# Majority Vote Dynamics for IOTA Transaction Consensus

Kenric Nelson & André Vilela

January 2020

## 1. Project Background and Description

The IOTA cryptocurrency network uses a Tangle, which is a directed acyclic graph, designed to enable fast processing of micropayments in order to facilitate Internet-of-Things transactions. The IOTA Foundation has developed complementary voting methods for transitioning IOTA's peer-to-peer (P2P) cryptocurrency network from a centralized to a decentralized validation of transactions on the Tangle. The Coordicide, killing of the centralized Coordinator, as this initiative is called, conceives of both fast-probabilistic consensus and cellular automata as complementary methods for voting. The fast-probabilistic consensus (FBC) has guarantees for convergence but is computationally expensive; while the cellular automata (CA) consensus is efficient, but its convergence properties are poorly understood.

The "Majority Vote Dynamics for IOTA Transaction Consensus," research project to be completed by Kenric Nelson and André Vilela will model and simulate the CA consensus to document its convergence properties. To achieve this goal the project will a) survey and model majority-vote dynamics of random k-nearest neighbor networks, b) provide computer simulations and numerical analysis comparing the effect of initial conditions on achieving consensus and c) report and discuss the impact of the results with regarding to designing a peer-to-peer voting protocol which can withstand malicious attacks.

## 2. Project Scope

Simulations of the majority vote mechanisms will be carried out on random k-nearest neighbor graphs. We will examine the impact the following features have on achieving consensus and avoiding meta-stable states of conflict: a) number of neighbors k (to confirm prior work), b) role of mana, which is delegated to nodes and weights the importance of their contribution, c) the initial conditions which provides a first-order examination of worst-case attack modes, and d) the distribution of cooperative nodes, which vote based on their neighbors opinion, and adversarial nodes, which exploit a separate sub-network. Monte Carlo analysis will provide an experimental foundation for characterizing the convergence properties of CA consensus, so that the protocol design can be improved and refined. This project will seek to provide scientific guidance regarding the dynamics of CA consensus in the midst of adversarial nodes, but will not seek to model details of cryptographic protocols.

## 3. Majority Dynamics in the Presence of Adversaries

The IOTA P2P network [1] must achieve accurate consensus regarding the validity of transactions in the presence of malicious nodes. Thus, quantifying the dynamical properties of majority-vote over a P2P network is critical for the successful design and operation of the cryptocurrency protocols. Majority-vote dynamics consists in a set of opinion states $\{\sigma\}$ in the nodes of a geometric network of interactions which evolves at each discrete time step $t$. The state of a node $i$ is represented by the variable $\sigma_i(t)$ that can assume one of two values $+1$ or $-1$ at a given time $t$. In a subsequent time step $t + 1$, the node $i$ has its state updated following the rule

$$\sigma_i(t+1) = \begin{cases} \mathrm{sgn}\,(S_i), & \text{if } S_i \neq 0; \\ \sigma_i(t+1) = \sigma_i(t), & \text{if } S_i = 0, \end{cases}$$

where $\mathrm{S_i} = \sum_{\delta=1}^{\mathrm{k_i}} \mathrm{w_i}(m,n,t)\sigma_{\mathrm{i}+\delta}(\mathrm{t})$, $\mathrm{sgn(x)} = +1, 0, -1$ in case $\mathrm{x} < 0, \mathrm{x} = 0$ and $\mathrm{x} > 0$, respectively. Here, $\mathrm{w}_i(m,n,t)$ is a function that models the weight of a voter in the network, and it may depends on the parameters mana $m$, proof-of-vote $n$, and time $t$. The sum runs over all $\mathrm{k_i}$ nodes attached to the spin $\sigma_{\mathrm{i}}(\mathrm{t})$. For the case of a random graph with eight neighbors, $\mathrm{k_i} = 8$ for all $i$. In this way, $\sigma_{\mathrm{i}}(\mathrm{t}+1)$ adopts the state of the majority of its neighbors, whereas, in the case of a tie, it remains in its previous state.

The majority-vote dynamics are affected by the structure of the network [2-5]. For the IOTA P2P communications network the structure is designed as a random k-nearest neighbor network. In [6] the dynamics of the IOTA CA consensus was investigated.  We propose to refine this analysis to model a k-nearest neighbor graph with random selection of neighbors. Each node will model a) whether it is a cooperative or adversarial node, b) the reputation of a node reflected by the quantity of mana staked to the node, and c) whether a neighbor's opinion is trusted or not-trusted, which simulates the role of proof-of-vote. A cooperative node is modeled by following the majority opinion of its neighbors. Research will be conducted regarding how best to model various adversarial attacks, but in each case the underlying premise will be that the adversary has achieved the ability to exploit more global knowledge regarding the opinion network.

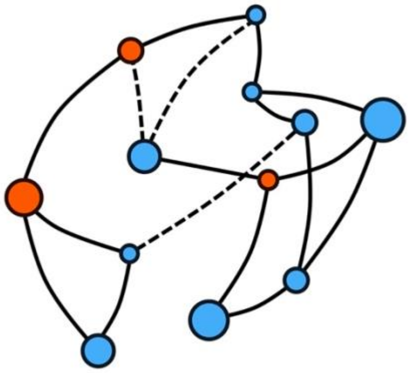

*Figure 1 - Schematic representation of a random 3-neighbor network with variation in mana (size), and cooperation (color) Red nodes represent adversaries.. Dashed lines represent connections in which the proof-of-vote was not accepted.*

## 4. Personnel Contributions

**Dr. Kenric Nelson** is an independent researcher developing novel approaches to Complex Decision Systems, including dynamics of cryptocurrency protocols, sensor systems for ecological studies, and robust machine learning methods.  His recent experience includes Research Professor with Boston University Electrical & Computer Engineering (2014-2019) and Sr. Principal Systems Engineer with Raytheon Company (2007-2019). He has pioneered novel approaches to measuring and fusing information. His *nonlinear statistical coupling* methods have been used to improve the accuracy and robustness of radar signal processing, sensor fusion, and machine learning algorithms. His education in electrical engineering includes completing a B.S. degree Summa Cum Laude from Tulane University, a M.S. degree from Rensselaer Polytechnic Institute, and a Ph.D. degree from Boston University. His professional education includes an Executive Certificate from MIT Sloan and a certification with the Program Management Institute.

**Dr. André L. M. Vilela** has investigated the dynamics of interacting agent-based models in statistical mechanics, combining phase transitions, critical phenomena, and finite-size scaling analysis with sociophysics, econophysics, and complex network theory. His research focuses on unveiling the underlying mathematical mechanisms that drive the behavior of agents in groups within social networks and financial markets, and how their decisions promote active collective phenomena. He is a distinguished visiting scientist at Boston University, full professor at the University of Pernambuco, and Coordinator of the Materials Physics undergraduate program. His education in Physics includes completing a B.S. degree With High Honors Award, a MSc. degree with Distinction Award, and a Ph.D. degree from the Federal University of Pernambuco.   andrevilela.com

## 5. References

[1] Popov, Serguei. The Tangle. White Paper, https://iota.org/IOTA_Whitepaper.pdf, 2017.

[2] Vilela, André L. M.; Stanley, H. Eugene. Effect of Strong Opinions on the Dynamics of the Majority-Vote Model. Scientific Reports, 2018.

[3] Vilela, André L. M.; Souza, A. J. F. Majority-vote model with a bimodal distribution of noises in small-world networks. Physica A - Statistical Mechanics and its Applications, v. 488, p. 216-223, 2017.

[4] Vilela, André L. M.; Wang, Chao; Nelson, Kenric P.; Stanley, H. Eugene. Majority-vote model for financial markets. Physica A - Statistical Mechanics and its Applications, 2019.

[5] Mendes, J. F. F. and Santos, M. A. Short-time dynamics of a two-dimensional majority vote model. Phys. Rev. E, 1998.

[6] Popov, Serguei, et al. The Coordicide. White Paper, https://files.iota.org/papers/Coordicide_WP.pdf, 2019.

[7] Mossel, Elchanan, Joe Neeman, and Omer Tamuz. Majority dynamics and aggregation of information in social networks, , *Autonomous Agents and Multi-Agent Systems* 28.3 (2014): 408-429