Weiss Cryptocurrency Ratings

WCY-062019

IOTA gets a technology upgrade

by Juan Villaverde on June 20, 2019 at 5:46 pm EST (2019-06-20)

Our ratings are updated weekly. For the latest list, click here.

IOTA gets technology upgrade; Nano faces three challenges.

by Juan M. Villaverde

I can think of no pair of cryptocurrencies that better illustrate the trials, tribulations, challenges and successes than IOTA and Nano; the former making positive strides in its evolution, while the latter fails to achieve its lofty goals.

I'll begin with the good news at IOTA. Then, I'll move on to the bad news at Nano.

IOTA's Long Road to a Technology Upgrade

IOTA aspires to be a crypto network in which payments can be made securely, and, more importantly, no individual or group can have special access or control.

This is a high standard that even Bitcoin fails to fully measure up to, since a handful of big-foot miners control most of the computing power on the Bitcoin network.

To avoid this problem, the IOTA team designed a non-blockchain ledger in which each network participant is equal to all others.

Instead of using the traditional Proof-of-Work consensus used by the likes of Bitcoin and Ethereum … or even the more modern Proof-of-Stake approach of EOS and Cardano … IOTA participants simply have to validate two prior transactions before broadcasting their own.

Problem: Such an open, decentralized design can be vulnerable. For example, what's to prevent bad actors from flooding the network with fake transactions, all validated by other fake transactions?

IOTA's "solution" was to create a central "Coordinator" (run by its founders) that determines which transactions are valid and which are not. Trouble is, this effectively replicated the role of a central bank with final authority over all transactions — a cure worse than the disease.

Mindful of this, the IOTA team promised to get rid of the Coordinator — a project they cheekily christened "Coordicide."

In a recently published paper, we got a glimpse of how they might achieve this: In essence, they plan to do it via an elaborate series of upgrades to the algorithms that comprise the IOTA consensus mechanism. One by one, these upgrades are designed to neutralize every possible attack that might render the network vulnerable once they kill off the Coordinator.

One of these upgrades is especially interesting. It's Shimmer, the name given to a new mechanism that will replace the Coordinator — so network participants can vote on what the real transactions are.

The procedure is a bit complicated, but if you're a participant, here's basically how it works:

Step 1. You vote on what you think happened.

Step 2. You look to see how your peers voted.

Step 3. You adjust your vote, taking into account what the majority thinks.

Step 4. You go back to step 1 and start all over again.

After several rounds of this, a consensus emerges on how to resolve a potential conflict.

Overall, we believe IOTA's upgrades are a step in the right direction, and the theory behind them is solid.

But will they work in the real world? Or, are there more subtle ways a malicious actor could exploit the network after Shimmer replaces the Coordinator? Still too soon to say.

The fact is, potential vulnerabilities to attack are notoriously difficult for even seasoned cryptographers to anticipate. Why? Because it's always hard to map out a defensive game plan before you even know what the enemy looks like. Ultimately, only real-world testing will reveal just how robust IOTA's new measures actually are.

Despite this uncertainty, we acknowledge the progress made and have upgraded Iota's technology score.

The IOTA team is among the best in the world. By moving beyond Proof of Work and Proof of Stake, they have sought to create an entirely new and unique form of distributed ledger technology (DLT): Where neither miners nor validators exist. Where all players are equal. All with no central clearinghouse or authority. And all with near-infinite scalability.

If they could actually achieve these lofty goals, IOTA might be the one of the most secure, most decentralized, and fastest DLT on the planet. And even if they fail to do so, the developer community will have learned valuable lessons from the experience.

Regardless of how this turns out, we're pleased to see the progress thus far. And we will certainly keep you posted on IOTA's evolution going forward.

Tech/Adoption Grade: B+

Risk/Reward Grade: D

Overall Weiss Crypto Rating: C+

NANO — a tall promise of radical decentralization and scalability betrayed

Like IOTA, Nano is a designed to be a distributed ledger that's not strictly based on blockchain. It was conceived strictly as a payment system with transactions strictly peer to peer, settled directly between remitter and receiver.

The way it's supposed to work, every network participant has his own mini-blockchain. The participants keep their own records of all the transactions they were involved in, whether remitting or receiving. And it's all recorded with a data architecture that Nano developers call "block lattice."

In theory, the concept is brilliant: Both remitters and receivers are empowered to keep a record of their own transactions. And since they're the only ones aware of their transactions, the system design is extremely decentralized.

Plus, it would also be an innovative way to scale: Unlike the vast majority of cryptos, the entire ledger does not have to process all activity on the network, and that makes it a lot easier to speed things up.

In actual practice, however …

Nano Faces Three Vexing Challenges

To create a cryptocurrency network in which each user efficiently and fairly verifies other users — all without central coordination — may be a worthy goal. But we believe Nano developers underestimated how truly hard it is. So, when they ran into unexpected roadblocks, they chose a series of band-aid solutions. And this has come back to haunt them. Here are three prime examples of the vexing challenges that have emerged:

Challenge #1. Vulnerability to cheating.

You ask: If only remitter and receiver are required to be aware of a transaction — with no one else overseeing it — isn't it possible that these two parties could collude to cheat the system?

You're damn right it is! Indeed, without anyone overseeing, you should also ask …

> **What would stop a bad actor from double-spending?** A Nano user could spend the same amounts repeatedly, without anyone being the wiser.
>
> **What would stop a bad actor from forging his account balance?** The network would not be able verify that a particular user actually has the funds he's attempting to spend.

A number of crypto projects, especially those that don't use blockchain, have wrestled with these issues, and the reason is clear: Without a blockchain for transparency, developers are pressed to come up with some other creative set of rules to prevent cheating.

This is why, as we discussed earlier, IOTA relied on a Coordinator for so long and only recently began to map out a plan to phase it out. Separately, it's also why another non-blockchain crypto we've reviewed extensively, Holochain, has no consensus at all, simply trusting each member of the community to police every other member they interact with.

How does Nano deal with this problem? By adding a layer of delegated Proof of Stake (DPoS).

But therein lies the dilemma: Nano had little choice but to establish a group of validators (which it calls "Representatives") to verify all of the activity on the ledger. And as we typically see in Proof-of-Stake solutions, token-holders vote for candidates to fulfill that role. The validators then use the tokens that have been delegated to them to vote on the validity of transactions.

If this sounds a lot like plain-vanilla DPoS, it's because it IS plain-vanilla DPoS.

To make matters worse, Nano doesn't limit Representatives to a small handful — the mechanism most DPoS cryptos use to accelerate processing speeds. Quite to the contrary, it has no cap on the number of Representatives; and currently, there are already 210 of them. Result: Processing speed is only about 300 transactions per second.

Challenge #2. Validators can't get paid.

All transactions on the Nano ledger are free, and all the tokens that will ever exist were created on day one.

Again, in theory at least, this made sense for a strictly peer-to-peer network; it made it lightweight and cheap to use. Moreover, if there are no validators, why bother issuing new tokens to reward them? So, it all *seemed* to fit together nicely.

But that neat construct crumbled when Nano tried to patch up the system with the added DPoS layer. So now, it does have validators. But with no new token issuance and no fees on the ledger, how in the heck are the validators going to get paid for the work they do?

Oops. The fact is they don't get paid. And that leads us to …

Challenge #3. Back to Semi-Centralized Control

Since they can't get paid, validators who are voted in have no incentive to run a node. In fact, only folks with a vested interest in the network have any motive for keeping the network running.

Who might those people be? You guessed it! None other than the Nano founders themselves.

End result …

> **Only three accounts control the overwhelming majority of Nano tokens. This gives them a huge controlling stake. They do whatever they want, and no one has standing to oppose them.**

When developers get in over their heads

Let's step back for a moment and look at what's happened here:

Nano was conceived to be one of the most decentralized ledgers on Earth. But a series of challenges and ad-hoc patches have reduced it to a semi-centralized ledger, run by just three big account holders.

It started off by promising a radical, innovative approach to decentralization, peer-to-peer transactions and scalability (based on its "block lattice"). It all sounded cool when they said it. But in actual practice, it was pie in the sky. And now Nano has effectively admitted defeat, retreating back to an approach that's same old, same old.

What a far cry from the promise it once had!

Summarizing our models:

Technology: On paper, Nano looks almost like an ideal payment network. It supposedly offers feeless transactions. And its block lattice concept was ingenious. But in its current implementation, it has become just another run-of-the-mill DPoS ledger with limited functionality. It cannot accommodate advanced smart contracts. And it has no incentives to reward validators, which creates a serious issue with centralization.

Adoption: Network activity isn't too bad, especially since Nano is a feeless system. There's also some tech and development work going into it, but nothing special.

Tech/Adoption Grade: D+

Investment Risk/Reward: There was initially lots of hype when the Nano token was first launched. But that enthusiasm has long since fizzled. Today, it trades in line with the rest of the crypto markets.

Risk/Reward Grade: D+

Overall Weiss Crypto Rating: D+

Had it lived up to its initial promise of near-infinite scalability and radical decentralization, Nano would be one of the best cryptos we've seen. But as it presently stands, it is wholly unremarkable.

Best,

Juan

Weiss Cryptocurrency Ratings
4400 Northcorp Pkwy, Palm Beach Gardens, FL 33410, USA
email: contactus@weissinc.com | phone: 877-934-7778 | Editor: Juan M. Villaverde.

provide a total picture of position results, and past results are no guarantee of future performance. For more details, see our terms and conditions at https://weissratings.com/help/terms-and-conditions Employees may sometimes own investments discussed in this publication, provided they abide by our Personal Transactions (PST) policy, designed to avoid even the appearance of conflicts of interest or the potential for unfair advantage.

.

Delivery of your issues: To prevent this e-mail newsletter from getting swept up by an overzealous spam filter, please add our "From" address (weisscryptocurrencyratings@eml.weissratings.com) to your address book. Click here for instructions.