Conference (FTC) 2020, Volume 2. FTC 2020*.

Popov, Müller, **Voting-based probabilistic consensuses and their applications in distributed ledgers**, *accepted in Annals of Telecommunications*

Moog, *https://husqy.medium.com/a-new-consensus-the-tangle-multiverse-part-1-da4cb2a69772*

Müller, *https://iota.cafe/t/on-tangle-voting-with-fpcs/1218*

Theis, *https://iota.cafe/t/dislike-switch/1219/10*

Nitchai, Popov, Müller, **Fast Probabilistic Consensus on a Set**, *work in progress*

IOTA Research Team, **On Tangle Voting with metastability breaking** *work in progress*

Questions