MEGAN FRYDEL 2ND OCTOBER 2018

HOW DOES IOTA TANGLE WORK?

With new cryptocurrencies appearing, and disappearing every single day, it is becoming increasingly difficult to know which currencies are worth investing in, and which ones are not.

For those that are just starting out, it can be a somewhat daunting prospect, particularly when you factor in the technological jargon, and concepts that work hand in hand with this type of innovation. IOTA is one of these currencies, and **Tangle is the system that it works on**.

For the uninitiated amongst us, one question we get asked a lot is "how does IOTA's Tangle work", and that is a question we will seek to answer in this article.

IOTA also happened to be **one of the most successful cryptocurrencies of 2017** – the price increased from few cents to almost $5 at times. Hence, the growing interest.

IOTA Explained

IOTA itself is an open-source distributed ledger, otherwise known as a cryptocurrency, and its aim is to **facilitate secure payments and communications** between devices that are a part of the Internet of Things.

Instead of using the blockchain technology as Bitcoin does, IOTA uses a directed acyclic graph and also allows users to transact without incurring any fees – much unlike other cryptocurrencies.

Confirmation and transaction times are **faster than the blockchain**, and the number of individual transactions that the system can process simultaneously is unlimited – a distinct advantage over the sometimes sluggish blockchain. Founded in 2015 by David Sonstebo, Dominik Schiener, Dr Serguei Popov, and Sergy Ivancheglo it has a market capitalisation of over **$3.5 billion which makes it the 10th largest** and most popular cryptocurrency in current circulation

What Is IOTA Tangle?

IOTA Tangle is the name for the platform or system on which IOTA works.

Instead of using a blockchain like most other **prominent cryptocurrencies**, it is replaced with a different concept, which in this case is colloquially referred to as 'The Tangle'.

It is mostly a generalisation of the established blockchain protocol and is known as a type of DAG.

The IOTA Tangle uses the Winternitz signature which is a hash-based cryptography and

is used instead of the usual elliptic curve cryptography or **ECC**.

These hash-based signatures offer much fasters processing times than the ECC signatures – one of the reasons why when it comes to speed, Tangle comes out on top.

In mid-2017, a vulnerability was discovered within the self-designed hash function of IOTA, known as Curl. It was discovered that signatures could be easily forged, but developers quickly replaced the hash function with **Kerl** – a version of SHA-3.

The new hash function operates with ternary, as opposed to binary operations which in turn made IOTA and Tangle a lot more secure.

How Does Tangle Work?

Several core aspects make up Tangle and the way it works. They are not the most straightforward concepts to explain or understand, but let's give it a go.

Scalability

Firstly, Tangle is designed to be scalable, and it operates on the idea that the more people that use IOTA and Tangle, the more transactions are referenced and confirmed.

This also means that as more people use it, the confirmation rates and timings improve, unlike the blockchain which experiences a pretty opposite effect.

The idea is that if you wish to use IOTA and Tangle to send a transaction, you need to **confirm two pre-existing transactions before you may send yours**.

It encourages use and uptake amongst users in the community.

Blockless

Another point is that Tangle does not use blocks and it does not require that the order values of seeds and addresses are kept in the right order. This means that all **transactions can be stored on multiple different devices**, in various locations, in different orders, and even split and mixed up.

When you sync your node, the system just iterates through all of the existing transactions and groups them into their addresses, regardless of order.

Once Tangle has processed all of the transactions, the ledger and addresses will display all of the balances and **all the user must do** is verify that there are no adverse balances amongst the addresses.

This a superb feature which is perfect for use with a distributed ledger where one has numerous devices all linked, or bound together.

Multi-transactions

IOTA and Tangle also give users the benefit of **multi-transactions**.

These are defined as a large number of transactions that are both chained, but that use the same address.

Additionally, these chains are designed so that only the very first transaction has a value while subsequent transactions are assigned a value of zero. This results in a situation where there is no need for any "order" and no need or occasion to skip transactions.

JINN Processors

As mentioned previously, Tangle works with ternary JINN processors as opposed to the typical and more widespread binary ones.

Little is known about them as their secrets are mainly **kept under wraps**, but we do know that they are unique and are set to change the way we interact with the Internet of Things.

They are general-purpose-processors that have the power and capability to **process thousands upon thousands** of transactions per second.

This is due, in part to the fact that unlike binary processors, they can circulate around 0 and + and – which results in a balanced transaction that helps to build an efficient, self-sustaining network such as Tangle.

Tangle vs Blockchain Technology

There are many differences between Tangle and Blockchain, and these can be summarised in a few key areas:

Centralisation of Control

Firstly, when you use something like Bitcoin on the blockchain, the way you acquire coins (unless you are purchasing them) is through **mining**. The process of cryptocurrency mining is complicated and expensive, and those who can afford to do so are doing it en masse.

While Bitcoin is supposed to be decentralised, a sort of monopoly on Bitcoin mining is emerging meaning that a select few have control over not just mining, but **policies, transaction times and more**.

Also as most miners are located in China, this adds additional **political and geographical concerns**, especially when you consider that 75% of mined blocks originate from the same area, from the same few people.

IOTA works by allowing you to make a transaction only after you have validated two pre-existing ones.

Therefore, as you take part in the network, **you are facilitating its speed and efficiency**, and this means that each user can be considered as a miner while still allowing decentralised protocol development.

Obsolete Cryptography

While large-scale quantum computers are not yet a reality, they could be a reality in the very near future.

Should they become a reality, then technology around Bitcoin and the blockchain would be utterly crippled by their deployment which would spell disaster for every currency running on the system, as well as every individual who holds BTC as an asset.

IOTA, on the other hand, uses quantum resistant cryptographic algorithms which are immune to attacks that blockchain projects are susceptible to.

The chances of a quantum attack impacting Tangle, are roughly 1 million times less than the blockchain – a big incentive to investigate Tangle as a viable alternative.

Micropayments

Back in the early days of the blockchain, it was possible to make transactions for a very low fee.This was one of the major selling points of cryptocurrencies such as Bitcoin at the time.

As time has passed and its popularity has grown, so have the associated fees which have made the marketplace inaccessible to many amateur or beginner cryptocurrency adventurers.

With IOTA there are entirely **no transaction fees regardless of the size** (big or small) of the transaction. It's a fundamental part of the appeal of cryptocurrencies and is a huge benefit to many.

Network Connection Limitations

With Bitcoin and most other blockchain based cryptocurrencies, **you need to be connected to the network** to make transactions. This is because the ledger must always be updated to be sure that no double spends are permitted.

IOTA, on the other hand, allows its nodes to operate without the need to be connected to Tangle.

Cryptocurrencies That Use Tangle

It is not just IOTA that uses Tangle to facilitate and record its transaction.

There are in fact several other cryptocurrencies that have realised its benefits and decided to function with it instead of the blockchain.

These include ParagonCoin, and Oyster Pearl, although some others use DAG technology, these are not explicitly using the IOTA Tangle system.

Is Tangle Going to Replace Blockchain?

This is the question on everyone's lips, but it is not one that can be answered easily.

The blockchain has quickly become an integral part of the new financial and digital revolution, and this is not something that can be overcome, or surpassed overnight.

Billions and billions of assets are tied up in the blockchain, and multiple multi-national companies have made significant investments in blockchain technology for businesses, and financial institutions. To pull the plug, or switch to an alternative would be a **dangerous move**, but there is something to be said for Tangle.

Many people have the idea that **Tangle is a new and improved version of the blockchain**.

While they differ in many ways, the argument is that Tangle has improved on the mistakes and errors that blockchain had and that features such as its zero transaction fees will soon far surpass the benefits that the blockchain has to offer.

IOTA and Tangle also need to get **credit for their scalability**.

No one knows yet whether the Blockchain will be able to handle an increase in usage at the current rate, and no one knows what will happen when it decides it cannot take any more. Nobody even knows if that day will ever come, and that creates a lot of uncertainty about its future.

This is not the case with Tangle as we are aware that its **potential for scalability is unlimited** and its unique technique of distributing and decentralising its ledger is going to be the key to its longevity and success.

Another reason why IOTA might be headed only for particular things is that it's so entangled with the Internet of Things. While you might think that this is just another millennial buzzword, it is, in fact, **one of the essential concepts** of recent years.

The IoT is a network of devices and appliances that can connect to a network to exchange information. These can include smart TVs, computers, sensors, toasters, air conditioning units, sat navs, and more. The concept is that the **IoT creates a web of connectivity** which allows devices to communicate with each other and to share information.

IOTA and Tangle are built with this concept in mind as it will allow these devices to communicate and exchange data, as well as facilitate payments and transactions safely and securely.

The benefits that this could have, as well as the fact that the IoT is a growing part of our everyday lives, means that its usefulness surpasses that of just a cryptocurrency, and this is where it could look to surpass Bitcoin.

At this stage, however, **IOTA is in its infancy**, and it would be premature to say that one day it will take over from blockchain. There is no doubt various flaws in its system and concept that need to be ironed out, and as mentioned, Bitcoin is so established now, it is difficult to imagine a world without it.

That said, many believe that Bitcoin and blockchain are just bubbles and that any day now, they will burst.

For those cynical people among us, IOTA and Tangle could well be worth a look.

If you're interested in investing in IOTA, read our guide on how to buy IOTA or signup with Bitfinex.

If you feel like you can add a valuable perspective to how does IOTA Tangle work, feel free to do so in the comments below!

SHARE

MEGAN FRYDEL

Megan is a self-taught blockchain enthusiast. She enjoys combining finance with technology, from a less-techy perspective. BiteMyCoin is her most recent project underneath the umbrella of an international digital marketing agency ANCHOVY.

SHOW COMMENTS ↓