All publications

Cryptocurrencies Without Blockchain? Learn More About Directed Acyclic Graphs (DAG)

#Blockchain

5 min read

Share this blog

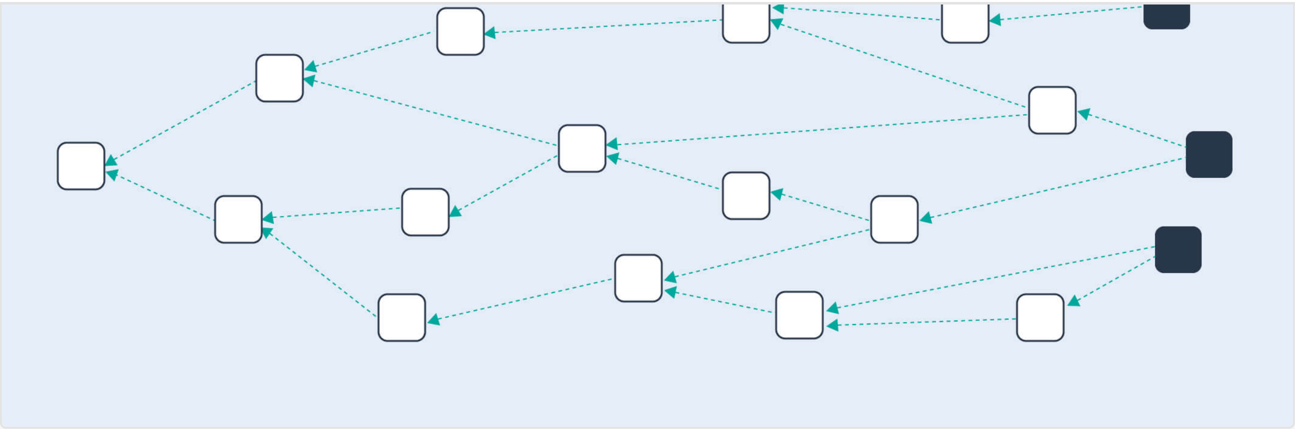
Scaling a blockchain has proved to be a daunting, complicated task. Bitcoin, a trailblazer for all digital currencies, has been a stagnant, low-throughput network for years for this very reason.

Currently, there are many initiatives circling around the crypto space that are aimed to enhance Bitcoin's (and other platform's) TPS. Some experts motion to have the block size increased, others want the processing time on the network to be reduced. There's a great deal of debate as to which variable should be changed and, given how resentful the Bitcoin community is to any modifications, there's no telling when the issue will be tackled.

Some projects, however, offer a more radical approach to remedy blockchain's problems: they've built completely new networks which do not use the blockchain data structure at all. The likes of IOTA and Byteball, which have already made waves in the crypto space, are set to redefine how cryptocurrencies are hosted. Instead of blockchain, they're seeking to implement something called Directed Acyclic Graph (DAG).

Today, we'll provide a brief overview of what is DAG, how the directed acyclic graphs work and describe, in detail, what IOTA and Byteball are trying to achieve by using it.

What is a DAG (Directed Acyclic Graph)?



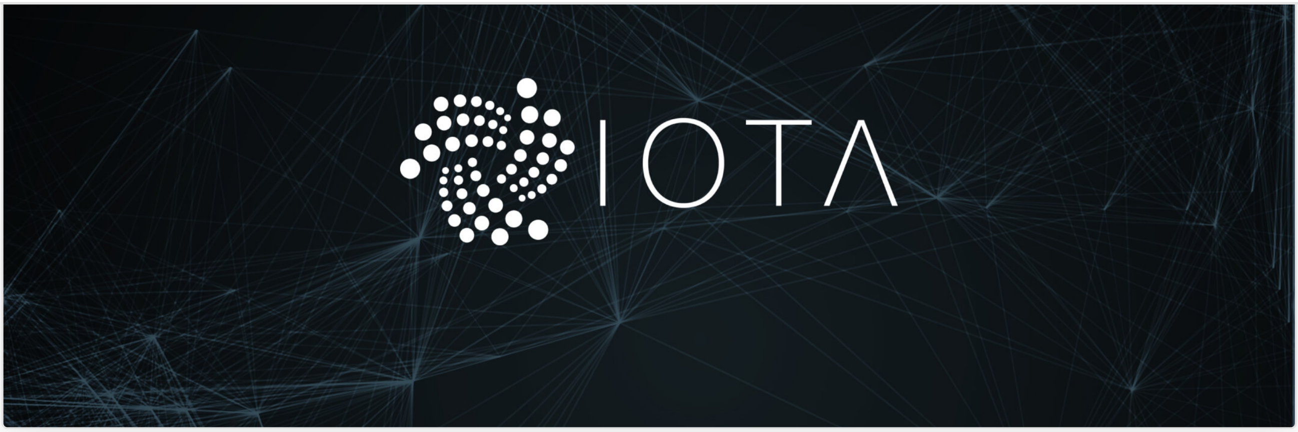
As far as data structures go, Blockchains can be thought of as simple linked lists. Each entry on Bitcoin or Ethereum (or other networks) is put on top of the previous one to which it holds a reference. That's how we get a linear sequence of digital events that we call a chain.

Blockchains allow one to track down any record stored in a ledger's history, but their sequential structure is also what hinders significantly their transaction throughput; the flat list nature of blockchains is the biggest bottleneck for their ability to scale.

Well, a DAG operates differently. This data structure resembles a flow chart where all points are headed in one direction. You can compare a Directed Acyclic Graph (DAG) to a file directory structure where folders have subfolders that branch into other subfolders and so on; they are tree-like.

The word acyclic just means that no node in the graph can reference back to itself; it can't be its own mother node.

How does IOTA use DAG (Tangle)?



The first crypto project we must mention when talking about DAG is IOTA. This “new generation” cryptocurrency is set out to eliminate completely the concept of a miner’s fee.

As you know, there are currently different roles for Bitcoin and Ethereum users; some submit transactions and others approve them. The fees are essential to such heterogeneous system as there’s always a need to incentivize validators to write to a blockchain’s history and secure the network.

Using DAG (which IOTA calls the Tangle), IOTA is able to assign the same exact duties to its every member; all the users on the network are both issues and transaction validators at the same time.

To have a transaction verified by IOTA, one has to approve two previous transactions (and ensure they’re not conflicting). Also, one needs to attach a tiny amount of proof of work as low difficulty computations are needed to prevent spam on the network.

This removes completely the need to pay fees to miners and thus opens up the possibility to execute microtransactions which could be worth as little as a few cents.

Besides, IOTA’s DAG data structure allows for the network’s easy scalability. Everyone is participating in reaching a consensus and, therefore, the more people are using IOTA, the faster the network becomes.

Apart from assets, the network allows attaching data to transactions; it has the potential to enable swift machine-to-machine transactions. Initially, IOTA was designed specifically to serve as a backbone for the Internet of Things (hence the

All of this indeed looks very promising.

IOTA drawbacks

IOTA has its flaws as does every breakthrough technology. Some of the most common concerns people have about it include the following:

IOTA is using **its own cryptographic algorithm**. The majority of the world-renowned cryptographers look with suspicion upon the proprietary algorithms that haven't been subjected to thorough scrutiny. Any project that rolls out its own crypto is considered shady. On account of that, IOTA has always been criticized as being potentially vulnerable. On September 2017, MIT issued a report which uncovered a serious weakness in IOTA's system. The project has patched the issue since then, but its trustworthiness has been shaken nonetheless.

Currently, IOTA has **a central point of failure**. As it doesn't take a lot of resources to mount a 34% attack on IOTA (equivalent to a %51 attack on Bitcoin), the network has a temporary centralized element – the Coordinator node ("Coo") – to prevent malicious activity. Every transaction goes through Coo in order to be validated and, therefore, at this point, a centralized entity is directing the path of the IOTA's DAG tree. This also results in the network's being slow. According to the founders, The Coordinator node will be rendered obsolete once the network generates enough organic activity to be able to evolve unassisted. However, there is no way to prove these claims until the platform (without Coo) has been tested in the wild.

What is Byteball?

The second famous blockchainless cryptocurrency we'll discuss is Byteball. It, too, utilizes a tree-like DAG data structure but, unlike IOTA, it is not set to operate without transaction fees (nor is it trying to get rid of centralization).

Byteball has its own coins bytes and is operated by 12 witnesses which validate each transaction on the network. These nodes are no doubt trusted by the developers and have uncovered their real-world identities. They will be held accountable in case some dishonest activity occurs.

Byteball is different from IOTA in other ways too – it presents a ton of additional features. It offers native smart contract functionality and a conditional payment platform (which is nowhere near as advanced as EVM), a messaging system, private transactions through a specialized currency blackbytes, and even a chatbot.

That said, Byteball is not perfect. Some people take issue with its 12 witness consensus structure. Though a clever approach to mitigating spam and preventing a 33% attack, this solution does come at the cost of decentralization which most crypto enthusiast are not comfortable with. 12 people operating the network makes Byteball look more like a privately owned small company than a public network.

If IOTA removes its coordinator node (thus providing complete decentralization) and Byteball keeps its current consensus system unmodified, the prior will surely become a way more appealing DAG-based cryptocurrency.

Conclusion

opinion, there's still a lot of improving to do for the developers. Technology evolution – the process of uncovering and patching issues – is what made Bitcoin and Ethereum the robust platforms they are today. IOTA and Byteball are destined to follow the same path.

Like the article? Would like to learn more about blockchain tech? Reach out to our expert your free consultation right now!

Other publications by Rostyslav Demush

Share this blog

Ivan Kohut

Chief Technology Officer

Ask our expert

Related service

Other publications

How IoT and Blockchain Help Secure Food and Pharmaceutical Cold Chains

by Rostyslav Demush September 17, 2019

Blockchain Dapps: the Opportunities They Bring and the Obstacles They're Facing

by Rostyslav Demush November 7, 2018

The Future of Ethereum: An Overview of Casper, Plasma, and Sharding Initiatives

by Rostyslav Demush July 13, 2018

Perfectial Group Offices

Perfectial Services

info@perfectial.com