Increasing the available time for receiving devices to act on incoming Iota Transactions

UP721426

Abstract

Iota is a new data transfer layer and transactional settlement for the Internet of Things. It is based on a new distributed ledger (like Blockchain) called the Tangle, which allows fee-less micro-transactions, and even nano-transactions. It rethinks the current implementations of Blockchain, and overcomes some of the current limitations. Iota aims to be the new backbone to the internet of things, and may be the missing piece for the machine economy to fully emerge.

Ultimately, Iota is trying to act as a data transfer protocol for the Internet of Things, such as MQTT, but with the added benefit of being able to transfer value as a cryptocurrency. The downside to Iota is that it is slower than these traditional data transfer protocols. The scope of this paper will be looking at how Iota and MQTT can be utilised together, to gain the benefits of both. It will research and implement an experiment to test if it is possible to couple MQTT and Iota together, to use MQTT to send data with fast transfer speeds, while linking to a slower Iota value transaction. This would theoretically allow the receiver device to act on, or prepare for, a transaction of value before it arrives.

Introduction

Iota is a relatively new technology that allows the transaction of value. It is a cryptocurrency, much like Bitcoin. The difference is that it utilises a Directed Acrylic Graph, rather than a Blockchain. This new peer-to-peer technology allows the transaction of value with *zero fees*, which in turn, allows extremely small micro and nano-transactions to be conducted between devices. Iota aims to be the new backbone to the Internet of Things.

There is, however, a problem that arises due to the way Iota is implemented to conduct these transactions of value. To allow transactions to occur in Iota, much like other cryptocurrencies, there are restrictions in place used to determine 'real' transactions. Currently, this means that Iota is inherently slower than traditional data protocols in the Internet of Things, such as MQTT and CoAP.

This paper proposes a way to implement a possible solution to this problem. The aim is to utilise MQTT, a traditional data transfer protocol, in parallel with Iota. This should give the benefits of fast data transfers through MQTT, while also linking these messages to a transaction on the Iota network. To do this, MQTT messages and Iota transactions will be linked through identifiers embedded in the messages themselves. In theory, this allows the receiving device to act upon an incoming transaction of value before it is received. This would allow Iota to be utilised in time critical systems.

This paper includes an experiment that will measure the amount of time this process saves. This will be determined by the difference in time between receiving the MQTT message and the Iota transaction. This paper will then discuss the advantages and disadvantages to using this solution, and what possible uses it has.

Problem statement

Iota, while providing significant potential benefits by enabling the transaction of value across the network, is currently too slow to use in time critical systems. Any system that requires fast data transfers will be bottlenecked by the Iota network if used as its sole data transfer means. By utilising traditional data transfer protocols alongside Iota, through linked identifiers, this problem could be overcome.

Iota

An R3 article ("Iota Announces", 2017) explains that Iota is an open source non-profit technology that allows companies to explore new business to business models. Technological resources can be a potential service to be traded on an open market in real time. The Iota ledger can settle transactions with zero fees, while also acting as a data transfer and store for sensors.

The technology behind Iota is an open source distributed ledger, also known as a cryptocurrency. 'Full nodes' store all transactions that have ever happened within the Iota network. To create a decentralised design, and prevent double spending and fraudulent transactions, anyone can run a full node. Popov (2017, p.3) explains that to make a transaction on the Iota network, Iota utilises 'proof of work', a process of solving cryptographic puzzles with computer resources. A news release ("What is proof of work", 2017) explains that the mathematical problems being solved are not utilised in any way, and that due to this requirement, resources need to be expended, thus simply creating a way to deter any abuse of the service by limiting how frequently transactions can be sent to the network. By showing that you have completed some proof of work, you gain the ability to make an Iota transaction. This proof of work must be done every time a device wishes to make a transaction.
Popov (2017, p.2) also states that for every transaction made, the device must confirm two other transactions. The combination of these fundamentals together prevents denial-of-service attacks, by limiting the number of spam transactions, and contributes to the overall security of the network by confirming that other transactions are real.

These extra steps make Iota useful as a transaction of value and settlement layer, but too slow for time critical systems. Iota transactions currently take significantly longer than other data transfer means. Traditional data transfer means are measured in milliseconds, an order of magnitude faster than Iota. This renders it not feasible to be used in any system that requires fast data transfers, and not worth the added benefit of value transactions.

Current solutions

As of the time of writing, there are few to no current solutions to this problem. This is because Iota itself was created as a solution to scaling and speed issues of *other* cryptocurrencies. This solution is the natural scaling of the Iota network. Transaction speed is measured as the time it takes between creating a transaction, and the recipient receiving the value. This relies on the transaction being confirmed by the network, as without this, it could still be considered invalid. Ramachandran and Sonstebo (n.d, p.3) mention that due to transaction confirmations being made by other transactions on the network, as the network gains users, the transaction throughput (transactions per second), and security should also increase. Due to every transaction having to confirm 2 other transactions, transaction speeds should also get faster, a correlation with the increase in transaction throughput. In the long term, with mass adoption, this could completely remove or minimise this problem, by making transactions significantly faster.

The problem with this is that it is theoretical, yet to be proven, and will rely on Iota being used by a significant, currently unknown portion of the Internet of Things. More importantly, the proof of work will still have to be completed for a transaction, which is not solved through this natural scaling of the network.

Solution

This papers' proposed solution to the transaction speed problem is to couple the Iota network together with another, more conventional data transfer protocol. Traditional data transfer protocols and middleware are capable of handling transfers of data at speeds much faster than that of the

Iota network. However, they are incapable of conducting transactions of value.

The idea is to link the messages of a traditional data transfer protocol with an Iota transaction using some *identifier*. The identifier could be thought of as a transaction ID or number. It does not matter what this ID is, it simply needs to be consistent across both linked messages. This identifier would be stored in both messages, and will be used to mutually exclusively link the messages once received by the receiving device. The aim is that the traditional transfer protocol message would be received first, and would contain all the information about the incoming Iota transaction. The receiving device could then act on this information *as if* it has already received it, and then confirm later that the transaction came through. This gives the benefit of both fast transfer speeds and transactions of value.

The benefits of doing this are that it cuts out the proof-of-work part of the Iota transaction creation. It is important to note that this in no way increases the speed that the Iota transaction is *confirmed* by the Iota network, and in fact does the opposite. It theoretically increases the time required for confirmation, by replacing the proof-of-work time with extra confirmation time. Essentially what it is doing is lowering the Proof of work time, but increasing the confirmation time. This means the transaction is 'seen' earlier, but has no effect on whether it will be confirmed, or how long that would take. This confirmation time would still rely on the natural scaling of the Iota network, and therefore would allow these two solutions to work in parallel.

MQTT

For the proposed solution, MQTT will be used as the data transfer messaging system that will link with Iota transactions using identifiers in the messages. However, MQTT could be swapped with any other data transfer protocol that best suits the purpose of the system, meaning that this proposed solution is not limited to this data transfer protocol. MQTT uses a publish/subscribe model. MQTT clients publish messages to a broker, which other clients subscribe to. It uses TCP as a transport protocol, and provides 3 levels of QoS for reliable delivery of service (Nitan, 2017, p.2). Just like Iota, MQTT is not designed for device to device communication, but instead for large scale networks, with lots of small devices. This is what makes it useful for the IoT.

Implementation

Unfortunately, challenges were encountered that were beyond the scope of the development of this prototype, which led to the Iota and MQTT parts being developed in different languages and libraries. This is due to Iota being a young open source technology, relying on volunteer developers, and therefore having many out of date libraries. This moved the aim of this paper away from an actual prototype implementation, towards finding a potential speed increase measurement by creating these separate parts, and comparing their speeds.

The MQTT part was developed in C#, using the M2Mqtt library, and the Iota part in Python using the *Pyota* library. The MQTT part creates a message, sends it to an open MQTT node, and then listens to the subscribed topic. The timer was set to start just before the message was sent, and stopped as soon as the subscribed topic listener saw the message. The time difference was used to calculate the time taken for the transfer. This was implemented in a loop, with messages being sent out every 5 seconds, for an hour. This should simulate a IoT device that is constantly transacting with other devices. By running this for an hour, the effect of traffic and fluctuations in bandwidth is limited.

The Iota section was developed the same way. The timer is started just before attempting to add a transaction to the network, *including* the proof-of-work portion. The difference, however, is that the timer was stopped as soon as the transaction was sent. This is because these measurements do not include the *confirmation* part of the transaction, and as stated before, only measures how much quicker the Iota transaction is 'seen' by the receiving device, rather than when it is 'confirmed'. Essentially, it is measuring the time it takes to conduct the proof-of-work for a transaction.

The following section compares the Iota and MQTT speed measurements to get a theoretical speed increase when utilised together in this way, cutting out the proof-of-work.

Outcome

Results

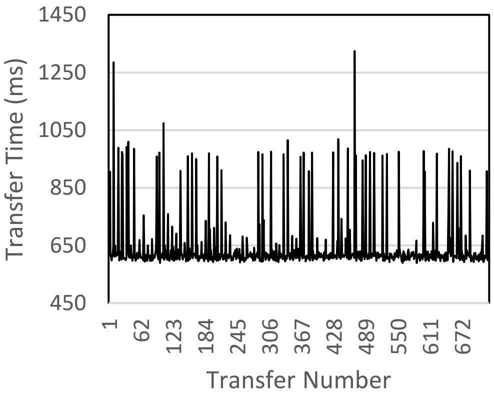

Figure 1 – MQTT Speeds

Figure 1 shows the transfer speeds of MQTT messages, sent five seconds apart for 1 hour. The diagram shows a steady rate, barring semi-consistent anomalies which spike up to around 1 second transfer speeds. The median for these transfer speeds is 612 milliseconds, with a mean of 640 milliseconds.

Figure 2 shows the transaction speeds of an Iota transaction being created and added to the Tangle (Iota network). It is important to note that the time it takes to create the transaction is included. This is because the creation of the transaction, including the proof of work, takes up the bulk of the transaction time.

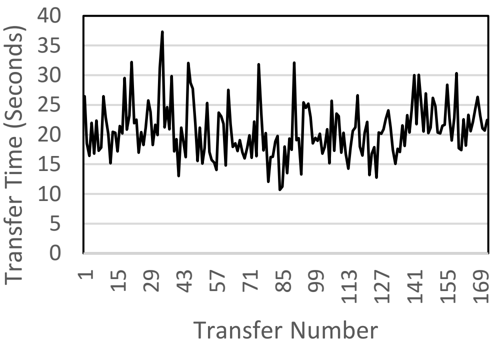

Figure 2 – Iota Speeds

The median of the Iota transaction speeds is 20.4 seconds, and the mean 20.7 seconds significantly more than the 640 *milliseconds* that MQTT messages takes.

A hypothetical potential time saved in transfer speeds can be calculated with the following formula *(1)*, which finds the difference between the means of the Iota transaction speeds and the MQTT transfer speeds respectively;

$$(Mean(Iota\ Speed)) - (\ Mean(MQTT\ Speed)) \quad (1)$$

The outcome of (1) is 20.06 seconds, which represents the difference between the means. This shows that this solution allows a potential average of more than 20 seconds extra time for the receiving device to act on the incoming Iota transaction. This is of course subject to change depending on bandwidth, and more importantly, hardware speeds. However, as both parts were tested on the same machine, this acts as a valid proof of concept and should provide a reliable order of magnitude of gained transaction time.

Analysis

Although saving theoretical 20 seconds in transaction time sounds significant, this solution does come with significant drawbacks. The aim of cryptocurrencies is to allow the transaction of value without *trusting* either party involved, and without delegating this trust to a third party. This solution goes against this philosophy, as it reintroduces trust into the system. The receiving device for a transaction, when using this proposed solution, must trust that the sending device will follow through with the Iota transaction. This, if not resolved, would narrow the use for this system down significantly. It is unlikely that two unknown devices, potentially on different sides of the globe, would participate in this system - as there would be a significant potential to be ‘scammed’ by receiving an MQTT message with false data, about a non-existent or inaccurate Iota transaction.

It would focus the potential of this solution to transfers between *trusted* parties and devices. This may be between two parties that have worked together before, or possibly internal systems within one company/institution. As well as this, it is unlikely that these speed increases are even necessary unless implemented in a time-critical system.

Future work

The most important aspect to be worked on in the future would be fully implementing this solution with identifiers that link the MQTT and Iota transactions together. This would prove the solution is possible, and work as a reference for any future real-use implementation.

It would also be beneficial to research ways in which to remove or validate trust from the system. One possibility is automatic blacklisting of devices that do not follow through with Iota transactions. This could possibly be recorded on the Iota network itself, allowing any device to inherently access this information. This information could be peer-reviewed in a rating system. While not removing trust, it could validate it significantly.

Conclusion

This paper discusses a potential solution to the transaction speed issue within Iota. It proved that this solution could potentially allow receiving devices to see Iota transactions 20 seconds sooner, by utilising a more traditional data transfer protocol. Practical implementations remain unsolved, such as a system to link MQTT and Iota transfers, which are both currently driven by different libraries and languages. The downside to this solution is that it reintroduces trust to the system. This goes against the philosophy that Iota, and other cryptocurrencies, are built upon. Due to this, it is safe to say that a possible implication of the reintroduction of trust into this system could be that the use cases for this solution are a more niche - only a small portion of the overall potential uses for Iota. However, in systems where trust already exists, this solution provides the massive benefit of fast transaction speeds in Iota.

References

- *Iota Announces $2 Million IOTA Ecosystem Fund*. (2017). Retrieved from the Cision PR Newswire website: https://www.prnewswire.com/news-releases/iota-announces-2-million-iota-ecosystem-fund-300457287.html
- Popov, S. (2017). *The Tangle, Iota Whitepaper*. Retrieved from web address: https://iota.org/IOTA_Whitepaper.pdf
- *What Is Proof of Work?* (2017). Retrieved from the R3 website: https://www.r3.com/blog/2017/07/18/what-is-proof-of-work/
- Nitin, N., (2017). *Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP*. Paper presented at the Systems Engineering Symposium (ISSE), 2017 IEEE International. Retrieved from http://ieeexplore.ieee.org/document/8088251/
- Ramachandran, N., & Sonstebo. D. (n.d). *The IOTA Distributed Ledger, A Massively Scalable Replacement for The Blockchain*. Retrieved from web address: http://iotanodes.org/IOTAAdvantages.pdf