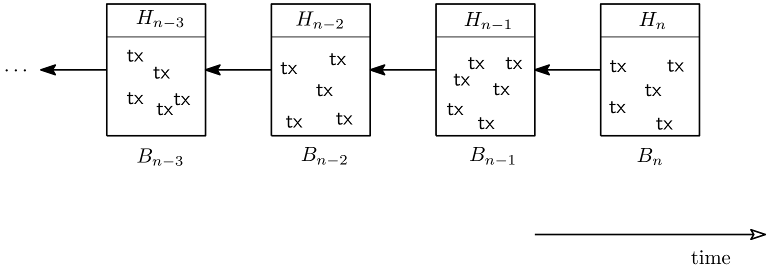
Introduction to IOTA – a feeless cryptocurrency

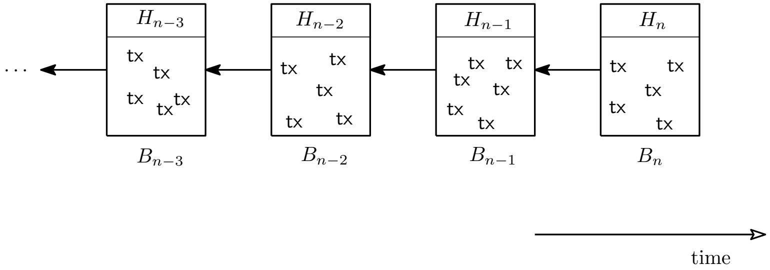
Serguei Popov

IOTA Foundation

Blockchain: decentralized consensus (Satoshi Nakamoto, 2008)



Blockchain: decentralized consensus (Satoshi Nakamoto, 2008)



Bitcoin mining: find a *nonce* N_{n+1} such that

$$\mathtt{hash}(H_n, N_{n+1}) \leq 0.00\ldots01$$

Two main types: Proof-of-Work (PoW) and Proof-of-Stake (PoS).

Two main types: Proof-of-Work (PoW) and Proof-of-Stake (PoS).
Problems:

- transaction fees

Two main types: Proof-of-Work (PoW) and Proof-of-Stake (PoS).
Problems:

- transaction fees
- difficult to scale

Two main types: Proof-of-Work (PoW) and Proof-of-Stake (PoS).
Problems:

- transaction fees
- difficult to scale
- PoW disproportionality and power consumption

Two main types: Proof-of-Work (PoW) and Proof-of-Stake (PoS). Problems:

- transaction fees
- difficult to scale
- PoW disproportionality and power consumption
- PoS and others also have their drawbacks (e.g. concentration of power, “nothing at stake”)

Two main types: Proof-of-Work (PoW) and Proof-of-Stake (PoS). Problems:

- transaction fees
- difficult to scale
- PoW disproportionality and power consumption
- PoS and others also have their drawbacks (e.g. concentration of power, “nothing at stake”)
- …

IOTA Tangle:

- started in 2015 as “cryptocurrency for IoT” ($\Rightarrow$ no fees)

IOTA Tangle:

- started in 2015 as “cryptocurrency for IoT” ($\Rightarrow$ no fees)
- no fees $\Rightarrow$ no miners (so no dichotomy “miners vs. simple users”)

IOTA Tangle:

- started in 2015 as “cryptocurrency for IoT” (⇒ no fees)
- no fees ⇒ no miners (so no dichotomy “miners vs. simple users”)
- collaborative system: “help the others, and the others will help you”

IOTA Tangle:

- started in 2015 as “cryptocurrency for IoT” (⇒ no fees)
- no fees ⇒ no miners (so no dichotomy “miners vs. simple users”)
- collaborative system: “help the others, and the others will help you”
- free riders?

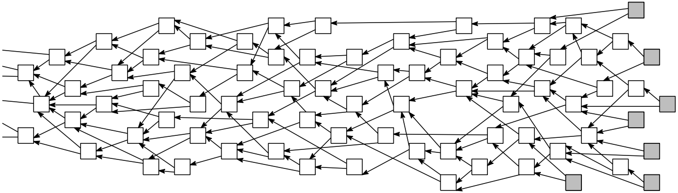
IOTA Tangle:

- started in 2015 as “cryptocurrency for IoT” (⇒ no fees)
- no fees ⇒ no miners (so no dichotomy “miners vs. simple users”)
- collaborative system: “help the others, and the others will help you”
- free riders?
- so: “help the others, and the others will help you; however, if you don’t help the others, the others won’t help you”

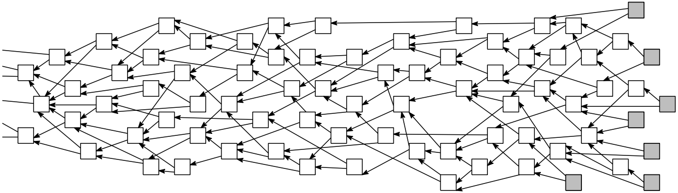
- no miners ⇒ no blocks

- no miners ⇒ no blocks
- no blocks + “help the others. . . ” ⇒ DAG

- no miners ⇒ no blocks
- no blocks + “help the others. . . ” ⇒ DAG

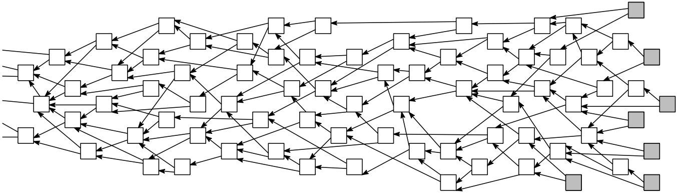


- no miners ⇒ no blocks
- no blocks + “help the others. . . ” ⇒ DAG



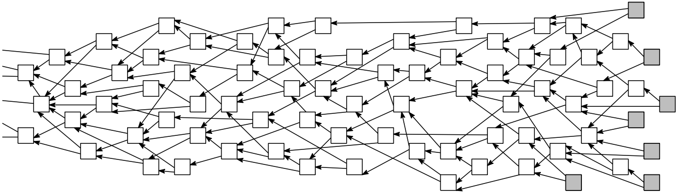
- only one rule: approve two transactions ⇒ freedom

- no miners ⇒ no blocks
- no blocks + "help the others. . . " ⇒ DAG



- only one rule: approve two transactions ⇒ freedom
- actors will behave in a "reasonable" way because it's a good idea to do so, and the designer's role is to propose a "good" set of rules (e.g. for tip selection)

- no miners ⇒ no blocks
- no blocks + “help the others. . . ” ⇒ DAG



- only one rule: approve two transactions ⇒ freedom
- actors will behave in a “reasonable” way because it’s a good idea to do so, and the designer’s role is to propose a “good” set of rules (e.g. for tip selection)
- possible applications of AI in the future versions of the protocol — for example, to approach better reputation systems (i.e., one can think about using AI for detecting node’s malicious behavior)

Deeper look: consensus in IOTA Tangle

The Coo:

- currently, the Coordinator protects the network

Deeper look: consensus in IOTA Tangle

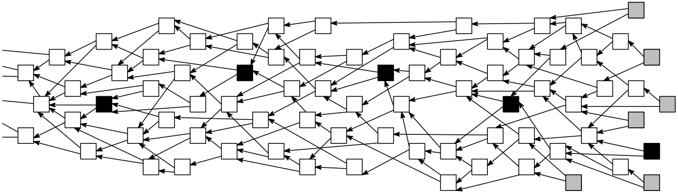
The Coo:

- currently, the Coordinator protects the network
- it issues *milestones*; a transaction is considered confirmed iff it is in the past cone of a milestone

Deeper look: consensus in IOTA Tangle

The Coo:

- currently, the Coordinator protects the network
- it issues *milestones*; a transaction is considered confirmed iff it is in the past cone of a milestone



Coordicide, general ideas:

- we are looking for a probabilistic consensus (“exponential beats polynomial” magic, $n^M e^{-\alpha n} \to 0$)

Coordicide, general ideas:

- we are looking for a probabilistic consensus (“exponential beats polynomial” magic, $n^M e^{-\alpha n} \to 0$)
- use an approximate consensus (e.g., on *time*) to achieve the total one whp

Coordicide, general ideas:

- we are looking for a probabilistic consensus (“exponential beats polynomial” magic, $n^M e^{-\alpha n} \to 0$)
- use an approximate consensus (e.g., on *time*) to achieve the total one whp
- consensus as an attracting state

Coordicide, some implementation details:

- voting layer: nodes can resolve conflicts pro-actively. FPC-BI: `arxiv.org/abs/1905.10895`

Coordicide, some implementation details:

- voting layer: nodes can resolve conflicts pro-actively. FPC-BI: `arxiv.org/abs/1905.10895`
- *mana*: Sybil protection and more

Coordicide, some implementation details:

- voting layer: nodes can resolve conflicts pro-actively. FPC-BI: `arxiv.org/abs/1905.10895`
- *mana*: Sybil protection and more
- auto-peering: creates a small-world network and protects against eclipse attacks

Coordicide, some implementation details:

- voting layer: nodes can resolve conflicts pro-actively. FPC-BI: `arxiv.org/abs/1905.10895`
- *mana*: Sybil protection and more
- auto-peering: creates a small-world network and protects against eclipse attacks
- node accountability: nodes have IDs and are “responsible” for their actions

Coordicide, some implementation details:

- voting layer: nodes can resolve conflicts pro-actively. FPC-BI: `arxiv.org/abs/1905.10895`
- *mana*: Sybil protection and more
- auto-peering: creates a small-world network and protects against eclipse attacks
- node accountability: nodes have IDs and are “responsible” for their actions
- `coordicide.iota.org` and `#tanglemath` channel at `discord.iota.org`

Coordicide, some implementation details:

- voting layer: nodes can resolve conflicts pro-actively. FPC-BI: `arxiv.org/abs/1905.10895`
- *mana*: Sybil protection and more
- auto-peering: creates a small-world network and protects against eclipse attacks
- node accountability: nodes have IDs and are “responsible” for their actions
- `coordicide.iota.org` and `#tanglemath` channel at `discord.iota.org`
- test implementation: `github.com/iotaledger/goshimmer`

More about Fast Probabilistic Consensus (FPC).

More about Fast Probabilistic Consensus (FPC).

Majority dynamics (threshold Voter Models):

- there is a graph, each site of which has an “opinion”, 0 or 1
- at random moments, each site consults *some* (few) neighbors, and adopts a new opinion using a “majority” rule.

More about Fast Probabilistic Consensus (FPC).

Majority dynamics (threshold Voter Models):

- there is a graph, each site of which has an “opinion”, 0 or 1
- at random moments, each site consults *some* (few) neighbors, and adopts a new opinion using a “majority” rule.

Properties:

More about Fast Probabilistic Consensus (FPC).

Majority dynamics (threshold Voter Models):

- there is a graph, each site of which has an “opinion”, 0 or 1
- at random moments, each site consults *some* (few) neighbors, and adopts a new opinion using a “majority” rule.

Properties:

- interesting and many (extensively studied since 70’s)

More about Fast Probabilistic Consensus (FPC).

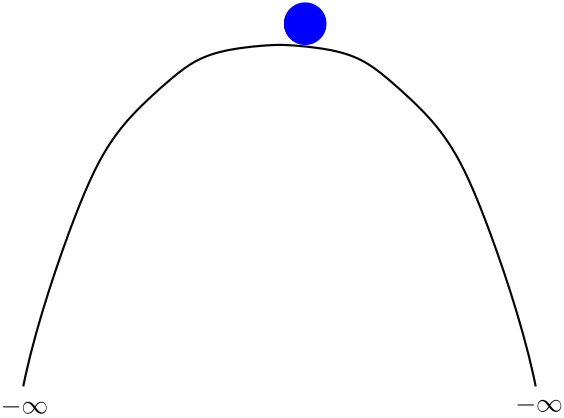
Majority dynamics (threshold Voter Models):

- there is a graph, each site of which has an “opinion”, 0 or 1
- at random moments, each site consults *some* (few) neighbors, and adopts a new opinion using a “majority” rule.

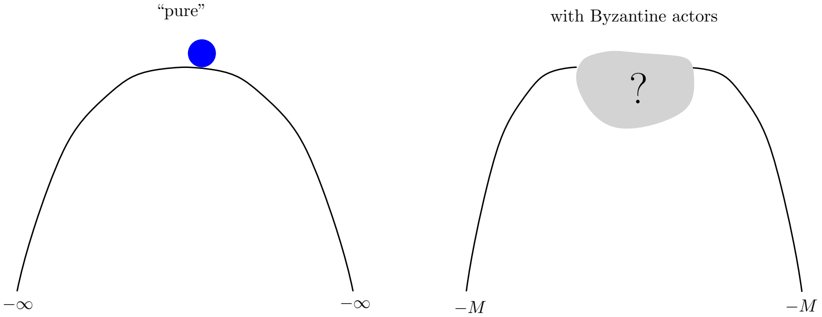
Properties:

- interesting and many (extensively studied since 70’s)
- in particular: only two extremal invariant measures (“all-0” and “all-1”), which are consensus states.

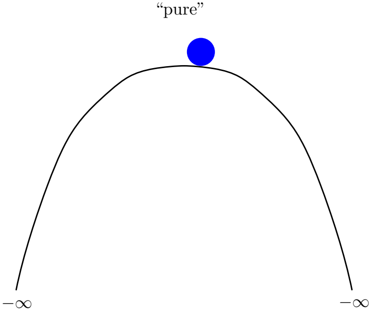
Majority dynamics as a RW on a potential:

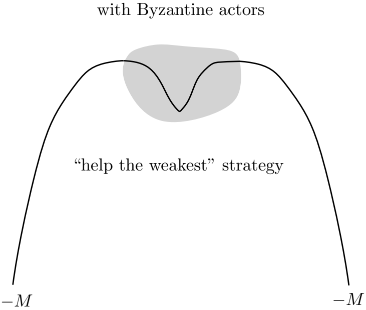


Majority dynamics with Byzantine actors:

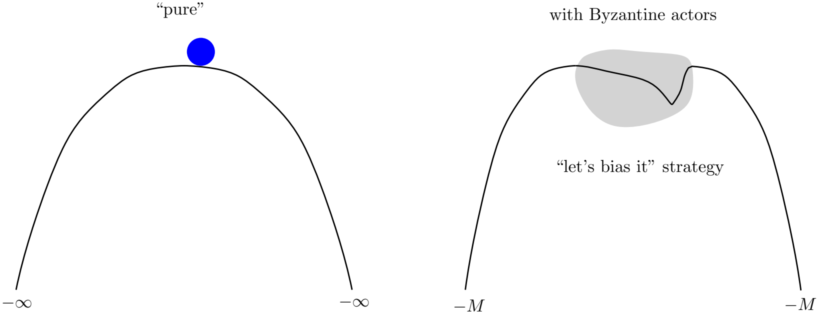


Majority dynamics with Byzantine actors: the curse of metastability

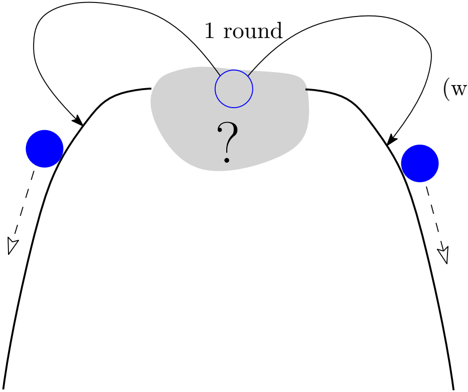




Majority dynamics with Byzantine actors: the curse of metastability



Fast Probabilistic Consensus (FPC): defeating the metastability with turn-based common random thresholds:



(with uniformly positive probability)

Questions?