FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

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

FAKULTÄT FÜR !NFORMATIK
Faculty of Informatics

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, 13th 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

CHAPTER 1

Introduction

The cryptocurrency Bitcoin started back in the year 2008 with the release of the Bitcoin white paper [Nak08]. As of today, the cryptocurrency has reached a market capitalization of over 20 billion dollars [Mar]. Internally the Bitcoin cryptocurrency records all transactions in a public ledger called *blockchain*. The blockchain is basically an immutable linked list of blocks where a block contains multiple transactions of the cryptocurrency. In Bitcoin, each block needs to contain a so-called proof of work (PoW) which is the solution to a costly and time-consuming cryptographic puzzle. Miners connected in a peer-to-peer network compete with their computation power to find solutions to the puzzle and hence to find the next block for the blockchain. Finding a block allows the miners to add a transaction to the block and gives them right to newly create a certain amount of bitcoins. Additionally, the grouping of the transactions in blocks creates a total order and hence makes it possible to prevent double-spending. After a block is found by a miner, all other miners should adopt to this new tip of the chain and try to find a new block on top. This mining process is considered as incentive compatible as long as no single miner has more than 50% of the total computation power.

[ES14] showed that also miners under 50% have an incentive to not follow the protocol as described depending on their connectivity and share of computation power in the peer-to-peer network. By implementing a so-called selfish mining strategy a miner can obtain relatively more revenue than his actual proportion of computational power in the network. In general, the miner simply does not share found blocks with the others and secretly mines on his own chain. If his chain is longer then the public chain, he is able to overwrite all blocks found by the honest miners. If the two chains have the same length the private miner also publishes his block and causes a block race. Now the network is split into two parts where one part is mining on the public tip and the other part is mining on the now public-private tip. In general, the selfish miner achieves that the other miners are wasting their computational power on blocks which will not end up in the longest chain.

Further research [NKMS16, SSZ16, GRKC15, GKW+16, Bah13] explored different modifications of the original selfish mining algorithm by [ES14] and found slightly modifications of the algorithm which perform better under certain circumstances. For example, it could make sense for the selfish miner to even trail behind the public chain.

To prove the existence and attributes of selfish mining different approaches were applied. The researchers used simple probabilistic arguments [ES14, Bah13], numeric simulation of paths with state machines [GRKC15, NKMS16], advanced Markov Decision Processes (MDP) [SSZ16, GKW+16] or gave results of closed-source simulations [ES14, SSZ16]. Unfortunately, we cannot discuss the closed source simulations in detail. All other above-mentioned methodologies have the following drawbacks:

- Abstraction of the Bitcoin source code which normally runs on a single node. Since there is no official specification of the Bitcoin protocol it is hard to capture all details. Furthermore, it is hard to keep the simulation software up-to-date because of the ongoing development of the protocol.
- Abstraction of the whole network layer of the peer-to-peer network. The available simulations abstract the network topology by either defining a single connectivity parameter [ES14, Bah13, NKMS16, SSZ16, GRKC15] or by using the block stale rate as input for the MDP [GKW+16]. Hence the highly abstract the presence of network delays and natural forks of the chain.

In this thesis, we propose a new simulation approach to more accurately capture the details of the Blockchain protocol under simulation, while allowing for a high degree of determinism. With our simulation, it would be possible to model the selfish mining attack with different network topologies and to use the Bitcoin source code directly in the simulation.

CHAPTER 2

State-of-the-art

Already in the year 2010 the user *ByteCoin* described the idea of selfish mining in the Bitcoin forum *bitcointalk* [Byt]. He provided simulation results of the attack which at that time was called *mining cartel attack*. Nevertheless, the discussions in the thread never caught fire and no further investigations or countermeasures were taken by the community [Bitc, Bah13].

Later in 2014 [ES14] released the paper *"Majority is not enough: Bitcoin mining is vulnerable."* and coined the term selfish mining. The paper gives a formal description of selfish mining and proves how a miner can earn more than his fair share by conducting the attack. Figure 2.1 shows the attack as a state machine where α denotes the mining power share of the selfish miner. The labels of the states are representing the lead of the selfish miner over the public chain. Whenever the public network finds a block and the selfish miner publishes a competing block of the same height a block race occurs denoted with the state *0'*. In the case of such a block race, the variable γ expresses the probability of the selfish miner to win the block race. Hence γ part of the miners are mining on the public-private block and respectively $(1 - \gamma)$ are mining on the public block. The labels on the transitions are representing the transition probabilities between the states. The profitability of the simple strategy of [ES14] was proven by using probability calculations based on the state machine of figure 2.1. Furthermore, results of an undisclosed Bitcoin protocol simulator were given. In the simulation, 1000 miners with the same mining power were simulated and a fraction of these miners formed a pool which applied the selfish mining algorithm. In the case of a block race they artificially split the network where one part is mining on the public block and one part is mining on the block of the selfish pool.

Further research showed that more generalised selfish mining strategies lead to even more relative gain for the selfish miner [NKMS16, SSZ16, GRKC15, GKW+16, Bah13]. Figure 2.2 shows a possible categorization of the different selfish mining strategies where α and γ is used equivalent as in figure 2.1 and β expresses (1 - α). Furthermore, the

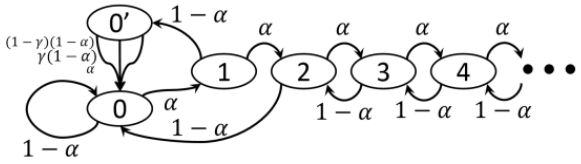


Figure 2.1: Selfish mining state machine with transition probabilities [ES14]

prime states are standing for states where a block race happens on certain height and the *0"* represent the state where both chains have the same height but the selfish miner and the rest of the network are mining on different branches. The idea behind the different variations of selfish mining strategies in figure 2.2 are:

- Lead stubborn mining strategy compromises the idea to cause as many block races as possible and to never overwrite the public chain with a longer chain. This strategy continuously tries to split the network to mine on different blocks and is therefore especially promising when the probability to win the block race is very high.
- Equal-fork stubborn mining strategy changes the selfish mining strategy just by one transition. In case the selfish miner finds a block during a block race, he does not publish his block to win the race but he also keeps this block undisclosed to secretly mine on this new tip of the chain.
- Trail stubborn mining strategies reflects the idea to even trail behind the public chain and to eventually catch up. The figure 2.2 depicts the trail stubborn mining strategy *T1*. The number one denotes that the selfish miner is allowed to trail one block behind the public chain.

The strategy space for a selfish miner is practically endless and combinations of the aforementioned strategies are possible and are leading to even more relative gain compared to honest miners[NKMS16, SSZ16, GRKC15, GKW$^+$16, Bah13].

To find the best strategy for a given mining power share α and connectivity γ researchers used different methodologies. [GRKC15, NKMS16] used numeric simulations of paths in the state machine to find optimal selfish mining strategies. [SSZ16, GKW$^+$16] on the other hand used MDPs based on a state machine to find strategies with the most relative gain. The basic structure of the used state machines is for all publications the same. To further validate their results [ES14, SSZ16] used a closed-source simulation.

Besides using variations of the selfish mining strategies, the attack can also be combined with other attacks to achieve better results [GKW$^+$16, SSZ16, NKMS16, GRKC15]. If the eclipse attack is used in combination with selfish mining the victim contributes its mining power to the private chain and hence, strengthens the position of the selfish miner [NKMS16, GKW$^+$16]. [NKMS16] additionally shows that the eclipsed victim

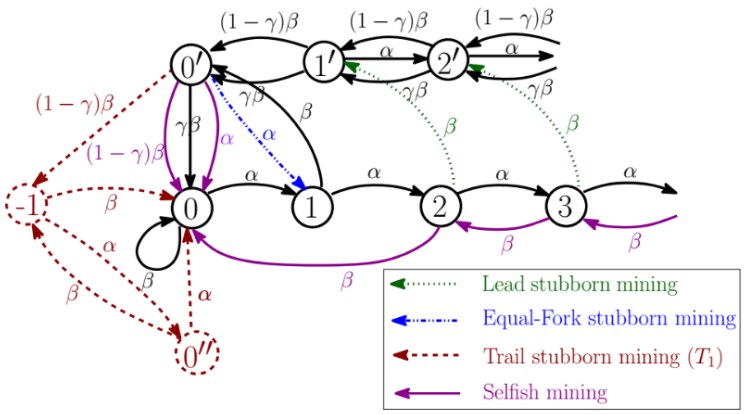


Figure 2.2: Categorization of different mining strategies [NKMS16]

under certain circumstances can benefit from the attack and therefore has no incentive to stop the attack. Another attack which can be used in combination with selfish mining is double-spending [SSZ16, GKW+16]. Every time the selfish miner starts his selfish mining attack he can publish a transaction and include a conflicting transaction in his first secret block. During the execution of the selfish mining attack, the payment receiver may accept the payment depending on his block confirmation time. Now in the case of a successful selfish mining attempt, the adversary can overwrite the public chain, which additionally results in a successful double spending. The operational costs of unsuccessful double-spending can be seen as low because the adversary still would get goods or a service in exchange for the transaction [SSZ16, GKW+16].

Last but not least also the prevention of selfish mining is part of the current work in selfish mining research [ES14, Bil15, SPB16, ZP17]. A backwards-compatible patch to mitigate selfish mining is uniform tie-breaking [ES14]. This means whenever a node receives two blocks of the same height he randomly select on of the blocks to mine on. [ES14] showed that this would raise the profit threshold to 25% of the computational power and hence mitigating selfish mining. The drawback of this proposed change is that it would increase the connectivity of badly connected attackers to almost 50% with no actual effort for them. Ethereum, the currently second largest cryptocurrency by market capitalization [Mar], has implemented uniform tie-breaking as a countermeasure against selfish mining [GKW+16, uni]. Another countermeasure foresees unforgeable timestamps to secure Bitcoin against selfish mining [Bil15]. This countermeasure would make all pre-mined blocks of the selfish miner invalid after a certain amount of time. The implementation of this patch would require random beacons and hence introduce complexity and a new attack vector [Bil15]. [ZP17] proposes backward-compatible countermeasure by neglecting blocks that are not published in time and allows incorporation of competing blocks in the chain similar to Ethereum's uncle blocks [Woo14]. This enables a new fork-resolving policy where a block always contributes to neither or both branches of the fork [ZP17]. All of this mentioned countermeasures are not planned to be implemented or implemented

in Bitcoin [bita, bitb].

CHAPTER 3

Expected results

The expected outcome of this thesis is a more accurate simulation of different selfish mining strategies and therefore a better understanding of the potential real world implications of such attacks. The selfish mining strategies include:

- selfish mining [ES14]
- lead stubborn mining [NKMS16]
- trail stubborn mining [NKMS16]
- equal-fork stubborn mining [NKMS16]

For the simulation, these strategies are combined with different distributions of computation power and different network topologies. The result of the simulations should show which strategy is the best strategy for a certain combination of a network topology and distribution of mining power. Thereby, also the influence of the network topology is studied in more detail compared to previous research. The simulation results should emphasise the recent work in the area of selfish mining and show that the current implementation of Bitcoin protocol is vulnerable against different selfish mining strategies.

An additional outcome of the thesis is the simulation software. The software should allow an accurate and deterministic simulation of the blockchain by using directly the reference implementation and a realistic network topology. Hence, the simulation software could not only be used to simulate selfish mining attacks but could for example also be used to simulate other attacks or new protocol versions of Bitcoin. Since many other cryptocurrencies are derived from Bitcoin, they simulation software could be used also to simulate their behaviour and properties.

CHAPTER 4

Methodology and Approach

First, the different strategies selfish, lead stubborn, trail stubborn and equal-fork stubborn mining from [NKMS16] and [ES14] need to be implemented. This is achieved by implementing a proxy which eclipses a normal Bitcoin client from the other nodes in the network. Now, if a block is found the proxy decides, depending on his selfish mining strategy, if a block should be transmitted from the eclipsed node to the rest of the network or vice versa. The proxy design pattern makes it possible to implement the selfish mining strategies without altering the reference implementation of Bitcoin and is therefore preferred over an implementation directly in the Bitcoin client.

In the next step, a simulation program is implemented. To be able to control when a certain node finds a block, all Bitcoin nodes should be executed in *regtest* mode. In this test mode, the real PoW-algorithm is disabled and every node accepts a command which lets the node create immediately a new block. With this functionality, it is possible to define a block discovery series which basically reflects the computation power of each node. The more blocks are found by a node the more simulated computation power the node has. Additionally to the block generation, the simulation program should also control the network topology and hence the connectivity of each node. For the simulation run, it is important that the connectivity of the nodes stays the same to make the results better comparable. This should be achieved by setting the connections from the nodes by the simulation program itself which is in contrast to normal behaviour. Normally Bitcoin nodes share their connections with other nodes over the Bitcoin protocol and try to improve the connectivity over time.

After the implementation of the selfish mining strategies and the simulation program, the mining strategies are simulated. Different network topologies and distributions of computation power are used to compare the relative gain of the selfish mining strategies over the normal, honest mining.

CHAPTER 5

Simulation framework

what are we doing now? - describing the simulation software - simulation software exposes six commands - nodes - network - connectivity - ticks - simulate - run - multi-run

5.1 Configuration files

nodes - let you create groups of node with the same configuration - group has type, amount, share, latency, docker image - groups are persisted in a csv

network - let you create a network configuration - takes nodes.csv and connects them based on defined connectivity - network configuration is persisted in a csv

ticks - let you create a certain amount of ticks - a tick contains block events - using a exponential distribution and depending on the computational share it is determined when a node finds a block - ticks are persisted in a csv

component diagram of simulation software - simulationfiles - run, multi-run - prepare - execution - post processing

flow chart of run command

5.2 Simulation

- executed eg. with simulate cmd - in the simulation docker is used - each simulation has three todophases/steps (which word should we use?) - takes configuration files as input

5.2.1 Preparation

- nodes are created and connected - create RPC-connection - wait until ready

5.2.2 Execution

- execute ticks from ticks.csv line by line - tick duration defined - execute all events in tick sequentially - afterwards sleep until tick is over, then start over again - during execution CPU & RAM usage is collected

5.2.3 Post processing

- get chaintips of all nodes - calculate consensus chain - start at first block height - request from all nodes blocks - if every node has a block and all blocks are the same, add block to consensus chain and heigt++ - otherwise stop - stop nodes - process log file of every node and log file of simulation software - parse log events: - BlockCreateEvent - BlockStatsEvent - UpdateTipEvent - PeerLogicValidationEvent - TxEvent - TickEvent - BlockReceivedEvent - BlockReconstructEvent - TxReceivedEvent - BlockExceptionEvent - TxExceptionEvent - RPCExceptionEvent - pre-processing csv - need to have one report.rmd for run and multi-runs - remove skip-ticks - files are not sorted because of multi-processed parsing; sort by timestamp - report creation - with Rmarkdown, R ... - calculate propagation time of blocks - calculate stale blocks - create useful stats about CPU & RAM usage, duration, blocks, propagation, exceptions...

5.2.4 Multi-runs

- runs a simulation multiple times with the same arguments - merges csv of all runs by type - create a report showing all results of all runs

CHAPTER 6

Evaluation of simulation framework

- we can execute simulation multiple times (100 times would last week) - then we can look at the stale block rate - check which distribution is appropriate - and then we will see :D

how should we do that?

CHAPTER 7

Selfish proxy

The selfish proxy is the node in our peer-to-peer network implementing the different selfish mining strategies. He eclipses a normal bitcoin node from the rest of the network and accepts blocks created by the eclipsed node or by the normal nodes. With the collected blocks he recreates the chain locally and on every received block he runs the configured selfish mining algorithm. The algorithm then decides if the received block should be withhold or relayed to the other part of the network.

not relaying tx

create a component diagram - network - chain - strategy create a picture showing how blocks are relayed in bitcoin

any software recommendation for charts/diagrams

7.1 Architecture

7.1.1 Network component

The implementation of network component is based on the two libraries *pycoin* and *python-bitcoinlib*. The library *pycoin* provides simple networking utilities to connect to other bitcoin nodes and to manage those connections. Where on the other hand the *python-bitcoinlib* library implements functionalities to serialize and deserialize bitcoin network messages. In general the network component is responsible for:

reference

- listening and accepting incoming connections
- be able to distinguish between connections from the eclipsed node or connections from the rest of the network
- managing and keep his connections a live by replying to ping messages
- accepting, processing and replying to messages relevant for the selfish relay
- detecting and re-triggering of failed requests

7.1.2 Chain component

The main responsibility of the chain component is to reassemble the chain with the blocks received by the network component. This can be done easily by just looking at the hash of the previous block stored in the received block. If the previous block is already in the chain, the newly received block gets added to the chain. In the case the block identified by its hash is not available in the chain, the block gets preserved as an orphan block. On every successful inserted block all orphaned blocks are checked if they can be added now to the chain. Along side the information stored in the block, the chain component also keeps track of the block origin and a boolean reflecting if the transfer of this block to other nodes is allowed. This information is necessary for the chain component to be able to calculate the current fork between the eclipsed node and the rest of the network.

7.1.3 Strategy component

The strategy component implements the four different selfish mining strategies:

- selfish mining
- trail stubborn mining
- equal-fork stubborn mining
- lead stubborn mining

The strategies are implemented by accepting the current fork as an input and based on that fork the action to be taken is determined with simple control structures like if and else.Additionally the strategy component contains a module for determining which blocks are supposed to be relayed depending on a determined action and a fork.

describe actions here? or in state-of-the-art

7.2 Selfish relaying

The overall concept of the selfish proxy is to do selfish mining without actually mining blocks. By eclipsing a node the selfish proxy is able to withhold and relay blocks corresponding to a selfish mining strategy. Hence the selfish proxy is, as we call it, selfish relaying.

To be able to do selfish relaying the proxy continuously collects all blocks advertised by the connected nodes. In bitcoin newly found blocks are broadcasted over the peer-to-peer network by sending the hash in an inv message. Whenever the proxy receives such a inv msg with a block hash unknown to him, he immediately requests the new block by sending a getdata message. The node, which found the block, replies then with a block message containing the actual block. The proxy, after receiving the block, tries to insert the block in his own local chain. If the block can be inserted on top of a tip in the chain, the proxy runs the selfish mining algorithm. The algorithm determines based on the

current fork between eclipsed node and the rest of the network an action. In the case that the action is one out of match or override, the algorithm further determines which blocks need to be relayed and sends out the corresponding block hashes over a inv message.

When a normal node receives a inv message with a unknown block from the proxy, the node first request all new headers with a getheaders call. The proxy replies to the node then the new headers, which are then

- block relay - how does block relay work - compact blocks - how did we implement it - no compact blocks - assuming all blocks are valid - when we have the whole block pass it to chain - receives height of private and public - searches action to execute - 4 different types of actions (wait, adopt, match, override) - executes by sending inv's - which strategies did we implement? - - how did we implement it? - search for an action - if-else control structure - many unit tests

why we used a proxy? - fast implementation - no need to touch reference implementation

disadvanteges - extra hop - not a real proxy - need to keep track of chain - bitcoin protocol not easy

figure block relay

how works each strategy? describe it here or in section simulation and reference to the section.

move maybe to another section. here we should only DESCRIBE the selfish proxy

CHAPTER 8

Simulation of selfish mining strategies

8.1 Results

CHAPTER 9

Discussion

9.1 Installation

CHAPTER 10

Further research

10.1 Installation

CHAPTER 11

Introduction to LaTeX

Since LaTeX 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 LaTeX.

11.1 Installation

A full LaTeX 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 11.1. **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.

11.2 Editors

A multitude of TeX 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	**yes**	yes	(yes)
MacTeX	no	no	**yes**
MikTeX	no	**yes**	no

Table 11.1: TeX/LaTeX distributions for different operating systems. Recomended 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	`pdflatex.exe  example`
2	`bibtex.exe  example`
3	`pdflatex.exe  example`
4	`pdflatex.exe  example`
5	`makeindex.exe -t example.glg -s example.ist -o example.gls example.glo`
6	`makeindex.exe -t example.alg -s example.ist -o example.acr example.acn`
7	`makeindex.exe -t example.ilg -o example.ind example.idx`
8	`pdflatex.exe  example`
9	`pdflatex.exe  example`

Table 11.2: 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`. 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.

11.3 Compilation

Modern editors usually provide the compilation programs to generate Portable Document Format (PDF) documents and for most LaTeX source files, this is sufficient. More advanced LaTeX 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 11.2 have to be taken.

11.4 Basic Functionality

In this section, various examples are given of the fundamental building blocks used in a thesis. Many 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.

11.4.1 Floats

Two main categories of page elements can be differentiated in the usual 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 11.3 and Figure 11.1) 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.

11.4.2 Tables

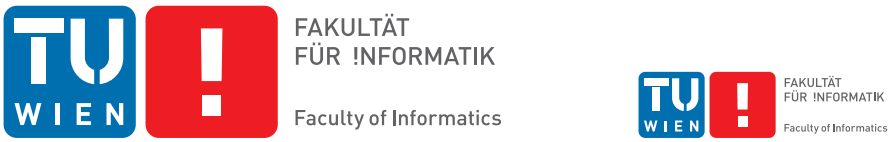
A table in LaTeX is created by using a `tabular` environment or any of its extensions, e.g., `tabularx`. The commands `\multirow` and `\multicolumn` allow table elements to span multiple rows and columns.

Position		
Group	Abbrev	Name
Goalkeeper	GK	Paul Robinson
Defenders	LB	Lucus Radebe
	DC	Michael Duburry
	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 11.3: Adapted example from the LaTeXguide 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.

11.4.3 Images

An image is added to a document via the `\includegraphics` command as shown in Figure 11.1. The `\subcaption` command can be used to reference subfigures, such as Figure 11.1a and 11.1b.



(a) The header logo at text width. (b) The header logo at half the text width.

Figure 11.1: The header logo at different sizes.

11.4.4 Mathematical Expressions

One of the original motivation to create the TeX system was the need for mathematical typesetting. To this day, LaTeX 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

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \tag{11.1}$$

11.4.5 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 `alogrithm2e` package is given with Algorithm 11.1.

11.5 Bibliography

The referencing of prior work is a fundamental requirement of academic writing and well supported by LaTeX. The BibTeX 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 [Tur36]. The generation of the formatted bibliography needs a separate execution of `bibtex.exe` (see Table 11.2).

Algorithm 11.1: Gauss-Seidel

Input: A scalar ϵ, a matrix $\mathbf{A} = (a_{ij})$, a vector $\vec{b}$, and an initial vector $\vec{x}^{(0)}$
Output: $\vec{x}^{(n)}$ with $\mathbf{A}\vec{x}^{(n)} \approx \vec{b}$

```
for k ← 1 to maximum iterations do
    for i ← 1 to n do
        x_i^(k) = (1/a_ii) (b_i − Σ_{j<i} a_ij x_j^(k) − Σ_{j>i} a_ij x_j^(k−1));
    end
    if |x^(k) − x^(k−1)| < ε then
        break for;
    end
end
return x^(k);
```

11.6 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.

11.7 Acronyms / Glossary / Index

The list of acronyms, the glossary, and the index need to be built with a separate execution of `makeindex` (see Table 11.2). 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.

11.8 Tips

Since 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 LaTeX system is the generation of PDF files via the PdfLaTeX binaries. In the current version of PdfLaTeX, 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 11.4 can be employed to strip all private information from the final PDF document.

	Command
1	Rename the PDF document `final.pdf` to `final.ps`.

2	Execute the following command:
	`ps2pdf -dPDFSETTINGS#/prepress ^`
	`-dCompatibilityLevel#1.4 ^`
	`-dAutoFilterColorImages#false ^`
	`-dAutoFilterGrayImages#false ^`
	`-dColorImageFilter#/FlateEncode ^`
	`-dGrayImageFilter#/FlateEncode ^`
	`-dMonoImageFilter#/FlateEncode ^`
	`-dDownsampleColorImages#false ^`
	`-dDownsampleGrayImages#false ^`
	`final.ps final.pdf`

On Unix-based systems, replace # with = and ^ with \.

Table 11.4: Anonymization of PDF documents.

11.9 Resources

11.9.1 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 LaTeX.

http://www.tex.ac.uk/faq A (huge) set of Frequently Asked Questions (FAQ) about TeX and LaTeX.

https://tex.stackexchange.com/ The definitive user forum for non-trivial LaTeX-related questions and answers.

11.9.2 Comprehensive TeX Archive Network (CTAN)

The CTAN is the official repository for all 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 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 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 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 LaTeX.

voss-mathmode A comprehensive overview of typesetting mathematics in LaTeX.

xcolor Allows the definition and use of colors.

List of Figures

List of Tables

List of Algorithms

Index

Glossary

editor A text editor is a type of program used for editing plain text files..

Private chain Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum..

Private lead Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum..

Public chain Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem Ipsum..

Acronyms

CTAN Comprehensive TeX Archive Network.

FAQ Frequently Asked Questions.

PDF Portable Document Format.

SVN Subversion.

WYSIWYG What You See Is What You Get.

Bibliography

[Bah13] Lear Bahack. Theoretical bitcoin attacks with less than half of the computational power (draft). *arXiv preprint arXiv:1312.7013*, 2013.

[Bil15] Saki Billah. One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. 2015.

[bita] Bitcoin - reference implementation of the bitcoin protocol. `https://github.com/bitcoin/bitcoin`. Accessed: 2017-06-21.

[bitb] Bitcoin bips - bitcoin improvment proposals. `https://github.com/bitcoin/bips`. Accessed: 2017-06-21.

[Bitc] Thread about mining cartel attack on bitcointalk. `https://bitcointalk.org/index.php?topic=2227.0`. Accessed: 2017-06-21.

[Byt] User bytecoin on the mining cartel attack. `https://bitcointalk.org/index.php?topic=2227.msg30064#msg30064`. Accessed: 2017-06-21.

[ES14] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *International Conference on Financial Cryptography and Data Security*, pages 436–454. Springer, 2014.

[GKW+16] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 3–16. ACM, 2016.

[GRKC15] Arthur Gervais, Hubert Ritzdorf, Ghassan O Karame, and Srdjan Capkun. Tampering with the delivery of blocks and transactions in bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 692–705. ACM, 2015.

[Mar] Cryptocurrency market capitalizations. `https://coinmarketcap.com/`. Accessed: 2017-06-21.

[Nak08] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[NKMS16] Kartik Nayak, Srijan Kumar, Andrew Miller, and Elaine Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, pages 305–320. IEEE, 2016.

[pyc] Minimalistic python implementation of the bitcoin networking stack. `https://github.com/cdecker/pycoin`. Accessed: 2017-10-30.

[pyt] Python2/3 library providing an easy interface to the bitcoin data structures and protocol. `https://github.com/petertodd/python-bitcoinlib`. Accessed: 2017-10-30.

[SPB16] Siamak Solat and Maria Potop-Butucaru. *ZeroBlock: Preventing Selfish Mining in Bitcoin*. PhD thesis, Sorbonne Universit es, UPMC University of Paris 6, 2016.

[SSZ16] Ayelet Sapirshtein, Yonatan Sompolinsky, and Aviv Zohar. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer, 2016.

[Tur36] Alan Mathison Turing. On computable numbers, with an application to the entscheidungsproblem. *J. of Math*, 58:345–363, 1936.

[uni] Release of uniform tie breaking in ethereum. `https://github.com/ethereum/go-ethereum/commit/bcf565730b1816304947021080981245d084a930`. Accessed: 2017-06-21.

[Woo14] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 151, 2014.

[ZP17] Ren Zhang and Bart Preneel. Publish or perish: A backward-compatible defense against selfish mining in bitcoin. In *Cryptographers' Track at the RSA Conference*, pages 277–292. Springer, 2017.