Media Backgrounder
IOTA

Munich, June 2018

Among the proliferation of Distributed Ledger Technologies (DLT) and cryptocurrencies to have emerged recently, the name IOTA stands out as offering distinctive new possibilities for organizations looking to implement Industry 4.0 solutions where IoT (the Internet of Things) is a key component.

The potential IOTA offers to achieve radical efficiencies in manufacturing and supply chains has led Fujitsu to become an advocate of this technology, with Dr. Rolf Werner, Head of Central Europe at Fujitsu, joining the IOTA Foundation Supervisory Council in April 2018, when he noted: "The possibilities of decentralized and secured applications based on IOTA are immense, going far beyond machine-to-machine payment and including, for example, tamper-proof monitoring of the supply chain and secure identity management."

IOTA's most distinctive characteristics derive from the fact that it is not based on Blockchain, which is the best-known example of a Distributed Ledger Technology, where data is multiplied and stored across a network of nodes to provide a high level of data trustworthiness without the need for a central, controlling authority. In the case of blockchain, the ledger is in the form of a linear 'chain' of nodes. New transactions are sent to the blockchain, where they are encrypted before being sent to every node for validation. Every new block is cryptographically linked to the previous block, which makes the chain immutable: any change in one block entails change in every subsequent block on every node.

But blockchain is not the only option to achieve trustworthiness without a central authority and other contenders are emerging, including IOTA, which is based on a DLT called Tangle.

IOTA and the Internet of Things (IoT)

As its name implies, IOTA is a DLT focused on providing secure communications and payments between machines and devices on the Internet of Things (IoT). It was founded in 2015 by David Sønstebø, Sergey Ivancheglo, Dominik Schiener, and Dr. Serguei Popov.

The underlying concept is a mechanism for transferring information and payments in a manner suitable for IoT, where automation is critical, the scale and speed of transactions need to be significantly high and where payments might be tiny or even non-existent. IOTA therefore allows automated transactions between any person or device, including true machine-to-machine transactions and has been designed with a number of features that are specifically geared to the needs of IoT:

- **Faster**: the way in which transactions are validated in IOTA requires much less processing than with blockchain, so that the network can operate much faster.
- **Scalable**: if the growth projections for IoT are anywhere near accurate, then any machine-to-machine transaction system designed for it must be able to absorb extremely rapid growth. IOTA has been designed to actually increase its processing capability as new participants enter the network. The underlying approach is a truly distributed one.
- **Low-cost**: simple data transactions or micropayments would be impractical if the cost of transaction were too high. In the case of IOTA, mining is not required, leading to zero transaction costs.

- **Micro-payment friendly**: With low or zero transaction costs, and a unit value of 1 IOTA currently worth 0.000002 Euro, IoT-based ecosystems can afford to initiate huge volumes of nano- and micro-transactions using IOTA.
- **Off-line operation:** many industrial environments cannot guarantee online status and therefore any DLT aiming for full IoT adoption must be able to operate offline. IOTA offers this, whereas in a blockchain, network participants must consistently synchronize.

Industry adoption of IOTA

Although still early in the development of IOTA, there is already a high level of interest and engagement from key players in IoT, including Fujitsu. Robert Bosch of Germany announced a major purchase of IOTA tokens in December 2017. Bosch said one aspect of its plans for IOTA was its XDK Cross Domain Development Kit, a programmable sensor device and prototyping platform for any IoT use, and which uses IOTA MAM for information and payment transactions. Volkswagen has also announced that it is working on projects involving IOTA.

At Hanover Fair 2018, the world's largest manufacturing fair, Fujitsu demonstrated an IOTA-based audit trail addressing issues such as product counterfeiting issues in the supply chain. The scenario consisted of two manufacturing sites, represented by two robots. Respective information of the single component, including component identifier, timestamp of production, and production information derived from sensors, such as power consumption or temperature, were written to the tangle by the first manufacturing site. The second site only acknowledged the component as being genuine from factory one if the respective information could be found in the IOTA tangle. As Dr. Werner pointed out, this takes IOTA well beyond the scope of a conventional cryptocurrency and opens the door to use cases where the information, audits and instructions transmitted across the network are as important as the transactions themselves.

Why do we need IOTA?

There are several limitations of blockchain which mean it is not necessarily suitable for all business or government processes. The first is the mining process – the way in which new Bitcoins are created. Bitcoin was designed to have a finite limit, beyond which no further Bitcoins can be created, and to be increasingly difficult and expensive to mine as we get closer to that limit. This is achieved by requiring more and more compute power to mine each new Bitcoin, to the point where the investment cost and energy input needed is already beyond the reach of all but the most specialized players. By contrast, all IOTAs have already been created – there is a finite limit of approximately 2.8 PetaIOTAs – removing the mining overhead and energy drain.

The second limitation is the transaction rate – the number of transactions a blockchain can handle per second, measured in transactions per second (TPS). If you think about the volume and speed of retail commerce around the world at any one time, for example, it is obvious that any commercial or industrial blockchain solution needs to be able to handle thousands of transactions per second. Visa's TPS limit is approximately 56,000, whereas Bitcoin's TPS is deliberately much lower, since it requires a high level of compute input to verify each transaction, known as the Proof of Work (PoW). The actual TPS for Bitcoin therefore varies, but is generally quoted as just 7, although a figure of about 18 might be more realistic. Even so, the number is much too low for practical commercial use.

For companies and organizations looking to build private ('permissioned')blockchains for specific use cases, there are work-arounds to increase the TPS. These involve decreasing the compute power required per transaction, by modifying the private blockchain algorithm to increase the number of parallel transactions possible in the ledger. However, the consequence of this approach is a downgrading of security to the point where the blockchain can be modified. Even if this is only possible by trusted participants within a ledger consortium, there is a dilemma for those companies that need to be able to prove the absolute immutability of ledger data.

IOTA is based on a DLT called 'Tangle', rather than blockchain. Tangle maps transactions as a network (or 'tangle'), rather than a linear chain, as in blockchain, and rewards participants for verifying adjacent transactions, as outlined below. This has the consequence of increasing the transaction rate – in fact the more activity within the network, the more participants are acting as validators and the faster transactions can be confirmed.

A third limitation is the cost of making micropayments. With Bitcoin, the miners - basically external data centers that generate new blocks and insert pending transactions – get a 'financial reward', for example, the fee set by the sender of the transaction. The higher that fee is, the more attractive the processing of the transaction for a miner. As a result, very small payment amounts ultimately become impractical, as the transaction fee might be higher than the value of crypto-currencies transferred.

IOTA on the other hand can handle micropayments easily. High transaction fees are completely eliminated by the nature of the Tangle DLT and the value of a single IOTA is low enough to be practical for micropayments. It is also possible to have zero IOTA transactions. Generally, when we talk about the value of IOTA, this refers to a Mega IOTA, of 1,000,000 IOTAs. Assuming a value for 1 Mega IOTA (or MIOTA) of 2 Euro, then 1 IOTA has a current value of about 0.000002 Euro.

The Tangle – a new kind of DLT

IOTA is an example of a 'gossip' communication protocol, which is a procedure based on the spread of information in social networks, and akin to the way epidemic diseases spread. This mechanism means that any data with sufficient weight can be dispersed to the opposite side of the cluster efficiently. Transactions can carry value or data from a car, a cargo ship, or an app on a phone—allowing any device or human to send messages across the globe.

In contrast to blockchain technologies, Tangle does not build a sequence, or chain, of static blocks, each one containing a number of transactions. The Tangle ledger is an example of what computer scientists call a Directed Acyclic Graph (DAG) - a collection of vertices (squares), which are connected to each other by edges (arrows). Tangle is a particular kind of DAG, which holds transactions, usually in the form 'person A gave 10 IOTAs to person B', but also any other kind of information.

When a new transaction joins the Tangle, it is required to choose two previous transactions to approve. Since these may have already been approved, validating them adds nothing to the overall progress of work. Therefore, Tangle has been constructed to encourage participants to work on unapproved transactions, called 'tips'. This overall structure means that no participant needs to see and validate all transactions on the ledger, as they do with blockchain, and this significantly increases performance over the network. Indeed, the addition of new participants, each required to share the load of validation, means that Tangle is highly scalable, with network performance actually increasing as the number of participants and transactions rises.

IOTA's designers have also given careful consideration to potential issues. For example, to resolve possible confirmation delays, while new tips are validated, a recipient needs to check whether a transaction has directly or indirectly referenced all available tips before deciding whether to take action, in the same way that in a blockchain, each new block increases the probability of certainty. In short term Tangle transactions, 100 percent direct/indirect validation may not be realistic, in which case the parties involved need to decide what level of validation – for example, 95 percent - is acceptable.

Another known issue with DLTs is 'double spend', where, perhaps as a result of two participants responding simultaneously to a single purchase request, the purchaser has requested a combined payment level higher than the available balance, which is not permitted under the IOTA protocol. This results in an unstable branch in the Tangle that is subsequently abandoned through an IOTA mechanism called the 'random weighted walk'. Once again, this highlights the requirement for reasonable certainty to arise in the Tangle before actioning transactions.

On the subject of branches in the Tangle, IOTA allows multiple Tangles to exist in disconnected clusters. These have a highly practical outcome in the context of IoT, as they open up the possibility for offline transactions, which is a necessary option in the real-world industrial environments where IoT operates. Invalid transactions in an offline Tangle may, however, prevent all transactions getting accepted when the Tangle is back online.

Data-only transactions currently often account for somewhere between 90 and 95% of the IOTA database growth rate, which means that disk space may quickly run out on smaller nodes. IOTA has introduced local 'snapshots', which reduce the capacity needed for nodes to save the entire Tangle to disk. In the foreseeable future, this process will be automated. One issue that can arise with Snapshot is that transactions with zero credit could be removed, even if they´are relevant to the value of others. In this case, the data has to be restored by using a specific kind of seed management.

Masked Authenticated Messaging (MAM)

Masked Authenticated Messaging (MAM) is an important driver for industry's adoption of IOTA in the context of IoT because it underpins the transfer of encrypted information across the network in a form that allows actions to be taken without human intervention and with authority.

MAM is an experimental module currently under peer review. It is a second layer data communication protocol which adds the ability to emit and access an encrypted data stream, like RSS, over the Tangle, regardless of the size or cost of device. IOTA's consensus protocol (see above) adds integrity to these message streams and the use of smaller messages - such as remote signaling and update coordination - avoid saturation of the network. Due to the fact, that these messages are part of the Tangle ledger, the overall security of the network is improved, increasing the total hash power.

Online resources

- IOTA posts on the Fujitsu blog: http://blog.global.fujitsu.com/
- Follow Fujitsu on Twitter: http://www.twitter.com/Fujitsu_Global
- Follow us on LinkedIn: http://www.linkedin.com/company/fujitsu
- Find Fujitsu on Facebook: http://www.facebook.com/FujitsuICT
- Fujitsu pictures and media server: http://mediaportal.ts.fujitsu.com/pages/portal.php
- For regular news updates, bookmark the Fujitsu newsroom: http://ts.fujitsu.com/ps2/nr/index.aspx

Media contacts

Isabell Horvath
Director of PR,
Corporate Communications, Global Marketing
Tel.: +49 (89) 62060 4419
E-Mail: isabell.horvath@ts.fujitsu.com

About Fujitsu

Fujitsu is the leading Japanese information and communication technology (ICT) company, offering a full range of technology products, solutions, and services. Approximately 140,000 Fujitsu people support customers in more than 100 countries. We use our experience and the power of ICT to shape the future of society with our customers. Fujitsu Limited (TSE: 6702) reported consolidated revenues of 4.1 trillion yen (US $39 billion) for the fiscal year ended March 31, 2018. For more information, please see http://www.fujitsu.com.

About Fujitsu EMEIA

Fujitsu promotes a Human Centric Intelligent Society, in which innovation is driven by the integration of people, information and infrastructure. In the Europe, Middle East, India and Africa region (EMEIA), our 27,000-strong workforce is committed to Digital Co-creation, blending business expertise with digital technology and creating new value with ecosystem partners and customers. We enable our customers to digitally transform with connected technology services, focused on Artificial Intelligence, the Internet of Things, and Cloud - all underpinned by Security. For more information, please visit http://www.fujitsu.com/fts/about/