

# Contents

<b>1</b>	<b>Title of My Seminar Work</b>	<b>3</b>
	<i>My Name</i>	
<b>2</b>	<b>Investigating the Blockchain Technology in the Context of Cybersecurity</b>	<b>9</b>
	<i>Lenz, Roland, Pascal, Silas</i>	



# Chapter 1

## Title of My Seminar Work

*My Name*

*This is the abstract. It fits pretty much on one page and is definitely not longer.*

**Contents**

---

<b>1.1</b>	<b>This is My First Section . . . . .</b>	<b>5</b>
<b>1.2</b>	<b>Report Structure . . . . .</b>	<b>5</b>
<b>1.3</b>	<b>Pictures and Tables . . . . .</b>	<b>6</b>
<b>1.4</b>	<b>Bibliography . . . . .</b>	<b>7</b>
<b>1.5</b>	<b>Compiling . . . . .</b>	<b>7</b>

---

## 1.1 This is My First Section

You only apply changes to the folder with your respective talk number. This means that if your talk has number **X** you place all your files, e.g., pictures, **exclusively** in folder **TalkX**. The (main) text of your seminar work goes in **Seminar-Arbeit.tex** in that folder. Please use file **Example.tex** as a basis. Formatting, page settings, and the file **talk.tex** must not be changed.

Do not – under no circumstances – change the file **talk.tex**. If it is impossible to avoid the use of further packages (or modify the preamble in any other way) you may apply these modifications to **TalkX/MyHeader.tex**. However, in this case it is important to consult your advisor beforehand, as **L<sup>A</sup>T<sub>E</sub>X** does not contain namespaces, which may result in conflicts between different packages.

## 1.2 Report Structure

Your seminar report is contained in a chapter (**\chapter**), wherefore you may use commands **\section{}**, **\subsection{}**, and **\subsubsection{}** to structure it.

In general, breaks need to be separated by an empty line but not **\\** or **\newline**. Please do not use **\newpage**, **\clearpage** etc.

Enumerations with and without numbers can be generated by use of the following commands:

```
\begin{enumerate}
  \item ...
  \item ...
\end{enumerate}

\begin{itemize}
  \item ...
  \item ...
\end{itemize}
```

For descriptions, the following command is suited:

```
\begin{description}
  \item[Term] Description
  \item[Term] Description
\end{description}
```

## 1.3 Pictures and Tables

Please embed **all** pictures without suffix and save the respective picture as `.jpg` or `.pdf` in folder `TalkX`. To embed pictures the following command can be used:

```
\begin{figure}[ht]
  \begin{center}
    \includegraphics[scale=0.6]{TalkX/filename}
  \end{center}
  \caption{Caption}
  \label{label}
\end{figure}
```



Figure 1.1: Caption

Do always use relative paths to embed pictures! To scale pictures you can also use `[width=4cm]` or `[width=0.6\textwidth]` instead of `[scale=0.6]`. All pictures to be included in the seminar work need to be generated with a resolution of at least 600dpi.

Table 1.1: Caption

	A	B	C
X	1	2	3
Y	4	5	6
Z	7	8	9

Table 1.1 can be generated by the following command.

```
\begin{table}
  \caption{Caption}
  \label{tab:label}
  \begin{center}
    \begin{tabular}{|c|c|c|c|} \hline
      & A & B & C \\ \hline
      X & 1 & 2 & 3 \\ \hline
      Y & 4 & 5 & 6 \\ \hline
      Z & 7 & 8 & 9 \\ \hline
    \end{tabular}
  \end{center}
\end{table}
```

Pictures and tables need to have a caption (`\caption`) and be referenced from within the running text by use of `\ref{label}`. In general, `caption` has to appear below pictures, but above tables!

## 1.4 Bibliography

The bibliography is placed at the end of your chapter. **Do not use marks on your bibitems** as the automatically generated marks [1],[2],... are used. For each reference the informations authors, title, publisher, and release date must be stated in the following form:

```
\bibitem {label} N. Author: Title of the document; Type of document
    (technical report, deliverable, Workshop/Conference Name ...),
    (Location, Vol. X, No. Y), Month, Year, pages, URL (if available).
```

```
\bibitem {label} Website title; \url{Website URL}, Month, Year of last visit.
```

If the reference uses an URL the latter must be given by `\url{http://...}`.

In running text, bibitems are referenced by the use of `\cite{label}`. For all papers, pictures and other works references need to appear at the according position.

A detailed instruction to the correct use of references can be found in *Guideline to Written Seminar Works* [1].

## 1.5 Compiling

L<sup>A</sup>T<sub>E</sub>X is included in all popular Linux distributions. Under Linux, the document is compiled by executing `pdflatex talk.tex` in the main directory, which generates `talk.pdf`.

For Windows, the T<sub>E</sub>X implementation MiKTeX (<http://www.miktex.org/>) in combination with the L<sup>A</sup>T<sub>E</sub>X tool TeXnicCenter (<http://www.toolscenter.org/>) is recommended. For Mac OS X, the T<sub>E</sub>X implementation MacTeX (<http://tug.org/mactex/>) in combination with the L<sup>A</sup>T<sub>E</sub>X tool TeXShop (<http://pages.uoregon.edu/koch/texshop/>) is recommended.

Problems, proposals, and questions regarding the generation of your document can be sent by email to your supervisor. To submit your seminar talk compress (zip oder tar) the directory `TalkX` and mail it to your supervisor.

# Bibliography

- [1] Martin Waldburger, Patrick Poullie, Burkhard Stiller: *Guideline for Seminar Reports*, Communication Systems Group, Department of Informat-ics, University of Zurich, January 2013. <http://www.csg.uzh.ch/teaching/guideline-seminar-report-v05.pdf>.



## Chapter 2

# Investigating the Blockchain Technology in the Context of Cybersecurity

*Lenz, Roland, Pascal, Silas*

*This is the abstract. It fits pretty much on one page and is definitely not longer.*

## Contents

---

<b>2.1</b>	<b>Introduction . . . . .</b>	<b>11</b>
<b>2.2</b>	<b>Background . . . . .</b>	<b>12</b>
2.2.1	Cybersecurity . . . . .	12
2.2.2	Blockchain . . . . .	12
2.2.3	Smart Contracts . . . . .	13
<b>2.3</b>	<b>Related Work . . . . .</b>	<b>14</b>
2.3.1	Distributed Denial of Service (DDoS) . . . . .	14
2.3.2	Public Key Infrastructure (PKI) . . . . .	14
2.3.3	Internet Infrastructure (DNS / BGP) . . . . .	15
2.3.4	Internet of Things (IoT) . . . . .	15
2.3.5	Specific Applications . . . . .	15
<b>2.4</b>	<b>Final Considerations . . . . .</b>	<b>17</b>
2.4.1	Summary . . . . .	17
2.4.2	Discussion . . . . .	17
2.4.3	Outlook . . . . .	17
<b>2.5</b>	<b>Bibliography . . . . .</b>	<b>17</b>

---

## **2.1 Introduction**

- Length: around 2 pages
- Describe current issues in cybersecurity
  - Motivate the topic in general
  - TODO:
- Provide some reasoning on the evolution of bitcoin
  - Money transfer security
  - Intermediaries
  - TODO:
- Provide an outline of the paper
  - Content structure
  - Covered topics

## 2.2 Background

- provide an overview of the section structure and contents (filler)

### 2.2.1 Cybersecurity

- Length: 2-3 pages
- Definition of Cybersecurity
- Information security vs. Cyber security
- Authentication and Authorization
- Cryptography?
- Cost-Benefit Analysis, Risk Analysis
- Attack possibilities (Worms, Viruses, Trojan Horses, Bugs, Botnets)

### 2.2.2 Blockchain

- Length: around 2 pages
- Definition of Blockchain
- Technical Advantages and Disadvantages
- Reason for popularity
- Common Scenarios for usage
  - Crypto-Currencies
  - Supply Chain Management (SCM)
  - Payment and Money Transactions
  - Smart Contracts
  - Decentralized Autonomous Organizations (DAO)
  - Proof of Ownership
  - E-Voting
  - IoT

### **2.2.3 Smart Contracts**

- Length: around 2 pages
- TODO:
- shortly summarize the section
- introduce the upcoming content (filler)

## 2.3 Related Work

### 2.3.1 Distributed Denial of Service (DDoS)

- Length: 3-4 pages
- What is DDoS?
  - Differences DoS and DDoS
- General Introduction about possibility of DDoS attacks
- Mitigation Possibilities
  - DDos Mitigation with Smart Contracts
  - Mitigation-as-a-service
  - Blockchain Signaling System (BloSS)

### 2.3.2 Public Key Infrastructure (PKI)

**Length: around 3 pages**

- Introduce PKI and provide an intuition for existing PKI systems and their challenges
- Motivate the role of PKI for cybersecurity (foundational principle)
- Present threats and vulnerabilities that are common and specific to PKI

#### 2.3.2.1 Decentralized PKI

- Provide an intuition on why centralization could lead to cybersecurity problems
- Present different approaches to the decentralization of PKI based on blockchain technologies and describe how trust and security can be achieved in such a decentralized system
- Discuss improvements to verification by the application of rich credentials on a blockchain PKI as a concrete application example

#### 2.3.2.2 Blockchain approaches to web certification

- Discuss the potential of web certification using Ethereum smart contracts
- Shortly elaborate on certificate and revocation transparency in general, as well as an approach based on blockchain

### **2.3.2.3 Keyless Signature Infrastructure (KSI) with blockchain**

- Shortly introduce KSI and its significance in a PKI context
- Show how KSI could be enhanced by the application of blockchain technologies

### **2.3.3 Internet Infrastructure (DNS / BGP)**

**Length: around 2 pages**

- Provide a short overview of the internet infrastructure with DNS/BGP, corresponding threats, and security mechanisms

#### **2.3.3.1 Decentralized DNS**

- Describe how blockchain-based DNS systems implement and enhance traditional DNS protocols
- Describe how domain management could work in such a distributed setting (i.e., if there are no central parties)
- Discuss security benefits of decentralizing DNS with blockchain when compared to traditional approaches

#### **2.3.3.2 BGP**

- Short excursion on how BGP could be implemented on a blockchain basis
- Discuss the benefits and big challenges of applying the blockchain to low-level internet infrastructure like BGP (scalability, performance, etc.)

### **2.3.4 Internet of Things (IoT)**

- Length: 2-3 pages
- TODO:

### **2.3.5 Specific Applications**

- Length: 3-4 pages
- Applications that are related on a second level
- Not a direct implication for CS measures

- Instead, BC helps to secure the security of a system Different classes of applications:
- Applications related to the fields of evaluated according to the following criteria:
  - Quality of the System: Advantages and Disadvantages
  - Is there an absolute need for BC or could this problem be solved without?
  - Relation to Cybersecurity and Security of related systems
- The following sections are to be explored further
  - E-Voting [?] [?]
  - Autonomous Vehicles [?] [?]
  - Personal Data Protection [?]
  - Personal Data Sharing and Patient Monitoring [?]
  - Smart Cities and IoT [?]
  - Communication [?]
  - Power Transaction
  - Data Exchange



## **2.4 Final Considerations**

- provide an overview of the section structure and contents (filler)

### **2.4.1 Summary**

- Length: around 1 page
- shortly summarize the overall work
- show the main thesis

### **2.4.2 Discussion**

- Length: around 1 page
- discuss any open questions about the contents

### **2.4.3 Outlook**

- Length: around 1 page
- describe possible topics of further research

## **2.5 Bibliography**



