Intro to Fintech: IOTA Cryptocurrency

Finance 3807

Palak Bhatia, Neville Fernandes, Jeffrey Glupker, Vinit Nair, Benjamin Richman

Introduction

Though great strides in technology have been made in recent years – and additional advancements are presumed to be right around the corner – no one knows for certain what the future holds. While newer innovations like mobile phones, cloud computing, and connected devices have certainly pushed the boundary of what's possible, our culture is anxiously awaiting a time when autonomous vehicles, delivery drones, and smart cities are the standard.

Imagine your car being able to transact directly with parking meters, charging stations, and toll booths; or being able to easily ship energy from rooftop solar panels to your neighbor through a connected wallet. This is what IOTA dreams to be: the machine-to-machine (M2M) transaction protocol for the connected world. Aptly named based on the "Internet of Things", IOTA certainly has a lot of promise. And the public has taken notice, pushing IOTA's market cap over $5 billion as one of the top-10 cryptocurrencies despite not yet reaching its true potential.

Like many cryptocurrencies, demand plays a big role in determining IOTA's value; however, unlike many others, there is no monetary value from mining tokens, but intrinsically from the maturation of its infrastructure. IOTA is a pluralized way of transacting by using a directed acyclic graph (DAG) methodology over a linear blockchain. Transaction fees are eliminated because the issuing nodes also act as approvers, with the proof of work (PoW) itself serving as the primary cost. With only a small amount of time and computing power required, the speed and scalability of IOTA increases, becoming highly attractive for M2M transactions. Strength in numbers becomes a profound truth as the network grows, and as more of these M2M transactions get posted and verified, the network becomes more and more secure.

What is IOTA's DAG?

IOTA is implemented using a structure based on a directed acyclic graph (DAG), operating more as an interconnected web than a linear blockchain, defined as follows:

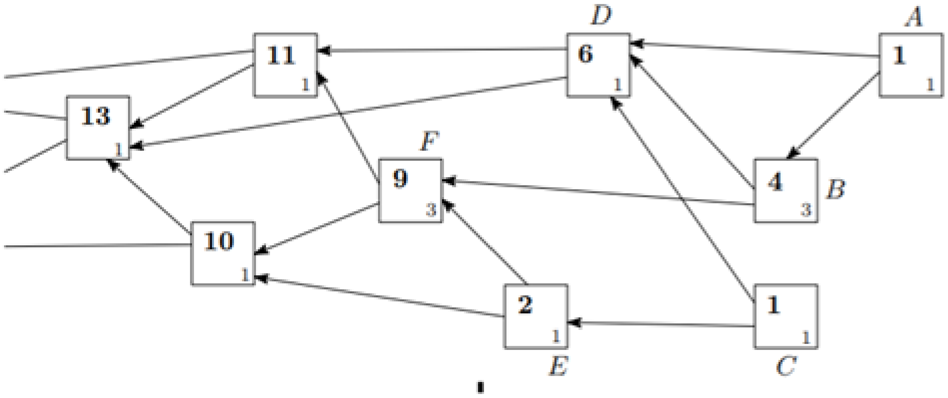
Directed: The connections between the vertices are directional: A > B is not the same as B > A.

Graph: A structure consisting of vertices, that are connected to each other by edges.
Acyclic: "non-circular": by moving directionally across the vertices along the edges, you will never encounter the same vertice twice.

IOTA’s custom implementation of the DAG is known as the *Tangle*, the architecture behind their distributed ledger and protocol. This was started by a single genesis token which created all of IOTA’s tokens - nearly 2.8 quadrillion of them. The genesis token then distributed these tokens out several other “founder" addresses, expanding out the Tangle while making the tokens available for exchange. Transactions on the Tangle remain anonymous: though every user privately holds a single seed address, they produce a public address off of that seed for each and every transaction. This feature allows for increased privacy, and is a differentiator from many other cryptocurrencies. While each user knows which public addresses belong to them, an observer on the Tangle will not be able to string together a user’s entire history.

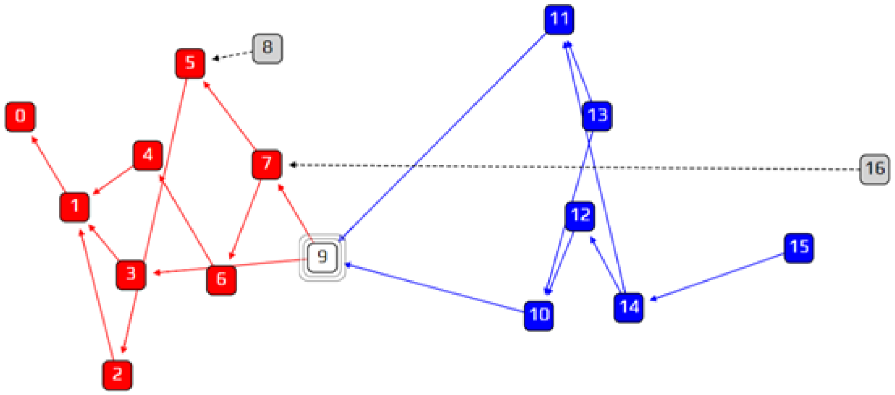
As another unique differentiator, each site on the Tangle represents a single transaction; transactions are both issued and approved by nodes. For a node to issue a valid transaction, it must select two other transactions to approve, adding two new edges to the graph. As long as the two selected transactions are not conflicting, and the approval wouldn’t result in a negative balance for an address, they can go through. Finally, the node must solve a cryptographic puzzle to find a nonce, such that the hash of the nonce combined with data from the transaction meets a particular standard.

Because the Tangle is directional, transactions on the right are always the most recent, with those that have not yet been approved known a *tips*. In the figure below, transactions ‘A’ and ‘C’ are tips, with ‘A’ directly approving transactions ‘D’ and ‘B’ and indirectly approving transaction ‘F’, while ‘C’ is directly approving ‘D’ and ‘E’ and indirectly approving ‘F’. New transactions can approve any prior transaction, however certain features of the Tangle attempt to encourage that new transactions approve tips and that the number of tips remains relatively constant, which in the long run will be better for IOTA.



Notice there are two numbers assigned to each transaction. The smaller number in the lower right is the transaction's *own weight*, which is proportional to the amount of work the issuing node invested in solving the cryptographic puzzle. The larger number in the upper left is the transaction's *cumulative weight*, which is the weight of all transactions that have directly or indirectly approved that transaction, plus its own weight. This is the most important measure in the Tangle, as large cumulative weights indicate higher trust in that transaction being valid. It also plays a significant role in transaction approval strategy. A tip that approves old transactions rather than new ones - a practice that does not help the network - is called a *lazy* tip; cumulative weights are meant to discourage this**.**

An example of a tip approval strategy involves deploying a *walker*, which starts at the genesis and moves toward the tips by jumping to one of the transactions that approved it. In the figure below, when the walker reaches transaction 7 it would chose to jump to transaction 9 over transaction 16 because 9 has a higher cumulative weight (there are more transactions approving it). Another important measure to note is *depth*, which is the length of the longest reverse-oriented path from the genesis to a tip. In the figure below, tips 13 and 15 have greater depth compared to tips 8 and 16 and would thus be more likely to be approved.



The walker does not, however, always directly move towards the heaviest transaction. The rule for deciding the probability of each transaction being the next step in a random walk is governed by the *Markov Chain Monte Carlo* technique. In a Markov chain, each step does not depend on the previous one, but on a rule decided in advance. Nodes can set a parameter, **α**, that determines whether it is biased towards selecting transactions with higher weights, or selecting transactions randomly. When α is zero, the walk is totally unbiased. In simulations, keeping α near zero is shown to keep the number of tips relatively constant, which is ideal. When it is high, the walk is biased towards heavier transactions, which causes tip volume to grow linearly. This is not ideal, since a high number of unapproved transactions will cause the Tangle to grow vertically rather than horizontally.

Transaction Confirmation & Security

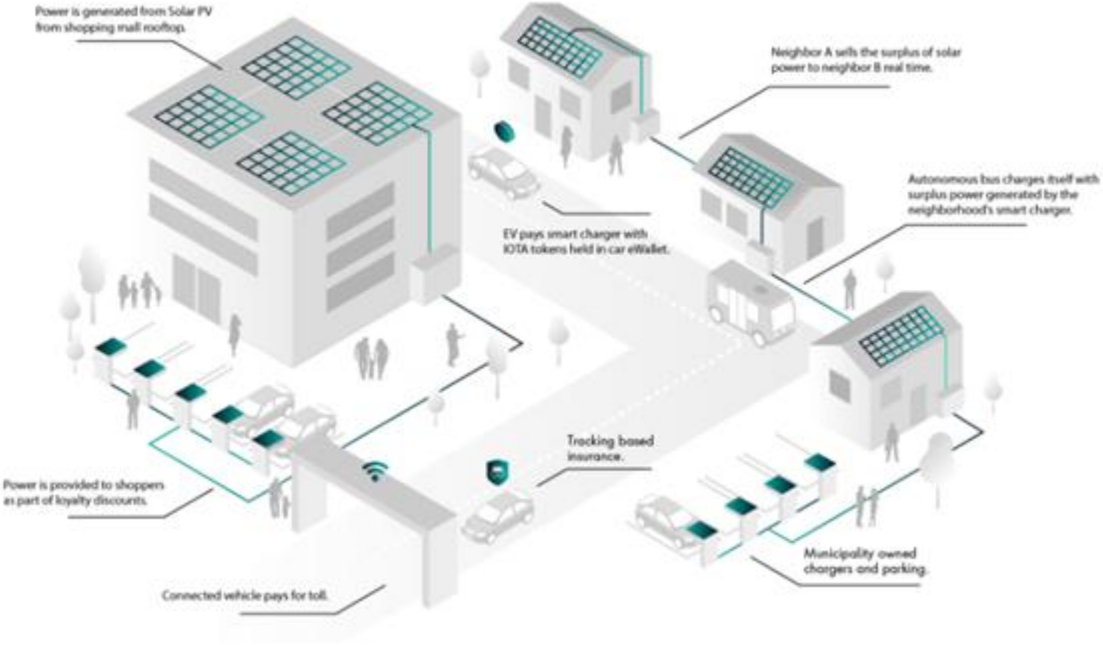
Creating a secure protocol is the top priority for IOTA, and a number of built-in features ensure that the Tangle is safe. When tokens are awarded for miners, it creates a singular incentive for nodes acting as such. IOTA has done away with this by first, creating all tokens at the genesis and second, requiring that all nodes act as both issuers and approvers. Rather than financial gain from mining tokens, the incentive becomes network security. Issuers want their transactions to be approved; since issuers must also approve two transactions, it is in their best interest to validate transactions that they trust to be accurate.

The double spending problem can be solved by weighted walk approach explained above. In case of a double spend, a node would have to approve only one of the two transactions depending on the cumulative weights. The measure of a transaction's level of acceptance by the rest of Tangle, or the percentage of tips that approve a transaction, is called *confirmation confidence*. Once a transaction attains high levels of confidence, it can be deemed safe and genuine. As an additional security measure, the *coordinator (COO)* acts as an overseer of the entire Tangle as a consensus mechanism employed by IOTA. Every two minutes, the COO issues a milestone transaction, and all transactions approved by it are considered to have a confidence of 100%. This is one of the key preventative measures against a concentrated double spending attack.

Use Cases

Already active is the IOTA Sensor, a platform for organizations or individual users to sell or purchase access to data streams using IOTA tokens. Current corporate data streams include InnoEnergy Sweden's weather station data in Stockholm, ISMB's humidity-temperature-sensor in Turin, and a few dozen other environmental and test data streams. Individuals can also sponsor their own data streams. This could provide cheaper, more accurate, and quicker access to many geographic variables, as well as placing data in the hands of landowners.

An in-development use case is the creation of an IOTA wallet within cars. Cars with native IOTA wallets synced to the user's account can accomplish machine-to-machine transactions that ease use, speed up transactions, and potentially revolutionize the ride-sharing future. The image below shows an example of an electric car automatically subtracting IOTA tokens to pay for charging. Car wallets could be to automatically pay for tolls or parking, supplement car insurance information, or charge users for ride shares based on usage. By connecting machines through transactions, cars become a central hub of an IoT-based infrastructure.


Power is generated from Solar PV from shopping mall rooftop.
Neighbor A sells the surplus of solar power to neighbor B real time.
Autonomous bus charges itself with surplus power generated by the neighborhood's smart charger.
EV pays smart charger with IOTA tokens held in car eWallet.
Tracking based insurance.
Power is provided to shoppers as part of loyalty discounts.
Municipality owned chargers and parking.
Connected vehicle pays for toll.

Comparison with a Primary Competitor: Byteball

There are a few, but not many, currencies that compete with IOTA either by using the same DAG technology (IoT Chain, Byteball) or by alternatively using the blockchain (Nano, Waltonchain). Of these, the closest in form and purpose is Byteball, but unlike IOTA it serves as both a currency and a platform for smart contracts. Byteball has been able to use more original features of the DAG, most notably their use of the *main chain*. Rather than participants serving a dual role as issuers and approvers, users on Byteball must simply confirm the existence of 1 previous transaction. Members of the main chain, a group of up to 12 third-party witnesses, give final transaction approval. While this validation system is limited to a small few trusted entities, it also results in Byteball having steep transaction fees to employ these witnesses, and also depends heavily on the size of the transaction. Once confirmed, Byteball's transactions are final, another differentiator from IOTA, in which the Tangle can contain *orphaned tips*, or those that no longer become indirectly approved by new transactions and thus remain at a constant cumulative weight.

Challenges

First and foremost, IOTA is irrelevant without pervasive use of IoT in society's future, everyday lives. For widespread adoption, the IoT devices that IOTA depend on must meet popular need for user friendly experiences, affordability, accessibility, and immediate impactfulness. While major corporate sponsorships with companies like Volkswagen and Bosch provide hope, there is no assurance of a product that meets these requirements.

Another class of concerns result from preventing attacker nodes in the case of conflicting transactions (link). Attackers can either try to set up a parasitic chain (essentially a subtangle, whose weights are equal to those of the 'honest' tips in the Tangle) or conduct a splitting attack (partition the Tangle into two branches and balancing the two so that one of them is approved). If the attacker then puts their malicious transactions in both, then a part of these transactions could possibly be approved. There is inherent protection against this - (i) sites from the malicious subtangle are less probable to be selected because the main tangle can have larger increases in cumulative weight than the subtangle, and (ii) the attacker has to know the topology of the network or needs awareness of a large number of recent/future transactions (making it difficult to establish/maintain the balance required). But both these attack strategies have at least a non-zero probability of the malicious transactions being approved, and if enough of them are, then that can lower trust in the Tangle.

Unlike many decentralized cryptocurrencies, IOTA is run by a body known as the IOTA Foundation. This foundation operates the COO, whose private key is closed source and hence, can’t be verified by the community as to how secure the private key is, or whether it has been compromised by a bad actor. The IOTA Foundation also deployed its own cryptographic hashing function, called Kerl, without having it reviewed for security and accuracy by other cryptographic experts in the field (link). This oversight has already led to a known bug; while that has been corrected there is still some unsureness as to the current level of security.

References

1. Sergui Popov, “The Tangle”, February 9, 2018. https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf

2. Laurence Tennent, “Improving the Anonymity of the IOTA Cryptocurrency”, October 9, 2017. https://assets.ctfassets.net/r1dr6vzfxhev/6StLLAy9b26eyUG8SGQqeu/e30c20f91e77e54d88b7644658912c7d/Improving_the_Anonymity_of_the_IOTA_Cryptocurrency.pdf

3. B. Kusmierz, “The first glance at the simulation of the Tangle: discrete model”, November 6, 2017 https://assets.ctfassets.net/r1dr6vzfxhev/2ZO5XxwehymSMsgusUE6YG/f15f4571500a64b7741963df5312c7e7/The_First_Glance_of_the_Simulation_Tangle_-_Discrete_Model_v0.1.pdf

4. https://byteball.org/Byteball.pdf