EXAMENSARBETE INOM TEKNIK,
GRUNDNIVÅ, 15 HP

STOCKHOLM, SVERIGE 2018

Micropayments Between IoT Devices

A Qualitative Study Analyzing the Usability of DLT:s in an IoT Environment

SEBASTIAN EL-HAGE

GUSTAV HOLST

KTH
SKOLAN FÖR ELEKTROTEKNIK OCH DATAVETENSKAP

Sammanfattning

Det finns idag ingen standardiserad betalningslösning för att genomföra mikrobetalningar mellan Internet of Things (IoT) enheter. Denna studie genomfördes för att undersöka huruvida Distributed Ledger Technology (DLT) skulle kunna användas som en mikrobetalningslösning för IoT. En mer generell efterfrågan för en skalbar mikrobetalningslösning, och effekterna av en sådan, undersöktes. En kvalitativ studie genomfördes, där åtta ostrukturerade intervjuver gällade ämnena DLT och IoT, hölls för att komplementera litteraturstudierna. Sedan genomfördes en ostrukturerad och fem semi-strukturerade intervjuer för att kunna besvara de frågeställningar som definierats. Bitcoin blockkedjan fungerar inte som en mikrobetalningslösning på grund utav dess skalbarhetsproblem. Studien identifierar en positiv syn på Lightning Network, som löser skalbarhetsproblemen genom att använda sig av transaktioner utanför kedjan. Denna lösning är dock inte fullständigt implementerad, vilket leder till flera osäkerheter angående exempelvis hur decentraliserat nätverket verkligen kommer att bli. Utöver detta finns även svårigheter med användandet av DLT:s för små IoT-enheter, vilket härstammar ifrån deras CPU- och lagringsbegränsningar. En efterfrågan på en hållbar mikrobetalningslösning identifierades, och denna skulle kunna fungera som en katalysator för etablerandet av pay-per-use affärsmodeller. Tittar vi på mer kraftfulla IoT-enheter skulle Lightning Network fungera som en mikrobetalningslösning. En sådan teknologi är eftertraktad och dess användbarhet kommer bara att växa i och med utvecklingen av IoT-enheter.

Micropayments Between IoT Devices; A Qualitative Study Analyzing the Usability of DLT:s in an IoT Environment

S. El-Hage, *Student, Royal Institute of Technology*, G. Holst, *Student, Royal Institute of Technology*

***Abstract*—Today there exist no standardized payment solution for performing micropayments between Internet of Things (IoT) devices. This study was conducted to examine whether Distributed Ledger Technology (DLT) could be suitable as a micropayment solution for IoT. Also, a more general demand for a scalable micropayment solution was examined, along with its potential. A qualitative study was performed by first conducting eight unstructured interviews regarding the subjects DLT and IoT, to be used as a complement to the literature research. Then, one unstructured and five semi-structured interviews were held to answer the research questions. The Bitcoin blockchain does not work as a micropayment solution, due to scalability issues. This study identified a positive outlook on the idea of Lightning Network, solving the scalability problems with off-chain transactions. However, since a fully functioning network is yet to be implemented, there exist uncertainties, for example regarding how decentralized it will really become. Also, issues considering the usage of DLT:s on small IoT devices arose, stemming from CPU and storage constraints. A demand of a sustainable micropayment solution was identified, possibly being a catalyst of the emergence of pay-per-use business models. Considering more powerful IoT devices, the Lightning Network could function as a micropayment solution. Such a technology is sought after, and its applicability will only increase as IoT devices evolve.**

***Index Terms*— Blockchain, Directed Acyclic Graph, Distributed Ledger Technology, Internet of Things, Micropayments.**

I. Introduction

A. Internet of Things

The Internet of Things (IoT) can briefly be defined as a system consisting of networks, containing vast amounts of connected devices. As of today, IoT is structured in a centralized way, in the sense that most devices interact through a central entity, e.g. a server. In the near future we are expected to see a rapid growth in the IoT market and as the number of devices and amount of interaction increases (Framingham, 2017). Intuitively, a centralized system combined with this growth could result in network bottlenecks and security concerns. Therefore, direct Peer-2-Peer (P2P) interaction, without always utilizing a central entity, could be important for the continuous IoT growth. This concept of a decentralized system, where the devices interact autonomously, is what henceforth will be referred to as "full-scale IoT".

.

B. Micropayments

This paper will focus on one type of device-to-device interaction, micropayments. Micropayments are defined as *"a payment of a small amount, e.g., a fraction of a penny"* (Coron & Nielsen, 2017). These are often issued as successive partial payments while utilizing a service or product (i.e. pay-per-use). Incorporating micropayments into a full-scale IoT, having a device autonomously pay another device, could enable a machine-to-machine economy. A concrete example could be a device renting CPU-power from a more powerful device, paying each second for the exact amount of power needed, thus creating a dynamic payment flow. However, issuing autonomous P2P micropayments has its challenges, one of them being that it would require a technology that is both secure and scalable.

C. Distributed Ledger Technology

One type of technology that has been identified as a potential way of managing and recording safe micropayments is Distributed Ledger Technology (DLT). DLT is defined by Prableen Bajpai (2018) as *"... the technological infrastructure and protocols that allows simultaneous access, validation and record updating in an immutable manner across a network spread across multiple entities or locations"*. The undoubtedly most renowned type of DLT is called blockchain. Blockchain is a ledger, or more comprehensive, a shared database, consisting of linked blocks which contains the transactions made within the network. The ledger is considered to be tamper-proof, making it exceptionally suitable for its main area of application - cryptocurrencies, e.g. Bitcoin. As of today, questions regarding the scalability of the Bitcoin blockchain has arisen, it is slow and expensive to perform transactions. This is one of the reasons why specialized adaptations and alterations of the original Bitcoin blockchain are being developed. Furthermore, even alternative DLT:s are developed, challenging the blockchain structure by storing the data in other ways than a sequence of blocks.

D. Problem definition

Today there exist no standardized way of performing micropayments between IoT devices. Even considering micropayment solutions in general, the transaction fees have been and are still a problem considering their relative size to the micropayment itself. IoT, as an evolving concept, is highly affected by the development of its surrounding technologies. This combined with the demand of enabling devices to perform increasingly complex tasks, insinuates that a micropayment solution is both highly demanded and would have a big impact on IoT.

Worth emphasizing is the fact that IoT is a multi-industry concept, thus a big impact on IoT itself may resonate even bigger considering the range of industries it could affect. Given the example of micropayments, this could be utilized in autonomous cars as well as in the monetizing of sensors by selling their data. Therefore, we identify a standardized micropayment solution as one of the voids needed to be filled for IoT to reach its full potential. This paper does not aim to identify an *optimal* transaction protocol, thus it will not consider the potential fit of other types of solutions other than DLT:s, e.g. Visa or PayPal.

E. Purpose and ethical aspects

The purpose of this paper is to identify if there is a potential use case of performing micropayments between IoT devices using DLT:s. The subjects addressed are relevant and actual research topics. Hopefully this paper can serve as a motivator to perform further research within the examined fields. Future work will be presented more thoroughly in section VI.B. This paper is intended for people with a technological background or interest, but could also serve a purpose for researchers within IoT and DLT.

Considering both societal and ethical aspects, this paper can contribute to an increased interest of blockchain technology and how this can be utilized in IoT. Also, the evolution of IoT is something that will affect a vast number of people in the coming years, being new inventions or an increased usage of IoT devices. At last, DLT is considered to be a general-purpose technology making research within the subject impactful.

F. Research questions

This paper will examine one main research-question. To be able to evaluate it thoroughly, the question is divided into three sub-questions explained further in this section. The main research-question follows:

- *"Are there existing DLT:s suitable to perform micropayments between IoT devices, and what economic effects could a sustainable micropayment solution have?"*

The first sub-question scrutinizes the scalability of DLT:s when issuing large numbers of small transactions.

- *"Are existing DLT:s suitable to perform micropayments?"*

In the second sub-question the objective is to answer to what extent DLT:s are applicable in an IoT environment.

- *"Are existing DLT:s utilizable for devices in the IoT environment?"*

The third sub-question has a distinct economic theme, examining the demand and effects of a sustainable micropayment solution.

- *"Does a demand of a sustainable micropayment solution exist and what business models could such a solution affect?"*

II. Background

A. DLT

DLT is an umbrella term for technologies that distribute ledgers and/or information among its users. The term is often used as a synonym of blockchain technology but is, in this paper, referring to the category of technology in which blockchains can be found. A distributed ledger can be described as a database where members of a P2P network all hold the information stored within it. There exists a consensus among the entities regarding the current state of the ledger, thus all updates demand the validation of the network (Drescher, 2017). Storing data in this manner leads to many benefits. One is that this mitigates the problems with a single point of failure meaning that to bring the system down, an attacker must target a majority of a network and not a single point (McPhee & Ljutic, 2017). Another benefit is that this enables true transparency, since the ledger is publicly distributed.

1) Blockchain

a) Blockchain structure

Blockchain technology is a disruptive technology. Blockchains are a subcategory of DLT where the distributed data is stored as a linear sequence of blocks, a form of linked list. The sequence is chronological, meaning the last block on the chain is also the most recently added. The blocks are linked together by a hashed pointer, meaning that each block contains a hash of the previous block's data (see *fig. 1*). This counteracts tampering of the ledger, since altering the data of an earlier block will produce a different hash not corresponding to the rest of the chain (Naranyan, 2016). The blocks also contain other information stored in different components of the block. For the purpose of understanding this study only two components of the blocks are necessary to explain, the transaction field and the block header. The transaction field stores the transactions included in that particular block (Drescher, 2017). The block header can be considered the identity of the block that contains, among other data, the earlier mentioned hashed pointer.

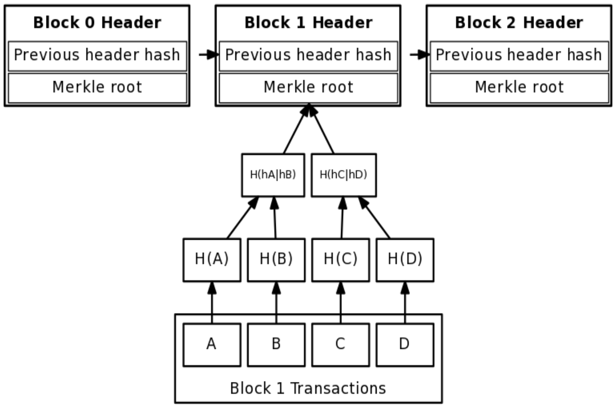

Fig 1: Illustration of the blockchain structure and its components (Riady, 2016)

b) Transactions

In a blockchain network transactions are performed using public key cryptography (Deloitte, 2016). Each user has a key pair consisting of a public and a private key. The public key is shared with the whole network to identify each users account and the private key is kept hidden. To perform a transaction, the user needs to broadcast a digitally signed transaction, this is basically the transaction information signed with the private key. The digitally signed message can only be created by the user with the right private key. The network can then check the digitally signed message by simply decrypt the message with the sender's public key and verify that the sender has the funds it wants to send. It is, if correct, then included in the data of the next block to be published (Drescher, 2017).

c) Consensus algorithm

The consensus algorithm is essentially the way that the network reaches an agreement about the current state of the ledger. Deciding what data is added to the ledger and electing who gets the right to add it (Drescher, 2017). This algorithm includes rules such as the Longest Chain Rule that comes into use when two miners finds two separate blocks at almost the exact same time. This is what is called forking. They will in this case, due to latency issues, not know about the other block and then the LCR is used to determine where to add the next block, i.e on the chain that is the longest (Judmayer, Stifter, Krombholz & Weippl, 2017). The most adopted and implemented consensus algorithm is the Proof-of-Work (PoW), used in the Bitcoin and Ethereum protocol (Gramoli, 2017). A more detailed description of the PoW is found in section II.A.2.b.

d) Types of blockchain

There are several types of blockchains: Public, consortium and private blockchains. A public blockchain is a fully decentralized blockchain with no access permission required and anyone can participate in the consensus process. In a consortium blockchain there is a predefined set of nodes that handle the consensus process and in a private blockchain it is that process is fully controlled and it is also decided who can read from it (Thompson, 2016). This article will only consider public blockchains where one of the most implemented blockchain protocols, Bitcoin, is included.

2) Bitcoin

The Bitcoin blockchain is one of many blockchain implementations (i.e. Ethereum, Ripple). However, for the understanding of this paper, the information about the Bitcoin blockchain and its properties is sufficient.

a) Merkle Tree

The transactions are all bundled in a data structure called a Merkle Tree. A Merkle Tree is a tree structure of hashes. In the case of Bitcoin, the hash values of all transactions are put on the lowest level of the tree (the leaves) and are hashed together in pairs to create their parent. The parents are then hashed together in pairs and this process continues until the two last parents are hashed into a so called Merkle Root which is stored inside the block header (see *fig 1.)*. The relationship that this creates between a single transaction and the whole hash tree is one of the reasons that Bitcoin is considered immutable. Changing a transaction leads to the hash value of the new changed tree to not conform to the Merkle Root (Drescher, 2017).

b) Proof-of-Work

To add a new block to the blockchain, one must provide a PoW. The PoW is a proof that a difficult mathematical puzzle has been solved, e.g. providing a solution. The mathematical puzzle essentially consists of finding a SHA-256 hash of the block header that is smaller than a predefined target value. To produce different hashes, a value called Nonce is added to the header hash. The Nonce increments by one each time, thus outputting different hashed values (Judmayer, Stifter, Krombholz & Weippl, 2017). The target value is a 256-bit number that starts with a specified number of zeroes. Increasing the number of zeroes required, also increases the difficulty of performing the PoW, since fewer values are accepted. In this way, by altering the difficulty of the PoW, the implementation of the protocol determines how often a new block can be created (Chen, Lin & Yung, 2015). In 2016, 18 leading zeros were required which led to the creation of a new block on average every 10:th minute. An important feature of the PoW is that the solution is easy verifiable by others in the network, leading to a fast process of reaching consensus regarding the updated state of the chain. (Drescher, 2017)

c) Mining

Mining in Bitcoin is the process of adding new blocks onto the blockchain. For a node to add a block, it has to spend computational power and energy on solving the PoW puzzle explained above. For this to be worthwhile the Bitcoin protocol issues a reward to whoever creates the block in form of some fixed amount of Bitcoin. In 2017 the reward was 25 bitcoins a block but this value halves every 210 000 block. (Grossklags & Preneel, 2017). The miner is also rewarded the transaction fees that each user performing a transaction pays. These fees vary and since each miner decides which transactions to include in its block. Meaning the miner is discriminatory to low fee transactions (Franco, 2015). The reason that the Bitcoin protocol has such an energy intensive consensus algorithm is to make sure that no miner creates a invalid block. The incentives for a miner to create a block with false transactions are small since it's easy for anyone to check the block and prove that it holds wrong information which leaves the creator with no reward.

d) Scalability issues
As mentioned the amount of transactions put in each block is finite, today the maximum limit of how much data a block can contain is one MB. (Göbel & Krzesinski, 2017) This together with the restrictions of the consensus algorithm, considering the time between each created block, leads to scalability issues regarding the speed of the transactions. The average of validated transactions per second (tx/s), as of today is 1-3,5 tx/s (Eyal, Gencer, Sirer & Van Renesse, 2015) The theoretical maximum is believed to lie around 7 tx/s (Karame, 2016). Also, especially regarding smaller transactions, since you are needed to pay a transaction fee, economical scalability issues arise.

3) Lightning Network
One approach to overcome these limitations is to perform transactions on a second layer of the main blockchain, i.e. off-chain transactions. By creating separate bi-directional payment channels, connected to the blockchain, it is possible to perform a near infinite number of payments within two or three transactions on the main-chain (Poon & Dryja, 2016). The transactions performed within the payment channel are not registered on the main-chain until the channel is closed. This drastically reduces the fee per transaction and enables near instant payments.

The payment channels are created by two parties depositing some amount to a multi signature address[1] with a local consensus regarding the allocation of the balance between them. This deposit is called a funding transaction (Poon & Dryja, 2016). To update this balance (i.e. making a payment) both parties need to accept by signing with their private keys and then save the updated balance, thus invalidating the prior. Any of the parties can, by themselves at any time, broadcast the most recent updated balance and redeeming each party its entitled funds and closing the channel. Would one party try to broadcast an *incorrect* balance, the other party is entitled to take the total amount shared in the channel, creating a non-deceiving incentive (Poon & Dryja, 2016).

The Bitcoin Lightning Network is a network consisting of these payment channels, enabling transactions to be routed across multiple channels without the sender and receiver being directly connected. To perform a routed payment, all payment channels throughout the chosen route must contain sufficient funds. To send one bitcoin from A to C, via B, both the A to B and B to C payment channels must contain at least one bitcoin each. However, conducting payments through an intermediate that could have malicious intents and chose not to forward the payment, wouldn't result in a trustless system. To solve this issue Hashed Timelock Contracts (HTLC:s) are implemented. The HTLC:s prevents any actual value to be extracted by the intermediates before the payment has reached its destination or been refunded. If an intermediary is offline or doesn't cooperate, meaning that it does not respond within a specific time called timeout, the sender will be refunded (Poon & Dryja, 2016). Further technological knowledge regarding HTLC:s is not needed to comprehend this article.

Worth mentioning is the existence of Raiden Network, the Ethereum equivalent to Lightning Network. However, since these two solutions are built on the same concept making them very similar, this study will only focus on the Lightning Network.

4) IOTA
A second approach to solve the scalability issues of the Bitcoin blockchain is to utilize a different data structure, a Directed Acyclic Graph (DAG), instead of a chain of blocks (Popov, 2018). A DAG is a graph consisting of vertices that are connected with directed edges, when following the edges from any vertex *v* there exists no path that loops back to *v*, thus making the graph acyclic (Fiore & Campos, 2013). An example of a DAG is illustrated below in *fig. 2*.

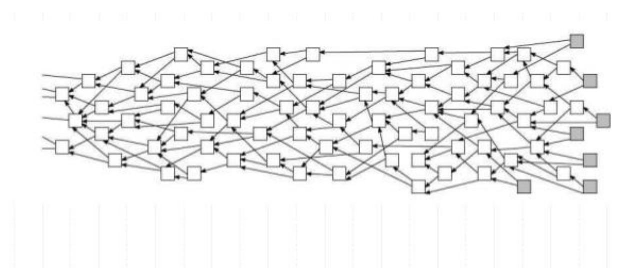

Fig 2: Visualization of the Tangle and its DAG structure (Popov, 2018)

IOTA is a cryptocurrency that implements this structure and its graph is called the Tangle. The vertices of the Tangle are called Sites, that similar to the blocks in the blockchain contains details about transactions. However, a site only contains a single transaction. To issue a new transaction the user lets a predefined algorithm locate two unapproved transactions in the edge of the graph, called Tips. The user then verifies that the transactions are valid and at last approve them by performing work similar to the Bitcoin PoW. This is arguably the most important property of IOTA to understand, since it generates two key effects. Firstly, there are no *direct* transaction fees since the users themselves perform the work. Secondly, the speed of the transactions increase with the number of transactions being made, the opposite to Bitcoin.

As of today, the number of users in the network is too small to fully prevent double spending attacks. To protect the graph and help it grow in the right direction, an address called the Coordinator (run by the IOTA Foundation) checks the Tangle and issues Milestone Transactions every minute. These milestones basically state that the transactions leading to them are 100% valid (Bramas, 2018). The Coordinator will eventually be removed when the number of users has reached a certain level to consider the network secure. Since the network is supervised by this central power, IOTA is not fully decentralized per say, even though it will be once the Coordinator is removed.

[1] A wallet that requires more than one signature to allocate funds

B. Internet of Things

IEEE defines IoT as: *"Broadly speaking, the Internet of Things (IoT) is a system consisting of networks of sensors, actuators, and smart objects whose purpose is to interconnect "all" things, including every day and industrial objects, in such a way as to make them intelligent, programmable, and more capable of interacting with humans and each other."* (IEEE Standards Association, 2015).

As of today, the majority of the interaction within the IoT network is performed in a centralized way, via servers. The devices, often sensors, mostly collect data and transfer this to a central entity that compiles the data and takes action. In the near future, the revenue of the IoT market is projected to grow rapidly. By 2020 it is forecasted to exceed $1000 Billion (Framingham, 2017). Intuitively this rapid growth will coincide with an increasing number of connected devices, leading to more extensive interactions.

One way to prevent bottlenecks being created and enable a scalable IoT is to implement a more decentralized IoT structure, utilizing direct device-to-device communication. This type of infrastructure has a greater significance by improving fault tolerance, scalability and integrity of the network (Suresh, Daniel, Parthasarathy & Aswathy, 2014). To enable this in a sustainable way, a big question is where in the network, i.e. on what devices, to manage the computations. Below are definitions of different types of architectures used to optimize computing, that are useful to comprehend in order to understand this paper.

Distributing computing, communication and storage on to nodes closer to the edge of the network, e.g. gateways and cloudlets, is called Fog Computing (Yeow et al., 2017). Having the actual edge-devices themselves process the data is called Edge Computing (Satyanarayanan, 2017) These architectures both reduce the occurrences of bottlenecks regarding latency and bandwidth constraints in the network. However, these architectures would increase the requirements of the, often resource constraint, near-edge devices since the distribution of computation will result in them performing more complex tasks.

C. Earlier work

The content of earlier work articles range from more theoretical research regarding performance of DLT:s to a practical small-scale implementation of a device issuing payments. The articles are based on the idea that a centralized structure of IoT is not sustainable and that a full-scale IoT environment will need a decentralized structure (Yeow et al., 2017; Lundqvist, De Blanche & Andersson, 2016; Conoscenti et al., 2016). The beliefs are that devices require low latency and real-time calculations which advocates the distribution of computations, e.g. Fog Computing (Yeow et al., 2017; Lundqvist, De Blanche & Andersson, 2016). To foster this, it is necessary to incentivize the sharing of resources such as calculation and storage capabilities (Yeow et al., 2017).

The idea of using a blockchain based technology for performing transactions between things is something looked at by all the articles. The articles draw the conclusion that the Bitcoin protocol isn't scalable enough since comes with high transactions fees that stems from the mining process (Yeow et al., 2017; Lundqvist, De Blanche & Andersson, 2016). To this problem the articles present solutions that bundles up transactions that are only broadcasted occasionally to avoid the transaction fees (Yeow et al., 2017; Lundqvist, De Blanche & Andersson, 2016). Furthermore, a decentralized technology is to be preferred since the payment solutions that exists today requires devices that wants to make purchases to have the account information stored. This problem does not exist with blockchain based technologies (Lundqvist, De Blanche & Andersson, 2016; Conoscenti et al., 2016).

Other solutions for IoT micropayments that are mentioned are so called DAG:s that incorporate graph structures instead of blockchains. These are believed to be infinitely which is essential to perform many transactions. Specifically, IOTA is mentioned as one technology that might be suitable, maybe even more suitable than blockchain-based technologies (Yeow et al., 2017). A mixture of blockchain and DAG:s are mentioned but will not be discussed since it's outside the scope of this paper.

III. Method

This study is of qualitative nature and based on interviews. 9 unstructured and 5 semi-structured. The chosen method consists of three phases: Research, Implementation and Evaluation. Further in-depth information regarding each phase and its components will follow later in this section. *Fig. 3* below illustrates the method, to provide a comprehensive overview and display the parallel parts of our workflow.

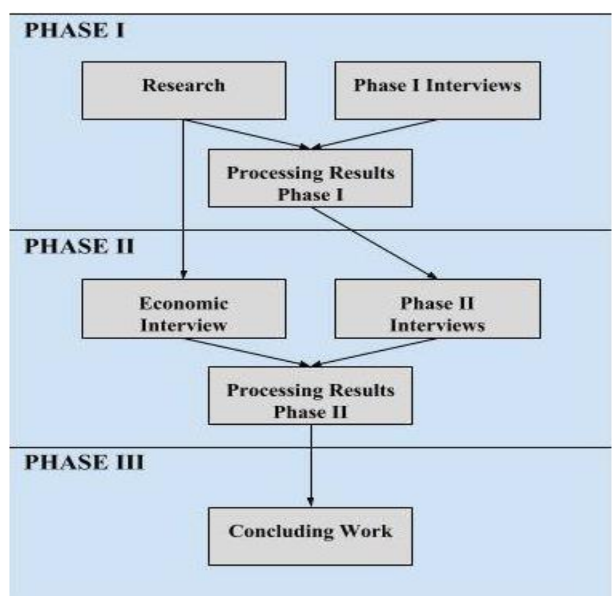

Fig 3: A visualization of the different phases in the method

A. Phase I

1) Research
A detailed and thorough study of both essential information needed to comprehend the research areas and regarding recent research to establish a complete understanding about IoT, micropayments and DLT:s. The purpose of the research is to lay a stable foundation of information to build the paper upon. The KTH Primo database is the main search engine used to discover relevant articles. Considering that some of the technologies researched are very modern, more general search engines are also used in a complementary manner.

2) Phase I Interviews
Eight unstructured interviews with knowledgeable people about one or more of the subjects IoT, micropayments and DLT:s. The interviews are conducted to complement and triangulate the information extracted from the research. They also serve a purpose of obtaining the actors opinion regarding the further development of the researched technologies, since some of the technologies are quite young and are subject to development. The interviewees range from PhD students to academic writers and people working in relevant sectors, providing a broad and dynamic informational input. The interviews are not limited in time and are conducted as an open dialogue. The questions are adjusted with consideration to the area of expertise of the interviewee. The participating actors are:

- Andreas de Blanche - Senior Lecturer at University West, Theme: DLT and IoT
- Carl Tönseth - Regional Manager - IoT, Sigma IT Consulting, Theme: IoT
- Torbjörn Fängström - IoT Sweden, Theme: IoT
- Thomas Lundqvist - Senior Lecturer at University West, Theme: DLT and IoT
- Serguei Popov - Prof. of Mathematics at University of Campinas, Ph.D in Math, Theme: IOTA
- Marco Conoscenti - Ph.D student with focus on Lightning Network, Theme: Lightning Network
- Anders Englund - CEO, Attentec AB, Theme: IoT
- Alexandru Adrian Ormenisan - Ph.D Student and teaching assistant at KTH, Theme: DLT and IoT

3) Processing results of Phase I
A thematic analysis of the Phase I interviews is conducted by listening to the recordings and identifying segments relevant to our work. For each segment a theme is identified. The occurrence of the themes is compiled in Appendix A and if they occur in three or more interviews they are considered highly relevant, an arbitrary limit based on the number of interviews held. The relevant themes are then used as a foundation, together with the research, when constructing evaluable questions to the Phase II interview.

B. Phase II - Implementation

1) Phase II interviews
Five semi-structured interviews are conducted to generate measurable results, each ten- to twenty minutes long. The targeted actors are knowledgeable in computer science and have an understanding regarding the subjects DLT and IoT. The interviews consist of three parts, first the interviewee presents themselves, then a conclusion of our Phase I work is presented to define our research subject, lastly five questions are asked. The questions, that revolve around micropayments using DLT:s in IoT, are asked in a specific order and all interviewees are asked the same questions. The participating actors are:

- Ittay Eyal - Senior Lecturer at Technion - Israel Institute of Technology
- Salil Kanhere - Associate Professor at UNSW in Sydney
- Simon Duquennoy - Research Scientist at SICS in Stockholm, Sweden
- Elias Rohrer - Ph.D. student at TU Berlin Germany and
- Alexandru Adrian Ormenisan - Ph.D. Student and teaching assistant at KTH, Theme: DLT:s and IoT

2) Economic perspective interview
One unstructured interview to establish a pure economic perspective on the effects regarding an implementation of the technologies treated in this article. The interviewee is Patrik Centellini, Lead Consultant - Payment at Tieto, who is knowledgeable about payment solutions. The theme of the interview is micropayments.

3) Processing results of interviews
The six semi-structured interviews are compiled into concluding texts, presented one by one as data in the results section.

C. Phase III

1) Concluding work
Analyzing and discussing the results, with respect to the research questions and earlier work, to draw conclusions and answer the main research-question.

D. Limitations of this study

The blockchain technology is relatively young and under constant change. New adaptations emerge very often, resulting in difficulties in acquiring detailed and reliable information about the technologies. Few scientific articles exist, there are constant updates to the technology and often the technologies are not fully implemented. Also, the developers often have economic incentives in portraying the technologies as revolutionary with credible white papers and modern web pages. These key factors need to be taken into account when analyzing the actual data of the sources to gather an objective result.

The main sources of primary data of this study are interviews. Considering the limited time frame, identifying a sufficient number of relevant and knowledgeable actors is a challenge. This leads to the results of this study to be based off a smaller knowledge base. Furthermore, basing our results on interviews could be problematic if the interviewees are indoctrinated in a certain area. To minimize this risk, the variety of the actors in this study is considered. However, in the purely economic part of the study, only one interview is conducted. This can lead to biased results which needs to be regarded when drawing conclusions. At last, introducing additional sources of data, i.e. using a poll, would triangulate the gathered data further, thus providing a more multifaceted result.

IV. Results

A. Phase I results

Listed below are the relevant themes extracted from the phase I interviews, together with a short explanation of what they refer to. The full thematic analysis, including themes that were not considered, are compiled in Appendix A.

- **IoT device limitation:** The resource limitations of smaller IoT devices, regarding CPU, storage and battery time.
- **IoT development:** The projected growth of the IoT and how it will evolve.
- **Ledger size issue:** The problem with storing a DLT on an IoT devices.
- **Throughput issue:** The problem regarding the speed of validating transactions with the Bitcoin protocol.
- **Transaction fee issue:** The high cost of performing a transaction on the Bitcoin blockchain.
- **Off-chain solutions:** Bitcoin Lightning Network, a possible solution to the throughput and transaction fee issues.
- **Decentralization:** The aspect of having a decentralized system, its possibilities and limitations.
- **DAG solutions:** IOTA, a DAG solution possibly solving the throughput and transaction fee issues.

B. Phase II results

Presented below are the results of the phase II interviews, each interview presented individually.

1) Phase II interviews:

a) Ittay Eyal

Eyal is a Senior Lecturer at Technion – Israel Institute of Technology and has written the article Bitcoin-NG which presents a solution to the scalability issues regarding variants of Bitcoin’s blockchain.

Eyal emphasizes the fact that the Lightning Network isn’t the panacea (i.e. single solution), merely part of a solution that could be used for micropayments between IoT devices from a scalability point of view. He also points out that the Lightning Network isn’t perfect in the sense of the existence of the timeouts. When considering the DAG structure as a possible solution, Eyal states that the existing DAG protocols existing are either less or more suitable for IoT devices. He is sceptical about requiring PoW from IoT devices, which is the basic concept of IOTA: *“If you have the IoT device you would want to pay a fee to put your transaction up to not waste battery.”*.

The resource limitations of the IoT devices is identified by Eyal as a difficulty of using DLT:s as a transaction protocol. He considers that even Simplified Verification Methods[2] (SPV:s) are too heavy for the devices themselves to perform. Eyal also address the security issue of having IoT devices performing transactions and handling value: *“You would need to rethink the security of the IoT devices when they start to control money”*.

A combination of centralization and decentralization is how Eyal imagines the future development of IoT interaction. He points out that different scenarios demand different levels of centralization. On one hand there is a need of quick device-to-device interaction when considering two cars that exchange real-time information, but on the other hand Eyal believes that a lot of positive effects stems from having central databases.

b) Salil Kanhere

Dr. Kanhere is an Associate Professor at UNSW in Sydney. His current research areas include IoT and blockchain technology.

Dr. Kanhere consider the off-chain solutions as promising approaches and that they could be suitable to perform micropayments between IoT devices. He points out the possible lowering of the transaction fees, by only having a few on-chain transactions, as a reason to why he considers these technologies to be suitable.

The need for standardization is identified by Dr. Kanhere as a possible difficulty to solve if DLT:s would be used for micropayments between IoT devices. Having the interacting devices all using the same or at least compatible technologies is essential. He also addresses the resource limitations of the IoT devices: *“Sure, you can do it on a Raspberry Pie, but can you scale it down to smaller devices?”*. As a last difficulty, Dr. Kanhere speaks about the need of a solution or standard on how to perform the account management of the devices, considering if all devices should have a separate account or not.

Dr. Kanhere believes that there are strong arguments for IoT developing into a more decentralized model, one of them being that this would result in a system with no single point of failure. However, he addresses the management and control of such a large and decentralized network as a challenge. Therefore, he identifies a form of hybrid solution as a possibility: *“...a hybrid solution, having a higher level of centralization with the smaller devices and for the bigger more decentralization”*.

c) Simon Duquennoy

Dr. Duquennoy is a Research Scientist at SICS in Stockholm, Sweden. His main area of focus is in IoT.

[2] A simplified method to check if transactions are included in a block for lightweight clients.

Dr. Duquennoy identifies that on-chain scaling has inherent limitations, and consider off-chain solutions as a good way to preserve security, decentralization and censorship resilience while scaling the transactions.

The resource constraints of the devices, considering for example bandwidth and memory, are described by Dr. Duquennoy as possible difficulties with using DLT:s for micropayments in IoT. He provides us with an intuitive example regarding the IoT devices he handles: *"In the kind of devices we work with, we cannot store a single full block in RAM, or a couple of hundred block headers."*.

When discussing the potential evolution of IoT, Dr. Duquennoy identifies potential scalability benefits of moving towards a more decentralized system. However, he stresses that this comes with difficulties of its own.

d) Elias Rohrer
Rohrer is a first year PhD student at TU Berlin Germany and his area of expertise is within networking security and privacy.

When discussing off-chain and DAG solutions, Rohrer presents opportunities and obstacles with both technologies. Considering off-chain solutions, he believes that they are very scalable and lightweight, and in the context of IoT they can be a good match since they are built on secure technologies. However, he addresses his concerns about small IoT devices issuing the funding transactions, where to store the keys for signing and generally managing the identities and accounts of the devices. Adding to his concerns, he talks about the Lightning Network and the possibility of it converging to a more federated network with central payment hubs, i.e. becoming centralized when fully in use.

Regarding IOTA's DAG solution, Rohrer expresses his concerns about having computational weak IoT devices performing the PoW. Thus, enabling a powerful node with a lot of CPU to overrun the smaller nodes. However, he has a positive view on the DAG-concept: *"I think IOTA and the tangle, this DAG, is a really interesting idea. I think, for a number of reasons, going from this chain concept towards a more graph-like structure is a really interesting research direction."*.

When talking about permissionless blockchain[3] systems like the Bitcoin blockchain, Rohrer argues that the level of decentralization is debatable. This since few mining pools have a very big impact on the security and trust of the system. He thinks that the big question the coming years will be how the trust model actually will look, even if the technology itself gets more decentralized and distributed. On the note of difficulties with using DLT:s for IoT, Rohrer identifies the tradeoff between privacy and transparency. The ledger should be verifiable but we might want to store the data privately. As a possible solution, that he finds interesting, he mentions a blockchain based cryptocurrency called Zcash, where details about each transaction are encrypted but still verifiable.

Considering the future evolution of IoT from a more general perspective, Rohrer does not consider today's centralized model sustainable for long. He identifies economical and CPU-related issues, as well as regarding privacy of the centralized model. The latter considering the aggregation of all data into a single point of failure.

e) Alexandru Adrian Ormenisan
Ormenisan is a PhD student at KTH Sweden and a teaching assistant in the course ID2210 Distributed Computing, Peer-to-Peer and GRIDS.

Regarding off-chain solutions as a solution for micropayments in IoT, Ormenisan believe that they can work as long as the transactions are small. On the note of IOTA, he considers himself to lack the expertise in the implementation of the technology to say if it would be a possible solution or not. More generally about using DLT:s for micropayments in IoT, Ormenisan sees the limitations of the devices, in terms of processing power and memory as an obstacle to overcome. Also, he talks about the rapid growth of the blockchain as an issue considering these limitations. The need of specialized nodes to store the blockchain, and having the IoT devices communicating through them, making the IoT devices not really being part of the blockchain network.

When discussing IoT as a concept and if it will develop into a more decentralized infrastructure in the future, Ormenisan identifies several issues of having all devices directly interacting. Having specialized hardware, more power consuming and CPU-powerful nodes cost both money and electricity and would complicate a full decentralization. However, he acknowledges the overload problem of having 50 billion devices that all interact through a small number of servers. This is why Ormenisan believes that a form of hybrid solution could be the proper way to go, having some more powerful devices working with filtering and aggregating the data before interacting with the main servers.

2) Economical perspective Patrik Centellini
Centellini is a Lead Consultant Payments at Tieto in Stockholm, Sweden. He has been active in the area of micropayments since the late nineties.

Centellini provides two examples regarding the role of payment solutions as a current research topic in organizations. First, he describes his work on a project in Africa with Grundfos. Grundfos is a pump manufacturer that develops smart water pumps driven by solar energy that extract fresh water from the ground. Centellini addresses the challenge of finding a suitable payment solution for the pumps, that should be administrable remotely. The other example considers Volvo and their solutions on how to conduct payments via the car. Today, they can utilize solutions connected to existing payment channels,

[3] A blockchain where anyone, without pre-existing trust or set identities, can join and participate in the blockchain network

e.g. payment cards, but they are looking at developing a form of smart wallet solution for the cars themselves.

Considering the existing payment solutions today, Centellini identify an issue regarding the transaction costs. He explains that they stem from how the ecosystem of payments look today and provides an example considering the connected actors to a payment card: *"If you consider the payment card industry today, you have card issuers & acquirers, processes, regulations, fraud management - there are so many actors integrated in these systems affecting the transaction costs"*. However, he emphasizes that this is a market undergoing a lot of changes and sees the transaction costs declining as changes regarding infrastructure and open access emerge.

Centellini identify a big demand for a payment solution for micropayments. He sees digital services as a market that could utilize a pay-per-use solution, e.g. session-based services. Also, the movement towards servitization, and the potential combination with micropayments is considered to be an interesting match by Centellini. Regarding the development of payment models, Centellini's personal belief is that we could see a shift from organizations tying up customers long term, towards a lowering of the *"enter and leave"-threshold*. If a useful micropayment solution is introduced, he thinks that many organizations would be interested, and that there exists a potential effect of an increased consumption with such a system.

When discussing micropayment solutions and adding in the perspective of decentralization, Centellini can see a potential growth of the sharing economy. Having two parts issuing a transaction directly between them, separating the actual payment from the company (e.g. Airbnb), thus creating a decentralized transaction would be very interesting according to Centellini.

V. Discussion

This chapter aims to discuss and analyze the results with regards to the research questions. It also provides the reader with a comparison to results in earlier work in an attempt to offer a nuanced perspective.The disposition of the discussion is formed to follow the same pattern as the research questions in section I.F.

A. Micropayments using DLT

1) *Bitcoin protocol*

During the research and Phase I interviews we identified two main issues in performing transactions with the Bitcoin protocol. These stem from the structure of blockchain technology. The issues are the low throughput and the high transaction fees, which becomes an even larger problem when performing many small transactions. The throughput issue stems from the block-size. This and the block generation-time are both predefined to prevent forks and to ensure that everyone in the network has a copy of the same ledger. The fee is essential since it is the economic incentive for miners, who are the backbone of the Bitcoin network.

The first, intuitive solution would be to alter the implementation of the Bitcoin protocol. I.e. enlarging the block size to increase the throughput. However, these types of modifications, that we also found skepticism about in earlier work (Conoscenti et al., 2016), generate new problems with for example double spending. During the Phase I interviews two main solutions were found that could mitigate the two mentioned scalability problems, possibly enabling micropayments. The first potential solution mentioned was an adapted blockchain where payments are performed off-chain. The second solution considered a DAG called IOTA. The usability of these two technologies will be discussed in sections V.A.2.a and V.A.2.b.

2) *Solutions to scaling problems*

To overcome the problems mentioned, these two types of solutions tackle the problems in different ways. The off-chain solutions are trying to complement the on-chain throughput with a second layer while the IOTA is going in a completely different direction by switching the chain for a graph-structure.

a) Lightning Network

Lightning network was identified by both the Phase II interviewees and in earlier work (Yeow et al., 2017) to be a possible way to improve the scalability problems of Bitcoin. These results were justified by the fact that the small transactions are handled off-chain and only periodically reported back to the main-chain. As brought up in the Phase II interviews and literature research you only have a few on-chain transactions with the Lightning Network. This is the most important feature of the Lightning Network since instead of multiple transactions being included in a block, you can aggregate many transactions before broadcasting the final state. We believe that this, for an already limited Bitcoin block, is advantageous since you don't want to increase the block size, making the ledger size grow too rapid. This because it would have centralizing effects on the network, since only more powerful miners will be able to store the ledger and participate in the consensus mechanism.

We share the concerns, as mentioned by Elias Rohrer in the Phase II interviews, regarding what direction the Lightning Network will evolve into when fully implemented. There could be issues regarding how the transactions are routed through the network of payment channels. The first issue is that creating many payment channels means many funding transactions, thus forcing the users to lock up value. This is negative from an economic standpoint since the locked funds are unusable, but it could also lead to the creation of payment hubs. Powerful actors with more capital can, in a larger extent, lock up funds to create many payment channels. Most likely being well connected, they are more probable to route payments, making the network centralized around them. Adding to this, Lightning Network demands that to make a transaction, sufficient funds must be distributed throughout the whole route. Meaning that the funding transactions of the intermediary payment channels must be at least as big as the transaction routed. Again, powerful nodes having more resources may become the only possible route to perform bigger payments, adding to the centralization even further. However, this study considers micropayments, making the the impact of the latter argument less powerful. Also, the economic incentives of creating these hubs are today uncertain and highly dependent on what fees that intermediates can and will obtain. Is it enough for these bigger organizations to even bother? These questions all depend on to what extent the Lightning Network will succeed in the future; as the number of users increase we believe the potential of this type of monetization could follow.

Another issue considering the Lightning Network which was addressed in our Phase II interviews, is the need for the intermediaries to stay online to complete the transactions. This is solved by having the earlier mentioned timeouts, but this is not a perfect solution since this results in the locking of value for a short period of time within the transaction. The last identified problem with the Lightning Network is the fact that it hasn't been fully implemented in writing moment. This means that everything is still only in theory, making it hard to predict how well the implementation will perform full-scale.

b) IOTA

By just considering IOTA as a framework to perform micropayments, it is in theory very fast and contains no fees, thus suitable. We believe that the most interesting aspect of IOTA is the principle of needing to participate, by validating other transactions, to utilize the payment solution. This is an innovative approach to eliminate the fees, that if implemented correctly could be revolutionizing. However, as noted in the results of our Phase II interviews, there exists doubts regarding IOTA. In our opinion, at this stage we cannot either fully dismiss nor acknowledge IOTA, but merely see that it might have potential as a micropayment solution in the future.

B. DLT:s used in an IoT environment

1) *General IoT limitations*

When considering IoT in general we have identified a need for the infrastructure to become more decentralized as the network grows. All five Phase II interviewees are unanimous on that scalability issues eventually will emerge, having a rapidly growing IoT but keeping a centralized structure. However, there is a limit to what extent IoT can be decentralized. As you decentralize the network you will have to increase the workload of the devices, thus increasing the requirements for each device. If we want an IoT sensor to perform more complicated tasks than sending data to a server every minute, resources like CPU-power and memory will need to be improved. A direct consequence of this will be increased power consumption of the device, and this is already an issue when looking at today's device. Therefore, a hybrid solution regarding the decentralization, a fog computing approach, is both interesting and probable as found in the results of Phase II interviews and in earlier work (Yeow et al., 2017). This meaning that we have a decentralized structure considering the more powerful devices, that in turn connect the smaller ones, giving the latter a higher level of centralization.

2) DLT:s in IoT

When considering the possibility of performing micropayments between IoT devices using DLT:s, we immediately see issues. Beginning by looking at more resource constrained devices (e.g. sensors), there are numerous difficulties. The CPU-power and memory required to perform any kind of PoW or storing of the blockchain, simply does not exist. Also, if the devices were to handle value, it would require a more secure, and thus power consuming, system on the devices. However, considering that there also exist more powerful IoT devices, the possibility of using DLT:s is not ruled out completely. When considering the limitations of decentralization of the IoT network, as addressed in V.B.1, we can identify similarities regarding the usage of DLT:s in IoT. The devices further out in the IoT network are more resource constraint, hence we see a decreasing possibility of utilizing a micropayment solution as we approach the network edges.

More specifically, examining the applicability of Lightning Network and IOTA in an IoT environment, we also identify the resource constraints of the IoT devices as the biggest uncertainty. Considering the Lightning Network, it is a lightweight solution that scales very well. However, questions about having IoT devices issuing the funding transactions, where to store signing keys and the ledger itself arise. Moving on to IOTA, similar questions about the resource requirements to utilize the technology arise. Having IoT devices themselves performing the PoW would firstly require them to be somewhat powerful and secondly it would consume more electricity, which in IoT is a limited resource. Another concern is that a more powerful node could overrun the smaller nodes, although this is temporarily solved by the Coordinator in the current version of IOTA. However, as we recognized the lack of detailed knowledge of this technology in our Phase II interviews. We find it hard to draw any decisive conclusions regarding IOTA, rather just express a concern about the mentioned questions.

The theme is quite obvious to us, DLT:s requires a certain amount of resources, which affects the possibility to utilize them for device-to-device micropayments in IoT. However, just because all devices cannot utilize these types of technologies it is important not to forget that some devices could. Is there even a need for all devices to conduct transactions? Furthermore, as technology progresses it is probable to believe that smaller devices will become more powerful. Therefore, we see a possibility of a DLT solution first being implemented in a limited part of the IoT network. Then, as more devices are able to participate, the network further decentralizes, increasing the significance of the solution and the possible use cases.

C. Demand and economic effects of a sustainable payment solution for microtransactions

The demand of a sustainable payment solution, considering the transaction fees, for micropayments was extracted as a result from the interview with Centellini and our research. When asked about what areas that this type of solution could be applied to, Centellini identified session based-services. These organizations could profit on a shift from the today more frequently used subscription based business models, towards a pay-per-use standard. We argue that this shift is highly probable if a sustainable payment solution for micropayments is found. The reason for this is that we believe that consumers would be interested in the most honest exchange of value possible, paying only for what they receive. This would result in the companies that stick with the older subscription model to be ousted naturally.

We see a big first mover advantage regarding these kinds of services. For example, a mobile operator that can provide their customers with a service that needs only to be paid for when utilized would be able to obtain market shares very fast. Intuitively, the consumers have economic incentives in a micropayment solution, because of the fair exchange of value. We find the thoughts expressed by Centellini, regarding the possible increased consumption when lowering the enter and leave thresholds, very interesting. This enlightened us by providing an example of economical intensives, seen from the supplying organizations point of view, in from of an increased revenue.

VI. Conclusions

A. Conclusions

In this section we will conclude our study and answer the three sub-questions one by one. These conclusions will then lead us to a complete answer regarding our main research-question.

1) RQ1: "Are existing DLT:s suitable to perform micropayments?"

a) Bitcoin

The Bitcoin blockchain protocol was ruled out in the early stages of the work as a potential micropayment solution. This due to the inherent problems of the transaction fees and low throughput.

b) Lightning Network

We identify the Lightning Network as a potential enabler of micropayments since it increases the speed and lowers the transaction fees.

c) IOTA

Regarding IOTA we cannot draw any decisive conclusions due to the absence of data in the results of the study. Although, we consider the approach as interesting and a future research area.

2) RQ2: "Are existing DLT:s utilizable for devices in the IoT environment?"

Yes, but to a limited extent. Today, the bigger devices have a lot of computational power but the further out towards the edges of the network, the weaker the devices get. The DLT:s, regardless of what implementation, demand resources non-existent considering smaller IoT devices. The resource constraint of the devices is identified as the main inhibitor.

As IoT devices develop, we see great potential in the Lightning Network being a future micropayment solution for the whole network, thus having a big impact on IoT.

Regarding IOTA we cannot draw any decisive conclusions due to the absence of data in the results of the study.

3) RQ3: "Does a demand of a sustainable micropayment solution exist and what business models could such a solution affect?"

Yes, we have identified a big demand for a sustainable micropayments solution.

A micropayment solution could be the catalyst of sustainable pay-per-use business models, enabling a fair exchange of value.

4) MRQ: "Are there existing DLT:s suitable to perform micropayments between IoT devices, and what economic effects could a sustainable micropayment solution have?"

The original Bitcoin blockchain is not a suitable technology for performing micropayments between IoT devices, due to transaction fees and scalability problems. The Lightning Network solves these scalability problems by reducing the transaction fees and increasing the performance of Bitcoin. However, considering the applicability of this technology in an IoT environment today, it is not fully implementable. This stems from the fact that many IoT devices are resource constraint, regarding CPU-power and storage. Although, we identify a great potential in the Lightning Network considering that IoT devices will evolve. Thus, believing it will be a possible future micropayment solution for IoT devices. The study also resulted in the identification of a big demand for a sustainable micropayment solution. This, we argue makes the Lightning Network an even more interesting technology, possibly catalyzing the emergence of pay-per-use business models.

B. Future work

This paper completely dismissed the Bitcoin implementation as a suitable protocol for microtransactions in an IoT environment and explored possible adaptations that could solve the scalability issues. This paper brought forward two modern and interesting technologies, but they both have been questioned regarding the ways they are implemented. Areas like decentralization, security and, more generally, logistical aspects of their full implementation are necessary to look further into.

Acknowledgement

We would like to thank all interviewees that contributed to our study by taking their time to answer the questions and provide us with directions on how to proceed with our work. We would also especially like to thank our supervisors Bo Karlsson and Jens Edlund at KTH for their opinions and ideas.

REFERENCES

Framingham, M. (2017). IDC Forecasts Worldwide Spending on the Internet of Things to Reach $772 Billion in 2018. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS43295217

Coron, J., & Nielsen, J. (2017). *Advances in Cryptology EUROCRYPT 2017* (p. 610). [S.l.]: International Association for Cryptologic Research.

Prableen Bajpai, C. (2018). Distributed Ledger Technology. Retrieved from https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp.

Drescher, D. (2017). *Blockchain Basics*. [S.l.]: Apress.

McPhee, C., & Ljutic, A. (2017). Editorial: Blockchain. *Technology Innovation Management Review, 7*(10), 3-5. doi: 10.22215/timreview/1108

Narayanan, A. (2016). *Bitcoin and cryptocurrency technologies*. Princeton: Princeton University Press.

Y.Riady (2016), Merkle Trees in Exlixir, Retrieved from https://yos.io/2016/05/19/merkle-trees-in-elixir/

Deloitte, *Blockchain Enigma. Paradox. Opportunity*. (2016). Retrieved from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

Judmayer, A., Stifter, N., Krombholz, K., & Weippl, E. (2017). *Blocks and Chains: introduction to Bitcoin, cryptocurrencies, and their consensus mechanisms* (p. 34). San Rafael, California : Morgan & Claypool.

Gramoli, V. (2017). From blockchain consensus back to Byzantine consensus. *Future Generation Computer Systems*. doi: 10.1016/j.future.2017.09.023

Thompson, C. (2016). How does the Blockchain Work?. Retrieved from https://medium.com/blockchain-review/what-blockchain-should-we-use-6ba9cca8df22

Chen, X., Lin, D., & Yung, M. (2015). *Information Security and Cryptology* (p. 266). Springer International Publishing Switzerland.

Grossklags, J., & Preneel, B. (2017). *Financial Cryptography and Data Security* (p. 477). International Financial Cryptography Association.

Franco, P. (2015). *Understanding bitcoin: cryptography, engineering and economics*(p. 156). Chichester, West Sussex: John Wiley & Sons.

Göbel, J., & Krzesinski, A.E. (2017). Increased block size and Bitcoin blockchain dynamics. *27Th International Telecommunication Networks And Applications Conference*.

Eyal, I., Gencer, A., Sirer, E., & Van Renesse, R. (2015). Bitcoin-NG: A Scalable Blockchain Protocol.

Karame, G. (2016). On the Security and Scalability of Bitcoin's Blockchain. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1861-1862.

Poon, J., & Dryja, T. (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Retrieved from https://lightning.network/lightning-network-paper.pdf

Popov, S. (2018). The Tangle. Retrieved from https://assets.ctfassets.net/r1dr6vzfxhev/4i3OM9JTleiE8M6Y04Ii28/d58bc5bb71cebe4adc18fadea1a79037/Tangle_White_Paper_v1.4.2.pdf

Fiore, M. D., & Campos, M. (2013). The algebra of directed acyclic graphs. *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 7860*, 37-51.

Bramas, Q. (2018). The Stability and the Security of the Tangle. Retrieved from https://hal.archives-ouvertes.fr/hal-01716111v1

IEEE Standards Association. (2015). Internet of Things (IoT) Ecosystem Study. Retrieved from https://standards.ieee.org/innovate/iot/iot_ecosystem_exec_summary.pdf

Suresh, P., Daniel, J., Parthasarathy, V., & Aswathy, R. (2014). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. 2014 International Conference on Science Engineering and Management Research, ICSEMR 2014

Yeow, K. W., Gani, A. J., Ahmad, R., Rodrigues, J., & Ko, K. (2017). Decentralized Consensus for Edge-Centric Internet of Things: A Review, Taxonomy, and Research Issues. *IEEE Access, 6*, .

Satyanarayanan, M. (2017). The Emergence of Edge Computing. Computer, 50(1), 30-39.

Lundqvist, T., De Blanche, A., & Andersson, H. (2017). Thing-to-thing electricity micro payments using blockchain technology. *Global Internet of Things Summit (GIoTS), 2017,* 1-6.

Conoscenti, M., Vetro, A., & De Martin, J. (2016). Blockchain for the Internet of Things: A systematic literature review. *Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of,* 1-6.

AUTHOR PRESENTATIONS

Author S.El-Hage is a student at the Royal Institute of Technology, Stockholm Sweden. S.El-Hage studies Industrial Engineering and Management with a focus in Computer Science. S.El-Hage has been involved throughout the whole process of this study, contributing to: Research, Phase I, II & Economic interviews (taking notes), writing the paper (contributing to all parts).

Author G.Holst is a student at the Royal Institute of Technology, Stockholm Sweden. G.Holst studies Industrial Engineering and Management with a focus in Computer Science. G.Holst has been involved throughout the whole process of this study, contributing to: Research, Phase I, II & Economic interviews (conducting the interviews), writing the paper (contributing to all parts).

APPENDIX

Appendix A: Themes identified during the interviews

Main theme	Sub-theme	No. of interviews theme identified
IoT	Interoperability	2
	Scalability issue	1
	IoT device limitation	**5**
	Data ownership issue	1
	IoT development	**4**
Blockchain	**Ledger size issue**	**5**
	Security benefits	2
	Transparency	1
	Throughput issue	**3**
	Private/Public	2
	Transaction fee issue	**4**
DLT adaptations	**Off-chain solutions**	**4**
	Hierarchical solutions	1
	Decentralization	**4**
	DAG solutions	**3**

TRITA EECS-EX-2018:433

www.kth.se