

# Simulation of different selfish mining strategies in Bitcoin

Simulation respecting network topology and reference implementation

DIPLOMARBEIT

zur Erlangung des akademischen Grades

**Diplom-Ingenieur**

im Rahmen des Studiums

**Software Engineering & Internet Computing**

eingereicht von

**Simon Mulser, BSc**

Matrikelnummer 01027478

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Edgar Weippl, Privatdoz. Mag.rer.soc.oec. Dipl.-Ing. Dr.techn.

Mitwirkung: Aljosha Judmayer, Univ.Lektor Dipl.-Ing.

Wien, 13. Oktober 2017

---

Simon Mulser

---

Edgar Weippl



# Simulation of different selfish mining strategies in Bitcoin

## Simulation respecting network topology and reference implementation

### DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

### Diplom-Ingenieur

in

### Software Engineering & Internet Computing

by

**Simon Mulser, BSc**

Registration Number 01027478

to the Faculty of Informatics

at the TU Wien

Advisor: Edgar Weippl, Privatdoz. Mag.rer.soc.oec. Dipl.-Ing. Dr.techn.

Assistance: Aljosha Judmayer, Univ.Lektor Dipl.-Ing.

Vienna, 13<sup>th</sup> October, 2017

---

Simon Mulser

---

Edgar Weippl



# Erklärung zur Verfassung der Arbeit

Simon Mulser, BSc  
Dadlergasse 18/1/7, 1150 Wien

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 13. Oktober 2017

---

Simon Mulser



# Danksagung

Meine Danksagung. Coming soon...





# Acknowledgements

My acks. Coming soon...



# Kurzfassung

Meine Kurzfassung. Coming soon...



# Abstract

My abstract. Coming soon...



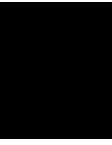
# Contents

<b>Kurzfassung</b>	<b>xi</b>
<b>Abstract</b>	<b>xiii</b>
<b>Contents</b>	<b>xv</b>
<b>1 Introduction</b>	<b>1</b>
<b>2 Additional Chapter</b>	<b>3</b>
<b>3 Introduction to L<sup>A</sup>T<sub>E</sub>X</b>	<b>5</b>
3.1 Installation . . . . .	5
3.2 Editors . . . . .	5
3.3 Compilation . . . . .	6
3.4 Basic Functionality . . . . .	7
3.5 Bibliography . . . . .	8
3.6 Table of Contents . . . . .	9
3.7 Acronyms / Glossary / Index . . . . .	9
3.8 Tips . . . . .	9
3.9 Resources . . . . .	10
<b>List of Figures</b>	<b>13</b>
<b>List of Tables</b>	<b>15</b>
<b>List of Algorithms</b>	<b>17</b>





# CHAPTER 1



## Introduction

My introduction. Coming soon...



# CHAPTER 2

## Additional Chapter

Enter your text here.



# Introduction to L<sup>A</sup>T<sub>E</sub>X

Since L<sup>A</sup>T<sub>E</sub>X is widely used in academia and industry, there exists a plethora of freely accessible introductions to the language. Reading through the guide at <https://en.wikibooks.org/wiki/LaTeX> serves as a comprehensive overview for most of the functionality and is highly recommended before starting with a thesis in L<sup>A</sup>T<sub>E</sub>X.

## 3.1 Installation

A full L<sup>A</sup>T<sub>E</sub>X distribution consists of not only of the binaries that convert the source files to the typeset documents, but also of a wide range of packages and their documentation. Depending on the operating system, different implementations are available as shown in Table 3.1. **Due to the large amount of packages that are in everyday use and due to their high interdependence, it is paramount to keep the installed distribution up to date.** Otherwise, obscure errors and tedious debugging ensue.

## 3.2 Editors

A multitude of T<sub>E</sub>X editors are available differing in their editing models, their supported operating systems and their feature sets. A comprehensive overview of editors can

Distribution	Unix	Windows	MacOS
TeX Live	<b>yes</b>	yes	(yes)
MacTeX	no	no	<b>yes</b>
MikTeX	no	<b>yes</b>	no

Table 3.1: T<sub>E</sub>X/L<sup>A</sup>T<sub>E</sub>X distributions for different operating systems. Recommended choice in **bold**.

Description	
1	Scan for refs, toc/lof/lot/loa items and cites
2	Build the bibliography
3	Link refs and build the toc/lof/lot/loa
4	Link the bibliography
5	Build the glossary
6	Build the acronyms
7	Build the index
8	Link the glossary, acronyms, and the index
9	Link the bookmarks
Command	
1	<code>pdflatex.exe example</code>
2	<code>bibtex.exe example</code>
3	<code>pdflatex.exe example</code>
4	<code>pdflatex.exe example</code>
5	<code>makeindex.exe -t example.glg -s example.ist</code> <code>-o example.gls example.glo</code>
6	<code>makeindex.exe -t example.alg -s example.ist</code> <code>-o example.acr example.acn</code>
7	<code>makeindex.exe -t example.ilg -o example.ind example.idx</code>
8	<code>pdflatex.exe example</code>
9	<code>pdflatex.exe example</code>

Table 3.2: Compilation steps for this document. The following abbreviations were used: table of contents (toc), list of figures (lof), list of tables (lot), list of algorithms (loa).

be found at the Wikipedia page [https://en.wikipedia.org/wiki/Comparison\\_of\\_TeX\\_editors](https://en.wikipedia.org/wiki/Comparison_of_TeX_editors). TeXstudio (<http://texstudio.sourceforge.net/>) is recommended. Most editors support the scrolling the typeset preview document to a location in the source document by `Ctrl` clicking the location in the source document.

### 3.3 Compilation

Modern editors usually provide the compilation programs to generate Portable Document Format (PDF) documents and for most L<sup>A</sup>T<sub>E</sub>X source files, this is sufficient. More advanced L<sup>A</sup>T<sub>E</sub>X functionality, such as glossaries and bibliographies, needs additional compilation steps, however. It is also possible that errors in the compilation process invalidate intermediate files and force subsequent compilation runs to fail. It is advisable to delete intermediate files (`.aux`, `.bbl`, etc.), if errors occur and persist. All files that are not generated by the user are automatically regenerated. To compile the current document, the steps as shown in Table 3.2 have to be taken.

## 3.4 Basic Functionality

In this section, various examples are given of the fundamental building blocks used in a thesis. Many  $\text{\LaTeX}$  commands have a rich set of options that can be supplied as optional arguments. The documentation of each command should be consulted to get an impression of the full spectrum of its functionality.

### 3.4.1 Floats

Two main categories of page elements can be differentiated in the usual  $\text{\LaTeX}$  workflow: *(i)* the main stream of text and *(ii)* floating containers that are positioned at convenient positions throughout the document. In most cases, tables, plots, and images are put into such containers since they are usually positioned at the top or bottom of pages. These are realized by the two environments `figure` and `table`, which also provide functionality for cross-referencing (see Table 3.3 and Figure 3.1) and the generation of corresponding entries in the list of figures and the list of tables. Note that these environments solely act as containers and can be assigned arbitrary content.

### 3.4.2 Tables

A table in  $\text{\LaTeX}$  is created by using a `tabular` environment or any of its extensions, e.g., `tabularx`. The commands `\multirow` and `\multicolumn` allow table elements to span multiple rows and columns.

Position		
Group	Abbrev	Name
Goalkeeper	GK	Paul Robinson
Defenders	LB	Lucas Radebe
	DC	Michael Duburrry
	DC	Dominic Matteo
	RB	Didier Domi
Midfielders	MC	David Batty
	MC	Eirik Bakke
	MC	Jody Morris
Forward	FW	Jamie McMaster
Strikers	ST	Alan Smith
	ST	Mark Viduka

Table 3.3: Adapted example from the  $\text{\LaTeX}$ guide at <https://en.wikibooks.org/wiki/LaTeX/Tables>. This example uses rules specific to the `booktabs` package and employs the multi-row functionality of the `multirow` package.

### 3.4.3 Images

An image is added to a document via the `\includegraphics` command as shown in Figure 3.1. The `\subcaption` command can be used to reference subfigures, such as Figure 3.1a and 3.1b.

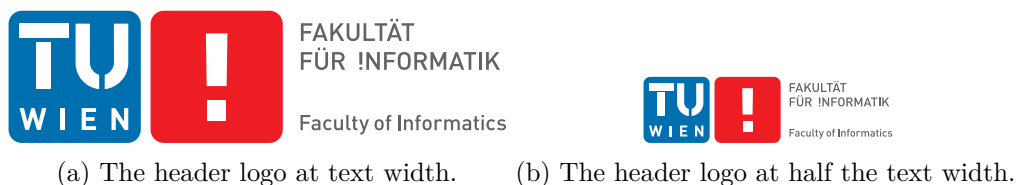


Figure 3.1: The header logo at different sizes.

### 3.4.4 Mathematical Expressions

One of the original motivation to create the T<sub>E</sub>X system was the need for mathematical typesetting. To this day, L<sup>A</sup>T<sub>E</sub>X is the preferred system to write math-heavy documents and a wide variety of functions aids the author in this task. A mathematical expression can be inserted inline as  $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$  outside of the text stream as

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

or as numbered equation with

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{3.1}$$

### 3.4.5 Pseudo Code

The presentation of algorithms can be achieved with various packages; the most popular are `algorithmic`, `algorithm2e`, `algorithmicx`, or `algpseudocode`. An overview is given at <https://tex.stackexchange.com/questions/229355>. An example of the use of the `algorithm2e` package is given with Algorithm 3.1.

## 3.5 Bibliography

The referencing of prior work is a fundamental requirement of academic writing and well supported by L<sup>A</sup>T<sub>E</sub>X. The B<sub>I</sub>B<sub>T</sub>E<sub>X</sub> reference management software is the most commonly used system for this purpose. Using the `\cite` command, it is possible to reference entries in a `.bib` file out of the text stream, e.g., as `[?]`. The generation of the formatted bibliography needs a separate execution of `bibtex.exe` (see Table 3.2).



---

**Algorithm 3.1:** Gauss-Seidel

---

**Input:** A scalar  $\epsilon$ , a matrix  $\mathbf{A} = (a_{ij})$ , a vector  $\vec{b}$ , and an initial vector  $\vec{x}^{(0)}$

**Output:**  $\vec{x}^{(n)}$  with  $\mathbf{A}\vec{x}^{(n)} \approx \vec{b}$

```
1 for  $k \leftarrow 1$  to maximum iterations do
2   for  $i \leftarrow 1$  to  $n$  do
3      $x_i^{(k)} = \frac{1}{a_{ii}} \left( b_i - \sum_{j < i} a_{ij} x_j^{(k)} - \sum_{j > i} a_{ij} x_j^{(k-1)} \right);$ 
4   end
5   if  $|\vec{x}^{(k)} - \vec{x}^{(k-1)}| < \epsilon$  then
6     break for;
7   end
8 end
9 return  $\vec{x}^{(k)}$ ;
```

---

## 3.6 Table of Contents

The table of contents is automatically built by successive runs of the compilation, e.g., of `pdflatex.exe`. The command `\setsecnumdepth` allows the specification of the depth of the table of contents and additional entries can be added to the table of contents using `\addcontentsline`. The starred versions of the sectioning commands, i.e., `\chapter*`, `\section*`, etc., remove the corresponding entry from the table of contents.

## 3.7 Acronyms / Glossary / Index

The list of acronyms, the glossary, and the index need to be built with a separate execution of `makeindex` (see Table 3.2). Acronyms have to be specified with `\newacronym` while glossary entries use `\newglossaryentry`. Both are then used in the document content with one of the variants of `\gls`, such as `\Gls`, `\glspl`, or `\Glspl`. Index items are simply generated by placing `\index{<entry>}` next to all the words that correspond to the index entry `<entry>`. Note that many enhancements exist for these functionalities and the documentation of the `makeindex` and the `glossaries` packages should be consulted.

## 3.8 Tips

Since  $\text{\TeX}$  and its successors do not employ a What You See Is What You Get (WYSIWYG) editing scheme, several guidelines improve the readability of the source content:

- Each sentence in the source text should start with a new line. This helps not only the user navigation through the text, but also enables revision control systems

(e.g. Subversion (SVN), Git) to show the exact changes authored by different users. Paragraphs are separated by one (or more) empty lines.

- Environments, which are defined by a matching pair of `\begin{name}` and `\end{name}`, can be indented by whitespace to show their hierarchical structure.
- In most cases, the explicit use of whitespace (e.g. by adding `\hspace{4em}` or `\vspace{1.5cm}`) violates typographic guidelines and rules. Explicit formatting should only be employed as a last resort and, most likely, better ways to achieve the desired layout can be found by a quick web search.
- The use of bold or italic text is generally not supported by typographic considerations and the semantically meaningful `\emph{...}` should be used.

The predominant application of the L<sup>A</sup>T<sub>E</sub>X system is the generation of PDF files via the PDFL<sup>A</sup>T<sub>E</sub>X binaries. In the current version of PDFL<sup>A</sup>T<sub>E</sub>X, it is possible that absolute file paths and user account names are embedded in the final PDF document. While this poses only a minor security issue for all documents, it is highly problematic for double blind reviews. The process shown in Table 3.4 can be employed to strip all private information from the final PDF document.

	Command
1	Rename the PDF document <code>final.pdf</code> to <code>final.ps</code> .
2	Execute the following command: <pre>ps2pdf -dPDFSETTINGS#/prepress ^       -dCompatibilityLevel#1.4 ^       -dAutoFilterColorImages#false ^       -dAutoFilterGrayImages#false ^       -dColorImageFilter#/FlateEncode ^       -dGrayImageFilter#/FlateEncode ^       -dMonoImageFilter#/FlateEncode ^       -dDownsampleColorImages#false ^       -dDownsampleGrayImages#false ^       final.ps final.pdf</pre>
	On Unix-based systems, replace <code>#</code> with <code>=</code> and <code>^</code> with <code>\</code> .

Table 3.4: Anonymization of PDF documents.

## 3.9 Resources

### 3.9.1 Useful Links

In the following, a listing of useful web resources is given.

**<https://en.wikibooks.org/wiki/LaTeX>** An extensive wiki-based guide to  $\text{\LaTeX}$ .

**<http://www.tex.ac.uk/faq>** A (huge) set of Frequently Asked Questions (FAQ) about  $\text{\TeX}$  and  $\text{\LaTeX}$ .

**<https://tex.stackexchange.com/>** The definitive user forum for non-trivial  $\text{\LaTeX}$ -related questions and answers.

### 3.9.2 Comprehensive TeX Archive Network (CTAN)

The CTAN is the official repository for all  $\text{\TeX}$  related material. It can be accessed via <https://www.ctan.org/> and hosts (among other things) a huge variety of packages that provide extended functionality for  $\text{\TeX}$  and its successors. Note that most packages contain PDF documentation that can be directly accessed via CTAN.

In the following, a short, non-exhaustive list of relevant CTAN-hosted packages is given together with their relative path.

**algorithm2e** Functionality for writing pseudo code.

**amsmath** Enhanced functionality for typesetting mathematical expressions.

**amssymb** Provides a multitude of mathematical symbols.

**booktabs** Improved typesetting of tables.

**enumitem** Control over the layout of lists (`itemize`, `enumerate`, `description`).

**fontenc** Determines font encoding of the output.

**glossaries** Create glossaries and list of acronyms.

**graphicx** Insert images into the document.

**inputenc** Determines encoding of the input.

**l2tabu** A description of bad practices when using  $\text{\LaTeX}$ .

**mathtools** Further extension of mathematical typesetting.

**memoir** The document class on upon which the `vutinfth` document class is based.

**multirow** Allows table elements to span several rows.

**pgfplots** Function plot drawings.

**pgf/TikZ** Creating graphics inside  $\text{\LaTeX}$  documents.

**subcaption** Allows the use of subfigures and enables their referencing.

**symbols/comprehensive** A listing of around 5000 symbols that can be used with  $\text{\LaTeX}$ .

**voss-mathmode** A comprehensive overview of typesetting mathematics in  $\text{\LaTeX}$ .

**xcolor** Allows the definition and use of colors.



# List of Figures

3.1	The header logo at different sizes. . . . .	8
-----	---	---



# List of Tables

3.1	T <sub>E</sub> X/L <sup>A</sup> T <sub>E</sub> X distributions for different operating systems. Recommended choice in <b>bold</b> . . . . .	5
3.2	Compilation steps for this document. The following abbreviations were used: table of contents (toc), list of figures (lof), list of tables (lot), list of algorithms (loa). . . . .	6
3.3	Adapted example from the L <sup>A</sup> T <sub>E</sub> Xguide at <a href="https://en.wikibooks.org/wiki/LaTeX/Tables">https://en.wikibooks.org/wiki/LaTeX/Tables</a> . This example uses rules specific to the booktabs package and employs the multi-row functionality of the multirow package. . . . .	7
3.4	Anonymization of PDF documents. . . . .	10





# List of Algorithms

3.1	Gauss-Seidel . . . . .	9
-----	------------------------	---