Distributed Ledger Technologies for M2M Communications

Natasa Zivic
Carmeq GmbH
Berlin, Germany
natasa.zivic@carmeq.com

Christoph Ruland
University of Siegen
Siegen, Germany
christoph.ruland@uni-siegen.de

Jochen Sassmannshausen
University of Siegen
Siegen, Germany
jochen.sassmannshausen@uni-siegen.de

***Abstract*—Distributed Ledger Technologies (DLT) are seen as data bases of the future, which reduce the cost of trust and revolutionize transactions between individuals, companies and governments. They are considered as one of the main drivers of future applications, especially in field of Machine to Machine (M2) communications which are one of the basic technologies for Internet of Things (IoT). Therefore, Distributed Ledger Technologies with their inherent property to provide security, privacy and decentralized operation are engine for todays and future reliable, autonomous and trusted IoT platforms. For this reason, IoT using DLT can be considered as "Internet of Trusted Things". This paper considers tree basic DLT technologies according to their architecture: blockchain, tangle and hashgraph. Their characteristics are compared considering number of criteria, with the aim to find a proper architecture for a specific M2M application.**

Keywords—Distributed Ledger Technology, Internet of Things, Machine-to-Machine, transactions, Proof of Work, Proof of Stake, stability, trust, blockchain, tangle, hashgraph, hash function, digital signature, directed acyclic graph, consensus algorithm, mining, Winternitz signatures, IOTA, Bitcoin, Byzantine error, quantum computing

I. Introduction

Distributed Ledger Technology (DLT) is a technology enabling a special form of electronic data processing and data memorizing. The main component of it is a decentralized database called "distributed ledger", that allow data writing and reading for all members of a network, for which a database is implemented. A DLT needs no central instance allowing data writing and reading, like centralized databases. Rather every network member can add data anytime, followed by a data actualization process which enables, that all network members are up-to-date with the newest state of a database.

The sense of using a DLT is usage of new tools which minimize the probability of errors, successful frauds and paper-intensive processes. For these reasons, DLTs are considered as a driver of future technologies which will have a significant impact to the society and every day's life.

The remaining part of the paper is organized as follows: Chapter II explains basics of different DLT architectures, which are taken as a basis for a comparison of DLT properties. Chapter III considers DL technologies defined in Chapter II and compares them according to their decentralization stage, accessibility, transaction costs, market decentralization, consensus algorithms and mining, speed, off-chain functionality, stability, security, resistance against brute force attacks using quantum computers, resistance against Sybil attacks, Byzantine error tolerance, double spending resistance, suitability for usage at Internet of Things and problems they are facing to. Chapter IV concludes the paper with a consideration for future use cases.

II. Basic Concepts

A. Basic DLT Architectures

There are three basic DLT architectures, which will be considered for comparison of DLT characteristics in the remaining part of the paper: chain or list, Directed Acyclic Graph (DAG) as tangle and DAG as tree.

Chain or list is a sequential data structure consisting of a list of blocks connected to each other. Every block consists of a time stamp, transactions made in the time marked by a time stamp and a hash value of the previous block:

$$Block\ n = Hash(Block\ n\text{-}1) \,||\, Timestamp \,||\, (Trans1, Trans2, Trans3, Trans4) \quad (1)$$

Typical representative of the chain or list architecture is a blockchain, which is a basis for the oldest and the mostly spread cryptocurrency: Bitcoin invented in 2008 by Satoshi Nakamoto [1].

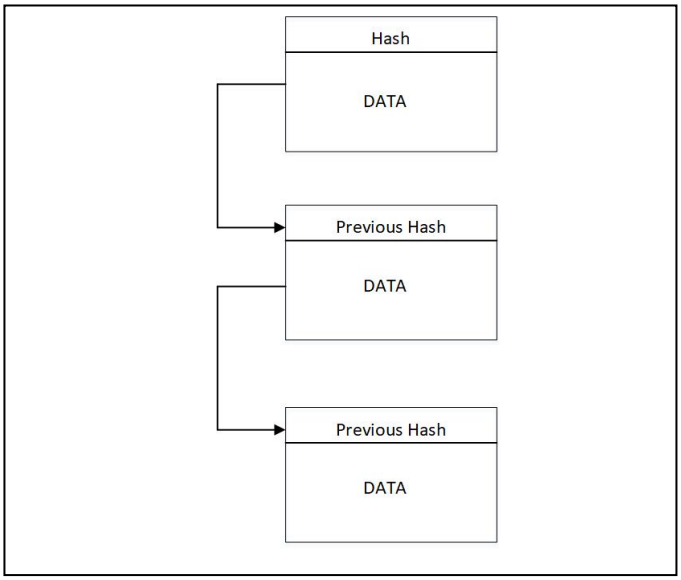

Fig. 1. Blockchain.

Directed Acyclic Graph (DAG) is a finite directed graph with no directed cycles consisting of finitely many vertices and edges, with each edge directed from one vertex to another, but without back loops. A tangle is a network of nodes, which grows with every transaction. Transactions are stored in nodes and verify the validity of transactions in other nodes, which can be seen as a directed connection between nodes. Tangle's grow in more than one direction means that transactions are processed at the same time, such speeding up the network.

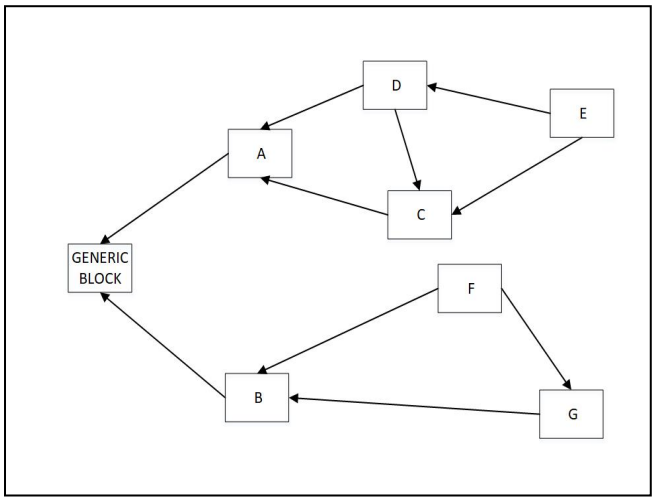

Fig. 2. Tangle.

Tangle is a basis for IOTA, a cryptocurrency which is one of the main concurrent of Bitcoin, especially in the field of M2M communications. IOTA was founded in 2015 by David Sønstebø, Sergey Ivancheglo, Dominik Schiener und Serguei Popov [2] and works formally as IOTA Foundation since 2017.

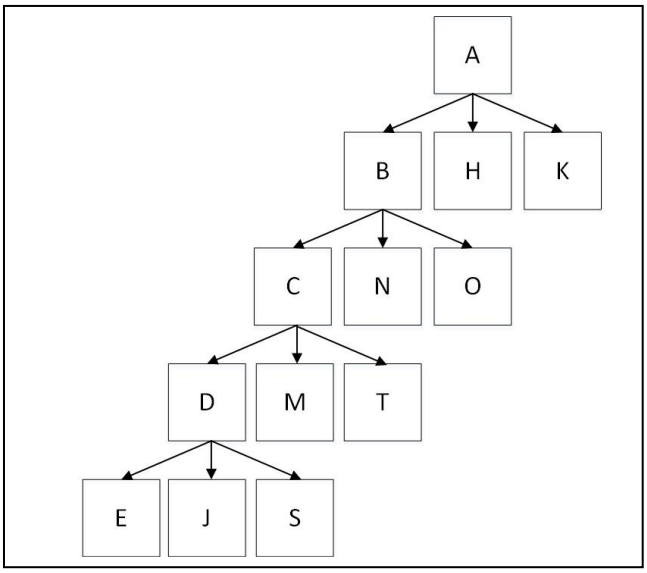

Fig. 3. Hashgraph.

Directed Acyclic Graph (DAG) as a tree is the youngest DLT architecture, which is the basis for a hashgraph. Hashgraph is a data structure which documents, who and in which order gossiped with whom. It is an all the time growing tree, whose fruits spread gossip: information about the communications between the network member, including who communicated with whom, is memorized in a hash. All the hashes together make a hashgraph. Data are organized as blocks, so called "events" consisting of transactions together with time stamps and hash values of so called "parent – events", i.e. blocks (i.e. events) which caused them:

$$Block\ n = Hash(Parent\ a) \,||\, Hash(Parent\ b) \,||\, Timestamp \,||\, (Trans1, Trans2, Trans3, Trans4) \quad (3)$$

Hashgraph was invented by US professor Leemon Bairds in 2016 [3].

B. Restrictions in Participation

The german IT Security Association (TeleTrusT) published a paper, which compares blockchain systems regarding participation restrictions [6]. Although the focus of the evaluation is set on blockchain systems, the mentioned concepts (mainly identity management and reading access) are also considerable aspects of alternative design principles such as Tangle- or Hashgraphs.

There are three different system types, which have different restrictions for participation and reading access: *Public permissionless systems*, *public permissioned systems* and *private permissioned systems* [6][7]. The first type, the public permissinless systems do not have restrictions on both reading access and participation in the system. This means that every entity can read and write to the blockchain. Bitcoin is the most popular example for such systems. However, since there are no restrictions in participation and no restrictions for creation of new identities (Bitcoin), there have to be mechanisms that restrict influence of single individuals to the whole system. Bitcoin uses the so-called proof-of-work, which limits influence of entities by their provided limited calculation power. However, public permissionless systems are sensitive for attacks like the 51% attack, where an attacker can manipulate the blockchain if it provides more than 50% of the overall available calculation power. This problem makes public permissionless systems infeasible for scenarios with only a few devices that have only limited computation resources.

Another system type is called *public permissioned.* The term "public" refers to the reading access to the system: Every entity can participate in the system and submit transactions. However, the instances that write to the blockchain are known and trusted by every participant. This is a contrast to fully decentralized systems like Bitcoin that explicitly do not require trust between any involved entities [1]. Advantages of permissioned systems are the known number of identities that write to the blockchain and further limited influence of single entities independent of their calculation power. This enables more efficient consensus-finding algorithms like Byzantine-fault-tolerance. Possible disadvantages of this system design is the more centralized architecture that requires trust in the miners (also sometimes called "committee"). This can lead to intransparencies and there must be rules that regulate the participation into this committee. These rules must be accepted by all participating entities. This design can have advantages for IoT

environments that require an efficient consensus finding mechanisms that are robust against the 51% attack.

The third system type *are private permissioned* systems. This type is similar to the public permissioned systems, but with additional restrictions on reading access to the blockchain. This scenario can be interesting for company-intern distributed-ledger-systems where the identities of the participating entities are known, and the data stored by the distributed ledger can be considered confidential.

C. Representation of Identities and Proof of Work

Systems that do not have restrictions for creation of identities and participation in the mining process have to limit influence of single entities of the system. There are two popular mechanisms: Proof of Work (PoW) and Proof of Stake (PoS). The PoW-principle was described in [1] and works as follows: All participants agree that the longest blockchain in the system is valid. If an attacker tries to manipulate data in a block *n* (e.g. double-spend a coin), it must build a chain of blocks with new blocks that is longer than the current valid blockchain. Every block has a hash of the previous block, several transactions and a nonce. The nonce has to be manipulated in a way that the hash over the whole block has a certain pattern, e.g. starts with a defined number of zeros. Since the output of a cryptographic hash function (e.g. SHA-256) can be seen as random, the miners have to use brute-force search algorithms. The PoW can adjust the probability by which an entity finds a nonce that results in a hash with the provided pattern. An attacker must have more than 50% of the overall calculation power to let the "own" manipulated chain grow faster than the valid chain (Also see [1]). This is because the honest miners will work on the valid chain and the possibility that one of the honest miners fill find a new block is proportional to the overall available computation power in the network of honest miners. However, this mechanism leads to high energy consumption and requires a network of honest participants with sufficient computational resources.

A variation of the PoW principle is the "proof of stake" (PoS) principle. The miners have to solve riddles just like in PoW-based systems, but the possibility to find a solution increases with the amount of tokens (coins) that are owned by this particular entity. The idea behind PoS is the assumption that an entity that owns a large amount of tokens does not want the system to be attacked. The PoS also aims to prevent the 51% attack that only requires more than 50% of the overall available calculation power. It is assumed that owning more than 50% of the networks tokens is more difficult to achieve than achieving a required amount of calculation power. The PoS can be an interesting for comparatively small IoT environments that are sensitive for attacks basing only on calculation power. However, the PoS principle does not automatically prevent the double-spending problem. Additional efforts are required to prevent entities to misuse their influence for own purposes. Miners can still try to double-spend tokens and vote for manipulated chains without having to waste computational resources for this effort. For PoS and PoW, also see [8]. PoS could be interesting for IoT environments with fair distribution of tokens and a basic level of trust between peers.

III. DLT Comparative Characteristics

A. Suitability for M2M in Internet of Things

For M2M communications, the most important characteristic is low cost (or zero cost) transactions (so called "microtransaction").

Bitcoin is, thanks to its high transactions costs, not suitable at the moment for microtransactions. Nevertheless, smart contracts of Ethereum, which is also based on a blockchain technology, offer an important approach to the interaction between man and machine as well as between several machines. Communications is particularly costly when it comes to a chain of multiple actions involving different devices.

IOTA is applied primarily to IoT for M2M payments and data integrity. Toll-free IOTA transactions are therefore suitable for IoT, e.g.:

- sensors that sell data in real time to computer stations;
- sensors that purchase analytical capabilities from computer stations;
- consumers who buy electricity from any electricity producer;
- devices that buy storage space;
- devices that buy bandwidth on demand, without subscriptions;
- data integrity that is guaranteed for many devices;
- tamper-proof events logging that is guaranteed for each type of infrastructure;
- E-Voting and e-governance.

Since the end of June 2018, hashgraph (in a scope of the Hedera enterprise) is a member of the Trusted IoT Alliance (an open Source software consortium) with the goal of creating a secure, scalable, interoperable and trustworthy IoT ecosystem. Hashgraph transaction fees are expected to be a small fraction of other public platforms on the market today because the Hedera network has high throughput and does not require Proof of Work (PoW).

B. Decentralization

Decentralization is a requested property DLTs, as it comprises independence of one (or more) persons/machines controlling the network. Instead, peer-to-peer interaction drives the network, as no third party is needed. Nevertheless, it is not easy to establish a stable decentralized network, especially in an early stage of an early development.

Bitcoin is an example of a decentralized blockchain: the decentralized database contains an all the time growing list of transactions data. The databank is chronologically linearly extended, like a chain adding new elements at the end of it. When one block is complete, a generation of the next one starts.

IOTA is partly decentralized, i.e. it cannot be defined as a decentralized as long as a so called "coordinator" exists, which protects the network from malicious attacks. The role of the coordinator is to issue periodic milestone transactions, which reference valid transactions. On the mainnet, these milestones are issued every minute. It is planned to completely remove the coordinator once the network is large enough, enabling complete IOTA decentralization.

Hashgraph has been developed as a centralized private structure based on access control (for joining and leaving). Decentralization of the network would be possible, if an additional protocol under the hashgraph-protocol would take care of admission controls. Nevertheless, such a solution would delay the hashgraph communications and in this way it would lose its main advantage over other (also previously mentioned) networks: speed. Nevertheless, improvements in direction of public network and decentralization are published in 2018 [4].

C. Accessability of the Technology

Bitcoin is a closed source network, as it is licensed by Massachusetts Institute of Technology (MIT). Both IOTA and Hedera hashgraph are open source, in difference to Bitcoin.

D. Transactions Costs

Transaction costs are generally market dependent and therefore always fluctuating. Ethereum [5], which is based on a blockchain technology like Bitcoin, is invented for the purpose of smart contracts. Therefore, the aim of Ethereum (and other blockchain-based technologies) is further reduction of transactions costs, as an imperative for a M2M communications for IoT.

IOTA network allows transaction of a negligible costs, which can be considered as "zero" transactions. For this reason is IOTA meant to be the main cryptocurrency for IoT transactions, so called "microtransactions" between machines. There are numerous examples for such present and future transactions in the field of industrial automation, autonomous driving and robotics. Additionally, tangle's architecture is capable to enable a large number of mictrotransactions in a few seconds and has a high scalability.

Hashgraph aims to have similar desired properties as IOTA: cheap transactions as a results of an inexpensive hardware and absence of Proof of Work concept.

E. Market-oriented Decentralization

Decentralization can be observed not only as a network property, but also as a market-oriented characteristic, i.e. as business model.

Bitcoin, for example, is an example of a business model without data sharing: data are observed as a competitive advantage, i.e. resources which have to be protected.

IOTA presents a new, decentralized business model with data sharing, whereby data are shared between sensors and actors for a wealth being of a M2M communications. Therefore, the transactions costs are aimed to approach zero.

The business model of a hashgraph follows the one of IOTA: data are shared between network nodes using a gossip protocol and aiming zero transactions costs.

F. Consensus Mechanism and Mining

Consensus is a key mechanism for DLTs, as it insures, that the network nodes control their transactions and that they approve the existence of those transactions. Consensus is crucial for prevention of double spending and other non-valid data on the ledger. This is especially important in cases of crypto currencies.

Nowadays information is mostly centralized and their users are forced to trust the enterprises or persons possessing and/or controlling those information. Big centralized systems do not have to use any consensus mechanisms and therefore they information processing is efficient and well scalable.

Decentralized systems provide per definition no central control. A DLT is properly designed if the system users do not have to trust the third person or other system users. In order to enable functioning of such systems, there are different consensus mechanisms, all of them having their advantages and disadvantages.

In case of Bitcoin, consensus is reached by a competition mechanism: several parties (network users) compete with each other to add the next block to the blockchain and receive the reward in form of transaction fees. The production of a next block is done by so called "mining", which is based on Proof-of-Work (PoW). PoW is used to confirm transactions and create new blocks in the chain. With PoW, miners (users which take a part in mining) compete against each other to complete and reward transactions on the network. On a network users send each other digital tokens. A decentralized ledger collects all transactions into blocks. Miners take care of the mining process to confirm the transactions and to arrange blocks. The most important working principles are a complicated mathematical puzzle and the possibility to prove the solution easily. Consensus depends on the generation of the transaction and is largely carried out by a small group of miners on the network. This results in what cryptocurrencies should avoid: centralization. The most important mining principles are a complicated mathematical puzzle and the possibility to prove the solution easily. There are many possible puzzles, for example:

- Hash function: To find a collision
- Integer Factorization: To present a number as multiplication of two other numbers
- Guided Tour Puzzle Protocol: If the server suspects a Denial-of-Service (DoS) attack, it requires a computation of the hash functions for some nodes in a defined order: the problem is to find a chain of collisions of hash functions.

As the network grows, it is facing ever more difficulties in finding a hash collision. The algorithms need more and more hash power to solve the collision problem. The complexity of the task is therefore an important issue.

Consensus mechanisms of IOTA is based on PoW without mining (and thus without transaction fee): every user in the network must participate in the consensus, i.e. the one who executes a transaction in the tangle has to automatically check two further transactions, with a small riddle (PoW) to be solved. Here, however, the current version serves to protect against spam and Sybil attacks. IOTA consensus is not based on PoW, like in case of Bitcoin. Therefore, the network decentralizing is supported, as trust is not delegated to miners. Additionally, there are no transaction fees, such supporting IoT applications.

Consensus mechanism of a hashgraph is based on the open consensus model called "gossip-over-gossip" without

mining (and thus without transaction fee). This refers to the process in which the nodes join the network and a consensus in the order of the transactions in the hashgraph platform. The consensus timestamp prevents an individual from influencing the consensus sequence of transactions. New node operators join the network and are paid for their services when they maintain the hashgraph. The model was designed in order to prevent the centralization of power through consensus, by encouraging the development of a decentralized network with potentially millions of nodes.

G. Speed

Blockchains get slower and slower with the increased number of users. This property is very problematic for large blockchain networks, as Bitcoin, where the actual time for the realization of one transaction lasts ca. 10 minutes.

The concept of tangle is much friendlier considering the network speed in dependency on the network size: automatic prove of two other transactions for running a new transaction has an additional advantage to speed up the network with the increase of network users. This is possible, however, if two conditions are fulfilled: if there are enough (full) nodes to perform the transaction validation and if they have sufficient fast Internet connections for synchronization of actual information between the nodes. Therefore, network capacity becomes a main problem of tangle's speed.

Hashgraph has a much higher throughput than other DLTs: hundreds of thousands of transactions per second can be performed thanks to the used gossip protocol. Acceleration is achieved by dividing the hash graph into so-called rounds, whereby only in the first events (so called witnesses) in each round, transaction invoices take place. The delay is very small: sending a transaction takes only a few seconds.

H. Off-chain functionality

Off-chain functionality can be compared with the off-line functionality: if a DLT can partly function without the connection to the main ledger, it possesses an off-chain functionality. At the moment, when the connection to the main ledger is built up again, the off-chain nodes synchronize with the main DLT and upload the information from other nodes and about the transactions they missed in time they were off-chain.

In case of Bitcoin, transactions must be routed through network nodes (on-chain). Transactions cannot occur outside the blockchain because the ledger must be updated constantly to avoid double spending. Nevertheless, Ethereum works on the on-chain scalability.

As a difference to Bitcoin, IOTA nodes can work without being connected to the main tangle (off-chain). If the node wants to connect to the network later (for example, when an Internet connection becomes available), it can be easily done (getting on-chain).

The gossip protocol of a hashgraph allows members to have a copy of the hash graph (the full image and history of all transactions are split between nodes). In case a member is off-chain (e.g. PC turned off), it gets all the missing information from other members as soon as it is back on-chain.

I. Stability

Stability of the network is a very important and desired property. In some systems, there can be central instances that ensure stability of the system.

Stability of the Bitcoin is realized on a decentral manner: the difficulty in the blockchain is set in such a way that in average 10 minutes are needed to find a suitable hash and thus generate a block. This difficulty is adjusted every two weeks (after 2016 blocks), because for a stable blockchain it is important that the PoW has a considerable effort (in case of a too small PoW the probability of successful Sybil attacks grows). A good measure of the strength of the PoW is the time required to perform this PoW, i.e. to find a hash with the required zeros at the beginning.

Stability of the IOTA's tangle is, as a difference to Bitcoin's blockchain, centrally controlled: the so-called "coordinator" (a server that currently has full control over all transactions) takes care of keeping the tangle "in-the-box" and hindering disagreement in consensus, so that no mesh forking happens. This works by allowing milestones to set the "full nodes" (computers that take care of validating transactions) to the validation direction and to starve old transactions that would allow the tangle to grow in the wrong direction.

Similar, to IOTA's network, stability of a hashgraph is also centrally controlled, relying on technical and legal controls to guarantee the stability of the hash graph. Technical controls mean that only verified software clients are allowed to use the hashgraph (thus it is not possible for a network node to branch the official software version of the hashgraph platform and make changes). Legal controls ensure that the hashgraph platform does not convert to a competing platform.

J. Resistence against brute force attacks with quantum computers

According to IBM research, "Today, quantum computing is a researcher's playground. In five years, it will be mainstream. In five years, the effects of quantum computing will reach beyond the research lab"[5].

There are many discussions and assumptions about the eventual existence of quantum computers and the remaining time, until they start be produced/used. Anyway, their appearance in the nearer future is certain. Therefore, today's crypto systems should be prepared for the possible (mis-) usage of quantum computers and develop resistance against brute force attacks using quantum computing.

Blockchain technology is based on public key cryptography to ensure the security of the ledger: it functions using hashing and digital signatures. Hashing provides a way for everyone on the blockchain to agree on the current world state, while digital signatures provide a way to ensure that all transactions are only made by the rightful owners. In addition, Bitcoin relies on the work of the miners to solve certain complex mathematical problems in order to verify transactions: a task that could be solved exponentially faster using quantum computing platforms (up to 100 million times faster!).

In contrast to Bitcoin and many of other existing cryptographic systems that would be weakened or broken if

quantum computing were available, IOTA uses a cryptographic signature scheme (Winternitz signatures) that belongs to the so-called "exclusive quantum resistant Cryptographic algorithms".

Since hashgraph does not use PoW, there is no danger of quantum computing. Unlike Bitcoin and to a lesser degree to IOTA, hashgraph is also not susceptible to attacks by quantum computers. The hashgraph system is based on "virtual voting", which does not require solving any puzzles that a quantum computer could affect. However, brute force attacks with quantum computers for private keys could be dangerous, but only when the hashgraph platform becomes public.

K. *Resistance against Sybil attacks*

Resistance against Sybil attacks or forging identity attacks are important for applications connected to transactions, therefore also cryptocurrencies. The attack would mean that one DLT user generates several entities, in order to impact the consensus and successfully perform double spends.

Bitcoin uses PoW for transaction verification as a protection against Sybil attacks: block generation ability is proportional to computational power available through the PoW mechanism. An adversary is in this way limited in how many blocks they can produce. This provides strong cryptographic guarantees of Sybil resistance.

IOTA uses PoW only as a guard against Sybil attacks and not, as a difference to Bitcoin, for mining.

Hashgraph, as long as used as a private network, is naturally protected against Sybil attacks, like all other private networks, thanks to the prior knowledge of the identity of the participating nodes (all nodes are known beforehand and the network is not open for non-proven i.e. not registered participants). This means that no Sybil resistance mechanism has to be set up and thus the throughput can be drastically increased.

L. *Byzantine Error Resitance*

A Byzantine tolerant network has following properties:

- It must reach consensus,
- It knows when it achieves consensus, and
- It knows that enough nodes will reach the same consensus, so that consensus is declared true.

Miner in Bitcoin use their hardware to keep or delay the progress of the block. This means that individual members can influence the consensus.

The IOTA network is asynchronous: generally, nodes do not necessarily see the same amount of transactions. The tangle can contain conflicting transactions. The nodes do not have to reach a consensus on which valid transactions have the right to be in the ledger, meaning that all transactions can be in the tangle. However, in cases where there are conflicting transactions, the nodes must decide which transactions are orphaned, whereby this decision can be false.

Hashgraph uses the "gossip about gossip" principle for reaching the consensus. Thus the developers promise to deal with the problem of the Byzantine Error. Hashgraph characterizes asynchronous Byzantine Error Tolerance, which allows the network to continue functioning even in the case of internal attacks.

M. *Double Spending Resistence*

Blockchain for Bitcoin formed the first digital currency that solved the problem of double spending issues without a trustworthy third instance. Bitcoin users protect themselves from double spends by waiting for confirmations when they receive payments through the blockchain.

IOTA, compared to Bitcoin, has a disadvantage not to guarantee a 100% double spending, rather a certain probability, that double spending will not happen.

Hashgraph is, thanks to its resistance against Sybil attacks and timestamping of events, resistant against double spending.

IV. DLT Problems and Conclusion

The Distributed Ledger Technologies are promising to be the driver of future M2M applications thanks to their properties of distributed trust, which is based on cryptographic mechanisms. This paper presents comparative characteristics of three representative DL technologies based on different ledger architecture. Nevertheless, there are many more DLTs with their advantages and disadvantages, but all of them can be considered to belong one of those architectural groups.

The main problems which DLTs are facing are following:

Bitcoin has a problem of a low speed (low transaction volume) and high energy consumption for block production.

The main problem of IOTA is existence of a coordinator and such network centralization, as well as certain (not precise defined) probability of double spending. Hashgraph is good for a closed, private network.

Acknowledgment

The material used in this paper is partly the result of the first phase of the project in scope of a „Mobility 2030" project at Carmeq GmbH.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," https://Bitcoin.org/Bitcoin.pdf, 2008

[2] S. Popov, "The Tangle", https://iotatoken.com/IOTA_Whitepaper.pdf, 2017

[3] L. Baird, "Overview of Swirlds Hashgraph", https://www.swirlds.com/downloads/Overview-of-Swirlds-Hashgraph.pdf, 2016

[4] L Baird, M. Harmon and P. Madsen, "Hedera: a Governing Council & Pubilic Hashgraph Network, https://s3.amazonaws.com/hedera-hashgraph/hh-whitepaper-v1.1-180518.pdf, 2018

[5] "The future is quantum", https://www.research.ibm.com/ibm-q/

[6] TeleTrusT – Positionspapier "Blockchain" - Bundesverband IT-Sicherheit e.V, https://www.teletrust.de/fileadmin/docs/publikationen/broschueren/Blockchain/2017_TeleTrusT-Positionspapier_Blockchain_.pdf. 2017

[7] Daniel Drescher, Blockchain Basics, 2017 DOI: 10.1007/978-1-4842-2604-9_1

[8] ddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. 2014. Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *SIGMETRICS Perform. Eval. Rev.* 42, 3 (December 2014), 34-37. DOI: https://doi.org/10.1145/2695533.2695545