TALLINN UNIVERSITY OF TECHNOLOGY

Faculty of Information Technology

Department of Computer Science

Centre for Digital Forensics & Cyber Security

Jan Johan Karst & Guillaume Brodar

CONNECTING MULTIPLE DEVICES WITH BLOCKCHAIN IN THE INTERNET OF THINGS

Research paper for "Seminar on Blockchain Technology (MTAT.03.323)"

Tallinn/Tartu 2017

We declare that we have written this paper independently. All works and major viewpoints of other authors, data from other sources of literature and elsewhere have been referenced.

Jan Johan Karst
Student code: 157383IVCM
Student e-mail: johnkarst@hotmail.com

and

Guillaume Brodar
Student code: 156342IVCM
Student e-mail: gbrodar@gmail.com

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	Meaning
HIS	Hardware Intrinsic Security
IERC	IoT European Research Cluster
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IoT	Internet of Things
KSI	Keyless Signature Initiative
PKI	Public Key Infrastructure
PUF	Physically Unclonable Functions

Table 1: Acronyms and Abbreviations

GLOSSARY OF TERMS

Term	Definition
Blockchain	A distributed database that maintains a continuously-growing list of ordered records called *blocks*. Each block contains a timestamp and a link to a previous block. By design blockchains are inherently resistant to modification of the data — once recorded, the data in a block cannot be altered retroactively. Blockchains are secure by design and an example of a distributed computing system with high byzantine fault tolerance. Decentralised consensus can therefore be achieved with a blockchain. This makes blockchains suitable for the recording of events, title, medical records and other records management activities, identity management, transaction processing and proving provenance. This offers the potential of mass disintermediation and vast repercussions for how global trade is conducted.
Hardware Intrinsic Security (HIS)	Intrinsic-ID's core PUF security technology is called Hardware Intrinsic Security (HIS). It is a secure and robust approach to embedding Physical Unclonable Functions (PUF) in integrated circuits.
Keyless Signature Initiative (KSI)	Keyless Signature Infrastructure (KSI) is designed to provide scalable digital signature based authentication for electronic data, machines and humans.

	Unlike traditional approaches that depend on asymmetric key cryptography, KSI uses only hash-function cryptography, allowing verification to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain. A blockchain is a distributed public ledger; a database of transactions such that there is a set of pre-defined rules as to how the ledger gets appended, achieved by distributed consensus of participants in the system. The KSI blockchain overcomes three major weaknesses of mainstream blockchain technologies - which were designed to facilitate asset transactions - making KSI suitable also for cybersecurity and data governance applications: 1. Scalability: One of the most significant challenges with traditional blockchain approaches is scalability – they scale at O(n) scale complexity, meaning they grow linearly with the number of transactions. In contrast the KSI blockchain scales at O(t) space complexity – it grows linearly with time and independently from the number of transactions. KSI can sustain billions of asset registration events every second without growing out of control. 2. Settlement time: In contrast to the widely distributed crypto-currency approach, the number of participants in KSI blockchain distributed consensus protocol is limited. By limiting the number of participants, it becomes possible to achieve consensus synchronously, eliminating the need for Proof of Work and ensuring settlement can occur within one second. 3. Formal security proof: Unlike other blockchains, KSI blockchain has been subjected to end-to-end formal mathematical proof that provides assurance that the protocol does precisely what it says it does.
Physically Unclonable Functions (PUF)	An invention by Intrinsic-ID. Silicon PUFs or Silicon Physically Unclonable Functions use random patterns to differentiate chips from each other. Physically unclonable functions also enable you to extract a unique identifier for the chip and to create a unique cryptographic key. PUF is build on the core security technology Hardware Intrinsic Security (HIS).

Table 2: Glossary of Terms

Introduction

The scope of this research paper is “Connecting multiple devices with blockchain in the Internet of Things (IoT)”, and it intends to give a literature overview. Please be aware that this survey paper in no way is intended to be an extensive/complete overview of blockchain as an enabling technology for the IoT. The authors have selected a couple of interesting applications of blockchain in the IoT, and dive into these applications in more detail. The following four questions will be answered in the next chapters for these selected applications of blockchain in the IoT:

1. Chapter 1: “Identification of entities applying blockchain in the Internet of Things”.
   This chapter will give an overview of a selection of interesting entities (companies / startups / initiatives / projects) in the business/scientific world that apply blockchain on the IoT. The selection is made by the authors of this paper based on interesting applications of blockchain technology in the IoT;
2. Chapter 2: “How do those entities aim to disrupt the industry?”
   Here we will elaborate how each company/startup/initiative/project identified in chapter 1 is aiming to disrupt the industry. We will describe in more detail each application of blockchain in the IoT;
3. Chapter 3: “Comparison and analysis of blockchain applications”.
   We will focus on the comparison and analysis of the entities (companies / startups / initiatives / projects) of the intended application of blockchain technology. We find similarities, differences, advantages and disadvantages of the IoT blockchain application for each entity selected in chapter 1;
4. Chapter “Conclusions and thoughts”.
   This final chapter describes the conclusions and thoughts about the degree of hype, and what components might be valuable and most likely become reality in a few years.

1 Identification of entities applying blockchain in the Internet of Things

This chapter will give an overview of a selection of interesting entities (companies / startups / initiatives / projects) in the business/scientific world that apply blockchain on the IoT. The selection is made by the authors of this paper based on interesting applications of blockchain technology in the IoT. See Figure 1: The Internet of Things (IoT) Integration and 6A Connectivity (IERC n.d.) for two representations of the IoT.

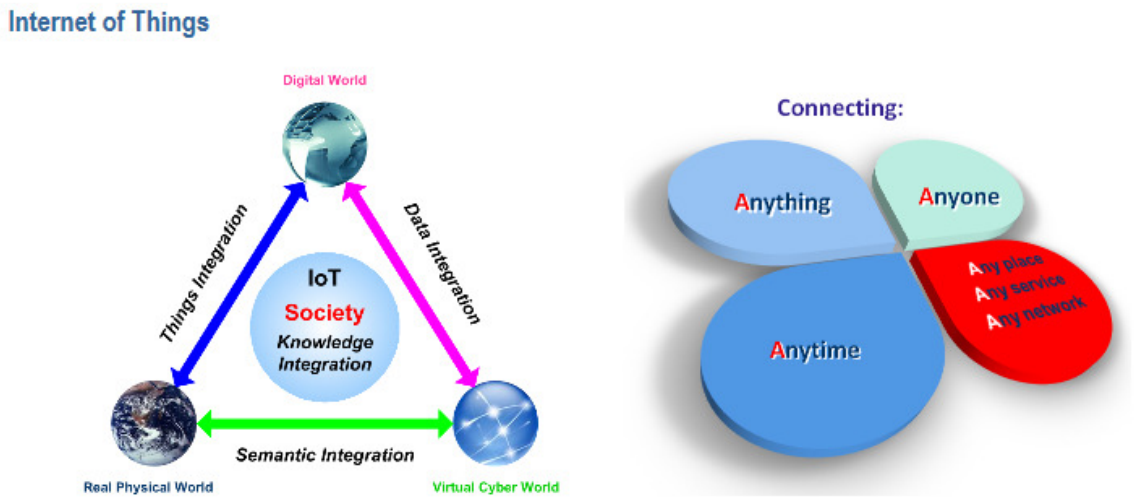

Figure 1: The Internet of Things (IoT) Integration and 6A Connectivity (IERC n.d.)

1.1 Entities: IBM and Samsung ➔ ADEPT project

The IoT is a network of devices that can communicate with each other over the internet. When those devices can also configure and maintain themselves we refer to them as smart devices/smart objects. Examples of smart objects can be e.g. a smart fridge, a smart thermostat, or even a smart washer.

IBM is building a blockchain powered technology dubbed *ADEPT* [2] [3] in collaboration with Samsung, based on the Ethereum protocol, to support this network of devices interacting

with each other through smart contracts. They give this example of how IoT can be utilised:

> *"We demonstrate how, using ADEPT, a humble washer can become a semi-autonomous device capable of managing its own consumables supply, performing self-service and maintenance, and even negotiating with other peer devices both in the home and outside to optimize its environment." [2]*

1.2 Entities: Guardtime and Intrinsic-ID ➔ Alliance on IoT Blockchain

Guardtime and Intrinsic-ID have formed an alliance on IoT Blockchain [10] bringing their security technologies KSI [8] and PUF [9] together. This way they are able to deliver customer solutions combining Intrinsic-ID's SRAM Physical Unclonable Functions (PUFs) and Guardtime's Keyless Signature Infrastructure (KSI) Blockchain technology, providing a new level of security and governance for the Internet of Things [10].

Intrinsic-ID and PUF

"Intrinsic-ID is the world leading embedded authentication company based on the unique and patented technology called SRAM Physical Unclonable Function or SRAM PUF. Its solutions and products create a unique ID and cryptographically secure keys from the physical behavior of the SRAM PUF. This key is invisible to attackers, unique per device and can be leveraged to authenticate the chip, the data on the chip, the device and even the whole system. On top of this, Intrinsic-ID offers solutions to protect the supply chain. These range from tracking and monitoring chips and devices (even in the case of remote contract manufacturers) to low cost, simplified key provisioning and protection against counterfeiting and overbuilding. Due to its simplicity, these products can be applied to all modern chips, microcontrollers and CPUs without making a change to the hardware. Currently this technology is being used by its customers in the field to protect the most sensitive payment, content, connectivity, sensor and government data and systems." [10]

Guardtime and KSI

"Guardtime is the first and only platform for ensuring the integrity of data and systems at industrial scale. Guardtime created Keyless Signature Infrastructure (KSI) to take on the challenges of today's perimeter-based security systems and secure the integrity of data in

today's increasingly digital world. Built on an industrial Blockchain, KSI signs any and all data across a system, allowing independent verification of time, integrity and identity for any moment in history. Guardtime's mission is to build the essential backbone for truth, assurance and integrity for our digital world." [10]

1.3 Entities: Slock.it and RWE ➔ BlockCharge

Slock.it is a startup company founded in 2015 based in Mittweida, Germany and pushes the idea of "Rent, share or sell anything without middlemen". From a general perspective, Slock.it seesm to position itself as a blockchain enabler and has been able to establish partnerships with several major companies such as Samsung, Microsoft, RWE, etcetera.

RWE is a major German energy company that counts more than 30 million customers and addresses retail as well as business markets.

Slock.it and RWE have partnered together to address the specific use-case of electric vehicle charging stations under the BlockCharge project. The aim of BlockCharge is to use the Ethereum public blockchain and smart contracts as a supporting infrastructure between electricity providers and end-users.

From an end-user perspective, this partnership provides the possibility to rent charging stations via the use of a mobile application and independently of the underlying energy provider or physical infrastructure operators. On the other end, those providers and operators would benefit from the decentralized nature of a blockchain-based billing system that frees them from deploying specific and centralized systems as we know them today.

RWE has identified a wide-range of customer segments such as city governments, utility companies, automotive OEMs, SMEs, etcetera, that could benefit from this integration effort and ongoing projects are being led with the city of Berlin.

1.4 Entity: Chronicled.com

Chronicled.com is a startup company based in San Francisco and incorporated in 2015. They claim that their expertise is in “developing software at the intersection of blockchain technology, IoT, and user engagement” and are specifically tackling the problems of identity and authenticity for brands and consumers.

Their narrative is built around the fact that counterfeit products are a major issue on both side of the consumer spectrum and that current protection mechanisms such as barcodes, QR codes and other seals of authenticity can be easily forged.

Their product proposition is based along the following elements:

- A set of BLE and NFC chips used to “register” on the Ethereum blockchain;
- An open registry of registered products;
- A companion iOS and Android app that lets end-users check the status of their purchases.

Their target markets are luxury and fashion brands for which consumers pay a high premium for the uniqueness and degree of craft that is associated with the product.

Their open registry is based on the Ethereum blockchain and allows for further feature development by embedding smart contracts. Product registration is done by inserting their BLE or NFC chips’ (called Identity Inlay and CryptoSeal) public key on the Ethereum blockchain.

Consumers and brands thus benefit from the tamper-proof feature of the blockchain to certify the authenticity of their goods.

1.5 Other interesting entities not further discussed in the next chapters

In the paragraphs above we have shown just a few very interesting entities applications of blockchain in the IoT (taking more entities would create a survey and resulting report that would become too large). However, there are more applications of blockchain in the IoT. The following table lists some of these applications, and we mention them without extensively discussing them or comparing them here or in the next chapters:

Company	Blockchain Application Description
21Inc	"21 Inc is a company specializing in embedded computer hardware with native support for cryptocurrency transactions. After raising $121 million of venture capital last year, 21 Inc has launched a developer version of the **21 Bitcoin Computer** – a portable cryptocurrency micropayment server with an integrated mining chip. The device has native protocol support for various cryptocurrency-related functions, so that by simply adding one line of code into its computer program, the device can, for example, be told to execute a cryptocurrency payment, or to wait until a payment is made to its account before continuing its program. The company's vision is to eventually incorporate a mining chip into every digital device, so that cryptocurrency mining capacity would ultimately constitute one fundamental system resource in computers alongside the CPU performance, amount of bandwidth, memory capacity, and hard disk space. With each device's stock of cryptocurrency constantly replenishing through the process of embedded mining, digital value transactions could be conveniently automated between devices by writing them directly into the computer program of virtually any device. In essence, 21 Inc's concept would allow for IoT devices to transact directly amongst themselves, without the need for any centralized background architecture. While enabling cost-savings and increased network robustness, the 21 Bitcoin Computer could in time also allow devices to autonomously exchange other resources than mere data, such as computing power, bandwidth, storage space, or even electricity, thus bringing us one step closer to the feasibility of IoT." [6]
Filament	"The company brought up a sensor device ***TAP*** which enables the deployment of a secure, all-range wireless network in seconds. The device can directly communicate to another TAP device at up to 10 miles, and can connect directly to a phone, tablet, or computer. The company is extending operations on its blockchain-based Technology Stack. Blockchain technology allows Filament devices to transact and enable smart contracts ensuring the trust in transactions independently." [7]
Ken Code	"**ePlug** is a Ken Code product. According to a white paper by Ken Code**, '***ePlug is a tiny circuit board that resides inside "ePlug-certified" electrical outlets and light switches*'. The product has a wide expanse of options for Meshnet, distributed computing, end-to-

	end data encryption, dead zone-free Wi-Fi, timer, USB ports, temperature, touch, light and motion sensors for safety and security, and LEDs for notifications and night lighting. The product uses blockchain-based login to ensure security. Upon entering the correct Internet address/URL, the ePlug owner will be presented with a login screen. Initially, blockchain platforms such as OneName.io and KeyBase.io will be used for ID authentication and access to the ePlug." [7]
Tilepay	"The company has successfully designed a micropayments platform. **Tilepay** is a decentralized payment system based on the bitcoin blockchain. It can be downloaded to a user's personal computer, laptop or mobile phone. Every IoT device will have a unique authentication token that can accept payments via blockchain technology." [7]

2 How do those entities aim to disrupt the industry?

Here we will elaborate how each entity (company/startup/initiative/project) identified in chapter 1 is aiming to disrupt the industry. We will describe in more detail each application of blockchain in the IoT

2.1 Entities: IBM and Samsung ➔ ADEPT project

The ADEPT project initiated by IBM in cooperation with Samsung has delivered in January 2015 a proof of concept of a decentralized blockchain powered Internet of Things. ADEPT stands for Autonomous Decentralized Peer-to-Peer Telemetry [3]. ADEPT uses blockchain technology to build a distributed network of devices: a decentralized Internet of Things.

The goal of the ADEPT project is to decentralize the IoT in order to address typical IoT problems of cost, scalability, longevity, privacy and security. As typical IoT problems are addressed by ADEPT in a proof of concept that is open source, this project can be considered a truly good basis for future "blockchain for the IoT" developments. Therefore, this project can be called disruptive, as others might follow a realistic proof of concept based on open source.

ADEPT Architectural Key Components

The ADEPT architecture consists of 3 key components, called foundational components by IBM [3] [5]:

1. P2P (Peer to Peer) Encrypted Messaging:
   For this ADEPT uses an open source encrypted mesh protocol called TeleHash (www.telehash.org);
2. Distributed File Sharing:
   ADEPT uses the proven technology protocol BitTorrent (www.bittorent.com) for sharing of mainly larger files between devices;
3. Decentralized Programming Language for the Blockchain:
   In absence of a centralized controller there is a need for some mechanism for device communication & coordination and for this Ethereum (https://www.ethereum.org/) is

used. With Ethereum the devices get the ability to create binding contracts (smart contracts) between each other. This way devices can set their own roles, responsibilities and permissions, and perform fairly complex bartering / negotiating with other devices, which makes the devices almost completely autonomous [5].

The ADEPT system would serve as a ledger of existence for billions of IoT devices that would autonomously broadcast transactions (Ethereum smart contracts) between peers in a three-tier system architecture of peer devices. By using the blockchain protocol in combination with Ethereum, ADEPT could serve as a bridge between many IoT devices at low cost [2].

IBM and Samsung want to create IoT devices that are autonomously maintaining themselves. The devices can for example retrieve software updates themselves, and initiate the order or required device supplies for uninterrupted functioning. Also, devices can initiate themselves a request for the required periodic maintenance service [2].

ADEPT Use Cases

The following use cases [4] [5] are implemented by IBM and Samsung to proof the ADEPT concept:

B2C Use Cases:

1. A Samsung W9000 washing machine autonomously reordering detergent;
2. A Samsung W9000 washing machine autonomously reordering service parts;
3. A Samsung W9000 washing machine autonomously negotiating power usage.

B2B Use Case:

1. AdCast Solution Owner who has large format displays (LFDs) hosted at strategic locations, and who rents out Ad display space slots on these displays. Clients can access the display slots information, and request space(s) and upload the Ad. After the to be displayed Ad content is approved, the AdCast Owner will request payment. After payment received the Ad will be spread to requested the LFDs, and displayed there at the requested time slots.

Typical IoT Problems: solved/not solved by ADEPT?

- Decentralize the IoT: solved, by using a P2P network, and not using a centralized control infrastructure;
- Lowering the cost of the IoT: solved, by decentralizing the IoT;
- Scalability of the IoT: not solved, because the IoT will continue to grow to many billions of devices. See page 15 and 16 of [2] for full details on scalability issues regarding the messaging component, the file sharing component, and the blockchain component;
- Longevity of the IoT: solved, because the device is fully autonomous, and can update itself with new firmware. Therefore, the device can be used safely for a longer time. Update of firmware is made possible because of distributed file sharing with ADEPTs BitTorrent;
- Privacy of the IoT: solved, ADEPT uses the principle of privacy by design & default in a decentralized infrastructure. This means that the owner of the device decides with whom he/she wants to share his/her data, and that the owner decides to whom he/she wants to reveal his/her identity;
- Security of the IoT: solved, by removing the trusted party, and applying blockchain encryption for transaction processing, storage of data and transport of data. Using open source protocols also increases the transparency of what technology we use, which increases trust (a feeling of security). Furthermore, trust between peers will evolve the longer they cooperate without issues; this way a trust relationship can evolve from not-trusted, to semi-trusted, to trusted.

2.2 Entities: Guardtime and Intrinsic-ID ➔ Alliance on IoT Blockchain

According to Guardtime and Intrinsic-ID they will provide a new level of security and governance for the IoT, by combining their KSI and PUF technologies.

The number of networked automated devices on the IoT is growing at an alarming pace. Estimations are in the billions of devices on the IoT in the near future. However, technologies currently used to secure networks are still based on legacy security techniques such as Firewalls, PKI, IDS/IPS systems and anti-virus software. Therefore, it is time for applying

the latest technologies for security in the IoT. Both companies consider it time to stop **firefighting security breaches**, but to come up with truly innovative technologies to guarantee security in the IoT [10].

A combination of SRAM PUF technologies and KSI Blockchains provides highly scalable data integrity and authentication down to the chip level [10].

“Guardtime and Intrinsic-ID will conduct a series of pilots in order to showcase customer security solutions, leveraging Intrinsic-ID’s SRAM PUF-based key management system, and Guardtime’s KSI Blockchain.” [10] Which customer security solutions those will be is not announced. Mission assurance for defense customers as well as telecom operators rolling out smart city solutions in energy, health care and transportation, seem to have the initial focus of the alliance [10].

PUF Technology

“Intrinsic-ID’s core SRAM PUF security technology is the foundation for establishing the latest advancement in key management and key protection in integrated circuits. Due to deep-submicron manufacturing process variations, every transistor in an Integrated Circuit (IC) has slightly different physical properties. Since these process variations are uncontrollable during manufacturing, the physical properties of a device, its fingerprint, can neither be copied nor cloned. The electronic fingerprint is used to securely and reliably derive a device-unique cryptographic key and removes the need to store any sensitive key material in non-volatile memory (NVM). As SRAM is already present on nearly every microcontroller and CPU and requires no NVM, this solution is very scalable and flexible.” [10]

KSI blockchain

“Guardtime’s KSI Blockchain is an industrial grade Blockchain stack that has been underpinning governments since 2007. The Blockchain encompasses both a distributed ledger for managing ownership of digital assets as a well as a generator for cryptographic metadata that proves the properties of the underlying data without reliance on trusted third parties.” [10]

Combining PUFs and Blockchain for IoT Governance

“By using PUF Technology to uniquely authenticate a device and registering that device with

ownership information on a ledger, the provenance (place of origin) and integrity of every piece of data generated by that device can be cryptographically proven and linked back to an authenticated device with end to end chain of custody. This way the data integrity and authentication perimeter is extended all the way to the silicon chips where the data originates." [10]

Therefore, we can call this alliance truly disruptive for applying blockchain on the IoT industry. Hardware based security technology like PUF, can only be corrupted by stealing the SRAM chip from which the key is derived. As this is very unlikely, this hardware based security technology together with KSI Blockchain technology is very promising for security on the IoT.

2.3 Entities: Slock.it and RWE ➔ BlockCharge

There is an ongoing trend in the development of electric vehicles both for private use or on a leased-basis and lots of incentives are currently being pushed to move traditional vehicle usage to a more eco-friendly environment.

Several issues currently exist in this area and the BlockCharge concept is looking at disrupting the current market by bringing the following advantages:

- An enhanced user experience: the end-user benefits from a single mobile application that lets him use any charging station that is part of BlockCharge, independently of the infrastructure or energy provider;
- A simplified billing and leaner infrastructure for the energy providers: user authentication and billing functions are integrated in the Ethereum blockchain and thus reduces the need to deploy those features from a centralized location. As a side-effect it also enables them to easily share the same physical infrastructure to push their own services;
- Fraud-proof accounting: both from an end-user and provider/operator perspective, this compelling feature is embedded into the design principle of a public blockchain as is the case with the Ethereum one.

From a market perspective, the cost for new entrants is also dramatically reduced as they can quickly onboard new customers and/or contract with providers and operators simply with the use of APIs.

2.4 Entity: Chronicled.com

Chronicled aims at bridging the gap between trust that can exist between luxury goods companies and their customers.

From a technical perspective, the proposed solution is straight-forward as it makes a direct use of the tamper-proof features of the Ethereum blockchain: by embedding the public key of their smart tags on it, the identity of the corresponding chip is then guaranteed and secured.

Chronicled brings a unique blend of skills in its team with software engineers alongside with fashion designers and retail industry people. In that respect, the disruption that they are trying to bring has a lot more to do with the bridging together of competences from two very different industries.

As such, they are looking at getting the trust from their target customers by showing that their solution has been created for their industry by people from their industry.

3 Comparison and analysis of blockchain applications

We will focus on the comparison and analysis of the IoT blockchain applications. We find similarities, differences, advantages and disadvantages of the IoT blockchain application for each entity selected in chapter 1.

In the following table we make a comparison (similarities and differences) between the 4 IoT blockchain applications described in the chapters above:

	IBM/Samsung ➔ ADEPT	**Guardtime / Intrinsic-ID ➔ PUF/KSI**	**Slock.it/RWE ➔ BlockCharge**	**Chronicled.com**
IBM/Samsung ➔ ADEPT				
Guardtime / Intrinsic-ID ➔ PUF/KSI	• ADEPT uses Ehtereum, and Guardtime/Intrinsic-ID uses KSI blockchain.			
Slock.it/RWE ➔ BlockCharge	• Both use Ethereum.	• Ethereum vs. KSI Blockchain.		
Chronicled.com	• Both use Ethereum.	• Both use device identity based on chips; • Device identity used by both for supply chain solutions.	• End user Interface is for both a mobile app; • Both use Ethereum.	

In the following table we make an analysis (advantages and disadvantages) of the 4 IoT blockchain applications described in the chapters above:

	Advantages	**Disadvantages**
IBM/Samsung ➔ ADEPT	• Open-source framework, so adoption by the market will be easier; • Use proven technologies (BitTorrent, TeleHash, Ethereum);	• Because it is a proof-of-concept it still has several challenges to overcome (see page 15/16 of [2]);
Guardtime / Intrinsic-ID ➔ PUF/KSI	• PUF is very secure hardware based key extraction technology (extremely difficult to tamper with); • PUF is scalable because SRAM is commonly used; • KSI is extremely scalable blockchain technology; • KSI is mathematically proven security technology;	• Both companies have a market dominance with their technology, causing high prices for customers and therefore slower adaptation;
Slock.it/RWE ➔ BlockCharge	• Shares the same physical infrastructure across different electricity providers / operators; • Possibility of OEM (licensing) for a quicker market adoption;	• Not an open source solution;
Chronicled.com	• Addresses the issue of counterfeiting of luxury products; • Guarantees an authentic product to the end-user.	• The Identity Inlay tags are quite big to use on luxury products like brand clothing.

Conclusions and thoughts

This final chapter describes some general conclusions and thoughts about the degree of hype, and what components might be valuable and most likely become reality in a few years.

Based on all stated in the chapters above we can draw the following conclusions/thoughts:
As concluding remarks and thoughts, we can see that there is indeed a lot of traction on blockchain-based applications and business-models for the IoT: well-established technology companies like IBM and Samsung are actively developing projects and commercial applications, smaller outlets like Guardtime have also been able to emerge as technology leaders and startups like Slock.it have developed partnerships with major companies whose business was traditionally outside of that technological environment.

The biggest challenges that we can identify at this stage are the following:

- Migrating end-user payments from a traditional "cash or card" transaction to an Ethereum or blockchain-based wallet which might face a lack of adoption or resistance from the general public;
- Mitigating the volatility of the Ether price and other crypto tokens for the end-users who expect price stability in their asset management;
- Scalability and performance issues in the Ethereum and blockchain model in order to process transactions and contracts quickly enough to be accepted for end-users as well as operators/providers. The ever-increasing size of blockchains also raises open questions on their long-term storage in public ledgers.

There still is a lot of uncertainty and hype surrounding the blockchain industry, but there is a direction taken towards the adoption of decentralized systems that allow transactions to be done without a third-party ensuring the needs for mutual trust. This makes it that devices on the IoT can perform autonomous.

References

Reference	Description
1.	IERC, Image. Available: http://www.internet-of-things-research.eu/about_iot.htm [Jan. 5th 2017].
2.	S. Panikkar, et al. *"IBM ADEPT: An IoT Practitioner Perspective - Draft Copy for Advance Review"* [Online], 7th Jan. 2015. Available: https://ia802601.us.archive.org/4/items/pdfy-esMcC00dKmdo53-_/IBM%20ADEPT%20Practictioner%20Perspective%20-%20Pre%20Publication%20Draft%20-%207%20Jan%202015.pdf [Jan. 5th 2017].
3.	IBM., "*Empowering the edge, Practical insights on a decentralized Internet of Things"* [Online], April 2015. Available: https://www-935.ibm.com/services/multimedia/GBE03662USEN.pdf [Jan. 5th 2017].
4.	IBM, "*Empowering the Edge - Use case abstract for the ADEPT proof-of-concept",* April 2015. Available: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03666USEN [Jan. 5th 2017].
5.	TheProtocol.TV. (2015, Feb. 3th). *IBM & Samsung live demo of ADEPT* [Online]. Available: https://www.youtube.com/watch?v=U1XOPIqyP7A [Jan. 5th 2017].
6.	Juri Matilla, "*The Blockchain Phenomenon, The Disruptive Potential of Distributed Consensus Architectures",* Berkeley Roundtable on the International Economy (BRIE), University of California, Berkeley [Online], Jan. 2016. Available: http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf [Jan. 5th 2017].
7.	Hitesh Malviya, "*How Blockchain Will Defend IoT"* [Online], 10th Dec. 2016. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2883711 [Jan. 5th 2017].
8.	Guardtime (2017, Jan. 05). *KSI Blockchain Technology* [Online]. Available: https://guardtime.com/technology/ksi-technology [Jan. 5th 2017].
9.	Intrinsic-ID. (2017, Jan. 05). *Intrinsic-ID Physical Unclonable Functions Technology* [Online]. Available: https://www.intrinsic-id.com/physical-unclonable-functions/ [Jan. 5th 2017].
10.	Intrinsic-ID. (2017, Jan. 05). *Intrinsic-ID and Guardtime Announce Alliance on IoT Blockchain* [Online]. Available: https://www.intrinsic-id.com/intrinsic-id-guardtime-announce-alliance-iot-blockchain/ [Jan. 5th 2017].

Table 3: References