# IOTA: Feeless and Free

**Serguei Popov**, IOTA Foundation

*IEEE Blockchain Technical Briefs*, January 2019

Discuss this topic on IEEE Collabratec (https://ieee-collabratec.ieee.org/app/community/102)

(https://ieee-collabratec.ieee.org/app/community/102)

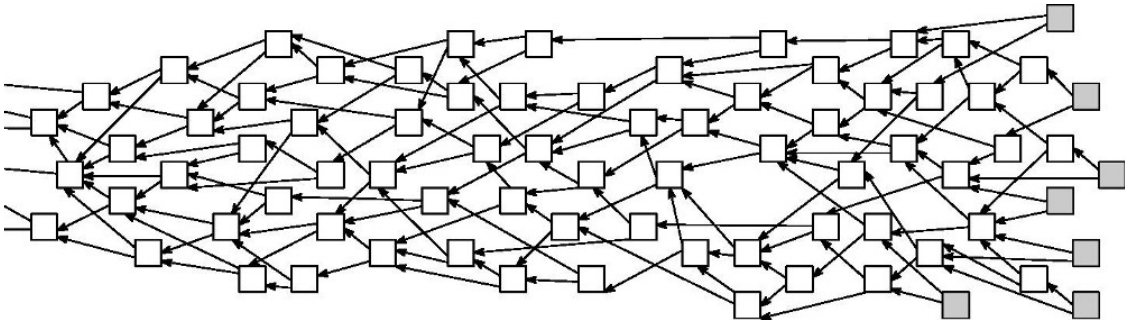
Internet of Things (IoT) data is becoming a new distributed, large-scale digital asset fueling a myriad of services in the connected world. However, as a *valuable* asset, IoT data needs to be protected by their producers. This limits its capability to be shared while hindering the innovation potential that IoT and data could deliver. IoT data and services have to live within the boundaries controlled by each service provider. This creates islands of services, powered by *Intranets of Things*. The promise of a truly connected world stops when we cross those boundaries and our devices and data stops to work. Imagine a high mobile IoT device, like an electric vehicle, that cannot charge when in a different city, just because charging stations are managed by a different provider and their availability is unknown. Exchanging data and delivery services requires costs and generates value. In a truly connected world, value needs to be shared across involved stakeholders, likewise the responsibilities. This implies a fundamental trust problem, that cannot be solved by one actor taking the responsibility for all the others. It is therefore important to provide a decentralized trust backbone that allows to trade data, manage access to them and track responsibilities [1]. Blockchain and DLTs provides this backbone. However, for this infrastructure to scale and be sustainable, its use should be free. Transacting on this infrastructure should cost zero, to allow access to billions of IoT devices and data. With such an infrastructure new business models for a *truly* connected world can be created, with no predefined rules imposed by pre-existing economic models. IOTA provides the technology to develop this infrastructure: it is feeless and free, scalable and lightweight enough to be integrated with IoT devices.

Our initial ambition was to create trust without monetary incentive for all the other properties to follow. This explains why from the beginning, we wanted to build a cryptosystem with no transaction fees that would be suitable for microtransactions. In traditional cryptocurrencies such as Bitcoin or Ethereum, there is a natural dichotomy: there are miners, who are rewarded for making the system work by producing the blocks which contain transactions (and possibly other information), and users who just use the system (e.g., by issuing transactions). To become a miner, an individual must have a sufficient quantity of some *scarce* resource (hashing power, stake, etc.) that “ordinary users” usually do not have. Since it is likely that the miners invested something in order to have that scarce resource, they would naturally want to make a profit by charging fees (and indeed they do: towards the end of 2017, the Bitcoin fees went up to as much as $50 per transaction, while the Ethereum network has already seen fees of around $5). Therefore, to get rid of the fees one has to get rid of the miners, so that the users themselves are responsible for inserting transactions into the ledger.

The implication is that without miners, the system needs to be *collaborative*: the users would have to help each other by vetting other users’ transactions. As with any such system, the existence of *free riders* is possible: individuals who want to *use* the system, but do not want to *contribute to it*. Indeed, everybody wants to be helped by others, but not everybody cares about helping others themselves. To resolve this without having to introduce monetary rewards, we could instead think of the reward simply as *not being punished* by others. The main principle of our system would then be: “Help others, and others will help you; however, if you choose not to help others, others will not help you either”. This collaborative system we are envisioning should also be able to defend itself against malicious actors — the fact that issuing a transaction does not cost anything makes the attacker’s task easier, in principle.

The mathematical model that was designed to serve as a base for such a system is called “The Tangle” (for its concrete description and discussion see [3,4]). The transactions can be thought of as vertices of a *Directed Acyclic Graph* (DAG), with arrows representing approvals, see Figure 1. When someone decides to issue a new transaction, (s)he must choose two existing transactions, and “attach” the new one to them. Some basic

terminology: we call the transactions which do not yet have any approvals "*tips*". By definition, all incoming transactions start out as tips.



(/images/files/newsletter/201901-popov-figure1.jpg)

***Figure 1**. Visual representation of the Tangle: each transaction (square) approves two other transactions (linked by arrows). Grey squares represent tips.*

The general idea is that, by approving a transaction, one also indirectly approves all of its "predecessor transactions" (by verifying that they are valid and do not contradict each other). When a transaction is "deep inside" the DAG (that is, approved by many transactions, directly or indirectly), it is reasonable to consider it "confirmed." Intuitively it is quite clear that, to help the system progress, incoming transactions *must* be attached to tips (rather than to old transactions) because this adds new information to the system. Unfortunately, information does not propagate immediately through the network; sometimes there are delays. Therefore, it is not really possible to *impose* a condition that incoming transactions only approve tips. After all, how would one know that a transaction, which one believes to be a tip, has not received an approval from someone else a fraction of a second ago?

Back in 2015, Sergey Ivancheglo and I spent a lot of time trying to figure out how to *force* nodes to behave in a certain way (e.g., to only approve tips). We considered some complicated rules that nodes would have to follow in order to get their transactions accepted by the system. However, nothing of that sort would work well in practice. Not only would those complicated rules lead to difficulties in honest nodes having their transactions accepted, but they would also open possibilities for attackers to interfere with the system. Then finally, we decided to stick to just one absolute rule: each transaction approves two previous transactions. The IOTA protocol itself does not enforce selection of any particular transactions, nor does it require approval according to any other set of rules. IOTA in this sense is *truly* open because one is free to accept whichever transactions one wants.

This made the system essentially *free*. Due to the small number of "hard" rules, actors would consider behaving in "natural" ways. Our role was then merely *proposing* a set of "principles" (such as the Markov chain Monte Carlo tip selection algorithm described in [3,4]) that are *voluntarily* accepted by the nodes, and that make the "society" of IOTA nodes function reasonably well. In a way, we (as designers of the system) are benevolent advisers, and nothing more. The papers [2,3] argue that the actual "principles" in place are already quite reasonable.

So, what are these "natural" node behaviors? One example is when a node has a neighbor which repeatedly misbehaves (e.g., by sending lots of spam or "bad" transactions) - it is only natural to cut the connections to this neighbor or censor it in some other way. Conversely, if you, for some reason, *trust* a certain entity or individual, it is then also quite reasonable for you to give more weight to transactions originating from them. There is also the idea of *local modifiers*: that nodes of the network can interact with the ledger in different ways, depending on information *locally* available to them, see [5]. For example: if a node sees from its local point of view that something suspicious was suddenly inserted into the ledger, then it can voluntarily give those suspicious transactions a lesser weight (as they could be one of many attacks of the type "*do-something-secretly-then-broadcast*"). The nodes are also free to form coalitions with other nodes they trust, for example, by using a consensus algorithm to decide which transactions should be accepted and which should not.

The main concern in the adoption of blockchain is its inherent scalability problem [2], where transaction throughput is effectively capped at maximum block size divided by block interval. Nowadays, Bitcoin achieves a maximum throughput of 7 transactions per second (TPS). Some solutions, such as Ethereum, offer a slight improvement but ultimately experience the same limitation. *In theory* there is no such limitation in IOTA. So far, the maximum TPS rate achieved on the main net was around a hundred, with internal tests showing a throughput of several thousand TPS. An additional feature of IOTA is that it uses quantum-resistant signature schemes; this is important because in IoT environment there will be devices that should work for years unattended, and so extra care should be taken against possible future advances in cryptography and computing. Also, as a special protecting measure, currently the IOTA network relies on a transaction finality device called the Coordinator, which is maintained by the IOTA Foundation; there is a lot of ongoing research on designing a safe Coordinator-

free network.

Finally, I would like to conclude that, as human society adapts itself to changing circumstances, the system that we build today will continually learn from the external world and evolve to defend itself against adversaries and free riders. This flexibility is allowed by the unique freedom that the open IOTA protocol provides to any node joining the Tangle, with the added benefit of the entire system improving its robustness and security as the network grows.

Bibliography:

[1] M. Nati, et al., “Toward trusted open data and services,” Internet Technology Letters. Wiley. https://doi.org/10.1002/itl2.69 (https://doi.org/10.1002/itl2.69)

[2] Croman, Kyle et al., “On Scaling Decentralized Blockchains”, International Conference on Financial Cryptography and Data Security, 2016.

[3] S. Popov, *The Tangle*. https://www.iota.org/research/academic-papers (https://www.iota.org/research/academic-papers)

[4] S. Popov, O. Saa, P. Finardi, *Equilibria in the Tangle*. https://arxiv.org/abs/1712.05385 (https://arxiv.org/abs/1712.05385)

[5] S. Popov, *Loctal Modifiers in the Tangle*. https://www.iota.org/research/academic-papers (https://www.iota.org/research/academic-papers)

**Serguei Popov** is a research mathematician (https://scholar.google.com.br/citations?user=z62rjg0AAAAJ) working in the field of Probability Theory and Stochastic Processes. He graduated from and attained his Ph.D. at the Moscow State University under the supervision of Professor Mikhail Menshikov (https://en.wikipedia.org/wiki/Mikhail_Menshikov). Around 20 years ago he moved to Brazil to do a postdoc, and then progressed to professorship first in the University of Sao Paulo, and then in the University of Campinas (http://www.ime.unicamp.br/%7Epopov/). Serguei began his interest in cryptos in late 2013 when, after stumbling upon an article about Bitcoin, he became an avid reader of bitcointalk.org (http://bitcointalk.org) and discovered an innovative project called Nxt. He achieved notoriety in the Nxt community after publishing a short note with calculations on the block generating process in Nxt (a revised and expanded version of these notes can be found here (https://ledgerjournal.org/ojs/index.php/ledger/article/view/46)). Together with the founder of the Nxt and other people from the Nxt community, he co-founded IOTA in 2015.

Editor:

**Dr. Qinghua Lu** is a senior research scientist at CSIRO, Australia. Before she joined CSIRO, she was an associate professor at China University of Petroleum. She formerly worked as a researcher at NICTA (National ICT Australia). She received her Ph.D. from University of New South Wales in 2013. Her research interest includes architecture design of blockchain applications, blockchain as a service, model-driven development of blockchain applications, reliability of cloud computing, and service engineering. She has published more than 70 peer-reviewed academic papers in international journals and conferences. She is an IEEE member and serves on the Program Committees of a number of international conferences in blockchain, cloud computing, big data and software engineering community.

Join our Blockchain Technical Community and receive our Technical Briefs by email.

Subscribe Now (https://www.ieee.org/membership-catalog/productdetail/showProductDetailPage.html?product=CMYBLK776)

**Article Contributions Welcomed**

IEEE Blockchain Technical Briefs Submission Guidelines (EasyChair) (https://easychair.org/cfp/IEEEBTB1)

If you wish to have an article considered for publication, please use the EasyChair submission link above. If you have any questions, contact the Managing Editor at blk-editor@ieee.org (mailto:blk-editor@ieee.org).


(/images/files/pdf/best-of-ieee-blockchain-technical-briefs-2018.pdf)

Read the top five most popular IEEE Blockchain Technical Briefs articles of 2018.
Read more (/images/files/pdf/best-of-ieee-blockchain-technical-briefs-2018.pdf) (PDF, 731 KB)

**Past Issues**

September 2019 (/technicalbriefs/september-2019)

June 2019 (/technicalbriefs/june-2019)

March 2019 (/technicalbriefs/march-2019)

January 2019 (/technicalbriefs/january-2019)

December 2018 (/technicalbriefs/december-2018)

September 2018 (/technicalbriefs/september-2018)

July 2018 (/technicalbriefs/july-2018)

**IEEE Blockchain Technical Briefs Editorial Board**