Master's Thesis

Rating-assisted Layer 2 Scaling of Distributed Ledger Technologies for the Internet of Things

Vanesco A. J. Boehm

Department of Computer Science and Engineering

Pohang University of Science and Technology

2018

Rating-assisted Layer 2 Scaling of Distributed Ledger Technologies for the Internet of Things

Rating-assisted Layer 2 Scaling of Distributed Ledger Technologies for the Internet of Things

by

Vanesco A. J. Boehm

Department of Computer Science and Engineering

Pohang University of Science and Technology

A thesis submitted to the faculty of the Pohang University of Science and Technology in partial fulfillment of the requirements for the degree of Master of Science in the Department of Computer Science and Engineering

Pohang, Korea

June, 12. 2018

Approved by

Prof. Jong Kim (Academic Advisor)

Rating-assisted Layer 2 Scaling of Distributed Ledger Technologies for the Internet of Things

Vanesco A. J. Boehm

The undersigned have examined this thesis and hereby certify that it is worthy of acceptance for a master's degree from POSTECH.

June/12/2018

Committee Chair	Jong Kim	(Seal)
Member	Chanik Park	(Seal)
Member	Hanjun Kim	(Seal)

MCSE 20162417

Vanesco A. J. Boehm. Rating-assisted Layer 2 Scaling of Distributed Ledger Technologies for the Internet of Things. Department of Computer Science and Engineering. 2018. 50P. Advisor: Prof. Jong Kim. Text in English.

Abstract

Experts herald that distributed ledger technologies (DLTs), such as the Ethereum platform, will eventually enable the Internet of Things (IoT) to be secure, scalable and autonomous. In this thesis, opportunities and limitations of state-of-the-art distributed ledger platforms to support the IoT have been investigated. State channels are a layer 2 scaling approach and do not require every transaction to be processed by the distributed ledger. This research suggests enhancing state channels by integrating a reputation system to improve the suitability of DLTs for the IoT. When opening a state channel, some funds must be locked up in a smart contract as deposit to prevent double-spending. To regain funds, participants of a state channel can close it cooperatively. However, if just one party requests closing of a channel, a challenge period must be waited until funds get paid out. To incentivize state channel participants to behave cooperatively and minimise periods of funds being held in escrow, the adoption of a smart contract-based reputation system is proposed. Assuming that entities behave economically driven, rating-assisted state channels have the potential to improve the liquidity, efficiency, transparency and overall service quality in digital machine-to-machine markets.

Contents

List of Abbreviations

ADEPT	Autonomous Decentralized Peer-to-Peer Telemetry
AWS	Amazon Web Services
CPU	Central Processing Unit
DAG	Directed Acyclic Graph
dApp	Decentralized Application
DLT	Distributed Ledger Technology
DLTs	Distributed Ledger Technologies
EU	European Union
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IT	Information Technology
min	minutes
RFID	Radio-frequency Identification

s	seconds
USD	US Dollar

List of Figures

List of Tables

1 Introduction

The motivation, research goal and approach of this thesis with the title '*Rating-assisted Layer 2 Scaling of Distributed Ledger Technologies for the Internet of Things'* are described in the following subsections. Abbreviations, that are specific to this work and not widely common in the IT space, are introduced at their first occurrence. Abbreviations can be looked up in the *List of Abbreviations*.

1.1 Motivation

Gartner predicts the number of internet-connected devices to grow exponentially in the near future and to already outnumber the global human population [Gartner2017]. Managing and controlling all these devices will become infeasible at some point. Thus, smart devices must become increasingly autonomous. With the help of digital marketplaces, devices may be able to interact with each other by offering and requesting services. To enable devices to conveniently trade with each other, some form of digital payment system is necessary. Moreover, device behaviour must be defined in a reliable manner.

Blockchain, which is widely known as the technology enabling the digital currency Bitcoin, ensures validity of transactions with the help of a distributed transaction ledger and cryptographic proofs [Nakamoto2008]. Researchers predict that blockchain technology will disrupt many industries and enable numerous use cases beyond digital

cash [Crosby+2015, Shrier+2016]. Distributed ledger-based systems offer opportunities for transaction-reliant processes to raise transparency, increase efficiencies and enforce compliance.

Every additional connected device adds to the attack surface [Pureswaran+2015a]. As more and more devices get connected to the internet and computing becomes ubiquitous, the risk that management of smart devices gets out-of-control grows. IBM heralds that distributed ledger technologies may save the future of the internet of things (IoT). Further, IBM predicts that blockchain-based, low-cost, private-by-design IoT solutions will pave the way for myriads of use cases and new business models.

Today, the IoT and distributed ledger technologies (DLTs) are still in its infancy and face similar challenges [Groopman+2018]. Both the IoT and DLTs are newly emerging technologies. Although the IoT is more mature than DLTs, IoT solutions are still highly fragmented and vendor-specific. Distributed ledger technology (DLT) platforms are primarily in proof-of-concept stages and seem to be not yet suitable for productive, large-scale use. Lack of standards, both for DLTs and the IoT, complicates interoperability of different solutions. Therefore, integration of different products may be cumbersome and compromise security. Inefficiencies, inhibited adoption as well as poor usability are further consequences. Reliance of the IoT on cloud infrastructure entails several risks. Data in the possession of a third party can be leaked, modified or deleted. Additionally, using a cloud means to depend on the service provider's terms and conditions. Costs can be considerable, especially to achieve high fault tolerance and availability. To benefit from cost reductions and efficiency improvements that the IoT and DLTs can offer, significant initial efforts and investments to create the right infrastructure are necessary. Because the IoT and DLTs are completely novel technologies, no best practices and precedents to learn from exist. Last but not least, the adoption and

development of the IoT and DLTs are decisively pushed by industries and enterprises as opposed to consumers.

Despite all their current limitations, DLTs and cryptocurrencies seem to be the perfect enabler for the vision of autonomously interacting smart devices. For machine-to-machine trading of services, especially fast, cheap and scalable micropayments are an essential requirement. However, widely adopted DLT solutions, such as the leading smart contract platform Ethereum, fail in these regards. One suggestion to mitigate these shortcomings is state channel technology which aims to allow more transactions by not requiring every transaction to be processed on the distributed ledger [Coleman2015].

1.2 Research Goal

Considering the immaturity and challenges of both the IoT and DLTs, assumptions that DLTs will be the enabler for the IoT appear still very theoretical. This work aims to add clarity in this regard by examining in particular three aspects. First, current limitations of DLTs to support IoT use cases shall be identified. The second goal is to detect current opportunities of DLTs to benefit the IoT already. Lastly, an enhanced state channel design to improve the Ethereum platform's suitability to support the IoT shall be elaborated. Concretely, a smart contract-based reputation system for state channels shall be investigated.

1.3 Approach

Following the description of the motivation and research goal of this thesis, the methods and structure of this work are outlined in this section. In chapter 2, fundamental technical knowledge, necessary for understanding the consecutive contents, is presented. Specifically, important definitions and concepts related to DLTs and the IoT are

introduced. After clarification of the technical background, chapter 3 is dedicated to inform about relevant, related work. Examination of the status quo of projects and initiatives aiming to utilize DLTs for the IoT was an important step of this research. Insights gained from the survey are presented in chapter 4 to motivate for an improved state channel design to support the IoT. Concretely, a rating-assisted state channel implementation is elaborated. In chapter 5, the proposed smart contract-based reputation system for state channels is evaluated. A discussion of the contributions and implications follows. The final chapter is a summary of the gist of this thesis and gives an outlook of related future research.

2 Preliminaries

In this chapter, an overview of the technologies and related concepts, that are object of this study, is given. First, DLTs will be characterized. Then, the blockchain data structure along with the most prominent blockchain-run DLT platforms, namely, Bitcoin and Ethereum, will be introduced. Next, a section about directed acyclic graph (DAG), which is an alternative data structure to blockchain for realizing a distributed ledger, follows. A presentation of major technical challenges that DLT solutions face these days together with some possible solutions closes the part about DLTs. The remainder of this chapter comprises fundamentals about the IoT. Besides basic definitions, the potential benefits and challenges of IoT will be discussed.

2.1 Distributed Ledger Technologies

2.1.1 Characteristics

Reaching consensus is a fundamental challenge of distributed computing [Lamport+1982]. This dilemma can be described with the Byzantine Generals' Problem. When troops of the Byzantine Empire encircled a city, that they wanted to capture, the generals of the troops depended on humans to deliver messages between each other. Because only a coordinated attack had chance to be successful, reliable message delivery was extremely important. However, some messengers could be traitors, who would either just not deliver the message or deliver a wrong message.

In the software world, Byzantine failure describes deviations of a system's behaviour from how it is expected to work. Network nodes that act in such a way are regarded as not honest or malicious. Byzantine fault tolerant networks can tolerate a certain number of malicious nodes and still function correctly.

Distributed ledger technologies achieve Byzantine fault tolerance by using a distributed ledger which is a record of replicated and synchronized data that members of a network agree on [Natarajan+2017]. The distributed ledger is maintained by a peer-to-peer network without dependence on a central instance. Consequently, distributed ledgers have no single-point-of-failure, no central authority and can achieve strong security. In general, distributed ledger technologies aim to revolutionize traditional centralized systems by being publicly auditable, highly secure, resilient against censorship as well as data tampering and allowing fast transactions at low cost.

Distributed ledgers allowing anyone to join their network and participate in the consensus finding process are called permissionless. In contrast, a distributed ledger is permissioned if network participation is regulated. A public distributed ledger can be read and accessed by anyone as opposed to a private distributed ledger.

The first implementation of a distributed ledger is the Bitcoin protocol, which is based on the blockchain data structure and cryptography [Gupta2017]. Smart contracts have been the next step in the evolution of distributed ledgers. Smart contracts are programs that run in a secure and predefined manner on a peer-to-peer network of non-trusting participants without a central authority. All outcomes of a smart contract are well-defined and transparent and which addresses can trigger certain procedures can be arbitrarily specified. The Ethereum blockchain is the first platform that has realized smart contracts. More recent innovations in the space of DLTs aim to overcome the scalability challenges of early blockchain solutions and strive for interoperability

between different distributed ledger-based platforms. An example of a third generation DLT is Cardano [Cardano].

2.1.2 Blockchain

2.1.2.1 Bitcoin

In 2008 the paper *Bitcoin: A Peer-to-Peer Electronic Cash System* was published under the pseudonym Satoshi Nakamoto [Nakamoto2008]. This paper is the blueprint for the Bitcoin cryptocurrency, which is a form of digital cash based on cryptography.

To perform asymmetric cryptography, users require a pair of a public and a corresponding private key. These keys can be generated based on some algorithm and input values. With the help of a user's public key, messages can be encrypted that only the owner of the corresponding private key can decrypt. Therefore, the private key must be kept confidential under all circumstances, otherwise the cryptographic protocol is broken. Further, values, such as messages, can be signed with a private key. Using the corresponding public key anyone can verify that the digital signature must have been created with the correct private key.

Bitcoin, which is purely peer-to-peer, uses digital signatures on transactions to allow network nodes to check whether a transaction is legit or not. However, digital signatures cannot detect double spending. This fundamental challenge of peer-to-peer digital cash systems equals the Byzantine Generals' problem. Bitcoin solves this by using a distributed shared ledger that stores the complete history of transactions. By checking the transaction history any double spend attempt can be identified. More precisely, signed transactions get first collected in a pool. Nodes of the peer-to-peer network choose transactions from this pool and verify them. Then, these nodes, which are called miners, create a timestamped block in which they include only valid transactions.

Every new block gets appended to the ledger resulting in an endless chain of blocks, which explains the notion blockchain.

A cryptographic hash function is a one-way function that maps input of arbitrary size to an output value of fixed length. This output is called the input's hash value. A Merkle tree is a tree whose leaf nodes are the hash values of some data and all non-leaf nodes are the hash values of their respective child nodes. The root node is called Merkle root. Any modification of a leaf node alters its hash value and the hash values of nodes using this value as their input. Ultimately, any such modification changes the Merkle root.

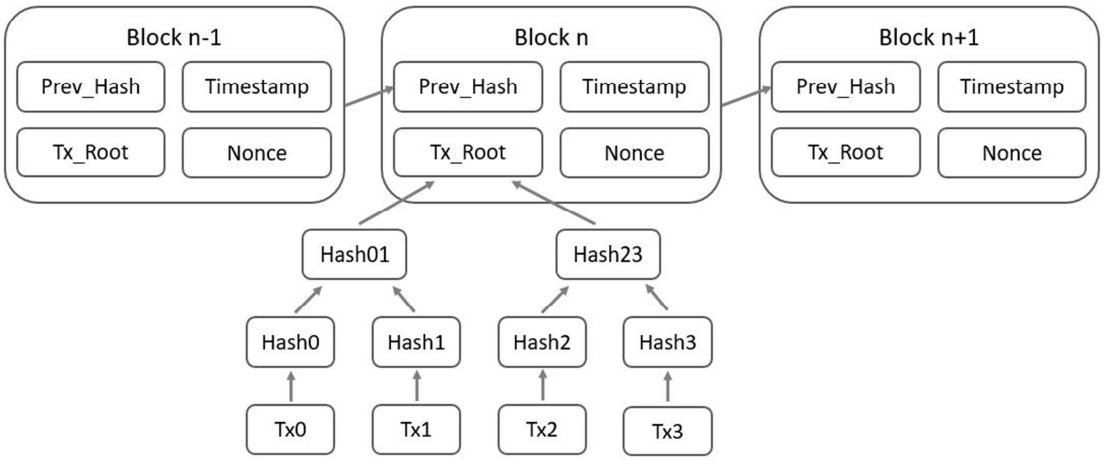


Fig. 2-1: Blockchain data structure.

The Bitcoin blockchain exploits the characteristics of Merkle trees and hash functions to allow easy detection of modifications of the transaction history (Fig. 2-1). To minimize the size of blocks, only the Merkle root (*Tx_Root*) of transactions gets included in a block. Further, every block references the hash value of its previous block. Consequently, if an earlier block gets changed, its hash value would be different and cause all following blocks to change as well.

Miners are competing against each other to create the next valid block of the blockchain. The victorious minor gets a reward in form of cryptocurrency. A miner was successful if the majority of the network has appended its block to their ledger.

Proof of work is a mechanism to counteract denial of service and spam attacks. By requiring a service requestor to do some computational effort the service becomes slightly more expensive to use. In contrast, checking that the work was actually done should be very easy. This concept is also employed to secure the Bitcoin blockchain. Miners must include a certain nonce value in blocks that they want to publish. Miners need to find a nonce which, when being part of the block, results in a hash value of the block in a specified format. To meet the requirement, the number of leading zeros of the block's hash value must be greater or equal to the mining difficulty, which is a measure used by the Bitcoin protocol to regulate the interval in which blocks are created. To compensate for improvements in hardware, the mining difficulty gets increased to keep the block creation time at around 10 min. Network nodes can easily verify if the proof of work was done for a proposed block. Because the only way to find the required nonce of a block is to try out all possible solutions until the value satisfies the condition, CPU power determines how likely it is to find a suitable nonce. As a result, the influence of networks nodes is limited by their computational resources. A so-called 51% attack is possible when more than 50% of the network's hash rate is controlled by one entity.

As soon as a valid next block is published, nodes append it to their ledger, discontinue their current effort of creating a block and instead continue with a new block. Thus, the fastest growing chain is regarded as the most up-to-date version of the blockchain. An attacker who would want to modify an already published block would have to redo its work of proof as well as the work of proof of every following block to

create an alternative longest chain. However, with every additional block the probability shrinks that an attacker can accomplish to outpace the longest chain with a modified version. In practice, when doing a transaction, the receiving party would wait a couple of blocks to get sufficient confidence that it is permanent. However, one can never be 100% assured that the Bitcoin's ledger will not eventually be tampered.

2.1.2.2 Ethereum

The Ethereum blockchain differs from the Bitcoin implementation in several ways. Ethereum is a transaction-based state machine, which uses an account model [Buterin2013]. Ethereum's current state, its canonical version, is the result of all transaction-triggered state changes that happened since its initial, genesis state up to the latest block. Ethereum offers smart contract functionality, which allows development of Turing-complete software. Due to the characteristics of the blockchain, smart contract applications, which are run on Ethereum's decentralized platform, have no downtime and behave in a deterministic manner, exactly like they were programmed.

Ethereum uses the concept of accounts. All accounts hold a balance and are referenced by unique addresses. Externally owned accounts belong to users who can use a private key to sign and initiate transactions. In contrast, smart contract accounts react on certain events, such as function calls and payments that they receive.

Gas is a mean to incentivize resource-economic usage of Ethereum as well as to sustain the network. For every transaction and computational operation, some fee needs to be paid. The exact price is expressed in gas and depends on the gas price. This way, the network fees are decoupled from the market price of Ethereum's cryptocurrency Ether. Miners can simply adjust the gas price. Further, miners can freely decide about which transactions to include in a block. Thus, they choose only transactions whose fees make them profitable enough for them. This mechanism allows the

network to finance itself and because only a limited number of transactions can be included per block, paying more for fees than others can increase the processing speed of a transaction. Additionally, the gas concept mitigates programming errors, such as endless loops. Because the fees must be paid in advance, program execution will be stopped and changes will be reverted as soon as the payment does not cover any further execution steps or when an exception occurs. If everything goes well and the execution finishes, any remaining gas gets refunded.

One of the major downsides of both Bitcoin and Ethereum is their reliance on proof of work, which wastes vast amounts of energy and bears the risk that mining pools dominate the network. An alternative, popular consensus algorithm is proof of stake [Buterin+2017]. This approach allows token holders to participate in the block creation process by locking some of their holdings as deposit. Stakeholders, who obey the rules, get rewarded. However, any malicious behaviour gets punished by taking away the offender's deposit. The Ethereum project aims to gradually switch to proof of stake in the near future.

Solidity is Ethereum's own smart contract programming language. Solidity code, which resembles JavaScript, must be compiled into Ethereum Virtual Machine bytecode, so that it can be deployed and run on the Ethereum network.

2.1.3 Directed Acyclic Graph

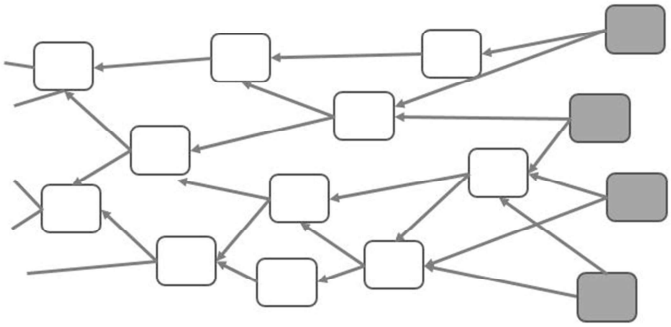


Fig. 2-2: Representation of a directed acyclic graph data structure.

DAG is an alternative to the blockchain data structure. In the case of DAG-based distributed ledger solutions, every transaction confirms one or more previous transactions (Fig. 2-2). The more confirmations a transaction gets, the more confidence users can have that the transaction is legit. The resulting structure is a directed graph without cycles. In comparison to blockchains, DAG platforms can achieve high transaction rates and low fees. However, due to their early state, they are not well explored yet and possible weaknesses are rather unknown. Iota and Swirlds Hashgraph are some of the projects that use DAG and claim to be highly secure, achieve enormous transaction speed and operate at extremely low costs [Iota, Baird2016]. Because of their infancy, DAG-based solutions have not been considered for the experiment of this work.

2.1.4 Technical Challenges

Technical hurdles prevent full exploitation of the potential of DLTs. Topics, that researchers are especially eager to solve, are related to usability, privacy, scalability, interoperability and waste of resources [YliHuumo+2016]. Further, considerations of ethical and legal aspects are integral to allow proper adoption. The characteristic of DLTs that appended data becomes immutable may conflict with laws when illegal, sen-

sitive or proprietary contents get stored on distributed ledger. A fundamental requirement to utilize smart contracts in a wider context is that authorities recognize them as legally binding. Due to the ever-growing amount of data that distributed ledgers produce, management of this data becomes increasingly hard. Moreover, running distributed ledgers on many nodes consumes vast amounts of energy. Especially, if proof of work is involved the energy consumption becomes even more enormous and morally questionable.

2.1.4.1 Privacy

In the case of Bitcoin all transactions, that ever happened, are publicly recorded. Although, no names of involved parties appear on the blockchain, the addresses of account holders and the amount that was sent are known to everyone [Fleder+2015]. Thus, transactions can be analysed, for example, using graph analysis, and conclusions can be drawn to link real-world identities to their Bitcoin addresses. Additionally, when using Bitcoin to order goods, the seller needs to know one's address to deliver the items. A best practice to maintain privacy is to never reuse a Bitcoin address for different payments. An alternative solution is mixing services, which are third parties that mix transactions of different people to obscure the real transactions.

Ethereum faces similar challenges. Ethereum offers no native privacy and sophisticated workarounds must be implemented for smart contracts that handle sensitive data. Because every computational step on the Ethereum blockchain costs gas, employment of encryption mechanisms in smart contracts is expensive and thus uneconomical for many use cases. Second-layer solutions, such as the Enigma privacy protocol, overcome this obstacle by performing operations with confidential data off-chain [Zyskind+2015]. Cryptographic proofs allow the blockchain to verify the correctness of the operations.

2.1.4.2 Scalability

Different distributed ledger platforms come up with different approaches to increase transaction speed and lower operation costs. Especially blockchain solutions tend to massively slow down when their network grows. With increasing number of nodes, communication and synchronization between nodes becomes more difficult. Thus, limiting the number of nodes can greatly improve the throughput, such as in the case of permissioned blockchains. Also, strategies to reduce the number of computational steps performed on the blockchain benefit the network to function better.

Sidechains are a popular idea to realize such approaches [Back+2014]. Instead of having one big blockchain, one main blockchain and several use case-specific sidechains, which are connected to the mainchain, are proposed. Sidechains can even work contrary to the mainchain with other protocols and other parameters. The reasoning is that any damage that happens on the sidechain cannot harm the mainchain. Besides having the freedom to use blockchain implementations, which are most suitable for a given use case, one can still use functionality of the mainchain, the more secure chain, for more critical operations. Depending on the purpose, some sidechains arguably require less security than others. In some cases, the incentive for an attacker to reverse or censor a transaction may be rather low and not worth the costs, for example, if a sidechain only stores data values and does not handle any money.

One of Ethereum's research projects concerning sidechains is Plasma [Poon+2017]. Plasma aims to realize tremendously fast smart contracts. These smart contracts would be executed on a sidechain or so-called child blockchain, which can have children as well. Periodically a hash value of the child's state, serving as a checkpoint, would be persisted on the parent blockchain. Only in the case of a dispute about the

computation on the child blockchain, the parent would have to determine the correct solution, punish the offender and roll back invalid changes.

Recently, Bitcoin released the lightning network [Poon+2016]. This technology allows drastic decrease of transaction fees by using off-blockchain payment channels. Two users can open a payment channel by depositing some amount of bitcoin. The deposit can be used for future payments until someone closes the payment channel. As a result, only two transactions are required: one to open the channel and one to close it. As long as the payment channel is open, a user can make payments until her deposit is used up. The lightning network can also route users' payments through other payment channels, so that they do not need to open an additional payment channel whenever they want to make a transaction to a new address for the first time. Any participant of a payment channel is free to close the channel at any time and to claim her current balance. Due to the counterparty's digital signature, the claimable amount is guaranteed.

Further parameters, such as block size, block creation time and the kind of consensus algorithm can influence the transaction speed. However, changing any parameters must be done very cautiously because of potential other negative consequences.

2.1.4.3 Interoperability

Since recently, numerous competing distributed ledger-related projects are appearing. These projects either attempt to serve a special use case or they aim for mass adoption. However, most solutions are not compatible with each other leading to fragmentation. If platforms could interoperate easily with each other, the whole ecosystem would benefit, because powerful applications could be built by combining different services.

Cryptographically-secure Off-chain Multi-asset Instant Transaction network (COMIT) is a proposal of a standard, geared towards distributed ledger technologies, similar like TCP/IP which allowed the internet to prosper [Hosp+2016]. The minimal requirements of COMIT are double-spend protection, multisig, time-locks and hashing functions. Multisig transactions require the signatures of several parties to be accepted by the network. COMIT uses smart contracts to connect different platforms. These smart contracts lock up some funds of parties wanting to connect. These funds are kept as deposit in case one party fails to obey the protocol. Time-locks are used to free any locked-up funds after a set period, for example, if one party stops responding.

2.2 Internet of Things

2.2.1 Characteristics

The IoT describes the phenomenon that computing is becoming increasingly ubiquitous and many objects can connect to the Internet [Mattern+2010]. Progress in science and mass production allow very cheap manufacturing of powerful microcomputers. With the help of sensors, objects can gather information about their physical environment. Besides interaction with things, the IoT aims to get a digital representation of the real world, so that physical objects can be computationally analysed and optimized. Initially, the IoT was mainly associated with Radio-frequency identification (RFID) technology. However, meanwhile the IoT encompasses a broad range of technologies.

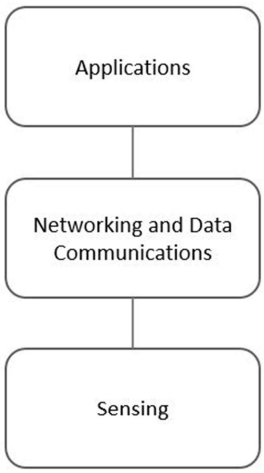


Fig. 2-3: Three-tier IoT architecture.

The IEEE Internet Initiative defines a three-tier architecture for the IoT [Minerva+2015]. The basic layer consists of sensors (Fig. 2-3). Networking and data communications technologies enable applications to access sensor data. Technologies used for sensing include RFID, barcodes and wireless sensor networks [Choudhary+2016]. The hardware of IoT devices should be optimized for low power consumption. Thus, protocols, such as IEEE 802.15.4, 6LoWPAN or ZigBee, which are designed for low data rate, short-range wireless networking and limited hardware capabilities are suitable to transfer sensor data to gateways. Commonly, data is transferred through heterogeneous networks. To allow efficient usage of sensing information, interface, service management, middleware and resource management and sharing for applications should be designed carefully.

Table I
Taxonomy of different complexity degrees of the IoT. '*' means least sophisticated, '**' means most sophisticated.**

	Technology	Complexity
Tagging Things	RFID	*
Feeling Things	Sensors	**
Thinking Things	Smart Technologies	***
Shrinking Things	Nanotechnology	****

IoT objects can demonstrate different degrees of complexity [Minerva+2015]. The most basic approach is to tag an object, so that it can be tracked automatically (Table I). '*Feeling Things*', in contrast, can capture all kind of information about their environment, such as temperature, humidity, speed, geo location and proximity to other objects. Such data can be reported for analysis and to decide further actions. '*Thinking Things'* do not even rely on external data processing and can respond autonomously to stimuli in their environment. *'Shrinking Things'* describes the fusion of technology and matter realized with nanotechnology.

2.2.2 Potential

The IoT may have major impacts on society and industries. Especially, businesses that have not yet undergone severe transformations by IT, such as agriculture, are likely to need to adapt to extreme changes caused by the IoT, to maintain competitive [Pureswaran+2015a]. The ultimate IoT is the digitalization of everything to make it manageable like digital content. Ideally, things should be able to communicate and interact with each other. They should be able to autonomously find and consume services for which they also pay. The IoT can make the real-world as efficient as the digital world. Utilization of things can be maximized by avoiding failure of devices, optimizing

maintenance and minimizing idle periods. Additionally, the sharing economy can be leveraged and boost monetization of things.

The IoT contributes decisively to making cities and factories more efficient which may reduce costs and pollution. Transportation can be optimized and become more secure. The health sector also benefits from the IoT and treatment of patients can be improved.

2.2.3 Challenges

The IoT has the potential to bring great benefits and the number of internet-connected devices grows rapidly. However, many IoT solutions, such as smart phone controllable toasters, have failed to find consumer acceptance [Pureswaran+2015a]. IBM states that for the IoT to flourish, the creation of improved products and user experiences is crucial. The IoT requires suitable business models and infrastructure. Trying to apply former business models and develop solutions like non-IoT systems will never allow to reach the IoT's full potential. Using cloud infrastructure for vast numbers of cheap devices will lead to high maintenance and provider costs that outdo its merit. Further, trusting third parties with data becomes less acceptable and users should have full control over their privacy. A paradigm shift from '*security through obscurity*' to '*security through transparency*' might be the only way to achieve systems that users can trust. When increasing numbers of sensors and actuators are integrated in our environment, for example, in buildings and transportation means, and our dependency on the IoT increases, longevity and reliability must be guaranteed. Thus, IoT products must be built future-proof and security must not rely solely on the manufacturer's support. Additionally, the limited hardware resources of IoT devices must be considered and systems should strive for low computational effort and require low bandwidth. Due to lack

of standards, IoT products of different manufacturers are often not compatible with each other and can only function with certain software solutions.

3 Previous Work

In this chapter, the results of an analysis of the current state of activities about fusion of DLTs and the IoT are presented. Considering related literature, three generic functions that distributed ledgers can provide for the IoT exist [Groopman+2018]. Distributed ledgers can serve the IoT primarily in an identity-related, transaction-related or interaction-related role. Based on recent research papers and by investigating major projects in this context, four main categories of applications that combine DLTs with the IoT have been identified. DLT-IoT merging applications fall into at least one of the following groups: supply chain, IoT network management, sharing economy and the Internet of value. This chapter closes with a description of the ADEPT proof-of-concept, which is a notable feasibility study on DLT-enabled IoT conducted by IBM.

3.1 Functions of Distributed Ledgers for the Internet of Things

3.1.1 Identity-related

With the help of asymmetric cryptography, the identity of entities can be verified. Only the holder of the correct private key can create digital signatures which are verifiable with a given public key. Consequently, this approach lets identities prove that certain actions were indeed intended by them. Moreover, identity-related information can be stored in a tamper-proof manner on a distributed ledger to allow public auditing and enforcement of compliance with the help of smart contracts.

3.1.2 Transaction-related

DLTs allow devices to autonomously trade with each other in a secure way. Devices can offer services and receive payments in the form of cryptocurrency. For example, devices may exchange tokenized assets, share data and use other devices' resources, such as storage and computing power. Smart contracts can enforce compliance with service conditions or compensation if terms are violated.

Micropayments between devices are a necessity for many IoT use cases [Lundqvist+2017]. Although cryptocurrencies seem to well serve this purpose, some hurdles must be overcome for broad adoption. For example, Bitcoin's limited throughput, long latency and high transaction costs make it unattractive for micropayments. However, pilot projects to realize machine-to-machine payments using the lightning network are already being conducted. An example of a popular use case being investigated is autonomous vehicles that buy their own fuel.

Iota is one of the pioneers building infrastructure to facilitate inter-device business use cases [Popov2016]. Iota's Tangle technology is a distributed ledger realized as DAG. Instead of miners that create blocks, every device that wants to send a transaction has to verify two other randomly assigned transactions. As a result, the network is self-sustaining and additional transaction fees are not required. In contrast to Bitcoin and similar blockchain solutions, which become slower when the number of nodes and transactions increases, Iota becomes faster and more secure if the number of participants rises because every additional device is contributing to the network. Iota also designs special IoT hardware which is optimized for the Tangle.

3.1.3 Interaction-related

With the help of DLTs, any events related to a device can be logged in a tamper-proof manner. Because nonrepudiation can be achieved with the help of such logs, fraud can easily be detected. Further, knowing a device's true state facilitates its maintenance. Secure DLT-based interaction with devices benefits many use cases, such us updating, patching or reparation of devices. Finally, DLTs are highly suitable to manage ownership and access rights of devices, while rules defined in smart contracts can allow automatized and scheduled device interaction.

Drones become increasingly significant in various contexts, such as agriculture and warfare. As drones become more powerful and fulfil critical tasks, the consequences of a drone malfunctioning or getting compromised can be fatal, especially in a military context. By storing all commands in a distributed ledger, integrity of interaction and trusted accountability can be ensured [Liang+2017]. As a result, anomalies can be traced back, while misbehaving entities can be identified and further investigated.

3.2 Applications of Distributed Ledgers to support the Internet of Things

3.2.1 Supply Chain

Tracking products is essential for supply chains. However, collected data is often not easily available for all stakeholders and data quality might be poor due to error-prone practices. A further risk poses re-use of tracking numbers for fake products by counterfeiters. Storing product-related information in a reliable manner on a distributed ledger and employing mechanisms for proving that a given product is genuine can mitigate such threads. DLT-based product tracking can achieve high confidence about the trustworthiness of data and enable stakeholders to independently audit information of a

product [Christidis+2016]. As a result, manufacturing conditions of products, such as fair labour and compliance adherence, can be verified.

Many start-ups offer DLT-supported supply chain solutions that allow stakeholders including end-customers to verify the history of goods. For example, everledger certifies authenticity of diamonds and other valuables by recording product-related events on a blockchain [Everledger]. With a similar approach, BlockVerify targets pharmaceuticals, luxury goods, diamonds and electronics [Venture_Proxy]. Chronicled builds end-to-end smart supply chain solutions completely with open technologies [Chronicled]. By incorporating IoT, their systems can help detect any non-compliance of manufactured products, e.g. if a product's storage conditions are insufficient. This might be the case for pharmaceuticals or food products which must be kept constantly in an environment of a certain temperature.

Filament offers applications and custom IoT chips to automatize steps in supply chain scenarios [Filament]. With the help of smart contracts, containers that arrive at a harbour or airport could even autonomously participate in arranging their transit. For example, containers could compare different shipping options to their next destination, choose one that meets certain criteria and pay for it.

3.2.2 Internet of Things Network Management

DLTs enable IoT networks to be manageable and secure by design. The key challenges of software defined networks – security, scalability and auditability – can be overcome by using a distributed ledger to organize IoT devices [Sytel_Reply]. The Securechain proof-of-concept showcases that DLT can enhance network security by ensuring that only trusted devices get added to a network. Further, hacking attempts or other irregularities can be detected reliably due to immutable logs. The need for trust gets

removed, because every device signs its transactions with its private key. In case of wrongdoings, an offender can be distinctly identified.

Traditionally, network administrators with special privileges can abuse their power to harm a system. By equipping a device with its own private key, so that it is only accessible for the device itself, such insider attacks can become impossible [Guardtime2016]. Because software evolves over time, reliable update mechanisms for devices are necessary [Banerjee+2017]. Fingerprints of software versions recorded on a distributed ledger enable devices to verify that they do not install compromised firmware. If a device detects that it runs corrupted code, it can heal itself by obtaining the proper software from a trusted peer device.

3.2.3 Sharing Economy

Cities are increasingly facing major challenges related to growth of population and pollution [Sun+2016]. Minimization of resource consumption and ideal utilization of assets are fundamental factors to mitigate such threads. To accommodate growing numbers of citizens, optimize traffic, provide enough resources, such as electricity, water and food, and to minimize waste and pollution, cities already highly depend on smart technologies. Car sharing and renting out of private rooms are already common in many places. DLTs can be used to leverage smart cities and the sharing economy even further by improving security, privacy, interoperability and inclusion of citizens.

Slock.it is a German start-up that aims to boost the sharing economy [Slock.it]. Slock.it's Universal Sharing Network is an Ethereum-based, open-source infrastructure which simplifies sharing of all kind of things. The solution allows users to register things that they want to rent out. Access control of smart devices including smart locks is managed with the help of Ethereum smart contracts. Objects that are unable to run an

Ethereum node must be connected with a more powerful access control device. With the help of a mobile app, people can discover and book things that they want to use. Payment is possible in Ethereum's cryptocurrency ETH and payment modalities depend on the owner's set up. For example, a deposit might be requested and once the usage period has terminated and if no problem has occurred, the deposit minus the rent would be returned. Moreover, with the help of a payment channel, users could be charged per unit of usage time. A user, who has successfully booked a thing, can unlock and control it via the mobile app. Therefore, the app sends commands to the rented device's related Ethereum client as messages which are signed with the private key of the authorized user.

3.2.4 Internet of Value

DLTs and the IoT have the potential to fundamentally change the internet as it is known today [Groopman+2018]. DLTs and smart contracts enable smart devices to autonomously participate in digital marketplaces and trade digital assets. Monetization of data, digital assets and resources, such as storage and power, may ultimately offer additional sources of income for the masses and shift the internet of things to an internet of value.

The use case of DLT-based smart grids aims to enable many people and ordinary households to participate in the energy market. To mitigate the fatal consequences of human-caused climate change, reduction of carbon-dioxide emissions seems strongly necessary. Consequently, alternatives to fossil energies, which lead to large amounts of carbon-dioxide emissions, are desirable. Further, nuclear energy poses major risks for humanity. No proper solutions to dispose nuclear waste exist and tragedies, such as the accidents at the nuclear power plants of Chernobyl and Fukushima, have shown the enormous difficulty of controlling nuclear energy. Renewable energies promise to

be more sustainable. However, generating solar, wind and water energy comes with its own challenges. Due to volatility of weather conditions, energy generation is hard to predict and control. As a result, matching demand and supply of energy, which is required for the proper functioning of a power grid, becomes extremely difficult. A surplus of energy may result in a collapse of the system and energy shortage is undesirable as well.

A solution is to regulate demand and supply with the help of the energy price [Fiedler+2016]. If energy supply exceeds the demand, lowering the price can incentive people to buy more electricity. Similarly, to counteract energy demand that is higher than the amount of produced energy, the price must increase. The revolutionizing idea of a DLT-based smart grid is to employ smart devices that aim to be economical by buying energy when it tends to be cheap. Additionally, with the help of smart contracts, individuals could profit from energy trading. For example, an electric car could be charged when energy is cheap. Any amount of the car's charge that exceeds the owner's needs could be released back into the grid and sold for profit. Likewise, owners of solar panels could participate in the energy market by selling overproduced electricity.

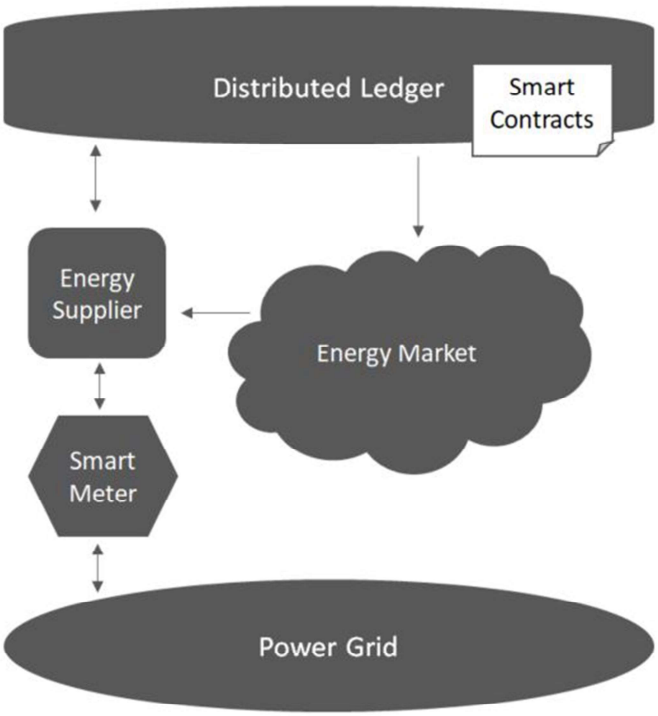


Fig. 3-1: DLT-based Smart Grid Architecture. Arrows indicate information flow.

A DLT-based smart grid requires several components (Fig. 3-1). Participants of the power grid are both producers and consumers of energy. Additionally, batteries, that store energy surpluses and offer available electricity, are fundamental for the smart grid to function. Smart meters let the energy supplier know demand and supply of electricity. The energy supplier acts as oracle whose data is trusted by the distributed ledger. The information provided by the energy supplier allows smart contract-based, automatized, real-time trading on the energy market. Smart devices can even further exploit the information available on the distributed ledger. Cold warehouses and refrigerators may cool down more than necessary when energy is cheap, so that they require less electricity when it is more expensive.

3.3 ADEPT Proof-of-Concept

IBM tested its vision of a decentralized IoT by conducting a proof-of-concept in close collaboration with Samsung Electronics [Pureswaran+2015b]. Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) serves as foundation for realizing fully decentralized IoT scenarios. The researchers admit that their solution has still some limitations which need to be overcome for commercial adoption. IBM predicts that IoT devices will complement centralized internet solutions. Due to new opportunities to generate business value that the '*edge*' offers, an Economy of Things will emerge. With the help of several use cases, such as washers that autonomously reorder detergent and service parts, IBM substantiated their statements.

Three fundamental functions are required for a decentralized IoT approach like ADEPT, namely, peer-to-peer messaging, distributed file sharing and autonomous device coordination. ADEPT uses Telehash as decentralized messaging protocol allowing server-less communication with IoT devices. Telehash supports trustless, encrypted message exchange with fast and guaranteed delivery plus further features. With the help of distributed hash tables, unique public key-based addresses of devices are managed enabling devices to find other peers on the network. Distributed file sharing uses the same approach to allow distribution of content, such as software or firmware updates, on peer-to-peer networks. ADEPT chose BitTorrent for this purpose.

Rules and contracts are necessary to manage device coordination. Device owners must be able to register and control their devices. Rules can be used to regulate device-specific interaction, such as proximity-based rules to define device behaviour considering physical, temporal and social aspects. Contracts allow the definition of more complex agreements enabling inter-device trade and commerce of services and re-

sources. ADEPT exploits Ethereum's functionality to solve autonomous device coordination.

IoT devices' functions in the network differ depending on their capabilities. Due to differences in computing power, storage space and so on, some devices can support more functionality than others. Also, relationships of devices can evolve over time and may develop from trustless over semi-trusted to trusted. Essentially, the kind of interaction, a device's type, constraints defined by the owner as well as the relationship with other devices determine the function of an IoT device.

Table II
Capabilities of different kind of peers. 'x' means that the functionality is supported, '-' means that the functionality is not supported, '(x)' means that the functionality is only supported to a limited extent.

	Peer Exchange	Standard Peer	Light Peer
Related Peer List	x	x	x
Messaging	x	x	x
File Transfer	x	x	(x)
Blockchain Node	x	(x)	-
Analytics	x	(x)	-
Marketplace Management	x	-	-

IBM differentiates between three categories of peers (Table II). All devices maintain related peer lists to keep track of the functionality that other peers in their proximity offer. Further, the capability to exchange messages is a basic requirement for all kinds of peers. In contrast, light peers with very restricted computational power and small storage depend on standard peers to perform blockchain-related actions. Also, the file transfer capabilities of light peers are restricted. Standard peers are able to act as

blockchain node. However, they cannot store the whole blockchain transaction history. Further, standard peers can perform some minor analytics with data of their close peers. Because storing the complete ledger of transaction requires vast amount of storage, only cloud or server-based peer exchanges are suitable for that task. These peers can also fulfil advanced analytics jobs and coordinate marketplaces to allow trade of digital assets, services and resources.

4 Rating-assisted State Channel Design for the IoT

In this chapter, the results of the survey are presented to motivate the need for technology that allows scalable, low-cost and fast micropayments. Concretely, identified opportunities as well as limitations of leading DLT platforms to support the IoT are summarized. Next, state channels, which may leverage DLTs' suitability for the IoT, are introduced. Finally, an improved state channel design incorporating a smart contract-based reputation system is suggested.

4.1 Identified Opportunities of DLTs to support the IoT

DLT platforms can already enable many functions for the IoT. Cryptocurrencies allow smart devices to make payments. With the help of smart contracts many scenarios of autonomous device interaction are possible, such as trading of digital assets and sharing resources. Further, DLTs allow secure management of devices. Due to asymmetric cryptography, unambiguous authentication of entities is possible. In combination with tamper-proof logs stored on a distributed ledger, nonrepudiation of actors can be achieved leading to advanced security of systems. In general, DLT is an ideal mean to ensure data integrity. In a nutshell, current DLT solutions appear to be suitable to realize device-to-device payments, regulate autonomous behaviour of devices and leverage security of IoT networks including interaction with smart devices by achieving data integrity and accountability of involved actors.

4.2 Identified Limitations of DLTs to support the IoT

Prominent DLT solutions, such as the main Ethereum public blockchain, expose several flaws currently limiting their suitability to serve the IoT. A major drawback of these platforms is their limited transaction handling capabilities. Ethereum's throughput is about 15 transactions per second. Secondly, due to the block creation time, no constant finality of transactions is achieved. Ethereum miners create a new block about every 10 to 20 seconds. Additionally, several block confirmations should be waited to gain more confidence that a transaction did not end up in an orphaned block. As a result, real-time scenarios cannot be supported with such a technology.

Further, the transaction costs of DLTs make them unattractive for many use cases. Regular transactions on Ethereum cost about 0.3 USD. However, the costs for execution of smart contract functionality can be significantly higher if many computational steps are required. Because all transactions and data on Ethereum are publicly auditable by default, privacy is especially hard and expensive to achieve on this system.

The use of DLTs introduces even further complexity. Both application developers and users of decentralized applications (dApps) require special skills and knowledge. A purely centralized IoT solution, such as AWS IoT, can be set up with little effort compared to developing a dApp. Users of dApps have to use a special browser or a browser plugin, such as MetaMask [MetaMask]. Also, users are expected to know how to safely manage their accounts.

In summary, limitations due to inadequate privacy-support, delayed data processing, low throughput, additional costs and increase of complexity for users and developers appear to be major barriers for completely decentralized IoT scenarios.

4.3 State Channels

Several approaches are explored to overcome the shortcomings of DLTs. One possibility is layer 2 or off-chain scaling respectively, such as state channel solutions that allow private and almost instant transactions without the cost of the regular transaction fees [Coleman2015]. The Raiden network is Ethereum's pendant to Bitcoin's payment channel implementation lightning network [Brainbot_a]. Payment channels are a specialization of state channels because they solely focus on off-chain payments. In contrast, generalized state channels aim to make smart contract functionality executable off-chain [Counterfactual].

Balance proofs that do not rely on global consensus allow high throughput of transactions on payment channels. Balance proofs can be transferred using regular internet technology. Transactions get immediate finality as soon as the sender has signed a valid balance proof, because the sender's signature allows the receiver to enforce the payment any time by submitting the latest balance proof to the blockchain.

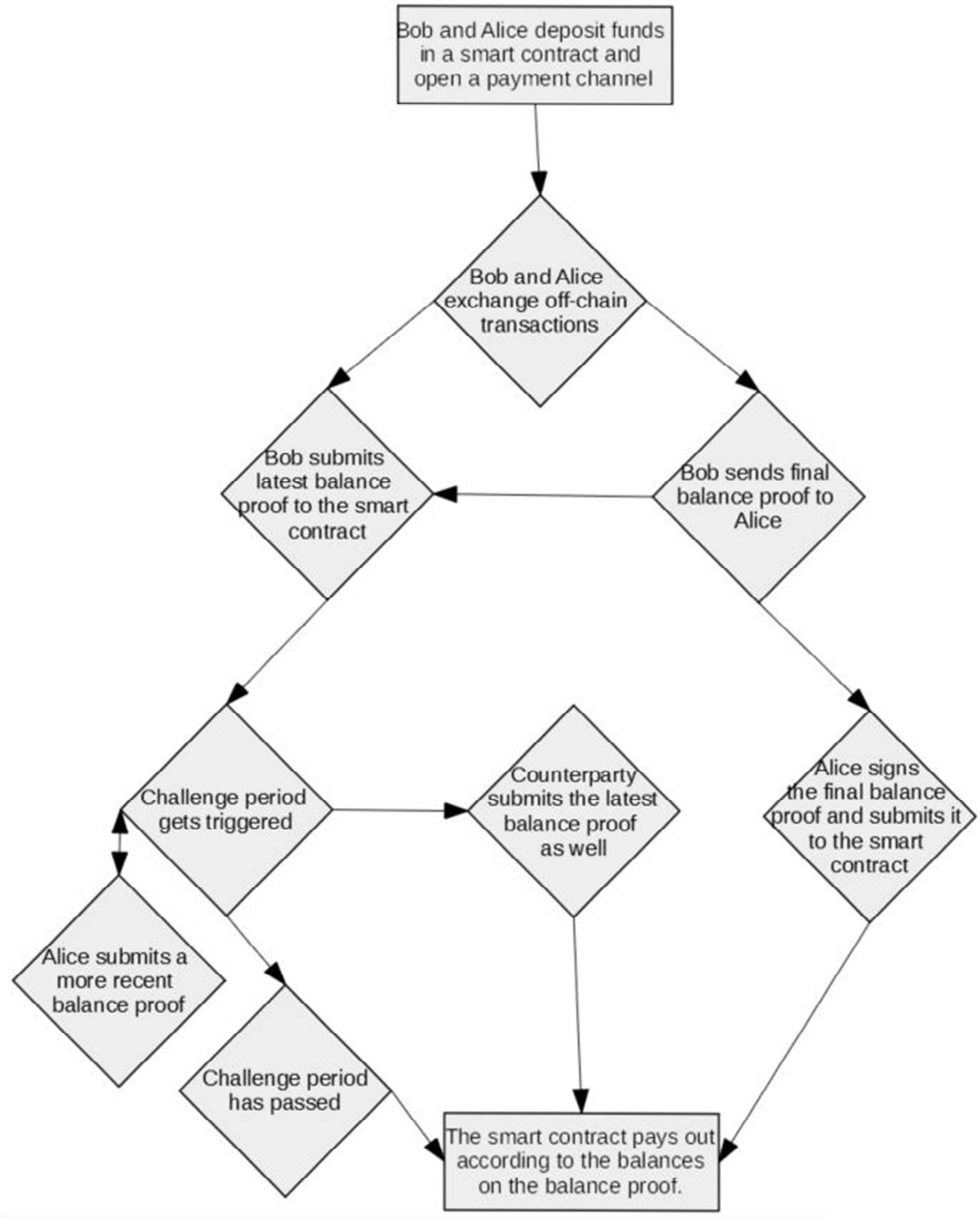


Fig. 4-1: Flow chart of payment channel example.

The following example demonstrates the working of a payment channel. To open a payment channel Alice and Bob have to deposit some amount of digital tokens in a smart contract (Fig. 4-1). All off-chain transactions must be backed by deposited funds.

Every balance sheet holds the balances of both Alice and Bob and a sequence number. The sum of Alice's and Bob's balance must equal the amount that is hold in escrow in the smart contract. An off-chain transaction is conducted by creating an updated balance sheet with the next sequence number. The transaction has validity once both Alice and Bob have confirmed their agreement by signing the balance sheet. This process can be repeated as often as required. A channel can be closed any time to claim the actual funds. Therefore, any party can submit the latest balance proof to the smart contract residing on the blockchain. The smart contract will then wait a challenge period to make sure that not a balance proof with a more recent sequence number exists and gets submitted. To avoid the challenge period and get payed out immediately, either both parties can submit the latest balance proof or they can both sign a balance proof that explicitly marks the final state.

Although state channels have several advantages, some drawbacks limit their applicability. In the previous described example, the participants must be known in advance and an additional payment channel must be opened for every two parties. Bitcoin's lightning network and the Raiden network mitigate this weakness with the help of an off-chain hub network that can connect any parties that have a payment channel with anyone being connected to this hub network. Because the maintenance of such a routing network depends on fees, this solution becomes slightly more expensive than a more primitive state channel approach.

Funds that are deposited in the smart contract are locked up and impair one's liquidity. In the worst case, one must wait the full challenge period until funds get disbursed if the counterparty does not cooperate. Moreover, once per challenge period participants of a state channel must check that no outdated balance proof was submitted by a

cheating counterparty. Finally, opening and closing of state channels still require regular on-chain transactions which entail transaction costs and delay.

4.4 Rating-assisted State Channels

The worst case scenario of state channels happens when the counterparty does not provide a signature for a final balance proof. In this situation, regaining deposited funds is only possible after the full challenge period has passed. Additionally, service requestors have no indication about the reliability of different service providers on a digital market. To incentivize cooperative behavior and increase transparency related to the service quality of market participants, this research suggests enhancing state channels by introducing a reputation system for account addresses.

Reputation systems are common for many online platforms, such as eBay, Amazon or Airbnb. Also, peer-to-peer-based technologies, e.g. for decentralized cloud storage like Bluzelle or Sia, exploit similar ideas [Murarka+2017, Nebulous]. Because bad-rated service providers will ultimately face monetary disadvantages, any economically driven entity would make efforts to receive good scores.

Table III
Rules of address rating logic.

Rating	Closing signature before number of blocks
5	3
4	5
3	13
2	49
1	*Value of challenge period*

A proof-of-concept of a smart contract-based reputation system, suitable to be adopted by state channel libraries and other use cases, was implemented to demonstrate a rating-assisted state channel solution. An Ethereum smart contract that manages ratings of addresses can be queried to receive the rating of a given address and authorized addresses can rate other addresses. In this work, a 5-point rating scale was chosen, 1 being the worst and 5 the best score. The implemented smart contract gives a rating based on the delay with which a payment receiver provides the signature for closing a channel (Table III). Further, the rating gets weighted with the value that was transacted off-chain which is the receiver's final balance.

For this work, the µRaiden (Micro Raiden) state channel library was modified to showcase how the address rating mechanism can be used. µRaiden supports unidirectional payment channels being geared towards scenarios consisting of a service provider and a service requestor [Brainbot_b]. With the help of µRaiden payment channels almost instant and feeless micropayments in cryptocurrency to charge accurately for the usage of services, such as data streams or buying electricity, are possible.

```
function settleChannel(address _sender_address, address _receiver_address,
    uint32 _open_block_number, uint192 _balance) private
{
    bytes32 key = getKey(_sender_address, _receiver_address,
_open_block_number);
    Channel memory channel = channels[key];
    require(channel.open_block_number > 0);
    require(_balance <= channel.deposit);
    require(withdrawn_balances[key] <= _balance);
    // additional logic for rating the receiver's address when a channel gets closed
    uint32 delayForClosing = closing_requests[key].settle_block_number -
uint32(block.number);
```

```
    if(delayForClosing < 0) {
        delayForClosing = challenge_period;
    }
    addressRatings.rateReceiver(_receiver_address, _balance, delayForClosing);
    […]
}
```

Listing 4-1 Extract of modified settleChannel method in µRaiden's Solidity smart contract.

When closing a payment channel, the *settleChannel* method of µRaiden's Solidity smart contract is eventually called (Listing 4-1). Initially, *settleChannel* generates the caller's key and retrieves its related channel object. Then, the function checks whether the caller satisfies all requirements to call this function. The logic for rating the payment receiver's address follows. To successfully rate an address, the receiver's balance as well as the amount of blocks that have passed until the receiver has provided the closing signature must be passed as arguments when calling *rateReceiver*. Additionally, the address that calls this function must be whitelisted in the smart contract handling the ratings or the call remains without effect.

5 Evaluation

This chapter contains an evaluation of the suggested rating-assisted state channel design. Opportunities and limitations of this research are depicted and its merit is quantifiably argued with the help of theoretic values.

This work suggested enhancing state channels by introducing a reputation system for account addresses. When comparing the computational effort for regular on-chain Ethereum transactions with off-chain transactions, the additional overhead due to the logic for the address rating is negligibly low. Further, the address rating only occurs once, namely, when a payment channel gets closed.

Table IV
Comparison of fees, duration and funds locked duration of 10 layer 1 with 10 layer 2 transactions. 1 Finney fee per transactions, 4 block confirmations, 15 s block creation time and 500 blocks challenge period are assumed.

	10 regular transactions (layer 1)	10 transactions using µRaiden payment channel (counterparty cooperates)	10 transactions using µRaiden payment channel (counterparty cooperates not)
Transaction fees (Finney)	10	2	2
Duration (min)	10	1	1
Duration funds locked (min)	0	2	127

Transaction speed and costs of regular transactions depend on the block creation time and the transaction fees. One Ethereum transaction can be assumed to cost about 0.3 USD which is about 0.001 ETH or 1 Finney. In the case of regular transactions, these costs must be paid for every additional transaction. Thus, 10 transactions would cost about 10 Finney (Table IV). However, state channels only require one transaction to open the channel and one to close it. Because all layer 2 transactions are feeless, payment channels are cheaper than on-chain transactions if at least three payments are made. In case four block confirmations are required and a new block is created about every 15 s, every on-chain transaction would take about one minute. Therefore, 10 regular transactions would result in a 10 min-duration. In contrast, only network latency needs to be considered for state channel-based payments. If the network latency is sufficiently low, only the time required for opening a channel is relevant which would be one minute in both cases. Consequently, payment channels are faster than regular transactions if at least two payments are made.

Table V
Formulas to determine the average challenge period duration and the funds locked period. *t* indicates a time unit, *p* indicates a likelihood percentage.

(1) $t_{\text{average challenge period}} = t_{\text{block creation}} * 500 * p_{\text{counterparty cooperates}}$

(2) $t_{\text{funds locked}} = t_{\text{open channel}} + t_{\text{close channel}} + t_{\text{channel is active}} + t_{\text{average challenge period duration}}$

$= 2 * t_{\text{transaction}} + t_{\text{average challenge period duration}}$

if $t_{\text{open channel}} = t_{\text{close channel}} = t_{\text{transaction}}$, $t_{\text{channel is active}} = 0$

Payment channels have the disadvantage that only funds held in escrow can be spent. If both parties cooperate, the smart contract will pay out as soon as a final balance proof is submitted. Thus, funds are locked for at least 2 min or the duration of

opening and closing the payment channel. In this case, $t_{average\ challenge\ period\ duration}$ in equation (Table V, 2) would be 0. Additionally, the funds are locked as long as the payment channel is open ($t_{channel\ is\ active}$). In case of an uncooperative close, the full challenge period must be waited until the funds can be received. µRaiden defines 500 blocks as minimum challenge period. If 15 s are assumed to be the block creation time, 500 blocks would be 125 min. If the duration of the channel being active is ignored and the time for opening and closing a channel is added, the duration of funds being locked results in 127 min being the worst case scenario.

Table VI
Average duration of funds being locked for different likelihood that counterparty does not cooperate. 4 block confirmations, 15 s block creation time and 500 blocks challenge period are assumed.

Likelihood that counterparty does not cooperate (%)	Average duration of funds being locked (min)
100	127
90	114.5
80	102
70	89.5
60	77
50	64.5
40	52
30	39.5
20	27
10	14.5
0	2

By employing rating-assisted state channels, a reduction of the possibility that the counterparty does not cooperate compared to the conventional implementation is ex-

pected. Assuming that channels either get closed immediately if both parties cooperate or otherwise only once the challenge period has passed, the average period that funds are locked decreases with decline of the likelihood that a payment receiver does not cooperate (Table VI). Based on the employed numbers and equation (Table V, 2), 10 % reduction of the likelihood that the counterparty does not sign the final balance proof entails that funds are locked in average 12.5 min less than before.

6 Discussion

In the following, the implications and contributions of this work are outlined. Moreover, the results of this research are put in context with related studies.

Rating-assisted state channels have the potential to improve digital marketplaces. Monetarisation of services that smart devices can offer, require functionality for inter-device micropayments. Cryptocurrencies might be well suited for this purpose if transactions can happen fast and at low costs. State channels and reputation systems might be a solution in this context. Studies about reputation systems of online platforms, such as eBay and Amazon, indicate that the ability to rate market participants benefits reliable entities [Chwelos+2006, Jøsang+2007, Melnik+2002]. Improvements of a seller's reputation have shown to increase her sales and in general buyers are willing to pay a premium when buying from highly rated sellers. Similarly, in digital IoT marketplaces service providers may aim for excellent service quality to increase their business. Highly reputable service providers might even be able to charge rates above the regular market price.

The suggested rating-assisted state channel approach has several shortcomings. A concern that researchers raise is that sellers that try to newly enter a market are disadvantaged, because they have to compete with the established vendors [Melnik+2002]. A strategy for them might be to offer their services below the market price in the very beginning and increase their charges once they have received sufficient positive ratings. The same would be necessary for anyone having received bad scores due to low

service quality. In contrast, making it hard for newly entering market participant to get established as reliable service provider has the benefit that it is rather unattractive to get rid of bad ratings by switching the account address. A further weakness is that occasionally service providers might not be able to respond and provide a signed final balance proof simply due to technical problems, such as an unreliable, slow or failed internet connection. If an unfortunate delay just happens rarely, the overall rating would only be affected slightly. However, to constantly fulfil high standards, service providers must ensure that their infrastructure is reliable and up-to-date. Nevertheless, service requestors have no guarantee that a highly rated service provider will always be completely reliable. As previously mentioned, due to unfortunate circumstances, a service provider might be occasionally unable to perform in a reliable manner. Finally, the code of smart contracts on the public Ethereum blockchain can be inspected by anyone. Consequently, trying to achieve security by obscuring the rating algorithm is impossible. Rather a reputation system design that can achieve security through transparency is required.

A smart contract-based reputation system exhibits various benefits in comparison to established human-involved rating mechanisms. A smart contract's rating is unbiased and follows clearly defined rules. Humans instead may be led by emotions and behave irrational. Studies reveal that reputation systems suffer from weaknesses, such as low incentives for providing ratings and unfair ratings [Jøsang+2007]. Because the smart contract automatically submits a rating when it is expected to do so and strictly follows algorithms, such problems are mitigated in the solution of this work. However, ratings might suffer from manipulation, for example, if transactions between devices belonging to the same owner are conducted. The fact that in such a case costs for opening and closing a channel as well as for provision of some service exist might be some form of

deterrent against such unfair behaviour. Moreover, if the service quality in all other interactions is poor, the rating will eventually converge to its true value.

Overall, rating-assisted state channels may benefit digital marketplaces in several ways. Economically motivated participants will try to behave in a manner to receive high ratings. Ratings increase transparency about the reliability of market participants allowing service requestors to identify service providers with high service quality. If cooperative behaviour increases and state channels are closed efficiently, the liquidity in digital markets raises, because funds are locked for shorter periods. Ultimately, rating-assisted state channels contribute to the realization of DLT-based device autonomy. Thus, a rating mechanism of Ethereum account addresses should be standardized, so that it can be integrated in other projects, such as µRaiden.

7 Conclusion and Future Research

In this final chapter, the main content of this thesis is summed up and an outlook on open follow-up research is given. Relevant topics and developments in the context of DLT-IoT convergence are pointed out.

This research investigated the current state of DLT-IoT fusion. According to relevant literature and insights gained by the examination of related initiatives, functions that distributed ledgers can perform for the IoT can be identity-related, transaction-related and interaction-related. Use cases of DLT-supported IoT may be associated with supply chain, IoT network management, sharing economy and Internet of value.

DLTs are potentially able to provide strongly needed functionality for the IoT, namely, digital value transfer, device autonomy and secure IoT networks. However, limited transaction throughput, low transaction speed, relatively high costs, lack of privacy and additional complexity restrain the applicability of prominent DLT solutions, such as the Ethereum platform. State channels appear as promising technology to mitigate some of these drawbacks.

Payment channels are especially suitable for micropayments by not requiring every transaction to be recorded on the distributed ledger. However, to prevent double spending of funds, some deposit must be locked in a smart contract when opening a payment channel. This reduces the liquidity of participants and if the counterparty fails to cooperate, a challenge period must be waited until locked up funds can be regained. To incentivise reliable behaviour and allow service requestors to estimate the likelihood

that a service provider will cooperate, enhancing state channel solutions with a smart contract-based reputation system is suggested.

Research indicates that reputation systems improve business opportunities of reputable sellers on online platforms, such as eBay. If this also applies to digital machine-to-machine marketplaces, highly reputable service providers may be able to charge prices above average and face higher demand than worse-rated suppliers. As a result, economically driven parties are incentivised to always provide the best possible service quality.

A limitation of this work is that the effectiveness of rating-assisted state channels could only be justified based on calculations with theoretic numbers. However, smart contract-based reputation systems do not suffer from all the reported drawbacks that established peer-to-peer rating systems have. Thus, advancement and standardization of the concepts proposed in this work seem worthwhile to step closer towards the vision of an autonomous IoT.

Based on this work, follow-up investigations can be conducted. Measuring the effectiveness of reputation systems for Ethereum account addresses in real-world systems remains an open challenge. So far, the degree of service quality improvement to which rating-assisted state channels would lead could not be determined.

Optimization of the rating algorithm might be possible. Different parameters and approaches should be compared. Especially, insights regarding the fairness and immunity against manipulation of smart contract-based reputation systems for the IoT are needed. Another topic is how newly emerging service providers should be treated. For example, a flag could indicate that they have not been rated yet or some default value could be given as initial score. Once a satisfying Ethereum account rating scheme has been developed, it should be standardized to foster adoption.

More research about state channel technology in general is needed. Ways to avoid opening and closing of state channels or at least to cut the involved overhead and costs should be investigated. Finally, the applicability of state channels to smart contracts requires more study, because current solutions mainly support payments.

Many challenges prevent DLT platforms to achieve wide adoption. To properly serve the IoT, shortcomings of DLTs, especially regarding scalability, privacy, cost and usability, must be overcome. Beside state channels, further technologies may show suitability for the IoT. For example, Practical Proof of Kernel Work is a consensus algorithm allowing even resource-restrained devices to vote in the block creation process [Lundbæk+]. Decentralized data storage for real-time purposes is also required for many IoT use cases.

Even if all technical challenges of distributed ledgers can be successfully solved, further aspects might need to be addressed. The legal situation of DLT-involved scenarios is often not clear and territorial differences may exist. Legal enforcement of smart contracts is a controversial topic as well as liability in IoT-related scenarios. Also, payments in cryptocurrency are not yet sufficiently regulated. Device-to-device payments and taxation-related matters need clear guidelines to allow the realization of envisioned IoT business models. Another pain point of DLTs is compliance with laws, such as the General Data Protection Regulation (GDPR). GDPR was recently introduced by the European Union and grants EU citizens the '*right to be forgotten*' by companies [Schulz2015]. However, personal data stored on a distributed ledger is technically non-erasable and cannot be modified anymore.

Standards and user adoption are further factors that are crucial for the success of DLT-enabled IoT. Even without the employment of DLTs, different IoT solutions are often difficult to integrate due to incompatible technologies. To have an easy-to-use

and highly efficient IoT, standards are a fundamental prerequisite. However, due to numerous, fragmented DLT platforms, integration of solutions can be sophisticated. Initiatives, such as COMIT, envision a standard that, if followed by all DLT platforms, can realize an infrastructure like the World Wide Web enabled by TCP/IP [Hosp+2016]. Once the technology is mature enough, end-user adoption must be fostered. People need to be educated about the usage of cryptocurrency and secure key management. At the same time, applications must be easy and intuitive to use.

Researchers see great potential for the combination of artificial intelligence, DLTs and the IoT. As the computational capabilities of smart devices increase, IoT devices might be able to autonomously use machine learning to gain insights from collected data and adjust their behaviour accordingly.

Finally, ethical aspects need to be addressed. As dependence of society on highly complex technology increases, the risk of a technocracy becomes more severe. Already today, no expert can completely grasp all aspects of comprehensive systems. Thus, consequences of system modifications are hard to predict and security flaws are difficult to discover. Additionally, as understanding of how systems work becomes increasingly hard, the elite can take advantage of this by watching, manipulating and controlling the average population. Last but not least, environmentally hazardous impacts due to the increased utilization of technologies, such as DLTs and smart devices, can be considerable. To some extent, these technologies may help to save resources and become more economical, but the introduction of additional use cases and functionality usually increases consumption of resources.

요약문 (Summary in Korean)

위 석사 논문은 DLT-IoT 융합의 현상을 조사하였습니다. 관련된 문헌과 검토를 기반으로 한 조치에 의하면, 분산된 재정 지원으로 수행 가능한 IoT 기능은 신원 관련, 거래 관련 및 상호 작용 관련을 실행하게 합니다. DLT 지원 IoT 의 활용 사례는 공급 망, IoT 네트워크 관리, 경제 공유 및 가치 인터넷과 연관 될 수 있습니다. DLT 는 IoT 에 디지털 가치 전송, 디바이스 자율성, IoT 네트워크 보안 등 강력하게 필요한 기능을 제공할 가능성이 있습니다. 그러나 제한된 거래 처리 속도, 낮은 거래 속도, 상대적으로 높은 비용, 개인 정보 보호의 결여 및 추가적인 복잡성으로 인하여 Ethereum 플랫폼과 같은 주요 DLT 해결책 적용이 제한됩니다. 스테이트 채널들은 이러한 단점의 일부를 완화할 수 있는 유망한 기술로 보입니다. 결제 채널들은 모든 거래가 분산된 장부에 기록되도록 요구하지 않음으로써 소액 대출에 특히 적합합니다.

그러나, 자금의 이중 지출을 막기 위해서는, 결제 채널을 개설할 때 일부 예금이 스마트 컨트랙트로 잠겨 있어야 한다. 이는 실험 참가자들의 유동성을 줄이고 만약 위의

계약으로 맺어진 당사자가 협조하지 않는 경우에는 잠금 기금이 되찾기 전 까지는 기다리는 기간이 요구됩니다. 이러한 위험을 완화하고 서비스 요청자가 서비스 제공자가 협력할지 여부를 추정할 수 있도록 허용하여 스마트 컨트랙트 기반 평판 시스템으로 스테이트 채널 솔루션을 개선할 것을 제안합니다. 연구에 따르면, 평판 시스템은 eBay 와 같은 온라인 플랫폼에서 평판이 좋은 판매자의 사업 기회를 향상시킨다고 보고가 되어있습니다. 디지털 기기가 기계 시장에도 동일하게 적용된다면, 매우 평판이 좋은 서비스 제공 업체들은 평균 이상으로 가격을 부과할 수 있으며, 낮은 등급의 공급 업체들보다 더 많은 수요에 직면합니다.

결과적으로, 경제적으로 주도되는 당사자들은 항상 최상의 서비스 품질을 제공하도록 장려가 됩니다. 이 작업의 제한 사항은 등급 보조 스테이트 채널의 효율성은 오직 이론적으로만 유효 숫자 계산에 근거하여 나타낼 수 있다는 것이다. 그러나 스마트 컨트랙트 기반 평판 시스템은 공통 P2P 등급 시스템이 가지고 있는 보고된 단점의 일부를 겪지 않습니다.

따라서 본 연구에서 제시된 개념의 발전과 표준화는 자율형 IoT 의 비전을 향해 한발 더 다가설 가치가 있는 것으로 보입니다.

References

[Back+2014] Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., and Wuille, P. (2014). *Enabling blockchain innovations with pegged sidechains*. URL: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains.

[Baird2016] Baird, L. (2016). *The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance*. Swirlds.

[Banerjee+2017] Banerjee, M., Lee, J., and Choo, K. K. R. (2017). *A blockchain future to Internet of Things security: A position paper*. Digital Communications and Networks.

[Buterin2013] Buterin, V. (2013). *Ethereum white paper*. GitHub repository.

[Buterin+2017] Buterin, V., and Griffith, V. (2017). *Casper the Friendly Finality Gadget*. arXiv preprint arXiv:1710.09437.

[Brainbot_a] Brainbot (n. d.). What is the Raiden Network? Retrieved Mai 6, 2018, from https://raiden.network/101.html

[Brainbot_b] Brainbot (n. d.). µRaiden. Retrieved Mai 6, 2018, from https://raiden.network/micro.html

[Cardano] The Cardano Foundation (n.d.). *The Cardano Project*. Retrieved April 3, 2018, from https://www.cardano.org/

[Choudhary+2016] Choudhary, G., and Jain, A. K. (2016, December). *Internet of Things: A survey on architecture, technologies, protocols and challenges*. In *Recent Advances and Innovations in Engineering (ICRAIE)*, 2016 International Conference on (pp. 1-8). IEEE.

[Christidis+2016] Christidis, K., and Devetsikiotis, M. (2016). *Blockchains and Smart Contracts for the Internet of Things*. IEEE Access, 4, 2292-2303.

[Chronicled] Chronicled (n. d.). *Smart Supply Chain Solutions*. Retrieved April 4, 2018, from https://www.chronicled.com/

[Chwelos+2006] Chwelos, P., and Dhar, T. (2006). *Caveat emptor: Differences in online reputation mechanisms*. Working Paper, Sauder School of Business, University of British Columbia.

[Coleman2015] Coleman, J. (2015). State Channels. Retrieved May 18, 2018, http://www.jeffcoleman.ca/state-channels/

[Crosby+2015] Crosby, M., Nachiappan, P., Pattanayak, P., Verma, S., and Kalyanaraman, V. (2015). *Blockchain Technology: Beyond Bitcoin*. Sutardja Center for Entrepreneurship & Technology Technical Report. http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

[Counterfactual] Counterfactual (n. d.). Retrieved Mai 6, 2018, from https://counterfactual.com/

[Everledger] Everledger Ltd. (n. d.). *Everledger - A Digital Global Ledger*. Retrieved April 3, 2018, from https://www.everledger.io/

[Fiedler+2016] Fiedler, I., Fiedler, F., and Ante, L. (2016). *Die Vision eines integrierten Energiemarktes*.

[Filament] Filament (n. d.). *Enabling the future of IoT*. Retrieved April 4, 2018, from https://www.filament.com/

[Fleder+2015] Fleder, M., Kester, M. S., and Pillai, S. (2015). *Bitcoin transaction graph analysis*. arXiv preprint arXiv:1502.01657.

[Gartner2017] Gartner Inc. (2017). *Leading the IoT*.

[Groopman+2018] Groopman, J., and Owyang, J. (2018). *The Internet of Trusted Things*. Kaleido Insights.

[Guardtime2016] Guardtime (2016). *Use of a globally distributed blockchain to secure SDN*.

[Gupta2017] Gupta, V. (2017). *A brief History of Blockchain*. Harvard Business Review, 28.

[Hosp+2016] Hosp, J., Hoenisch, T., and Kittiwongsunthorn, P. (2016). *COMIT - Cryptographically-secure Off-chain Multi-asset Instant Transaction network*. White paper version v1.0.2.

[Iota] The Iota Foundation (n. d.). *Iota*. Retrieved March 23, 2018, from https://iota.org/

[Jøsang+2007] Jøsang, A., Ismail, R., and Boyd, C. (2007). *A survey of trust and reputation systems for online service provision*. Decision support systems, 43(2), 618-644.

[Lamport+1982] Lamport, L., Shostak, R., & Pease, M. (1982). *The Byzantine generals problem*. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3), 382-401.

[Liang+2017] Liang, X., Zhao, J., Shetty, S., and Li, D. (2017, October). *Towards data assurance and resilience in IoT using blockchain*. In *Military Communications Conference (MILCOM)*, MILCOM 2017-2017 IEEE (pp. 261-266). IEEE.

[Lundbæk+] Lundbæk, L. N., Beutel, D. J., Huth, M., & Kirk, L. (n. d.). *Practical Proof of Kernel Work & Distributed Adaptiveness*.

[Lundqvist+2017] Lundqvist, T., de Blanche, A., and Andersson, H. R. H. (2017, June). *Thing-to-thing electricity micro payments using blockchain technology.* In *Global Internet of Things Summit (GIoTS)*, 2017 (pp. 1-6). IEEE.

[Mattern+2010] Mattern, F., and Floerkemeier, C. (2010). *From the Internet of Computers to the Internet of Things*. In *From active data management to event-based systems and more* (pp. 242-259). Springer, Berlin, Heidelberg.

[Melnik+2002] Melnik, M. I., and Alm, J. (2002). *Does a seller's ecommerce reputation matter? Evidence from eBay auctions*. The journal of industrial economics, 50(3), 337-349.

[MetaMask] MetaMask (n. d.). *Metamask*. Retrieved April 5, 2018, from https://metamask.io/

[Minerva+2015] Minerva, R., Biru, A., and Rotondi, D. (2015). *Towards a definition of the Internet of Things (IoT)*. IEEE Internet Initiative, 1.

[Murarka+2017] Murarka, N., and Bains, P. (2017, October 1). *Bluzelle*. Technical Paper. Release 1.0.

[Nakamoto2008] Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

[Natarajan+2017] Natarajan, H., Krause, S., and Gradstein, H. (2017). *Distributed Ledger Technology (DLT) and Blockchain*. World Bank Group.

[Nebulous] Nebulous Inc. (n. d.). *Cloud storage is about to change. Are you ready?* Retrieved April 6, 2018, https://sia.tech/

[Node.js] Node.js Foundation (n. d.). *About Node.js*. Retrieved April 5, 2018, https://nodejs.org/en/about/

[Poon+2016] Poon, J., and Dryja, T. (2016). *The Bitcoin lightning network: Scalable off-chain instant payments*. Draft version 0.5, 9, 14.

[Poon+2017] Poon, J., and Buterin, V. (2017). *Plasma: Scalable Autonomous Smart Contracts*. White paper.

[Popov2016] Popov, S. (2016). *The Tangle*. cit. on, 131.

[Pureswaran+2015a] Pureswaran, V., and Brody, P. (2015). *Device democracy*. IBM Institute for Business Value.

[Pureswaran+2015b] Pureswaran, V., Panikkar, S., Nair, S., and Brody, P. (2015). *Empowering the edge-practical insights on a decentralized internet of things. Empowering the Edge-Practical Insights on a Decentralized Internet of Things*. IBM Institute for Business Value, 17.

[Schulz2015] Schulz, M. (2015, June 11). *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. PDF, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

[Shrier+2016] Shrier, D., Wu, W., and Pentland, A. (2016). *Blockchain & infrastructure (identity, data security) part 3*. Massachusetts Institute of Technology.

[Slock.it] Slock.it GmbH (n.d.). *The USN*. Retrieved April 4, 2018, from https://slock.it/usn.html

[Sun+2016] Sun, J., Yan, J., and Zhang, K. Z. (2016). *Blockchain-based sharing services: What blockchain technology can contribute to smart cities*. Financial Innovation, 2(1), 26.

[Sytel_Reply] Sytel Reply (n.d.). *Securechain*.

[Venture_Proxy] Venture Proxy Ltd. (n.d.). *Blockchain Based Anti-Counterfeit Solution*. Retrieved April 4, 2018, from http://blockverify.io/

[YliHuumo+2016] Yli-Huumo, J., Ko, D., Choi, S., Park, S., and Smolander, K. (2016). *Where is current research on blockchain technology? — a systematic review*. PloS one, 11(10), e0163477.

[Zyskind+2015] Zyskind, G., and Nathan, O. (2015, May). *Decentralizing privacy: Using blockchain to protect personal data*. In *Security and Privacy Workshops (SPW),* 2015 IEEE (pp. 180-184). IEEE.

Acknowledgments

It has been a long journey until this document came to existence. Only due to the support, love and generosity of many, I made it that far. Much appreciation goes to my academic advisor Prof. Jong Kim for his kindness and excellent supervision. Further, I'm highly grateful for Prof. Chanik Park and Prof. Hanjun Kim who supported me as thesis committee members.

Thanks to Prof. James Won-Ki Hong, I got accepted at POSTECH University and discovered that I'm of more capable than I believed (both mentally and physically). The DPNM lab members (Jong-Hwan Hyun, Do-Young Lee, Se-Yeon Jeong, June-Muk Choi, Kyung-Chan Ko, Ji-Bum Hong, Heegon Kim, Tu Van Nguyen, Chae-Hyeon Lee, Taeyeol Jeong, Dong-Ho Son) did me so many favors, such as helping me moving to my apartment, explaining me contents, making inquiries for me in Korean and giving me a wonderful early birthday surprise.

All the courses that I have taken at POSTECH helped me to broaden my knowledge and improve my technical and academic skills. I'm grateful that I had the chance to learn from highly knowledgeable mentors who challenged me countless times:

Prof. Heecheon You (Biomechanics)

Prof. Pil Joong Lee (Information and Communications Security)

Prof. Young Joo Suh (Wireless Mobile Networks)

Prof. Jong Kim (Computer Security)

Prof. Kyungmin Bae (Software Engineering)

Prof. Jong-Hyeok Lee (Information Retrieval)

Prof. Derek Jon Lactin (IT Scientific Writing)

Special thanks go to Oscar Montes, Prof. Minsung Kim, Prof. Jin-Soo Lee and the Smart Control and Power Systems Lab for accommodating me in their facilities and treating me with greatest friendliness.

Dmitrii Kuvaiskii and Simon Ostendorff gave me helpful feedback on my research. I enjoyed all the enlightening discussions that I had with them and other fellow students. Daniela Dongheun Lee did a wonderful job in helping me with the Korean summary of this thesis.

Receiving a scholarship to study in Korea required much preparation and effort. Words cannot express my gratitude for the trust that my former undergraduate professors Prof. Dr. Gabriele Schäfer and Prof. Dr.-Ing. Carsten Lanquillon showed me by recommending me for the Global Korea Scholarship and as Master candidate at POSTECH University.

Although not physically present, without my friends and family back home in Germany, I would not have been as motivated and energetic as I always tried to be. Knowing that there are people who will always welcome you and take care of you is priceless for me. My mother and father, my sister Fabia, my brother Nino, Uwe, Gaby and all other family members showed me so much love that thinking of them always warms my heart. In this context, I also want to mention Paul Lajer, my incredible manager at CGI. Despite his busy schedule, he has taken time to support me with my studies and given me valuable inspiration for my course work and thesis research.

I could always rely on support from Minah Shin, Dr. Sung of the Counseling Center, the members of ISSS as well as the university and department staff. I felt deeply honored to be a recipient of the Global Korea Scholarship. I sincerely want to thank the Korean government for funding foreign students like me and giving them a chance to experience Korea. The kindness of all the people in my daily life during my period in South Korea was just overwhelming. I will always happily remember Korea and its culture. These memories now own a special place in my heart and fill me with bliss.

Vanesco A. J. Boehm

Curriculum Vitae

Name: Vanesco A. J. Boehm

Education

2009.09 – 2013.08 B.S. in Business Informatics, Heilbronn University, Germany

2016.09 – 2018.08 M.S. in High Performance Computing Lab, Department of Computer Science and Engineering, Pohang University of Science and Technology

Experience

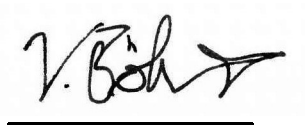
2012.03 – 2013.07 Web Developer at SAP AG, Head Office, Walldorf, Germany

2013.08 – 2015.08 IT Consultant for Java and Web Technologies at CGI Germany

I hereby grant Pohang University of Science and Technology (POSTECH) the right to make use of my thesis for scholarly and educational purposes.

Pohang, Korea

2018.06.12



Vanesco A. J. Boehm