BearingPoint®

DAG – A potential game changer in the field of M2M communication

DAG – A potential game changer in the field of M2M communication

Table of contents

Executive summary

Applications in the field of machine-to-machine (M2M) communication can become a persistent driver of future growth for many industries. The machine economy offers a way to monetize data streams and create new services. Currently, data warehouses within companies prevent the establishment of a machine economy, as there is no common standard regarding data formats and database interfaces between companies. Furthermore, these so-called data silos are not only inefficient, but also prone to be compromised due to their centralized nature. For these reasons, the exchange of data is still difficult between companies within the same or other industries.

Distributed ledger technologies (DLT) could lay the groundwork to enable a standard for the machine economy. The Blockchain-technology[1] with its prominent example of Bitcoin could be a solution. Even the Blockchain features decentralized and high encoding standards, it lacks scalability for the machine economy and fast services. Although still in an early stage, directed acyclic graph (DAG) technologies, with IOTA as its most known representative, are increasingly promising. DAGs offer the technological platform to enhance decentralized data sharing and therefore services of the future. These services enable new business models based on cross-industrial data. With provided conditions, automated services offer several benefits for companies and customers.

Introduction: IoT and M2M economy

The rise of IoT applications

The internet of things (IoT), with all its areas of application in the consumer industries or the industrial sector, is no longer just a buzz topic in management media but rather a driver of corporate growth. On the one hand, governments and private consortia try to push industrial developments and communication standards to gain comparative advantages, especially in the production industry. On the other hand, customer behavior and following market demand pull commercial developments. Corporate representatives already experienced that the introduction of IoT applications sooner rather than later leads to positive returns within their businesses.[2]

Predictive maintenance, the discipline of forecasting maintenance requirements before major malfunctions, is currently one of the main application fields of IoT within the industrial sector.[3] Another driver of IoT development are connected machines. Machinery that communicates with each other sums up under the umbrella term machine to machine (M2M) communication. The communication is enabled by data exchanges among the machines, allowing for valuable data streams. The amount of data can further be used, thereby generating positive feedback loops for existing services or helping to create entirely new service lines. Industries with a high level of automation, as the car industry, are a good example of such. As a result, M2M communication is becoming a field of high interest across major industries.[4]

[1] This paper gives an overview of some of its properties and comparisons with the Bitcoin-Blockchain. In this paper, the term "Blockchain" will generally refer to the system used in Bitcoin, rather than the large number of variants that have been proposed. Furthermore the "Lightning-Network", a second-layer protocol on the Bitcoin-Blockchain which is currently being tested, is not within the scope of this paper.

[2] See IDG (2018)

[3] See Paul (2018)

[4] See Gartner (2018)

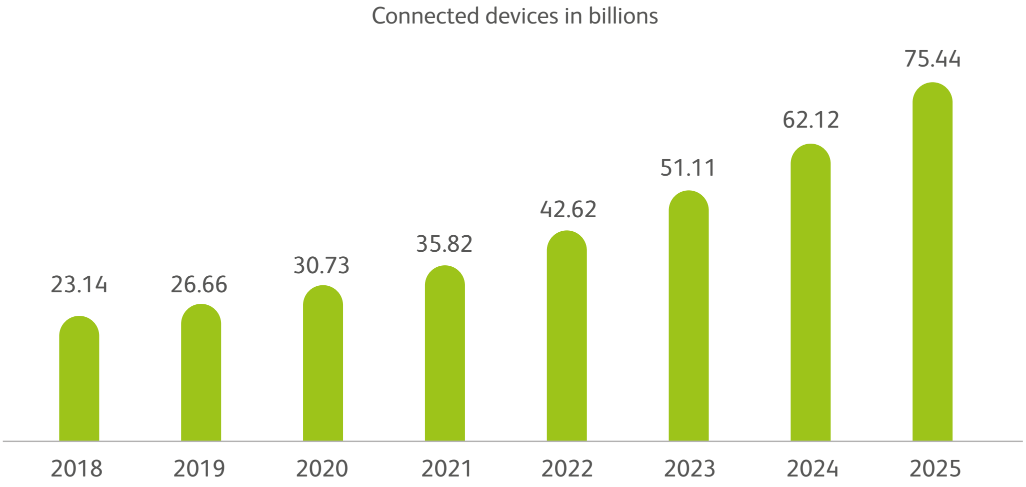


Figure 1: Connected devices 2018-2025[5]

Machine-to-machine applications and predictive maintenance are just two trends contributing to the vast increase in data traffic across industries:

- According to Statista, by 2025 the number of connected devices will have been tripled, as it is expected that these devices will reach a total number of more than 75 billion. Household machines, production plants and any sort of sensors are among some of those devices.
- The increase in devices results in a massive increase in valuable data streams. Sensors and devices record data, allowing a detailed analysis and optimization of existing processes. Moreover, the devices generate additional meta data. IT giant Cisco has already proclaimed the *zettabyte era*[6], stating that the worldwide IP traffic will threefold from 2017 to 2022, which would lead to approximately 4.75 zettabytes[7] (ZB) in 2022.[8]
- Following a perspective until 2025, IDC expects a total data volume (not only IP) of 175 ZB. Moreover, *“nearly 30 percent of the global datasphere will be real-time by 2025. Enterprises looking to provide superior customer experience and grow share must have data infrastructures that can meet this growth in real-time data.”*[9]
- M2M connections are expected to accelerate by 75 percent from 2018 to 2021, increasing from a total of 8 billion connections in 2018 to 14 billion in 2021. IoT is vastly contributing to the trend of increasing internet protocol (IP) traffic and data traffic in general.[8]

[5] Own figure based on Statista (2016)

[6] See Barnett Jr. (2016)

[7] A zettabyte consists of 10^{11} (one trillion) gigabyte

[8] See Cisco (2018)

[9] IDC (2018)

IoT and the rising problem of data security

Although IoT in general and especially M2M solutions are already starting to change businesses and the existing service landscape, there are still some general issues that discomfit decision-makers and to some extinct customers. In a representative survey by the International Data Group (IDG), 44 percent of questioned business representatives rank the topic of security, for example in the sense of unsafe gateways, as the major challenge for IoT/ M2M solutions and implementations, followed by data safety.[10]

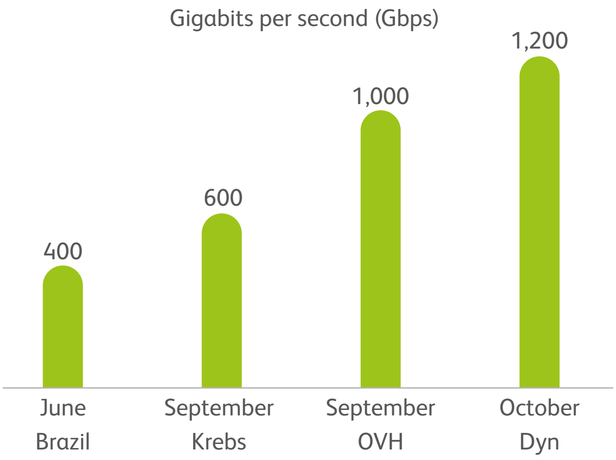


Figure 2: Notable 2016 IoT botnet DDOS attacks[11]

Keeping that in mind, most IoT ecosystems exhibit a centralized server architecture which identifies and authenticates the individual devices as being part of the network. This architecture represents a single point of interest and facilitates the possibility of attacks, for example in the fashion of brute force attacks. That being said, IoT end-devices are directly being targeted by malware, adding the IoT devices to large botnets which follow the purpose of distributed denial of service (DDoS) attacks.[12] In 2016 an increase of about 200 percent capacity of infected IoT devices got recognized by security specialists (see figure 2). This became evident with the large DDoS attack by the Dyn botnet in October 2016, affecting a variety of companies such as Amazon and Deutsche Telekom.[13] According to Cisco *"one of the fundamental elements in securing an IoT infrastructure is around device identity and mechanisms to authenticate it."*[14]

How DLT can help solve the question of data access and security

Distributed ledger technologies could inhibit the highlighted (and more) challenges. In current architectures, IoT networks and the respective devices within the network usually require some sort of centralized authentication as a process to generate trust between the devices. DLT, exhibiting peer-to-peer (P2P) communication, is not in need of a centralized server and therefore removes the single point of failure by design. The validation of transmissions within the network, being tokens, messages or other forms of data, are assured by nodes within the network. Therefore, devices, users and transmissions would no longer need to authenticate themselves with a central authority.

Besides the highlighted design feature of DLTs, the combination of cryptocurrencies (tokens) and M2M communication also paves the way for the so-called machine economy.[15] In the machine economy devices, sensors or in general electronic objects interact with each other. They are enabled to exchange data in return for a (financial) reward. A classic example would be a rooftop solar panel on a house receiving data from the nearest weather station and thereby being able to align its panels accordingly to the distribution of sunlight. In the machine economy, machines become an entity with their own wallet and profit and loss statement (P&L). Due to the underlying DLT, all sorts of data, such as tokens, messages or raw data itself, can be transferred from one user to another. As mentioned, a user does not need to be a physical individual but can be any form of electronic object.[16]

Most of the machine economy, such as in the solar panel example, rests on so called smart contracts. Smart contracts follow a fixed *if-then* reasoning with a predefined process. They usually take advantage of the peer-to-peer structure of the DLT network and remove every third party from the contract equation. Given the solar panel example, the machine checks its utilization every morning and, if a predefined threshold is not reached for a certain amount of time, a smart contract is triggered, which will lead to the acquisition of information.[17]

IoT and M2M communication rely on a dense network of sensors and connected devices, exchanging data on a large scale, which leads to a large throughput of information. Logically, a prerequisite for a capable network is the capability to handle the increasing data streams in the following years.[18] Distributed ledger technologies differ strongly in their throughput of transactions, also known as scalability. Although DLTs are by far not limited to financial

[10] See IDG (2018)

[11] Own figure based on Sutherland (2017)

[12] A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security. (www.techopedia.com/definition/18091/brute-force-attack).

[13] See Sutherland (2017)

[14] Cisco (2015)

[15] Please see BearingPoint publication: Initial Coin Offerings – Tokens im Kontext der Shared Economy

[16] See Rouse (2018) or Commonwealth Bank of Australia (2017)

[17] See Küfner (2018) for an overview regarding smart contracts

[18] See Shields (2017)

transactions in the form of tokens, the throughput of other forms of data exhibits the same restrictions. The throughput depends partly on the design and difficulty of the safety mechanism of the technology, such as proof of work (PoW), as well as the allowed size of transactions, thereby representing a tradeoff between scalability and security. Difficulty translates to the amount of computing power, therefore time, and the relative energy usage needed for the security mechanism of the solution. That being said, most sensors and other small connected devices, which communicate heavily, only exhibit a limited amount of computing power and in some cases battery-life. The PoW of the original Bitcoin-Blockchain is an example of a resource and time demanding security mechanism. In addition, blocks are capped to a size of 1 Mb, further limiting the amount of data being transmitted.[19]

An energy and time demanding security mechanism such as the PoW of the original Bitcoin-Blockchain makes the technology poorly suitable for highly frequent data exchanges, as M2M communication requires. Some modified Blockchain-technologies try to tackle the high computing power by changing from a proof of work to a proof of stake or other consensus mechanisms. The fundamental design, being the creation of blocks, does not change. Moreover, it is suggested to develop a *"layered architecture which supports thin clients to allow IoT devices with limited resources to store only a portion of the Blockchain"*[20], a feature not yet present.

M2M communication has a high potential to further flourish existing services or create entire new ones. Nevertheless, with centralized points of failure, data security is still an issue. DLTs could hit the mark, however, they exhibit some limitations. The limitations could be tackled by directed acyclic graph (DAG) solutions, another form of distributed ledger technology. Keeping that in mind, the following chapter will highlight key features of DAGs, also by a head-to-head comparison to features of the Bitcoin-Blockchain.

[19] See Conoscenti, Vetrò, & De Martin (2016)
[20] Conoscenti, Vetrò, & De Martin (2016), p. 5

A technological introduction to directed acyclic graph-based ledgers

In simple terms, directed acyclic graph (DAG) is a method of how data is stored and how new data is added. A Blockchain organizes data in a chain of blocks. A new data block gets verified, validated and added next to the previous block. DAG-based DLTs do not use data blocks or a single chain. Although the approach differs from a Blockchain, it is still considered a DLT. To understand its specifics and differences from the Blockchain DLT, this chapter will briefly take you through the technological features and how they work.

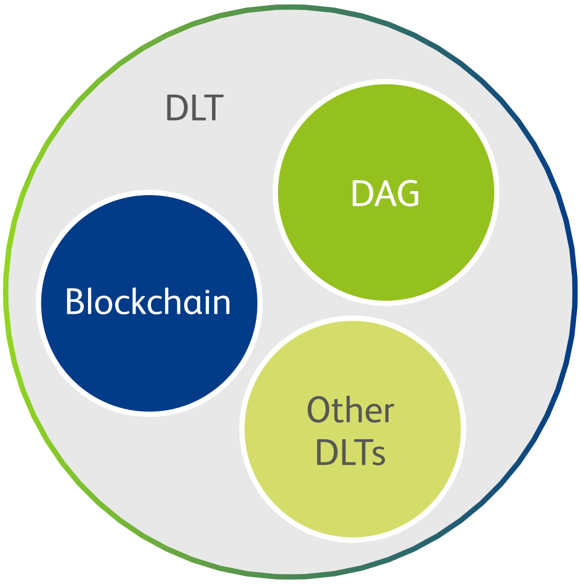


Figure 3: DLT categories[21]

The DLT technology is more than just Blockchain. Blockchain, which is mostly associated with when people think about distributed ledgers, is just one type amongst others. Many Blockchain projects followed the prominent Bitcoin in this space and made distributed ledgers a hot topic. The DAG, not being a Blockchain, is another form of DLT (see figure 3). While the mathematical concept of directed acyclic graphs exists for a long time, it has found its way to the DLT-space through the IOTA cryptocurrency. The concept has gained public awareness through the marketing weary IOTA foundation.

As shown in figure 4, the directed acyclic graph is characterized by following only one direction as well as a lack of cycles. DAGs are used to model probability, causality and connectivity. One simple example for a DAG is a family tree. Keeping any possibility for a time machine aside, you are the child of your parents (directed) and your ancestors can never be your descendant (acyclic).

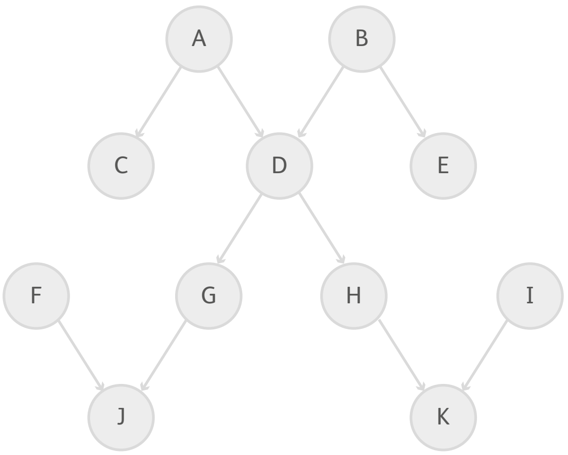


Figure 4: Mathematical concept of DAG[21]

Bridging the gap to the ledger world, the concept in general is as simple as the above graph: To add new data, e.g. a transaction, the user simply must verify and reference at least one previous transaction, before itself can become validated (by new transactions).[22] The number of how many previous transactions to confirm varies between DAG implementations. For example, IOTA requires the verification of two previous transactions.
The consensus system and the data structure make the DAG suitable for use cases that require a high volume of transactions within seconds. The general idea behind the DAG is the more transactions occur, the faster previous transactions become verified. This is what is currently referred to as scalability.[23] Figure 5 shows a compressed comparison between Blockchain and DAG, which highlights some key indicators. The comparison will be discussed in detail in the following chapters with the examples of Bitcoin (Blockchain), IOTA (DAG) and Obyte (DAG).

[21] Own figure (Franz Weisenberger)

[22] See Sink (2011), p. 47-51

[23] Although the scalability is limited by current technical infrastructure such as broadband.

	Blockchain	DAG	
	Bitcoin	IOTA	Obyte
DLT	√	√	√
Scalability	Gradually	Continuous/smooth	Continuous/smooth
User & validator	Different parties	The same	The same
Transaction fees	√	X	√
Finality	Probabilistic	Probabilistic/currently centralized snapshots + milestones	√ (Stability points)
Offline transactions	X	√	(√)
Degree of quantum resistance	Very low	High (at current standard)	n/a

Figure 5: Blockchain vs. DAG

Scalability

If transaction A is confirmed by transaction C via at least one other transaction (B), then A is indirectly confirmed by C.

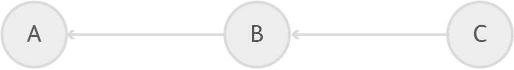


Figure 6: Simplified scheme of the DAG[24]

While this scheme looks quite similar to the Blockchain, it differs in the sense that new data gets added continuously rather than in blocks every fixed number of minutes. This resolves the issue of scaling, since the blocks in a Blockchain are also limited in size. Even the size of the blocks can be adjusted, while only in gradual steps which requires a change in the underlying protocol. Figure 6 is a very simplified illustration of that process. In reality, however, this process is further intertwined and thus resembles a large web (see figure 7).

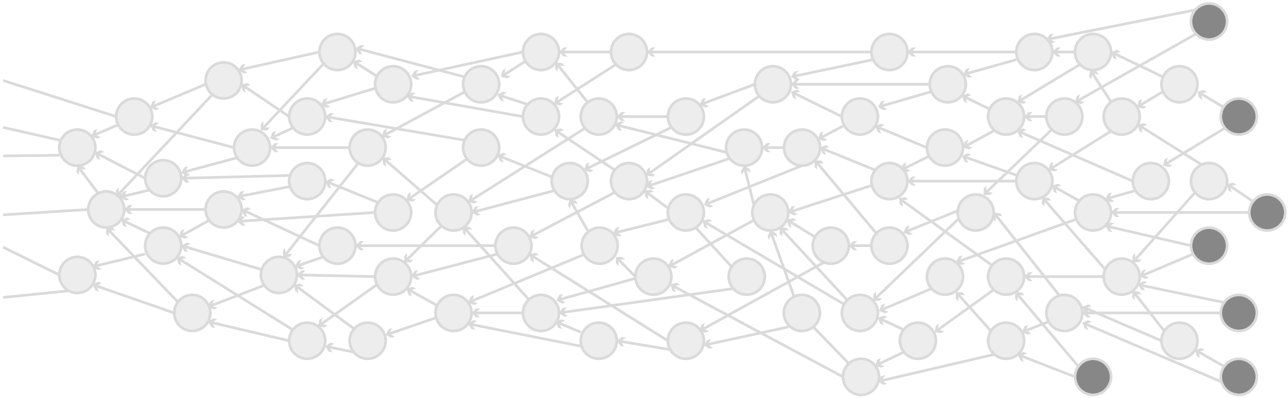


Figure 7: The web of the tangle[25]

[24] Own figure (Franz Weisenberger)

[25] Figure from Popov (2018)

Figure 7 shows the DAG of IOTA, also known as tangle (and thus its name becomes clearer looking at the intertwined nature of the web of transactions). The principles of the DAG in this paper mostly refer to the DAG of IOTA, since the project has received a lot of attention in the last months. The tangle is actually a theoretical concept whereas IOTA is an implementation of that concept using different features which are currently being developed and tested.

The functionality of the tangle

The tangle uses the rule of two confirmations, meaning a transaction must first confirm and refer to two previous transactions before being published to the network and becoming confirmed. The dark grey circles on the right end are unconfirmed transactions called tips. At the beginning of the DAG, there is a genesis-transaction, which is confirmed directly or indirectly by all other transactions. The genesis-transaction distributed all tokens to several addresses. In the concept of the IOTA-tangle, no new tokens will be created. This means, that the total number of tokens is limited from the start. Furthermore, tokens are pre-mined, resulting in no new ones being created.[26]

As new transactions are made within the network, the size of the DAG increases. Especially for high-volume traffic, this could mean a vast need of storage to store all the history of transactions. IOTA solves this by using a feature called *snapshot*. This feature saves the balances of all addresses at a given point and deletes all the history. As in the IoT-environment, devices do not need to know about the history, but only the current balance of an address. By now, these snapshots are organized centrally, so all nodes take a snapshot at the same time. The aim of IOTA is to further develop this function, so snapshots can be done automatically by every node when they need to (local snapshot). Especially for small nodes with smaller storage units, this function could be very beneficial. So-called *permanodes* would store the whole history of the IOTA-tangle, in order to use the history for e.g. audit or credit history purposes.[27]

User & validator role

Contrary to common Blockchain systems, where user and validator roles are usually separate parties, there is only one party in a DAG-based network. User and validator are the same. To create and publish a transaction to the network, one must first confirm at least one previous transaction (two in IOTAs tangle) as a return of consideration. Therefore, a user directly contributes to the networks security when making a transaction. The so-called nodes then have the task to publish the transaction into the network, after they made sure that the transaction will not conflict with another transaction (e.g. double spending patterns). In case there is a conflicting transaction, the node usually declines the transaction to be published. Nodes would still be able to publish the transaction, but the transaction probably will not be confirmed by other nodes who publish transactions. The more transactions confirm the respective transaction, the safer it is considered to be.[27] Obyte (previously Byteball) is another network using the DAG as data structure. Obyte incentivizes users to confirm as many previous transactions as they want, but it would be also possible to just confirm one previous transaction. The incentive is monetary by receiving a small reward.[28]

Transaction fees

To ensure a network or system is self-sufficient, there must be an incentive for the participants. As in the Blockchain-based ledgers, the concept of fees play an important role in the DAG-based ledger technology. However, projects implement the concept differently.

Obyte uses a reward system with its native currency unit called *bytes*. To attach data, e.g. a transaction to the Obyte-DAG, one has to pay the equal amount of the size in the native currency. To calculate the data size, it is always assumed that the transaction confirms two previous transactions.[29] A part of the fee paid goes to the user, who confirms the transaction first. Therefore, the system incentivizes users to confirm as many recent transactions as possible. The other part of the fee goes to so-called *witnesses*, who are trusted users in the network.[30]

IOTAs tangle has no fees in a monetary way. Users merely undertake a small proof-of-work calculation. The main purpose of this mechanism is spam-protection and resembles the concept of *hashcash*[31] in the e-mail context. Therefore, the only fee that users must account for is the electricity needed for a little computational power. While this fee is of rather indirect nature, it is worthwhile to mention it. This computation undertaken requires much less power than similar process of the Blockchain-based ledger and therefore constitutes a much more sustainable practice regarding environment, but especially also for small IoT-sensors with low processing power. The concept of IOTA not having fees, allows it also as a high-frequency communication tool to exchange information other than transactions. The proof-of-work of IOTA cannot be compared to the one used in the Bitcoin network, as it is used for a different purpose. The Bitcoin proof of work is used to determine who is entitled to verify the next block. As all miners

[26] See Popov (2018)

[27] See Moog (2018)

[28] See Churyumov (2016)

[29] The referenced transactions are included in the data package and therefore increase the data size. As the fee to add data to the Obyte-DAG depends on the size of the data, it would be counterproductive to pay for any additional transaction. Even referencing more than one, the fee is calculated for only two transactions.

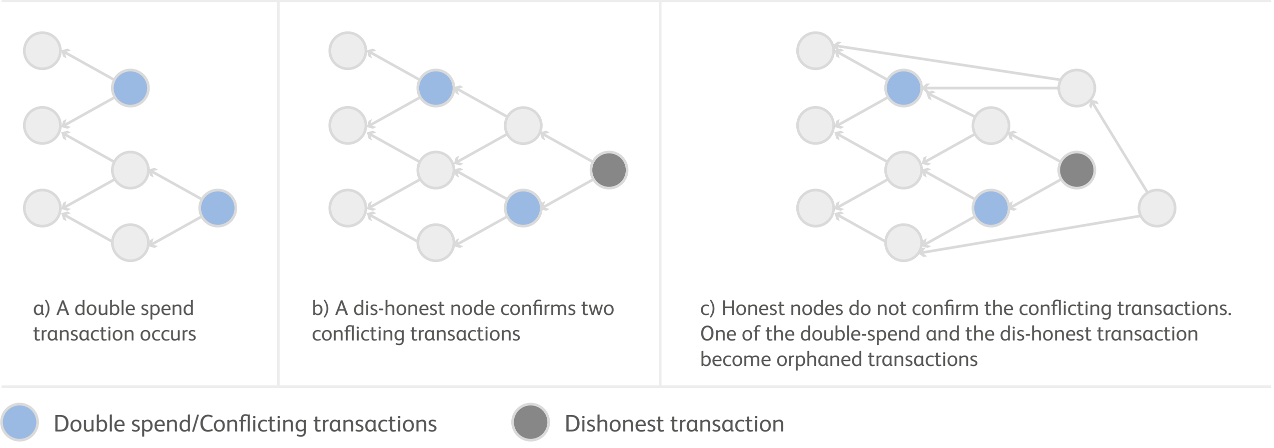
[30] See Churyumov (2016)

[31] Hashcash is a proof-of-work algorithm, which has been used as a denial-of-service counter measure technique in a number of systems. (Source: http://www.hashcash.org/)

compete for that entitlement, the Bitcoin proof-of-work accounts for a large amount of energy. While there are other Blockchains using an improved proof-of-work or alternatives like proof-of-stake, the two-party approval process will always imply a need for fee to incentivize the players to participate in this system with validation. As Blockchains are having a limited block size, fees will rise if the amount of transactions fitting into a single block reaches the upper limit or even surpasses the block size. Miners only pick transactions to verify where they can collect the highest fees, leading to transactions with low fees left in the *mempool*[32], as long as transaction activity will not decrease or the block size increases.

Double spend

Whereas Obyte and IOTA both use the directed acyclic graph as database structure, the systems have different implementations as already noticeable in the previous paragraphs. This is also highlighted in the manner they deal with conflicting transactions (double spend). IOTA uses a scheme, which is mostly based on honesty. A transaction should only confirm non-conflicting transactions, as otherwise the transaction itself will not be confirmed by other *"honest"* users, resulting in an orphaned transaction (see figure 8).[33]



a) A double spend transaction occurs

b) A dis-honest node confirms two conflicting transactions

c) Honest nodes do not confirm the conflicting transactions. One of the double-spend and the dis-honest transaction become orphaned transactions

Figure 8: Double spend in the IOTA-tangle[34]

Obyte includes every transaction in its network, but only considers the first one as valid, by using a serial number for transactions posted from one user (see figure 9). It is also possible not to use a serial number. In this case, the order will be determined through the system of a main chain later and through previously mentioned witnesses. There can even be several main chains, the chain including the most transaction of witnesses is considered more real. The transaction which first gets confirmed by this mainchain is treated as valid.[35]

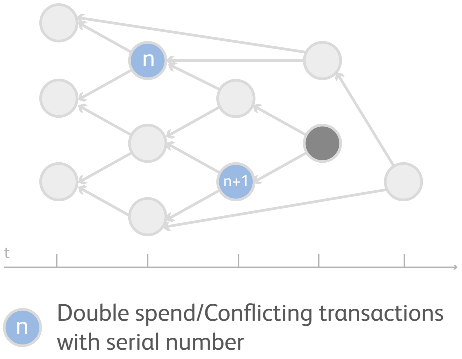
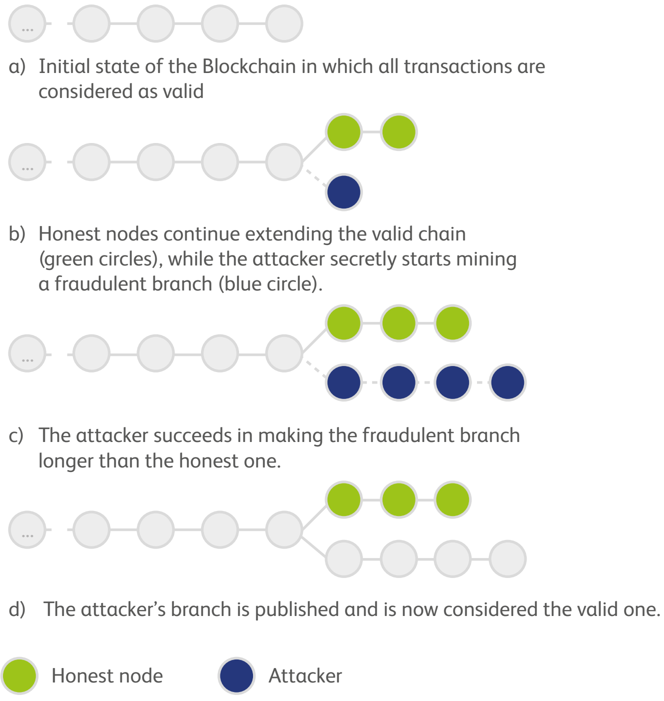


Figure 9: Double spend in the Obyte-DAG[34]

The Bitcoin-Blockchain solves the problem of double-spending by maintaining a chronologically-ordered and timestamped ledger. Conflicting transactions cannot be included in the same block and later blocks that contain a conflicting transaction cannot reference to the previous block. If the conflicting transactions are each included in different blocks, which both directly reference to the same previous block, only one of the double spend-blocks will become confirmed by the following blocks. The other block will become an abandoned block (see figure 10). Therefore, one should wait for several confirmations by following blocks before accepting a payment.[36]



a) Initial state of the Blockchain in which all transactions are considered as valid

b) Honest nodes continue extending the valid chain (green circles), while the attacker secretly starts mining a fraudulent branch (blue circle).

c) The attacker succeeds in making the fraudulent branch longer than the honest one.

d) The attacker's branch is published and is now considered the valid one.

Figure 10: Double spend in the Bitcoin-Blockchain[37]

[32] Mempool: The aggregate size of transactions waiting to be confirmed (Source: blockchain.com)
[33] See Popov (2018)
[34] Own figure (Franz Weisenberger)
[35] See Churyumov (2016)
[36] See Nakamoto (2008)
[37] Own figure based on Sameeh (2016)

Finality

Another big question when discussing DLT is the finality of a transaction. Finality describes a point in time when one can assume, that a transaction is irreversible. Using the Bitcoin-Blockchain, a rule of thumb states that after six confirmations, a transaction is considered to be safe. This assumption is only a probabilistic approach, as it is theoretically possible to build a side-chain which becomes the mainchain. Practically, this is almost impossible, as this requires a huge amount of computing power when using proof-of-work, as in the Bitcoin-Blockchain.

Obyte's DAG has a definite finality through using stability points. Stability points determine the point at which the DAG cannot be changed anymore. If a unit in the DAG is the ancestor of the majority of observation units, which are published by the witnesses, it becomes a new stability point. Therefore, a transaction that was either directly or indirectly confirmed by a stability point is final.[38]

IOTA's tangle uses a Markov-Chain-Monte-Carlo-algorithm to determine the level of confirmation. The algorithm checks how many of the new tips indirectly or directly confirm the relevant transaction. Each network user decides for itself, which degree of confirmation is necessary to accept the transaction. Some might say that 60 percent of the tips confirming the relevant transaction is necessary, others may wait until 99 percent or even 100 percent. Figure 10 illustrates this situation: The green circles represent the transactions where consensus is achieved, and 100 percent confirmation is reached. The blue circles are uncertain transactions, which are not fully confirmed, and the grey circles are tips (having no confirmation at all). With new transactions arriving, the whole structure gets more interconnected and the blue circles eventually become green circles.[39] Nevertheless, it is possible to secretly build a side tangle which eventually outruns the main tangle and becomes the main tangle itself. Depending on the size of the tangle-network, this is unlikely to happen, as that would require a large amount of computational power (*spam-protection*) and the tip-selection algorithm used by honest users.

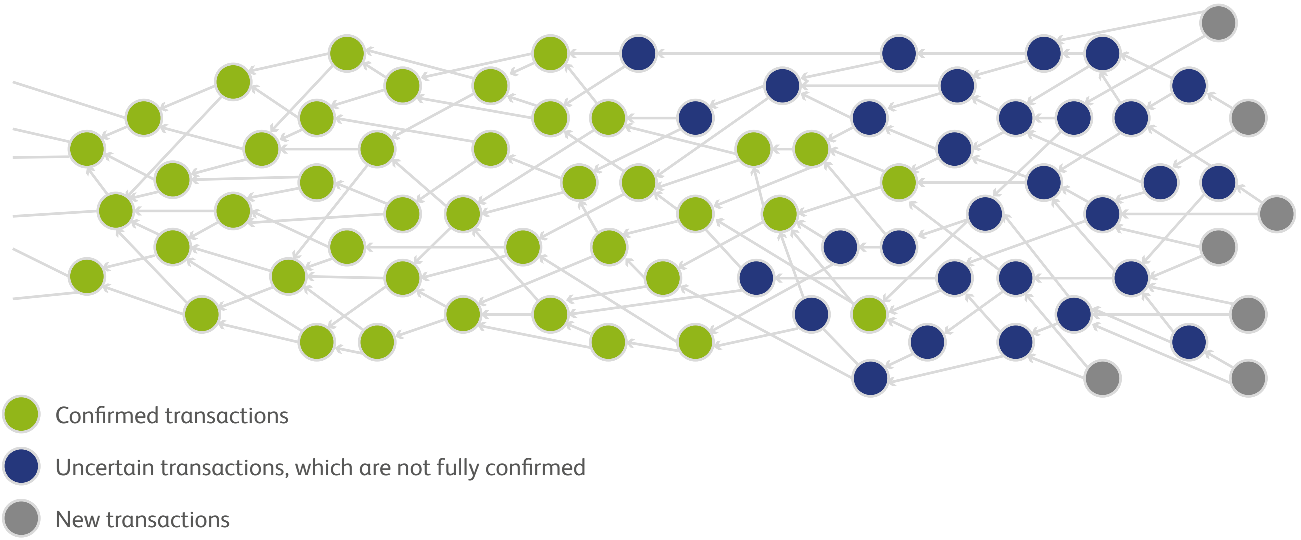


Figure 11: Confirmation in the tangle[40]

DAGs, like IOTAs tangle or Obyte, are said to solve the scalability issue and the use of resources better than the Blockchain technology. Whether this is true remains to be seen. Scalability is especially important regarding IoT applications and the machine economy. Being at a very early stage, the practical implementations of the DAG are far away from the theoretical concepts. The DAG seems more suitable than Blockchain regarding a high transaction volume. But the implementations have problems with low transaction volume, as there is no recurrence frequency of confirmations. In scenarios of low volume, DAG networks are more vulnerable to attacks. That is why they cannot be fully decentralized in their early stage. IOTA has a central coordinator which is said to be shut down if the network is big enough to sustain itself. There are already plans to shut down the coordinator, which are said to be executed in 2019. The coordinator makes transactions which are called milestones. If directly or indirectly verified by a milestone, the transaction is confirmed.[41]

Obyte has witnesses as central points of trust. Witnesses are linked to known individuals in the network. Every transaction includes a list of 12 witnesses, whereof the majority has to show the path to the main chain. The security of the network would be threatened if they colluded together, which is currently the main trust issue as the most of those witnesses are controlled by the founder.[42]

[38] See Churyumov (2016)
[39] See Scott (2017)
[40] Own figure based on *stardust* in Scott (2017)
[41] See Sheikh (2018)
[42] See Bohne (2018)

Offline transactions

According to the CAP-theorem, a distributed ledger can only fulfill two of the following three features at the same time:

- Consistency
- Availability
- Partition tolerance

Consistency refers to a global state where every participant has the same view of the network. Availability means to get an answer if sending a request to the network. Partition-tolerance is a fluid interaction of going back online again while still retaining the data, meaning the system continues to run even when there are local network failures.[43]

IOTA claims that its tangle will be able to perform offline transactions[44] by simply branching off a part of the tangle and attach it later as soon as online connectivity is given. This feature is essential in the IoT-environment, as there is no *always-online* for every single device, such as a sensor. When looking at the CAP-theorem, IOTA does not violate the rules as it is available, partition tolerant, but only eventually consistent. This means that after some time everyone has the same view about past transactions (green circles in figure 11), but no one can see all new transactions (blue and grey circles in figure 11).

When looking at the Bitcoin-Blockchain regarding the CAP-theorem, it is consistent and available but performs poorly in partition tolerance. When trying to branch off some blocks and adding them on later, it would end up in a side-chain, which would probably become an orphaned chain.

According to the Obyte white paper, the network is not able to partition into two parts, as they rely on the majority of the witnesses to continue advancing the stability point. But the connection can be restored to reach consistency. Therefore, Obytes DAG also features partition tolerance, availability but only an eventual consistency. Obyte does not aim to feature offline transactions, even though they are theoretically possible when using the DAG.[45]

Area of application

Obyte is a system created for a tamper proof storage of data including data representing transferrable value (transactions). To add data to the network, a fee is applied which depends on the size of the data package. The applications include features for assets, smart contracts and a non-traceable currency called *blackbytes* for improved privacy.[45] Whereas Obyte is designed for a human to human (H2H) environment with e.g. user-friendly wallets, IOTA is designed to function as a standard for M2M-communication in the field of IoT. Therefore, the two systems are not in direct competition with each other. A feature of the IOTA-tangle is high quantum-resistance due to the so called Winternitz-signature, meaning quantum computing will not have an extreme advantage in comparison to normal computing.[46] In the crypto-currency space, quantum computing is a threat to all the cryptographic security mechanisms, as they all rely on heavy computation, which is said to be easier with quantum computing. As of today, no marketable quantum computing has been developed. Therefore, this feature is currently not relevant, but should be kept in mind.

[43] See Nazrul (2018)

[44] See Bowles (2018)

[45] See Churyumov (2016)

[46] See Popov (2018)

The technology in practice: insure my car by bIOTAsphere

Given that the DAG technology is in a stage of early development, few use cases exist that have evolved to proof of concepts (PoCs). Since there is a lot of illegitimate material and alleged use cases out there, we decided to introduce a proof-of-concept that has been tested.

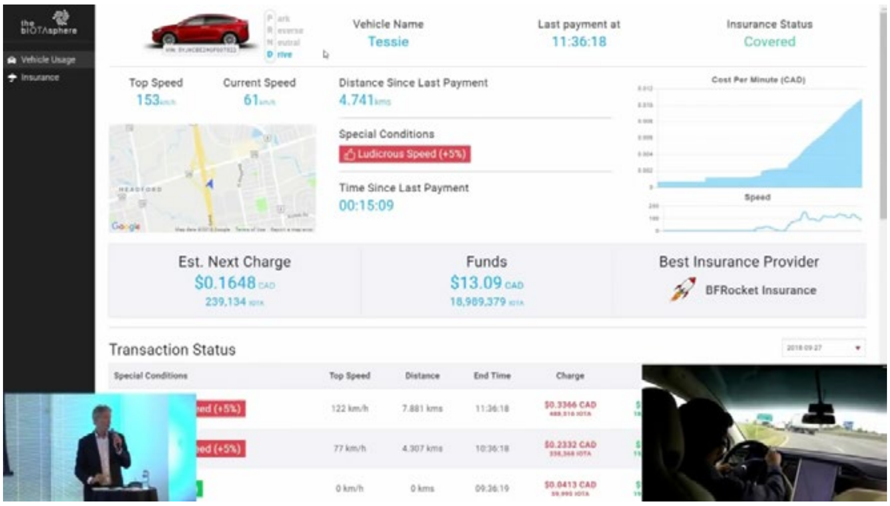
What it is about

Vehicle insurance is mandatory in many countries. The standard model of pricing uses risk clusters, which are based on statistical groups usually relying on historical data like gender, age and accident history. The fairness of pricing, depending on the driving style, is not given. This system does not reward *good* or punish *bad* (within road traffic regulations) driving, as it lacks real-time data. We can perceive a shift to the rise of a sharing economy with examples in the hotel and transportation industry, which is supported by new technology.[47] Insurance companies must rethink their business models and adapt to that change to stay competitive. Therefore, several insurance companies from different countries are experimenting with pay-as-you-drive models, including rewards. Those business models usually rely on smartphone apps based on data silos within the companies using different data formats. Those data silos exhibit the risk of being manipulated or compromised. Moreover, the offers are tied to a single provider of insurance. Modern cars already generate a lot of data, which is used by the manufacturers. Since data is the so-called *new oil*, manufacturers are not willing to share the data that the insurance companies require, as they are afraid to lose a competitive advantage. With all centralized models, the user who is the real owner of the data is not rewarded for generating and sharing it. The following proof-of-concept shows a way to implement a pay-as-you-drive pricing model which needs a minimum amount of data of the actual user.[48]

The proof of concept

The proof of concept *insure my car* was developed by the group bIOTAsphere, which is in close contact with the IOTA foundation[49].

Insure my car in a nutshell: A car, which is a part of the machine economy, pays for the cheapest insurance by itself on a moment to moment basis with its own wallet. For this PoC, the only factor for calculating the risk – and therefore the premium – is the speed of the car. If the car is in parking mode, the car chooses the *standby insurance* which offers a 70 percent discount when the car is parked. Starting slowly to drive, the car switches automatically to the next cheapest insurance, which in this case is called *tortoise insurance*, having no extra fees up to 30 km/h. If the car is above 30 km/h there is a penalty of 30 percent. If far above that speed for a longer period, the car will switch to the next cheapest insurance called *BFRocket insurance* which gives a better rate for higher speeds than the tortoise insurance with penalties. A dashboard showing all relevant information can be seen in figure 12. The premiums of the insurances in this PoC are simply connected to the higher risk level at higher speeds. In this use case, the focus is on the car itself, as it chooses and pays the insurance. Data about the driver like age or weight are not relevant. This model potentially functions in car fleets, car-sharing or ride-sharing as well.[48]



Vehicle Name: Tessie
Last payment at: 11:36:18
Insurance Status: Covered
Top Speed: 153 km/h
Current Speed: 61 km/h
Distance Since Last Payment: 4.741 kms
Special Conditions: Ludicrous Speed (+5%)
Time Since Last Payment: 00:15:09
Est. Next Charge: $0.1648 CAD, 239,134 IOTA
Funds: $13.09 CAD, 18,989,379 IOTA
Best Insurance Provider: BFRocket Insurance

Transaction Status 2018-09-27

Special Conditions	Top Speed	Distance	End Time	Charge
ed (+5%)	122 km/h	7.881 kms	11:36:18	$0.3366 CAD
ed (+5%)	77 km/h	4.307 kms	10:36:18	$0.2332 CAD
	0 km/h	0 kms	09:36:19	$0.0413 CAD

Figure 12: Dashboard insure my car[50]

[47] Please see BearingPoint publication: Initial Coin Offerings – Tokens im Kontext der Shared Economy

[48] See Shane (2018)

[49] The non-profit IOTA foundation is the organization behind IOTA and mainly develops the protocol of the IOTA-tangle. The foundation was established in Germany (Berlin) in 2017.

[50] Figure from Shane (2018)

For the testing, bIOTAsphere used a Tesla. Besides its electric engine, the main reason of choice is the fact that Tesla offers an API with real-time data such as location and speed. The use case also works with cars which do not have a firsthand installed API. Without an integrated API, the car can be equipped with a telematics device. A suitable port is integrated in all vehicles from 1996 or newer.[51] In general, smartphones would also be an option. Nevertheless, they are not preferred by bIOTAsphere, since they are usually directly linked to a single person.[52]

The insurance company receives all the data they need to develop new statistical models and information about the real risk arrives in real time. If an accident happens, the insurance company which covers the car in that exact moment is responsible for covering the cost. In case the car is offline, there is a special offline insurance plan in place which has a higher premium, as the data does not arrive in real-time.[53]

Why insure my car uses the DAG of IOTA as underlying protocol

The data the car provides is stored encrypted in the IOTA-tangle. Since the IOTA-tangle is immutable, nobody can change the data afterwards. Therefore, the user does not have to rely on the company providing the correct data. The data is written in real-time on the IOTA-tangle. It is possible to make transactions with a fraction of a penny requiring no fee for a transfer. Furthermore, low resource requirements and a secure data transfer on the IOTA-tangle are making this use case possible. The user is still the owner of his data even though it is a distributed ledger. As for encryption, no information is publicly accessible.[52]

Possible scenarios on top of the PoC – within the insurance industry

To widen the scope of the use case, more data could be used for insurance companies to develop their pricing models. Someone driving 100 km/h on a sunny day represents an entirely different risk than the same speed during a snow-storm in winter. Further information like the condition of the road, speed limits and congestions could lead to a new pricing model based on real-time data. Even heart-rate acceleration or deceleration, monitoring the driver's fatigue, could be considered to determine a premium model. The risk of all these factors could be broken down into small pieces and allocated dynamically into diverse new insurance products.[52]

Further possibilities beyond the use case

The possibilities beyond the insurance use case are very broad. If the car must pay for insurance, of course someone is responsible for charging up the car's wallet. To ensure compliance with regulations having mandatory insurance, this could also act like fuel. In case the wallet does not have enough funds, the car might not drive. In fact, the car itself could earn money from cargo items and payments for services such as selling power which is stored in the car's battery when it is not in use. Autonomous cars could act as taxies and earn money to pay insurance and other expenses. Other ideas reach from paying a car in front of you to moving aside to get to your destination faster to use cases of trucks paying the truck in front for so-called platooning[54] to gain efficiencies and benefit from slipstream effects. If the car has a camera for the front-road, the data could be shared to trigger road-maintenance in case there are several damages reported. The car could pay directly for tolls and the infrastructure costs of the road.[52]

Take-away for the use case insure my car

A short summary of the key advantages the PoC provides are as shown in figure 13.

Advantages	
Insurance company	**Customer**
Insurance company gets all the data it needs to allow better decision-making	Consumer does not have to choose an insurance, as the car chooses the best/ cheapest option
Developing individual products could be key to success in this highly competitive market	User can rely on a tamper proof storage of his own data and having control of access rights
Cost savings, as premiums are usually used for sales, marketing and commissions for intermediaries	Cost saving options lead to cheaper offers for the customer

Figure 13: Advantages for the insurance company and the customer

[51] See Intelligent Mechatronic Systems Inc. (2018)
[52] See Shane (2018)
[53] See Boht (2018)

[54] Platooning: Truck platooning is the linking of two or more trucks in convoy, using connectivity technology and auto-mated driving support systems. (Source: https://www.acea.be/uploads/publications/Platooning_roadmap.pdf)

For this use case to go into production, there are still several issues to solve, according to an interview with bIOTAsphere. The application is not yet ready for a scaling to a potential use of several million vehicles.[55] bIOTAsphere encourages potential collaboration with insurances and other partners to work further on this use case. Furthermore, bIOTAsphere is also working on projects in other fields like smart energy, document management, recycling, identity and more.[56]

Conclusion and Outlook

IoT is currently on the rise to maintain and enhance corporate growth. Although the most prominent representative of IoT is currently predictive maintenance, machine to machine communication is becoming more relevant. Furthermore, M2M communication as a field of technology allows for the creation of the so-called machine economy, where machinery and devices, in simple terms, are able to carry their own wallets.

M2M communication is increasing the global data stream as more firms push their data into the internet. That being said, many companies notice or already experience the risk of security breaches regarding their data warehouses or communication networks. Most of the corporate M2M communication is happening on an interfirm or interindustry level, resulting not only in data silos, but also single points of failure.

The Blockchain-technology, with its high encoding standards and decentralized architecture, could help secure the data transferred and distributed, not only on an intra-firm or intra-industry level, but also on a cross industry level. Opening data silos and granting access to unused data can further enhance existing services or allow for the creation of new ones. Keeping that in mind, the Blockchain-technology, especially its most prominent representative Bitcoin, exhibits some drawbacks which limit the usage in the field of M2M communication and the machine economy. Particularly responsible for the limited functionality are the reduced scalability, the restricted data throughput and the high use of resources in the sense of computing power and therefore energy. These limitations are challenged by directed acyclic graph-based ledgers. IOTA, the most known representative of the DAG based ledger technology, is designed to work in the field of M2M communication and the machine economy. The tangle, IOTAs DAG network, is increasing its performance with the increasing number of network users. Moreover, its design enables a secure data transfer amongst machines. Features such as offline transactions are essential for the adaption of IoT in various industries. The use case insure my car proves that the IOTA-Protocol makes a combination of real-time driving-data and insurances possible in order to offer new and improved services.

Briefly summarized, DAGs, in this case the tangle, are currently among the most promising technologies in the field of M2M communication and the machine economy. They allow for a consistent and solid data throughput while simultaneously ensuring data security. However, looking at the current market solutions, the DAG technology, with its most prominent representative IOTA, is still at the beginning of commercialization. Therefore, it remains to be seen whether this protocol will become a broadly accepted standard and a key driver of new digital services, as the highlighted example of insure my car. The IOTA foundation stands out due to strong partnerships with established companies like Volkswagen and Bosch.[57]

[55] See Boht (2018)

[56] See Shane (2018)

[57] See for example a potential cooperative use case of IOTA and Bosch: https://www.bosch-connectivity.com/newsroom/blog/xdk2mam/.

Sources

Barnett Jr., T. (2016, September). The Zettabyte Era Officially Begins (How Much is That?). Retrieved from Cisco: https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that

Bohne, J. (2018). Witness. Retrieved from wiki.obyte.org: https://wiki.obyte.org/Witness

Boht, M. (2018). Developer Insights - Insure My Car Proof of Concept. (J. Molyneux, Interviewer) Retrieved from https://www.linkedin.com/company/the-biotasphere/

Bowles, J. (2018, May). Can IOTA'S blockless blockchain become the IoT standard? Retrieved from diginomica.com: https://diginomica.com/2018/05/02/can-iotas-blockless-blockchain-become-iot-standard/

Churyumov, A. (2016). Byteball: A Decentralized System fo Storage and Transfer of Value. Retrieved from https://obyte.org/: https://obyte.org/Byteball.pdf

Cisco. (2015, May). Securing the Internet of Things: A Proposed Framework. Retrieved from https://www.cisco.com: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

Cisco. (2018, November). Cisco Visual Networking Index: Forecast and Trends, 2017–2022. Retrieved from cisco.com: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc529314186

Commonwealth Bank of Australia. (2017, November). Welcome to the machine-to-machine economy - Opportunities and challenges in a connected world. Retrieved from https://www.commbank.com.au: https://www.commbank.com.au/content/dam/caas/newsroom/docs/Commbank-Whitepaper-Machine-to-Machine-economy.pdf

Conoscenti, M., Vetrò, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. IEEE. Retrieved from IEEE Xplore Digital Library: https://ieeexplore.ieee.org/document/7945805/

Gartner. (2018, December). Magic Quadrant for Managed M2M Services, Worldwide. Retrieved from https://www.gartner.com: https://www.gartner.com/doc/reprints?id=1-5P8M88O&ct=181101&st=sb

IDC. (2018, November). The Digitization of the World. Retrieved from Seagate.com: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

IDG. (2018, April). Studie Internet of Things 2018. Retrieved from https://m2m.telefonica.de: https://m2m.telefonica.de/wp-content/uploads/2018/01/IoT_Studie_Deutschland_2018.pdf

Intelligent Mechatronic Systems Inc. (2018, January). What is a Telematics Device? Retrieved from intellimec.com: https://www.intellimec.com/ims-blog/telematics-device

Küfner, R. A. (2018, April). DLT & the Financial Industry: Smart Contracts. Retrieved from https://medium.com/: https://medium.com/nakamo-to/dlt-the-financial-industry-smart-contracts-5051a52cb9a1

Moog, H. (2018, September). Coming Up: Local Snapshots - A development status update. Retrieved from blog.iota.org: https://blog.iota.org/coming-up-local-snapshots-7018ff0ed5db

Nakamoto, S. (2008, October). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from www.bitcoin.org: https://bitcoin.org/bitcoin.pdf

Nazrul, S. S. (2018, April). CAP Theorem and Distributed Database Management Systems. Retrieved from towardsdatascience.com: https://towardsdatascience.com/cap-theorem-and-distributed-database-management-systems-5c2be977950e

Paul, F. (2018, September). Is predictive maintenance the 'gateway drug' to the Industrial IoT? Retrieved from www.NetworkWorld.com: https://www.networkworld.com/article/3305952/internet-of-things/is-predictive-maintenance-the-gateway-drug-to-the-industrial-iot.html

Popov, S. (2018, April). The Tangle. Retrieved from IOTA Academic Papers: https://www.iota.org/research/academic-papers

Rouse, M. (2018, March). M2M economy (machine-to-machine economy) . Retrieved from https://whatis.techtarget.com/: https://whatis.techtarget.com/definition/M2M-economy-machine-to-machine-economy

Sameeh, T. (2016, December). Two New Models For Double Spending Attacks On Bitcoin's Blockchain. Retrieved from Deep.Dot.Web: https://www.deepdotweb.com/2016/12/31/two-new-models-double-spending-attacks-bitcoins-blockchain/

Scott, J. (2017, March). IOTA Consensus Masterclass. Retrieved from forum.iota.org: https://forum.IOTA.org/t/IOTA-consensus-masterclass/1193

Shane, T. (2018). Insure My Car: A deeper dive interview with Terry Shane, Founder of bIOTAsphere. Retrieved from https://insuremycar.biotasphere.com/

Sheikh, Y. (2018, December). IOTA/USD Continues To Hold Around $0.23 As The Team Prepares To Remove Their Coordinator Node In 2019. Retrieved from investinblockchain.com: https://www.investinblockchain.com/iota-remove-centralized-coordinator-node/

Shields, N. (2017, June). Here's how 5G will revolutionize the Internet of Things. Retrieved from https://www.businessinsider.de: https://www.businessinsider.de/how-5g-will-revolutionize-the-internet-of-things-2017-6?r=US&IR=T

Sink, E. (2011). Version Control by Example. July: Pyrenean Gold Press. Retrieved from http://ericsink.com/vcbe/html/directed_acyclic_graphs.html

Statista. (2016, November). Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Retrieved from www.statista.com: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Sutherland, L. (2017, April). The Weaponization of IoT: Rise of the Thingbots. Retrieved from Security Intelligence: https://securityintelligence.com/the-weaponization-of-iot-rise-of-the-thingbots/

List of figures

Contact

Dr. Robert Bosch
Partner
robert.bosch@bearingpoint.com

Special thanks to the authors: Franz Weisenberger and Friso de Knegt

About BearingPoint

BearingPoint is an independent management and technology consultancy with European roots and a global reach. The company operates in four units: Consulting, Solutions, Business Services, and Ventures. Consulting covers the advisory business; Solutions provides the tools for successful digital transformation, advanced analytics and regulatory requirements; Business Services provides managed services beyond SaaS; Ventures drives the financing and development of start-ups. BearingPoint's clients include many of the world's leading companies and organizations. The firm has a global consulting network with more than 10,000 people and supports clients in over 75 countries, engaging with them to achieve measurable and sustainable success.

For more information, please visit: www.bearingpoint.com

BearingPoint®

www.bearingpoint.com