IOTA ($MIOTA) Analysis

Myles Snider, Kyle Samani, and Tushar Jain

January 23, 2018

Disclosure: Multicoin Capital does not have any position, long or short, in IOTA.

Introduction

IOTA is a digital currency project that aims to be the backbone of the internet of things (IoT). It is touted as having a “post-blockchain” architecture. While IOTA shares some similarities with many blockchain projects, its design does not include blocks or a single, linear chain. Instead, it is based on a concept called Directed Acyclic Graph (DAG). While IOTA is not a blockchain, its DAG is still a public, permissionless, distributed ledger. Because of its unique structure, it offers some advantages over traditional blockchains.

SUMMARY

Background

IOTA was first conceptualized in 2014 and later founded in 2015 by David Sønstebø, Sergey Ivancheglo, Dominik Schiener, and Dr. Serguei Popov. Several of the founders were working on a hardware startup with an IoT focus when they began to see the limitations of current options for IoT payments. They created IOTA as a solution to these problems.

The initial IOTA supply (2,779,530,283,277,761 IOTA) was distributed in a 2015 token sale that raised 1,337 BTC (~$584,000 at the time) for the development team. The IOTA supply is fixed, as there are

neither mining rewards nor inflation. The project is currently developed and managed by a Berlin-based non-profit called the IOTA Foundation.

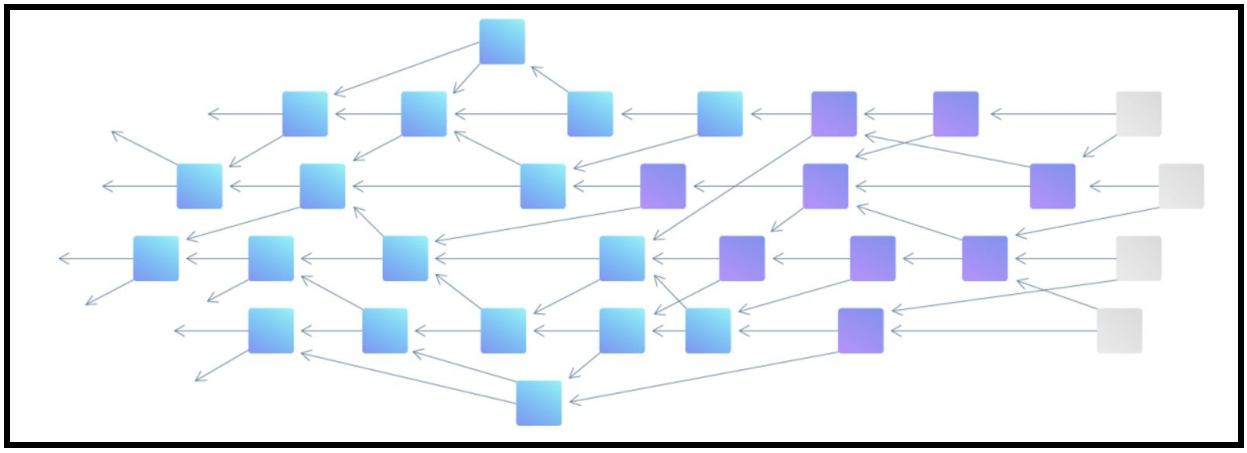
Features

The Tangle

IOTA implements The Tangle, which is a DAG.

- A graph is a network of nodes that are connected (in the case of IOTA, by referencing one another's transactions). These connections are called edges.
- An acyclic graph is one that does not loop; by moving from node to node along the edges, one will never come back to a previously encountered node. Each edge moves from a previous node to a later node.
- Finally, directed means that the connections between the nodes only move in one direction.

The combination of all three of these properties means that the network itself forms a structure of nodes and relationships that eventually converge. These properties can be mathematically proven, which allows the network to create a loosely structured ordering of transactions and to prevent double spends without dedicated miners, blocks, or a single chain.



A visualization of the Tangle

In IOTA, nodes and miners are not separate entities; instead, every node that generates a transaction must also confirm two previous transactions by performing a small proof-of-work (PoW). Users and miners are one and the same. Users are the nodes of the graph, and the confirmations of previous transactions form the edges. While transactions in IOTA don't require users to pay any transaction fees, the small proof-of-work serves the same anti-Sybil attack mechanism that fees serve in other systems.

Having a set of miners separate from users of the network can be dangerous. Miners have the ability to censor, front-run, and cheat users, and they may even have economic incentives to do so. IOTA eliminates these problems because all users act as validators, and they randomly select a subset of transactions to validate. Censorship and front-running wouldn't work, since those transactions would quickly be validated by other users.

IOTA works as follows: When a user wishes to generate a new transaction, she must first sign the transaction inputs with her private key. Then, her wallet uses a Markov Chain Monte Carlo (MCMC) selection algorithm to select two "tips" (unconfirmed transactions in the tangle) which she must confirm. Because not every node has the same state of the tangle at all times, two different transactions may confirm the same tip. The MCMC is not actually enforced at the protocol level, but the IOTA team has published research on Tangle equilibria even in the presence of "selfish tip selection." In order to have the newly generated transaction added to the tangle, the user must perform a small PoW to validate the two randomly selected tips. Once those have been validated, the user's new transaction is added to the tangle as a tip, where it waits until it is confirmed by another transaction. This process repeats in perpetuity.

As in Bitcoin, IOTA transactions become more likely to be included in the canonical ledger as time goes on. In Bitcoin, this involves waiting for a certain number of block confirmations (usually 6). In IOTA, this is done differently. A user can determine the confirmation level of her transaction by running the MCMC algorithm. If the algorithm is run N times and the transaction is confirmed M times, M of N is the probability that a randomly selected tip has a direct path to your transaction and thus is the probability that the transaction will be confirmed by the entire network. Those accepting IOTA as payment are free to determine the probability with which they are comfortable accepting a transaction as final. Time to acceptable finality should get shorter as the network grows, since more transactions will be confirming previous ones. Currently, transactions tend to be confirmed within a few minutes.

No Transaction Fees

As stated earlier, IOTA transactions don't include explicit fees. The requirement of performing work in order to generate a transaction can be seen as a fee, but the distinction is important. Since IOTA is primarily aimed at being a solution for micropayments, eliminating transaction fees is essential. Transaction fees can make micropayments unfeasible. Bitcoin was lauded early on by many as a solution for micropayments on the internet, but high and unpredictable fees have made this next to impossible today. Instead of trying to structure fees in such a way that they are consistently low or more predictable, IOTA does away with transaction fees entirely. With IOTA, a set of machines could send a stream of payments to another, each less than 1 cent, without having to calculate or pay any transaction fees. If a payment of 1 IOTA is sent, then exactly 1 IOTA is received.

Scalability

IOTA's unique design should, in theory, allow it to scale as it grows. Transactions can be processed in parallel, and since each transaction confirms two previous transactions, the time to confirmation decreases as more users join the network. Because IOTA has no blocks, it is not limited by block size to including only a certain number of transactions in each time period. However, this architecture only scales if there are a sufficient number of full nodes in the network.

Decentralization

In IOTA, there is no concept of miners or validators that are separate from users, as there are in blockchains. Instead, each and every user acts as a validator every time they send a transaction. This is intended to solve a few problems. The first is that users and validators have the exact same set of incentives, since the two groups are actually one and the same. Users are validating others' transactions each time they send a transaction, and since there are no block rewards or transaction fees, there is no incentive for validators to compete.

Because decentralization is often measured by how many parties control validation of transactions, IOTA at scale could, in theory, be far more decentralized than almost any blockchain, whose block production tends to centralize with economies of scale. One issue with IOTA is that, because there are no fees or block rewards, there is no incentive for users to run a full node. Right now most wallets are light clients that connect to a full node running the IOTA IRI, which performs the MCMC for light client users. Some of IOTA's past network issues have been blamed on a lack of full nodes, and these issues may get worse as more IoT devices, which are too small to run full nodes (and possibly even too small to perform the PoW), join the network.

Malicious actors are also incentivized to execute a Sybil attack to gain control of a majority of validating power and execute a double spend attack. IOTA is particularly vulnerable to these types of attacks until the network has reached a scale large enough to make such an attack unfeasible. For this reason, the network currently relies on a centralized, closed-source "Coordinator" (Coo) run by the IOTA Foundation. The structure and implications of the coordinator will be explored later in this analysis.

Quantum-Resistance

Another one of IOTA's features is its future-proof integration of quantum-resistant hash-based signatures instead of elliptic curve cryptography. Specifically, it uses Winternitz signatures.

Note that this is not unique to IOTA. The Ethereum and Cardano communities are moving towards including quantum-proof encryption in their protocols.

Use Cases

IOTA aims to be the backbone for the financial system of the IoT. Additionally, it also has integrated other features like secure messaging and a data marketplace. These features are all part of the future machine economy envisioned by IOTA in which millions of machines exchange data and payments in real time. This could include anything from an electric car paying a charging station to weather sensors worldwide selling their data to scientists working on predicting weather patterns.

IOTA's main feature that makes it suitable for the internet of things is its lack of payment fees. While there are many theoretical use cases for such a system, **IOTA has not yet found a real product-market fit**. The "use cases" section of the IOTA documentation is sparse and unspecific, saying "The primary focus area is obviously the Internet of Things, especially in areas such as Smart Cities, Infrastructure and Smart Grid, Supply Chain, Transportation and Mobility." It is not clear whether any of these examples require a steady stream of payments instead of a single upfront payment or a "tab" that can be settled periodically.

In some cases, two parties that do not trust one another will not want to exchange payment upfront or at the end; sending a stream of payments could allow either party to back out of the transaction at any time without losing a significant amount of money. The total addressable market for low-value transactions that require a stream of payments rather than discrete payments is currently quite small and likely does not present enough of a hurdle to justify users' switching costs.

It is possible that this market expands in the future as internet-connected sensors begin to sell data or as new business models like micropayment-enabled mesh networking gain traction. Even in those cases, IOTA will have to compete with layer-two blockchain solutions like Lightning Network, Raiden, and probabilistic micropayments, as well as other fee-less blockchains like EOS.

Challenges

While the core mathematical ideas behind DAG-ledgers like IOTA are compelling, the promise of IOTA relies entirely on proposed future features with significant technical challenges. This is the case for many experimental crypto projects, but the difference between IOTA's current implementation and its proposed features is especially stark.

The Coordinator is Highly Centralized

IOTA currently relies on the use of a centralized coordinator (Coo) that is run by the IOTA Foundation and managed by a multi-signature account of its members. The coordinator's code is not open-source. The coordinator is described as a form of "training wheels" for the network that will be removed once the network is large enough that attacks become computationally unfeasible.

The Coo is a node that makes a transaction every minute. These transactions are called milestones, and they serve as valid reference points for others using the network. They are essentially snapshots of the network's state that can be trusted as valid. As long as one's transaction is directly or indirectly referenced by a Coo transaction, then it can be considered valid. While there are limits on what the Coo can do (it can't, for example, create IOTAs out of thin air), it is a central point of failure for the network. **Further, because transactions must be confirmed by the Coo in order to be considered valid, IOTA is neither censorship resistant nor decentralized in its current form.**

The reason for the Coo is that the network is not currently large enough to prevent attacks, since a malicious actor could still relatively easily gain control over 34% of the network, allowing them to create invalid transactions that still get referenced by others. An attacker would simply have to create a certain number of transactions (and do the appropriate number of validations) each time period that amounted to more than ⅓ of the total network transactions during that period. Because there are no transaction fees in IOTA, the only cost to attack the network is the cost of the computing power.

Another major issue with the Coo is that the IOTA team has not provided clear guidance about when exactly the Coo will be shut down. Nor have they given a scale for how large the network needs to grow before it is self-sustainable. The IOTA team initially gave a tentative date of summer 2017, but the Coo is still up and running.

Specifics about the functioning of the Coo are hard to find in official IOTA documentation. The dev team has claimed in various posts on Reddit, Slack, and Twitter that attacks on the network are unfeasible even in its current state, positing that spam attacks or attempts to flood the network actually benefit the network by increasing the number of confirmations. They also claim that a 34% attack would require more than just sufficient computing power. This begs the question of why the Coo is even needed in the first place. Further, if spam transactions actually help the network, there does not seem to be any reason why a small PoW is required on transactions. The team has claimed that IOTA is 100% decentralized, even with the Coo. As such, it is unclear why the Coo is necessary and also why the Coo should need to be removed in the future.

Despite the team's claims, some potential attack vectors have been identified:

- A double spend attack in which the attacker partitions the network into two sub-tangles, and then uses a majority hash power to give the invalid sub-tangle more weight.
- A double spend attack by the Coordinator itself.
- Another double spend attack based on control of majority hashpower.
- This discussion of selfish network usage and network convergence.
- Even with a large network, some suspect that the hashing power of many small IoT devices will not be enough to withstand an attacker with large computing resources.

Finally, the IOTA network has suffered in the past when the Coo has been temporarily shut down due to an attack or bug. This happened in October, and the official wallet (which only accepts transactions that have been confirmed by the Coo) was unable to confirm transactions for a period of several days. Given that Bitcoin and Ethereum have had nearly 100% uptime for years, this is highly alarming. Through decentralization, crypto networks are designed to never go down.

IOTA also required exchanges to halt deposits and withdrawals while the issue was being resolved. The team claimed that the network itself didn't halt and that users who weren't using the official wallet could still transact. This is hard to verify, since almost every user was using the official wallet. Further, because the attack put some IOTA users' funds at risk, the IOTA team decided to take custody of the at-risk funds and later required users to reclaim their balances—compromising even the appearance of trustlessness.

While bugs are inevitable, the IOTA team has not been clear about whether this issue was caused by an attack or a bug, and what role the Coo played in the ability to take control of users' funds. The fact that this was possible at all is a major red flag and further emphasizes the fact that IOTA is not a decentralized network.

Hardware Requirements

In order for IOTA to reach its full potential, certain hardware changes will be required for IoT devices participating in the IOTA network. As the IOTA team describes, a Curl hasher will be a required component of hardware devices in order to allow them to perform the PoW necessary to generate an IOTA transaction. The team describes this as a "trivial matter" and says that this will become a part of the standard hardware stack as IoT devices require more decentralized ledger connectivity. However, they may be putting the cart before the horse. This could easily become a chicken-and-egg problem; IOTA can't grow to its full potential unless these hardware changes are made, and hardware companies won't be incentivized to add this new hardware unless IOTA becomes the standard for IoT payments and data sharing. IOTA's go-to-market strategy is dependent on its own success and there is no backup plan.

Major Concerns

Network Usability

One of the issues with IOTA is that is has experienced several sustained periods of network downtime. In fact, when we first purchased IOTA to test out the functionality ourselves, we were unable to withdraw our IOTA from the exchange because of network issues. Although exchanges have, at times, suspended Bitcoin and Ether withdrawals, this has been a recurring issue for IOTA. In fact, the Github issues for IOTA reveal consistent problems with unconfirmed transactions, missing funds, and the inability to reclaim funds held by the Foundation.

As noted before, the network became unusable following the temporary shutdown of the coordinator. Several "spam attacks" have halted the network, at least according to users on Reddit and Github. One attack was blamed on a lack of full nodes; IOTA team members claimed that the network was working perfectly during this time (see comments on this article), while users on Reddit claimed the opposite.

Another attack that occurred in early December resulted in users being unable to confirm transactions and possibly even stopped all network activity:

- Reddit discussion of the spam attack
- Community members asking for spammers to stop
- IOTA devs confirming that a spam attack is happening
- Github issue about unconfirmed transactions during this time

Almost every decentralized ledger has seen times of limited network usability. This has happened on Ethereum during certain ICOs and during peak-Cryptokitties when the network was operating at capacity. However, this issue appears to happen much more frequently in IOTA, and there are far more discrepancies with wallet balances. It has also proved difficult to determine which periods of network unusability were caused by attacks and which were caused by bugs. For IOTA, this distinction is important. The IOTA team has claimed in the past that spam attacks actually strengthen the network, since they increase throughput, but elsewhere (including the links above) they have denied this. Given the issues that spam attacks have caused, it is unclear how the network will be able to handle these attacks (or even times of extremely high throughput) in the future.

IOTA has had major issues with user experience that have resulted in users losing funds. For example, several million dollars' worth of IOTA tokens were recently stolen from users who used malicious

online seed generators. Since randomness generation is a key feature for seed-based wallets, it seems like a poor decision for IOTA to delegate this process to users rather than offer it built into the official wallet software. In fact, at one point the official IOTA wallet had a seed generator, but this was removed by the developers with no official explanation.

Cryptography and Software Vulnerabilities

Perhaps the most concerning development regarding IOTA was a report published by Neha Narula, Director of the Digital Currency Initiative at the MIT Media Lab, detailing critical flaws found in the hash function used by IOTA. Narula explains the concept well:

> *A cryptographic hash function takes an arbitrary amount of input and produces unpredictable output with a fixed size. The idea is that given an output, it's very hard to find an input that maps to that output, and given an input and output, it's very hard to find another input that maps to the same output. When two inputs map to the same output, that's called a collision. Being able to easily find collisions means the cryptographic hash function is broken.*
>
> *Cryptographic hash functions are important for cryptocurrencies because usually a transaction is hashed before it's signed. So if you can break a hash function, you can potentially break signatures as well, meaning that the mechanism used to determine if a transaction is a valid and authorized spend is broken. The mathematical integrity that cryptocurrencies provide hinges on this relationship being secure.*

Narula and her team were able to easily find collisions in IOTA's Curl hash function, which had been custom-built by the IOTA team because they used ternary, rather than binary, notation. This violated what has been called the golden rule of building cryptocurrencies, which is "don't roll your own crypto." Projects should only use well-tested cryptographic libraries that have been peer-reviewed. While we certainly acknowledge that some situations require researchers to explore the bleeding edge of novel cryptography, the vulnerabilities found in IOTA's function show clearly that they should have followed this golden rule. When this vulnerability was revealed, the team switched from Curl to Keccak-384 (SHA-3) for cryptographic signing.

Poor decisions are one thing. However, how teams respond in the face of adversity is another. The IOTA team's response to this situation is simply appalling.

The team gave several (sometimes conflicting) explanations on Reddit, Medium, and personal blogs before finally publishing what appears to be their definitive response (this is part 4 of a series of articles on the subject, released nearly 6 months after the incident). In the article, the team claims that

the possibility of collisions was a deliberate design choice meant to prevent the IOTA software from being used by bad actors. The use of the (centralized, closed-source) Coordinator prevented IOTA transactions from being affected by this vulnerability, but the IOTA team knew of its existence. They claim that any good-faith open-source project that attempted to use IOTA's source code would discover this vulnerability and change the hash function, but that bad-faith projects would not (likely due to negligence).

The IOTA team claimed that their intention was to prevent users from losing money and being scammed by bad projects. This is an absurd claim that not only completely violates the ethos of the open-source community, but also begs the question of how the IOTA team would have reacted to another project using their source code without being aware of the vulnerability. Allowing a known vulnerability to persist that allows users to lose money is entirely unacceptable.

We don't believe the IOTA team's rationalization of this situation. Individual investors are free to make their own assessments of the ethical implications of the IOTA team's actions. We consider their behavior to be a showstopper, and thus consider IOTA un-investable. Furthermore, Sergey Ivancheglo's explanation of the vulnerability on Reddit *refused to acknowledge* whether additional, known defects were present in the IOTA software. Instead, he argued against the semantics of the word "defects" and then suggested that disclosing any additional ones publicly would render them useless against "scammers." This is a terrifying reality for a multi-billion dollar network: the IOTA team may have access to exploits that allow them to control the IOTA network with no accountability whatsoever.

Conclusion

The Directed Acyclic Graph (DAG) architecture presents an interesting, novel mechanism to organize a distributed ledger. While we don't believe that DAGs make blockchains obsolete, they offer certain features and tradeoffs that may make them a better fit for certain kinds of decentralized applications. Like many technologies in the distributed ledger space, DAGs are in their infancy and remain largely untested. We look forward to seeing continued research into this sector in the future.

While IOTA was one of the first major projects to build a DAG instead of a blockchain, we find that the approach taken by the IOTA team presents many reasons to be highly concerned. While DAG-based systems may form an important part of the future of the crypto ecosystem, we have reservations about the DAG implementation of IOTA. Specifically:

- The explicit centralization (through the use of the Coo), with no set date for decentralization
- Multiple instances of network downtime

- The team taking control of users' funds with no accountability or governance
- The decision to knowingly include one (or more) vulnerabilities in the code
- Contradicting explanations from the core IOTA team about these vulnerabilities
- A lack of clear use cases. To date, we've yet to see more than a handful of use cases that require machine-to-machine micropayments that can't be accommodated by probabilistic micropayments or state channels.

We wish the IOTA team all the best and hope that they are able to execute on their vision, as it represents a compelling step forward for the economy of the IoT. However, given the current state of the IOTA network, the substantial technical risk, and the overwhelming evidence of serious flaws in the protocol, we believe that IOTA is sharply overvalued at current prices. At the time of publication, IOTA's market cap is $6,807,664,212, and it is ranked 11th in terms of total market cap.

Disclosure:

As of the publication date of this report, Multicoin Capital Management LLC and its affiliates (collectively "Multicoin"), others that contributed research to this report and others that we have shared our research with (collectively, the "Investors") may have long or short positions in and may own options on the token of the project covered herein and stand to realize gains in the event that the price of the token increases or decreases. Following publication of the report, the Investors may transact in the tokens of the project covered herein. All content in this report represent the opinions of Multicoin. Multicoin has obtained all information herein from sources they believe to be accurate and reliable. However, such information is presented "as is," without warranty of any kind – whether express or implied.

This document is for informational purposes only and is not intended as an official confirmation of any transaction. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, and reflect prevailing conditions and Multicoin's views as of this date, all of which are accordingly subject to change without notice. Multicoin has no obligation to continue offering reports regarding the project. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances.

Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. This report's estimated fundamental value only represents a best efforts estimate of the potential fundamental valuation of a specific token, and is not expressed as, or implied as, assessments of the quality of a token, a summary of past performance, or an actionable investment strategy for an investor.

This document does not in any way constitute an offer or solicitation of an offer to buy or sell any investment or token discussed herein.

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond Multicoin's control. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on all tokens discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.