Resilience of IOTA Consensus

Hamed Nazim Mamache  
*Sorbonne University, Paris, France*  
hamed_nazim.mamache@etu.sorbonne-universite.fr

Gabin Mazué  
*Sorbonne University, Paris, France*  
gabin.mazué@etu.sorbonne-universite.fr

Osama Rashid  
*Sorbonne University, Paris, France*  
osama.rashid@etu.sorbonne-universite.fr

Gewu Bu  
*University Clermont Auvergne, Clermont Auvergne, France*  
gewu.bu@uca.fr

Maria Potop-Butucaru  
*Sorbonne University, Paris, France*  
maria.potop-butucaru@lip6.fr

Abstract—Blockchains are appealing technologies with various applications ranging from banking to networking. IOTA blockchain is one of the most prominent blockchain specifically designed for IoT environments. In this paper we investigate the convergence of two Consensus proposed by IOTA: Fast Probabilistic Consensus and Cellular Consensus, when run on top of various topologies. Furthermore, we investigate their resilience to various types of adversaries. Our extensive simulations show that both Cellular Consensus and Fast Probabilistic Consensus have poor convergence rates even under low power adversaries and have poor scaling performances except for the case of Watts Strogatz topologies. Our study points out that the design of IOTs dedicated blockchains is still an open research problem and gives hints design. Our results confirmed the motivation of the foundation IOTA who is working on a complete version of consensus, Coordicide, for the new IOTA, while regarding these two as components of.

Index Terms—Consensus, Byzantine fault, IOTA

I. INTRODUCTION

Internet of Things (IoT) devices are used in a large range of applications such as smart grids, smart foraging, smart buildings, smart supply chains or smart medical applications and the IoT environment [1] is expected to further expand even more ubiquitous deployment thanks to the fifth generation of networks (5G) [2] and beyond.

Due to the vulnerabilities of IoT to various attacks and the very harmful potential consequences, the currently dominating approach in the management of IoT devices is centralizing control operations at IoT gateways, which are considered as the natural function to absolve access control, data filtering and mixing operations. However, centralization does not appear viable when one envisions hundreds of thousands of devices per km2 or per cell [1], especially when those devices can be constrained in size and power supply.

The use of Distributed Ledger Technologies (DLT) can respond to both security and decentralization needs in the management of IoT devices. Distributed Ledger Technologies (DLT) such as blockchains provide a secure way to share information between a high number of independent nodes operating under different authorities, while ensuring high availability and immutability. Distributed Ledger Technology pioneered by Bitcoin technology created a new design philosophy for executing and storing transactions in a decentralized and secure fashion [3].

A blockchain is a distributed ledger that mimics the functioning of a classical traditional ledger (i.e. transparency and falsification-proof of documentation) in an untrusted environment where the computation is distributed. Traditional blockchain systems such as Bitcoin [3] or Ethereum [4] maintain a continuously-growing list of ordered blocks that include one or more transactions that have been verified by the members of the system, called miners. Blocks are linked using cryptography and the order of blocks in the blockchain is the result of a form of agreement (consensus) among the system participants. Bitcoin technology and similar proposals (e.g Ethereum) came with several drawbacks that prevent them from being used as standards for IoT industry. Therefore, alternative solutions have been opened by IOTA [5], IOTA’s data structure is a Directed Acyclic Graph (DAG) based distributed ledger, also known as the Tangle, aimed to overcome limitations of Bitcoin-like distributed ledgers when used in IoT environment while preserving equivalent security levels. Transactions are continuously appended to the tangle. Similar approaches have been proposed by Spectre or Phantom [6], [7]. However, IOTA and similar approaches have not yet been adopted by the IoT industry because of 1) lack of strong consistency guarantees and 2) unclear resistance to attacks. In order to respond to these criticism IOTA proposed recently in [8] attacks resilient consensus mechanisms that plugged into the IOTA Tangle will offer strong consistency guarantees.

Two consensus algorithms are proposed: Fast Probabilistic Consensus (FPC) and Cellular Consensus (CC). These two proposals have been partially evaluated in [9], [10].

In this work we investigate the performances of IOTA consensus in several aspects. First, we run Fast Probabilistic Consensus (FPC) and Cellular Consensus (CC) on top of various topologies, from theoretical to practical. (2D Grid, Torus and Watts-Strogatz model [11]) then we evaluate their resilience to adversarial behavior. Our evaluation is conducted with OMNET++ simulator enriched with three adversarial models introduced in [8]. Even though most of the results reported in our study are negative they contain hits in order to design an efficient IoT dedicated blockchain.
II. IOTA DISTRIBUTED CONSENSUS

In this section, we briefly describe the operating principles of the two consensus mechanisms proposed by IOTA [8]. The basic idea is all honest nodes in the system should agree dynamically with a common opinion by a distributed way, so that this opinion cannot be changed by others easily.

Consider a connected network composed of $N$ nodes, enumerated as $\{1, \ldots, N\}$. Some lossless links connect nodes in the network. Nodes connected directly are neighbors.

We follow the setting proposed in [9], [10], assuming that the time is discrete and divided into rounds.

Each node has an opinion status, $O_i(r) \in \{0, 1\}$ at the round $r$. Consensus is achieved, if $\forall i, j \in N, O_i(r_{end}) = O_j(r_{end})$, where $r_{end}$ is the last round of simulation.

An opinion held by most of the nodes is a major opinion. The convergence rate is the percentage of runs leading to a consensus stage given $P_0$, where $P_0$ is the probability that a node has opinion 0 at round 0. If a node does not have opinion 0 at round 0 it will have opinion 1.

A. Fast Probabilistic Consensus (FPC)

The idea of Fast Probabilistic Consensus algorithm is based on the query/reply of opinion from nodes in the network. Algorithm executed by each node is as follows:

- Query randomly a number of nodes in network at each discrete time round $t$;
- Wait for the chosen nodes to respond and give their opinions;
- Calculate the mean of the received opinions.

Once the node executing Fast Probabilistic Consensus algorithm has calculated the mean, if it is the first round, he will compare it to a threshold $\tau$, if the mean is bigger than $\tau$, then its opinion becomes 1, otherwise becomes 0. If it is not the first round, the node will generate a random variable $U_t$ following a uniform law in function of $\tau$ between $[\beta, 1 - \beta]$ (where $\beta$ is the uniform low parameter). If the mean is bigger than $U_t$, the opinion becomes 1, if it is smaller, the opinion becomes 0 and if they are equal, the opinion stays the same as the previous round.

We make following two adjustments form original FPC [9] to adapt realistic environment: 1) Remove the assumption about the common random values sequence. 2) The node only knows the nodes directly connected to it, the neighbors. We talked about this adjustment in the extended version of this paper [12]. When a node need to query others in each round, it launches a number of random walks with distance $D$. A random walk goes to one of the neighbors nodes and decrements $D$ by 1. When $D = 0$, a random walk stops, and this node arrived by will be chosen as a node to be queried.

B. Cellular Consensus (CC)

In Cellular Consensus (CC), each node acts as an individual agent, that changes its opinion in case of conflict with its neighbors and adopts the major opinion among its neighbors.

At the beginning of each round, every node sends a “heartbeat” of its signed current opinion and the opinions from the previous round of his neighbors, each one signed by the issuing node.

When a node receives an opinion given by one of its neighbors, it will evaluate this opinion by a “proof” accompanying the opinion. This “proof” is materialized by the opinions of the neighbor’s neighbors. That will allow nodes to monitor each other and to detect if someone is lying independently of its neighbors. If this “proof” shows that the neighbor is lying, it will immediately be blacklisted by the node and none of his opinions will be taken into account.

Since the previous opinions of the neighbors cannot be faked, every node can validate that the received opinion is indeed correct.

In detail, the cellular consensus algorithms work as follows. At each step of the algorithm, each node holds an opinion, which can be 0, 1 or a temporary opinion state $-1$.

If the major opinion among neighbors of node $i$ in round $r$ is:

- 0, then the opinion of node $i$ in round $r + 1$ will be 0,
- 1, then the opinion of node $i$ in round $r + 1$ will be 1,
- non-existent (i.e. there is no majority opinion), then the opinion of node $i$ in round $r + 1$ will be $-1$.

III. SIMULATION RESULTS

In this section we will present a selection of our extensive simulations related to the resilience of IOTA consensus algorithms with various adversaries and different network topologies. The topologies used in our simulations are 2D Grid, Torus, two topologies theoretical often used as reference topology in algorithm analyzing, and Watts-Strogatz [11], a realistic network model which is well-suitable for IoT. Due to space restriction, some of the results are reported in [12]. In order to simulate possible attacks and predict critical security cases, we implement the three Byzantine adversaries defined in [10]:

- **Cautious adversaries.** These nodes are able to lie on every round of the process with a probability $P_{\text{ping}}$. However, the opinion sent during the same round is always the same even though the queries come from different nodes.
- **Semi-Cautious adversaries** These nodes will not lie, however, they may not respond to a query, with a probability $P_{\text{silence}}$. Thus delaying the process of convergence and reducing the number of accessible nodes in the network.
- **Berserk adversaries** This adversary is stronger than the previous two adversaries. It behaves similar to Cautious, except that it is able to provide different responses to different queries received in the same round. Thus, during the same round, it can send his true opinion, then lie and respond with a wrong opinion.

We use OMNet++ simulator enriched with the three topologies and the three adversaries models. We run our simulations on a physical machine with 8 cores 16 threads and 16 GB RAM. We also run simulations in a virtual machine with 6 VCPU cores and 16 GB RAM.
Our extensive simulations show that there is no difference between Berserk adversaries and Cautious adversaries in terms of convergence rate. That is because, in long runs, both malicious nodes will give the same quantity of false information to their neighbors in average. If we consider $M$ the number of rounds and $X$ the number of queries that the malicious node will receive per round on average, a Cautious adversary will lie in $\frac{M \times X}{2}$. As for the Berserk adversary, it will lie in average of $\frac{X}{2}$ regardless of the round which also makes a total of $\frac{M \times X}{2}$ lies. In the following, we will detail only the resilience of Fast Probabilistic Consensus to cautious and semi-cautious adversaries.

A. Fast Probabilistic Consensus resilience

We list here the basic parameters involved in Fast Probabilistic Consensus.

- Distance (length) of the random walks: $D = 4$, a relative small value to represent a limited knowledge range of neighbors;
- Number of nodes queried 10;
- Initial threshold : $\tau = 0.5$;
- Uniform law parameter : $\beta = 0.25$;
- $K = 10, P = 1$ for Watts-Strogatz model [11] where $K$ is the average degree of the nodes in the network and $P$ is the probability allowing to change the edges;
- $P_{lying} = 50\%$ for Cautious;
- $P_{silence} = 50\%$ for Semi-Cautious;
- Number of rounds : $M = 30$, which is long enough according to our extended simulations [12].

1) Network Size and $P_0$ Impact without Malicious Nodes:

We first studied the impact of the number of nodes, $N$, and the initial opinion distribution, $P_0$ on the convergence rate. In Figure 1, we show the convergence rate function to the initial division probability $P_0$ in each topology and for different network sizes from $N = 49$ to $N = 1024$. In Torus, with small network sizes, the convergence rate is 100% regardless of the value of $P_0$. While in Grid, even with small network sizes, the convergence rate drops drastically when $P_0 \in [0.35, 0.75]$. In terms of network size, for the Grid and the Torus topologies, the more nodes are in network, the lower convergence rate is. Hence, Fast Probabilistic Consensus is not scalable. On the contrary, in Watts-Strogatz topology, the convergence rate is high regardless of the number of nodes. Moreover, our extended simulations [12] show that even the average number of neighbors, $K$, has no impact on the convergence rate.

2) Convergence rate with Cautious Adversaries:

We inspected first the Fast Probabilistic Consensus resilience when 33% of total nodes in the network ($N/3$) are Cautious adversaries. This is motivated by the fact that $N/3$ resilience is the upper bound in terms of Byzantine resilience for consensus protocols. In our extended simulations [12] we observed that in this case the convergence rate drops below 5% for all studied topologies regardless of the initial opinion distribution $P_0$ or the network size $N$. This is due to the fact that the Cautious adversaries can spread freely their lies across the network when nodes ask their opinions via the Fast Probabilistic Consensus queries. Honest nodes therefore cannot make a correct decision. In the following simulations, we fix the network size by choosing a reasonable medium network size, $N = 225$ and study the resilience of Fast Probabilistic Consensus to various percentages of Cautious adversaries.

In Figure 2, we vary the percentage of malicious nodes from 10% up to 50%. We can clearly notice a huge difference between $P_{\text{malicious}} = 0\%$ and $P_{\text{malicious}} = 10\%$. When the network is corrupted with only 10% of Cautious adversaries for both Grid and Torus, the convergence rate drops to 10% and 20%, respectively. Watts-Strogatz resists up to 10% Cautious adversaries with a convergence rate of around 80%. Even though Watts-Strogatz has a better resilience to Cautious than Grid and Torus, the convergence rate is catastrophic for all topologies starting with 20% of malicious nodes.

3) Convergence rate with Semi-Cautious Adversaries:

Furthermore we studied the impact of Semi-Cautious adversaries. We observed in our extended results [12] that for each topology, Semi-Cautious adversaries do not have an impact even $P_{\text{malicious}}$ is higher than 33%. The simulation results are similar to the situation when there are no malicious nodes. This can be explained by the fact that Semi-Cautious adversaries do not lie, they just do not answer which does not corrupt...
the network. We can therefore conclude that if some devices are slow or faulty and they cannot respond to the queries in time there is no impact on the Fast Probabilistic Consensus behavior.

B. Cellular Consensus resilience

Cellular Consensus (CC) has been evaluated using the same base configuration as Fast Probabilistic Consensus (FPC):

- $K = 10$, $P = 1$ for Watts-Strogatz model;
- $P_{	ext{tying}} = 50\%$ for Cautious;
- $P_{	ext{silence}} = 50\%$ for Semi-Cautious;
- Number of rounds : $M = 30$;

1) Network Size and $P_0$ Impact without Malicious Nodes: Through Figure 4, for the three topologies, we observe that the number of nodes, $N$, is still an important parameter for the convergence of the network as in the case of Fast Probabilistic Consensus. Indeed, when the number of nodes increases, the convergence rate decreases for both Grid and Torus topologies. However, in terms of initial opinion distribution $P_0$, Cellular Consensus on Grid and Torus become more sensitive compared with Fast Probabilistic Consensus. Convergence rates decrease drastically when $P_0 \in [0.25, 0.85]$ and never pass 50\%. In Watts-Strogatz model, Cellular Consensus has similar behavior as Fast Probabilistic Consensus and has a good scalability.

Contrary to Fast Probabilistic Consensus, in our extensive simulations \[12\] we show that adjusting $K$ for Watts-Strogatz topology impacts clearly the convergence rate in Cellular Consensus: when $K$ gets smaller, Watts-Strogatz topology becomes more sensitive to the initial opinion distribution $P_0$ and networks size $N$. We therefore test different $K$ values for the Watts-Strogatz model to evaluate the resilience of Cellular Consensus to Cautious and Semi-Cautious Adversaries. Recall that Cellular Consensus is based on the communication between neighbors and that we have the average number of neighbors $K < 4$ for Grid, $K = 4$ for Torus and $K = 10$ for Watts-Strogatz in our simulations. We conclude here that without malicious nodes, the higher the average number of neighbors is, the better the convergence rate will be.

2) Convergence rate Cautious Adversaries: First we study the convergence rate when $N/3$ (33\%) nodes are Cautious adversaries. When we introduce Cautious adversaries in Cellular Consensus, we observe, in Figure 5, the same tendency as without malicious nodes by adjusting network size $N$ however, the convergence rate is much lower. Indeed when the malicious nodes are detected, they are immediately blacklisted which means that some nodes lose neighbors, which leads to this decrease. However, compared with Fast Probabilistic Consensus, Cellular Consensus has a better resilience to Cautious Adversaries since it can detect malicious nodes and block them.
In the sequel, we fix the network size $N = 225$ as in Fast Probabilistic Consensus. When $P_{\text{malicious}}$ varies, we observed in [12] a decrease in the convergence rate. We observe that the results obtained with Torus are better than those in Grid. With $N = 255$, Cellular Consensus run in Watts-Strogatz model has a stable convergence rate.

In the following we study the convergence rate of Cellular Consensus in Watts-Strogatz model when varying $K$ and considering $N/3$ (33%) Cautious adversaries.

In Figure 6, the results confirm that the average number of neighbors influences the convergence rate.

3) Convergence rate with Semi-Cautious Adversaries: In the following we study first the convergence rate of Cellular Consensus with $N/3$ (33%) semi-cautious adversaries.

When we introduce Semi-Cautious adversaries, we observe in Figure 7 that when $0.3 \leq P_0 \leq 0.7$, the percentage of convergence is the same as without malicious nodes for Grid and Torus topologies.

Below, we analyze the convergence rate of Cellular Consensus when run on top of Watts-Strogatz topology with 33% Semi-Cautious adversaries.

The results in Figure 8 show that when the average number of neighbors is low, $K \leq 4$, the percentage of convergence is relatively low for $0 \leq P_0 < 0.3$ or $0.7 < P_0 \leq 1$ and similar to a network without malicious nodes for $0.3 \leq P_0 \leq 0.7$. When the average number of neighbors is higher, the results can be better. Same as in Cautious case, by adjusting $K$, Watts-Strogatz might have a good resilience to this type of attack.

In the following we study the convergence rate of Cellular Consensus when varying the percentage of Semi-Cautious adversaries $P_{\text{malicious}}$.

When we vary the percentage of chance that a node is a Semi-Cautious adversary in Figure 9, we observe a decrease in convergence rate. By comparing different topologies, we observe that the results obtained with the Torus are better than those obtained with the Grid.
IV. CONCLUSION

In this paper we extensively evaluate the resilience of Fast Probabilistic Consensus and Cellular Consensus (two agreement building blocks introduced for IOTA blockchain [8]). Our evaluation focused on the impact of the underlying network topology on the convergence rate of the algorithms and their resilience to various adversaries (cautious, semi-cautious and Berserk). We showed that the initial opinion state distribution of each node and the total number of nodes in the network will seriously affect the convergence results, especially in 2D Grid and Torus topologies. These effects will not be alleviated by increasing the run time.

In Fast Probabilistic Consensus, Cautious and Berserk adversaries will cause serious convergence issues even with low power adversaries. However, semi-cautious adversaries seem to not be a menace. In the Cellular Consensus, all three adversaries have an impact on the convergence, but none of them is as serious as in the case of Fast Probabilistic Consensus. Interestingly, the Watts-Strogatz topology when the density is properly adjusted can even eliminate the effects of adversaries. We plan to continue this work by giving mathematical modeling and explaining our results formally.

REFERENCES

[1] A. Ijaz, L. Zhang, M. Grau, A. Mohamed, S. Vural, A. U. Quddus, M. A. Imran, C. H. Foh, and R. Tafazolli, “Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations,” IEEE Access, vol. 4, pp. 3322–3339, 2016. [Online]. Available: https://doi.org/10.1109/ACCESS.2016.2584178
[2] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. E. Lozano, A. C. K. Soong, and J. C. Zhang, “What will 5G be?” IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065–1082, 2014. [Online]. Available: https://doi.org/10.1109/JSAC.2014.2328098
[3] S. Nakamoto et al., “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[4] G. Wood et al., “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.
[5] S. Popov, “The tangle,” 2018, accessed 30 June 2019. [Online]. Available: http://www.descryptions.com/Iota.pdf
[6] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, “SPECTRE: A fast and scalable cryptocurrency protocol,” IACR Cryptol. ePrint Arch., vol. 2016, p. 1159, 2016.
[7] Y. Sompolinsky and A. Zohar, “PHANTOM: A scalable blockchain protocol,” IACR Cryptol. ePrint Arch., vol. 2018, p. 104, 2018.
[8] P. Serguei, M. Hans, C. Darcy, C. Angelo, D. Vassil, G. Alon, G. Andrew, K. Bartosz, M. Sebastian, P. Andreas, S. Olivia, S. William, V. Luigi, W. Wolfgang, and A. Vidal, “The coordinate,” 2020, accessed 03 March 2020. [Online]. Available: https://files.iota.org/papers/20200120_Coordinate_WP.pdf
[9] S. Popov and W. J. Buchanan, “Fpc-bi: Fast probabilistic consensus within byzantine infrastructures,” Journal of Parallel and Distributed Computing, vol. 147, pp. 77–86, 2021.
[10] A. Capossele, S. Müller, and A. Penzkofer, “Robustness and efficiency of leaderless probabilistic consensus protocols within byzantine infrastructures,” arXiv preprint arXiv:1911.08787, 2019.
[11] D. J. Watts and S. H. Strogatz, “Collective dynamics of ‘small-world’ networks,” nature, vol. 393, no. 6684, pp. 440–442, 1998.
[12] H. N. Mamache, G. Mazué, O. Rashid, G. Bu, and M. Potop-Butucaru, “Resilience of IOTA Consensus,” Sorbonne Universités, UPMC University of Paris 6 ; Université Clermont Auvergne (UCA), Research Report, Nov. 2021. [Online]. Available: https://hal.archives-ouvertes.fr/hal-03427543