From closed source to open innovation: The Bitaxe project as a model for future developments in the field of Bitcoin mining

from
WantClue

Open Source Miners United
Labs

From closed source to open innovation: The Bitaxe project as a model for future developments in the field of Bitcoin mining

von
WantClue

Open Source Miners United
Labs

0.1 Abstract

In the context of the evolving landscape of Bitcoin mining, small-scale home miners play a pivotal role in promoting network decentralisation and enhancing the security of the blockchain. This thesis investigates the viability and impact of using Bitaxe Ultra ASIC chips for small-scale Bitcoin mining operations. The primary objectives of the study is to develop an accessible, cost-effective mining solution, analyse its performance metrics, and assess its contribution to the overall network hashrate.

The research involved both theoretical modelling and empirical analysis. A comprehensive evaluation was conducted to measure key performance indicators such as hashrate, power consumption, and efficiency. The Bitaxe Ultra, featuring the BM1366 ASIC chip demonstrated a hashrate of approximately 0.5 TH/s per device, with a power consumption of 12W. The study found that the deployment of approximately 1,380,000 Bitaxe Ultra devices could contribute 0.1% to the total Bitcoin network hashrate, equating to 0.69 EH/s. This contribution would significantly impact the network, enhancing decentralization and security. Additionally, the economic analysis revealed that the low operational costs make small-scale mining financially viable for individual users. The environmental impact can be minimized by leveraging renewable energy sources.

Future work should concentrate on developing a dedicated benchmarking tool, conducting detailed heat management studies, and fostering collaborations with large mining facilities with a view to further exploring the scalability and sustainability of small-scale mining solutions. The findings of this research provide a foundational understanding of the potential and challenges of integrating small-scale mining into the broader Bitcoin mining ecosystem.

Contents

1 Introduction

In the rapidly evolving landscape of Bitcoin mining, the maxim "don't trust, verify" is not just a slogan but a fundamental principle that underpins the entire ecosystem. This ethos, rooted deeply in the Bitcoin community, emphasizes the importance of transparency and trust through verification. However, the predominance of closed-source hardware in the mining industry presents a significant challenge to this principle, creating a paradox where trust is often placed in opaque systems that users cannot fully understand or verify. This thesis examines the Bitaxe project, an ambitious open-source initiative designed to bridge the gap between trust and transparency in Bitcoin mining.

The transition from closed-source dominance to open innovation represents a pivotal shift towards empowering users and operators in the Bitcoin mining ecosystem. While closed-source systems offer simplicity and ease of use, they often present users with a binary choice: to blindly trust the technology or to remain on the periphery of understanding. This segregation is particularly pronounced in Bitcoin mining, where the intricacies of hardware performance and reliability are pivotal to the network's security and efficiency. The Bitaxe project represents a paradigm shift in the field of open innovation, challenging the status quo by advocating for transparency, inclusivity, and the democratisation of mining technology.

This thesis examines the Bitaxe project as a model for future developments in Bitcoin mining. It considers the potential benefits and drawbacks of fostering open-source projects within a predominantly proprietary system. This thesis proposes that the future of Bitcoin mining and, by extension, the broader blockchain ecosystem lies in the adoption of open innovation, where trust is established not on the opacity of closed systems but on the verifiable transparency of open-source solutions. The Bitaxe project will serve as a lens through which this thesis will propose some changes in this transition. The objective is to gain insight into the potential of open-source principles to redefine the foundations of trust and innovation in Bitcoin mining.

1.1 Motivation

In the context of the rapidly evolving digital economy, it is becoming increasingly important to have a clear understanding of the intricate dynamics of the markets and the services on which we rely. As consumers and participants in the digital age, we often rely on the technologies and platforms that facilitate our daily transactions, placing our trust in them without question, sometimes without a comprehensive understanding of their inner workings. This blind trust presents a significant risk, particularly in the context of digital currencies such as Bitcoin, where transparency and security are of paramount importance. The Bitcoin community adheres to the ethos of "don't trust, verify", underscoring the necessity of tools that enable users to take ownership of their digital assets securely and transparently.

The necessity for research in this area arises from a critical examination of the current Bitcoin mining landscape, where the hiding power of proprietary mining hardware and software poses significant risks to the networks integrity and accessibility. By investigating the evolution and implications of open-source mining solutions, a confrontation of these challenges can be achieved directly, advocating for a return to Bitcoin's foundational principles of decentralization, transparency, and community participation.

Open-source initiatives like the Bitaxe project aim to democratize Bitcoin mining. Unlike the current landscape, dominated by proprietary mining hardware, from less than five different manufactures, Bitaxe represents a groundbreaking shift towards transparency, inclusivity, and empowerment for the individual miner and the broader community. By developing and supporting open-source mining solutions, projects like this, may have the potential to transform Bitcoin mining into a more open, equitable, and verifiable process like shown in Figure 1.1. In doing so, the community that drives the Bitaxe project Open Source Miners United (OSMU) not only advocate for a more transparent digital economy but also contribute to the foundational principles of decentralization and trust that Bitcoin was built upon.

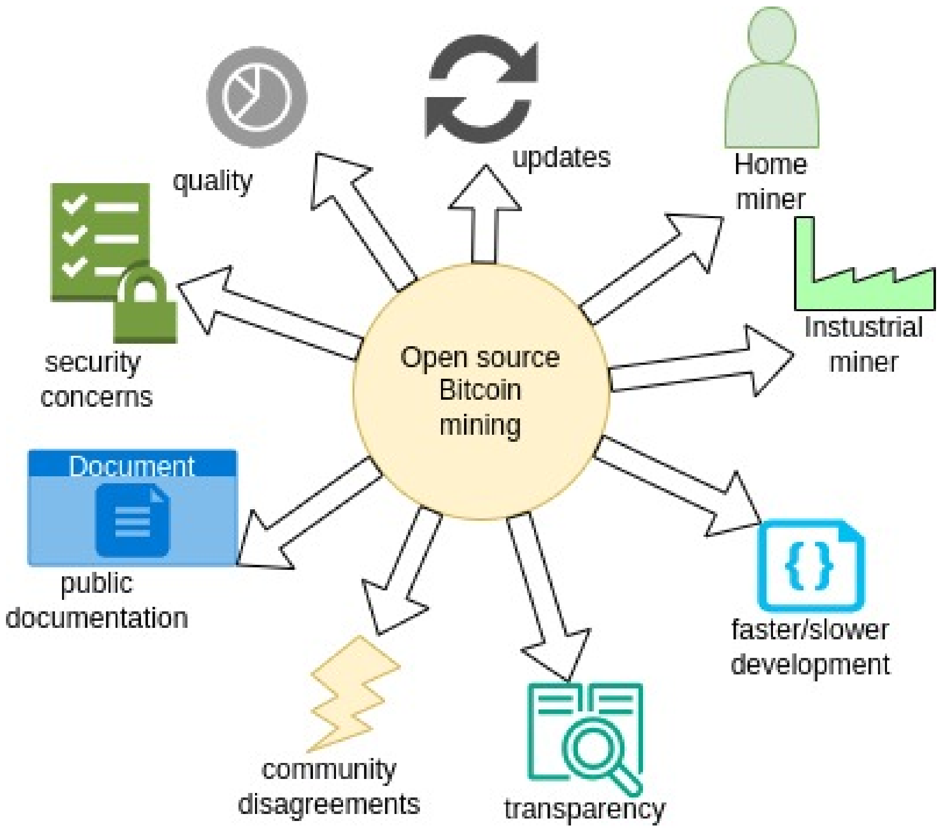

Figure 1.1: Open Source Development in Bitcoin Mining

1.2 Research Purpose and Approach

The advent of blockchain technology and cryptocurrency mining has highlighted the crucial role of hardware in maintaining and securing decentralized networks. However, the distribution of proprietary hardware in this field presents significant obstacles, including reduced transparency, limited accessibility, and the potential for centralization. This thesis proposes to explore these challenges through the lens of the Bitaxe project, an open-source hardware and software initiative designed to offer a viable alternative to proprietary systems.

Free and open source software (FOSS) embodies principles of transparency, collaboration, and freedom, enabling individuals and communities to contribute to and benefit from technology without restrictions. The Bitaxe project, rooted in Free Open Source (FOS) principles, aims not only to democratize access to cryptocurrency mining but also to foster innovation and inclusivity within the blockchain ecosystem. By developing an open-source Application-Specific Integrated Circuit (ASIC) benchmarking tool, Bitaxe's objective is to provide a comprehensive solution for testing and analyzing mining hardware, thereby facilitating greater transparency regarding the underlying technology used in such devices.

The utilization of collected data through the Bitaxe benchmarking tool will enable a systematic comparison between open-source and proprietary hardware projects. This comparative analysis aims to highlight the advantages of open-source solutions in terms of performance, cost-effectiveness, and community engagement. Alternatively, it would be beneficial to identify the disadvantages and lack of knowledge that may impede the ability to compete with proprietary hardware. The following research questions will guide this investigation:

- How can an open-source project like Bitaxe address the challenges posed by proprietary hardware in the cryptocurrency mining industry?
- What features and capabilities are essential for an effective ASIC benchmarking tool, and how can these be implemented in an open-source project?
- What are the potential impacts of Bitaxe on the broader blockchain and cryptocurrency mining communities?

1.3 Procedure and Structure

This section provides an overview of the research procedure and the structure of this thesis. It outlines the methodological approach taken to achieve the research objectives and provides a guide to the organization of the document.

The research for this thesis was conducted through a combination of theoretical modeling, empirical analysis, and practical implementation. The following steps outline the procedure followed:

- **Literature Review**: A comprehensive review of existing literature on Bitcoin mining, ASIC chips, and small-scale mining solutions was conducted to establish a foundation for the research.
- **Theoretical Modeling**: Mathematical models were developed to represent the relationship between hashrate and power consumption of ASIC chips.

- **Empirical Data Collection**: Data was collected from various Bitaxe Ultra devices to measure performance metrics such as hashrate, power consumption, and temperature under different operating conditions.
- **Data Analysis**: The collected data was analyzed to validate the theoretical models and to understand the performance and efficiency of the Bitaxe Ultra devices.
- **Cost and Energy Analysis**: An economic analysis was conducted to evaluate the initial and operational costs, and an energy consumption analysis was performed to assess the feasibility and sustainability of small-scale mining.
- **Future Work and Recommendations**: Based on the findings, recommendations for future research and development were proposed, focusing on areas such as benchmarking tools, heat management, and collaboration with large mining facilities.

The structure of this thesis is organized into the following chapters:

Chapter 1 introduces the background and the Bitaxe project, outlining the research objectives and questions. Chapter 2 describes the background basics needed for this thesis. Chapter 3 describes the current solution of the Bitcoin mining network and sets out the requirements for this thesis. Chapter 4 is a detailed review of existing literature on Bitcoin mining, ASIC technology, and small-scale mining operations. Chapter 5 introduces the concept of a Benchmarking Framework and the theoretical concept of small-scale mining operations. Chapter 6 features the implementation of the Concept of a Benchmarking Tool and Analyzing potential outcomes of small-scale mining solutions. Chapter 7 evaluates the key findings and compares them with the requirements. Chapter 8 summarizes the key findings, discusses their implications, and concludes the thesis.

2 Basics

This chapter will examine the fundamental concepts and topics that are essential for an understanding of the core thesis of this work. Topics like the open source ethos, the core principles of Blockchain technologies, are chosen for its direct relevance to the exploration of the Bitaxe project. In order to provide a comprehensive introduction to the topics that will be discussed in this section, it is necessary to first present a brief overview of the subject matter.

2.1 Open Source

Open source is a term that resonates deeply within the digital era, embodying a philosophy that extends far beyond the mere sharing of code. At its core, open source is about the freedom of knowledge, a meaningful aspect that has revolutionized the way we create, share, and utilize technology. The following introduction aims to examine the fundamental principles of open-source software, demonstrating how these principles encourage innovation, collaboration and the democratization of technology.

The open-source movement is founded on the premise that software and hardware should be freely available for anyone to use, modify, and distribute. This concept challenges traditional models of proprietary software and hardware, where source code is kept secret to maintain competitive advantage. Instead, open source thrives on the belief that sharing knowledge freely fosters a more inclusive, innovative, and efficient approach to problem-solving. It is a testament to the power of collective intelligence, where diverse perspectives and expertise converge to create robust, versatile, and secure software solutions.

The freedom associated with open source goes beyond the mere ability to access and modify code. It represents a broader ideology of knowledge sharing as a fundamental human right. This ethos is encapsulated in the four essential freedoms defined by the Free Software Foundation: the freedom to run the program for any purpose, the freedom to study how the program works and change it, the freedom to redistribute copies, and the freedom to distribute copies of your modified versions [fre]. These freedoms ensure that open source software remains a tool for empowerment, enabling individuals and organizations to adapt technology to their needs without the constraints of licensing fees or restrictive terms of use.

The impact of open source on the technological landscape is profound and far-reaching. It has been the driving force behind some of the most significant innovations in the digital age, including the Linux operating system, the Apache HTTP Server, and the Mozilla Firefox browser, among countless others. These projects exemplify how open source principles encourage experimentation, rapid iteration, and the sharing of knowledge, leading to high-quality software that benefits everyone [BHP+12].

Moreover, the open source movement has catalyzed a cultural shift in how we think about ownership and collaboration. It challenges the notion that progress is best achieved through competition and secrecy, proposing instead a model where sharing and collaboration are the keys to innovation. This approach has fostered a vibrant global community of developers, users, and advocates who are committed to making technology accessible and usable by as many people as possible [Fit06].

While the open-source model has been celebrated for its innovation, collaboration, and accessibility, there are instances where it faces challenges or negative outcomes [CV17]. These can range from security vulnerabilities to sustainability issues of projects. Many open source projects struggle with sustainability, as they rely heavily on volunteer contributions and may lack the financial support needed for maintenance. This can lead to outdated software, security vulnerabilities, and project abandonment [ÅF08].

Also the myth that open source software and hardware is inherently of higher quality due to its openness has been challenged. Without rigorous quality control and active maintenance, Open Source Software (OSS) projects can suffer from bugs and reliability issues, as [MFH00] stated.

Another issue of the open source ethos can be that the open source licensing can also feature a variety of issues, as it can be a legal minefield for businesses and developers. Mixing code with incompatible licenses can lead to legal challenged and restrict the use or distribution of software as been stated in this case study [VBP+17].

2.2 Bitcoin

This section will cover a brief overview of Bitcoin[1]. How it has been introduced in 2009 and what the core concept of a peer-to-peer cash system is.

2.2.1 Introduction into Bitcoin

Bitcoin, the world's first cryptocurrency, has emerged as a groundbreaking innovation in financial technology, challenging traditional notions of currency and banking. Introduced in 2009 by an enigmatic figure or group known as Satoshi Nakamoto, Bitcoin presented a novel concept: a digital currency operating independently of central banks, using a decentralized network to verify transactions and manage the issuance of new units. This introduction delves into the origins, mechanisms, significance, and challenges of Bitcoin, offering insights into its role as a pioneer in the cryptocurrency revolution [Nak08].

Bitcoin is a cryptographic currency based on ideas from Hashcash[B+02] and b-money[Dai98] which aims to be completely distributed, free of central authorities or points of control, using a peer-to-peer network to facilitate transactions. Bitcoin itself is defined by a short white paper published under a pseudonym Satoshi Nakamoto, with a reference implementation [Nak08]. As described in [KDF13], Bitcoin is a fixed-value cryptographic object represented as a chain of digital signatures over the transactions in which the coin was used. Furthermore,

[1] In this paper, "Bitcoin" refers to the ecosystem and the blockchain, while "bitcoins" refers to the actual coins.

this paper expresses that a coin in this Blockchain can be checked for validity simply by checking the cryptographic validity of the signatures that constitute its history. Ownership of bitcoins is defined by Bitcoin addresses, which correspond to public keys within the network's cryptographic framework. Technically, a Bitcoin address does not directly hold bitcoins; instead, it is associated with a set of Unspend Transaction Output (UTXO). These UTXOs can be accessed and transferred using the corresponding private key, allowing the owner to initiate transactions. When a user sends bitcoins, they effectively create a new transaction, signing it digitally to authorize the transfer of bitcoins from their address to another.

While the protocol underlying Bitcoin allows a recipient to cryptographically verify that a transaction is a legitimate instruction to transfer funds, it does not inherently safeguard against the risk of double spending. Specifically, although the recipient can confirm that the sender previously possessed the bitcoins being transferred, there is no way to ensure that these same coins have not already been used in another transaction. To address the issue of double spending, participants in the Bitcoin network employ a peer-to-peer protocol that includes a distributed timestamping service. This service maintains a sequential record of all Bitcoin transactions ever executed, structured into a log known as the blockchain. Transactions within this blockchain are grouped into blocks, each of which includes a sequence number, a timestamp, the cryptographic hash of the preceding block, some metadata, a nonce, and a collection of verified Bitcoin transactions [Nak08][KDF13].

The blocks are linked together in a hash chain, where each block references the cryptographic hash of its predecessor. This linkage ensures the integrity of the blockchain by enabling verification that no prior block has been altered. While the blockchain features backward links from each block to the original block or genesis block, it does not contain forward links. This absence of forward links means that while there is a clear path backward from any given block to the start of the blockchain, the path forward may not be singular, giving the blockchain the structure of a tree that may branch as it expands [KDF13]. The Blockchain is shown in Figure 2.1.

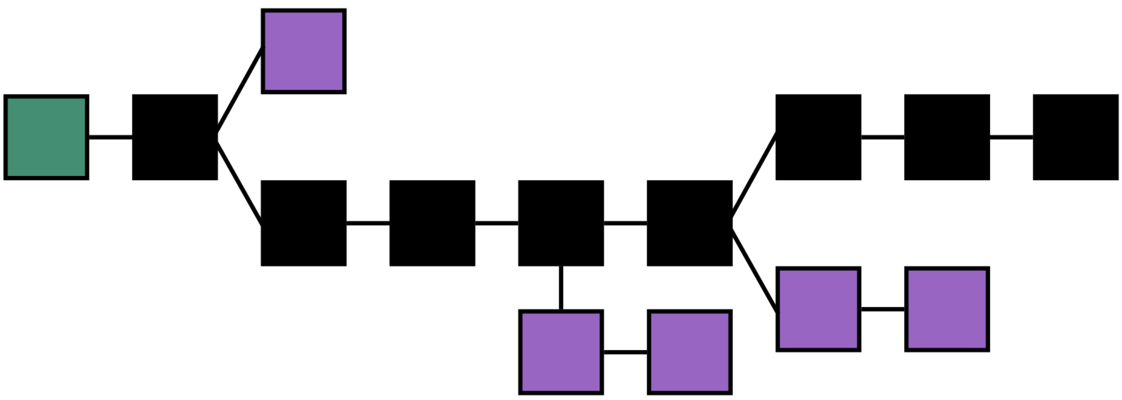

Figure 2.1: Example Blockchain. The genesis block is on the left. Mining (expanding) occurs on the longest branch.

In the Bitcoin Network, any participant has the opportunity to become a miner and contribute to the network by mining new blocks. These blocks, which append new transactions to the blockchain, are considered valid if the miner successfully selects a nonce that results in the block's hash being below a predetermined target. This requirement forms the basis of a proof-of-work puzzle, which is a computational challenge designed to be difficult to solve but straightforward to verify once completed. Successfully solving this proof-of-work puzzle serves as a demonstration that the miner has committed a significant amount of computational effort [BBH+13].

2.2.2 Origins and Philosophical Underpinnings

The inception of Bitcoin in 2009 was marked by the publication of the Bitcoin white paper [Nak08], where Satoshi Nakamoto outlined a vision for a peer-to-peer electronic cash system that would operate securely without the need for a central authority. The motivation behind Bitcoin's creation was multifaceted, rooted in a critique of the existing financial system's vulnerabilities — notably, inflation, privacy concerns, and the inefficiencies of cross-border transactions. Bitcoin's philosophical foundation is inseparable from the principles of financial autonomy, privacy, and resistance to censorship. This reflects a libertarian ethos that challenges the role of the state and financial institutions in controlling money.

2.2.3 Technological Innovation: Blockchain

At the heart of Bitcoin is blockchain technology, a distributed ledger that records all transactions across a network of computers. This technology ensures transparency, security, and integrity of data without the need for intermediaries. Each transaction is verified by network participants, known as miners, who use powerful computers to solve complex mathematical problems, a process that in turn rewards them with newly minted bitcoins. This mechanism, known as proof of work, not only facilitates the creation of new bitcoins but also secures the network against fraudulent activities.

The blockchain's immutable nature means that once a transaction is recorded, it cannot be altered or deleted, providing a tamper-proof record of transaction history. This aspect of blockchain technology has far-reaching implications beyond cryptocurrencies, with potential applications in supply chain management, voting systems, and digital identity verification.

2.2.4 The Evolution of Bitcoin

Bitcoin's journey from an obscure cryptographic experiment to a mainstream financial asset is a testament to its enduring appeal and resilience. The first known transaction with Bitcoin was the purchase of two pizzas in 2010, a milestone celebrated annually as "Bitcoin Pizza Day." Over the years, Bitcoin has experienced significant volatility, with dramatic price swings that have attracted both fervent supporters and skeptical critics. Despite this, Bitcoin has seen growing adoption as a means of payment and as an investment, spurred by increasing interest from institutional investors and recognition by major companies and financial institutions.

The history of cryptocurrency is also marked by challenges, including regulatory examination, concerns over its use for illicit activities, and debates over its environmental impact due to the energy-intensive nature of mining. Nevertheless, these challenges have also prompted discussions about potential avenues for innovation in regulatory approaches, the potential for more energy-efficient consensus mechanisms, and the broader implications of digital currencies for financial privacy and security.

2.2.5 Significance and Impact

Bitcoin's significance extends beyond its role as a digital currency. It represents a paradigm shift in how money is understood and used, highlighting the potential for technologies like blockchain to democratize financial systems and empower individuals. Bitcoin has spurred the development of thousands of other cryptocurrencies, each with unique features and potential use cases, contributing to a vibrant and diverse ecosystem of digital assets.

Moreover, Bitcoin has ignited a global conversation about the future of money, privacy, autonomy, and the role of technology in reshaping financial landscapes. It challenges traditional financial models and offers a glimpse into alternative forms of value exchange and storage, raising critical questions about trust, governance, and the equitable distribution of wealth.

2.2.6 Looking Ahead

As Bitcoin continues to evolve, its future remains a subject of intense speculation and debate. Issues like scalability, regulatory frameworks, and the advent of new technologies such as quantum computing represent both challenges and opportunities for Bitcoin. Nonetheless, its legacy as the first cryptocurrency and its role in popularizing blockchain technology are undisputed.

In conclusion, Bitcoin is not just a digital currency; it is a technological and philosophical movement that questions the very foundations of the financial system. Its development and adoption reflect a growing desire for greater control over personal financial transactions and skepticism towards traditional banking and monetary policies. Whether Bitcoin will become a universal form of currency or remain a niche digital asset, its impact on the financial industry and beyond is undeniable, paving the way for a future where digital currencies play a central role in our economic systems.

2.3 Bitcoin Mining

Bitcoin mining itself describes the process that is essential in creating new Blocks on the Blockchain. This mining process involves a mechanism called proof-of-work which is taken from Hashcash[B+02]. It describes a mechanism by an adaptive algorithm based on the recent blockchain history to maintain the long-term invariant that a newer block be mined every ten minutes on average.

Miners must find a nonce value that makes a double SHA-256 hash of the block's header be less than $\left(\frac{65535 \ll 208}{\text{difficulty}}\right)$ [BT17].

SHA-256 is designed to be non-invertable, the primary approach is to use a brute force method. Therefore, if the difficulty is twice as large, it would take twice as many brute-force tries on average to find the corresponding nonce.

The Bitcoin Mining difficulty is adjusted every 2016 blocks using the worlds total hashrate, the network hash rate, in order to target an average block-creation time of 10 minutes.

Each machine, that mines gets a correspondingly smaller fraction of the current $24 \times 6 \times 3.125 = 450$ BTCs bounty that is available per day[BT17].

2.4 Bitaxe-Project

Bitcoin introduced the world to a decentralized financial system, unlike anything before. However, the backbone of Bitcoin, blockchain technology, required a process known as mining to validate transactions and secure the network.

In the early days, mining was a simple task. Enthusiasts and pioneers could mine Bitcoin using the CPUs in their personal computers. As the network grew, so did the difficulty of mining, leading to the adoption of more powerful GPUs. This era marked the first evolution in Bitcoin mining, significantly increasing the hash rate and efficiency of mining operations.

However, the quest for efficiency did not stop there. The community saw the advent of FPGAs (Field-Programmable Gate Arrays), which offered better performance than GPUs but at a higher cost and complexity. FPGAs were a stepping stone, paving the way for a groundbreaking innovation: ASICs (Application-Specific Integrated Circuits).

ASICs were designed solely for Bitcoin mining, offering unparalleled efficiency and speed compared to their predecessors. This leap forward sparked a technological arms race, with companies and developers competing to create the most powerful and efficient miners.

The Bitaxe project, an embodiment of innovation and community-driven development in this narrative. Developed by a team of dedicated engineers and cryptocurrency enthusiasts, Bitaxe represented a significant leap forward in mining technology.

The Bitaxe project aimed to create a miner that is not only powerful but also accessible to the broader community. It featured cutting-edge ASIC chips, mainly from the already settled big ASIC manufacturers, optimized for maximum efficiency, and an open-source design that encouraged collaboration and improvement. The project symbolizes the potential of collective effort in advancing technology.

Bitaxe, previously known as DayMiner, was initially conceptualized by Skot in early 2021. The project embarked on its journey with the development of its first prototype, which made use of the BM1387 chip (an ASIC chip developed by Bitmain). This initial prototype not only proved to be functional but also laid the groundwork for the project's future innovations. As the project progressed, the team began to experiment with an array of chips, both in series and through the introduction of newer models. This phase of experimentation and advancement led to the project's rebranding as Bitaxe.

The primary goal of Bitaxe is to democratize the mining industry by focusing on the development of an open-source miner tailored for home mining enthusiasts rather than catering to large-scale industrial mining operations. This initiative is driven by the belief that the decentralization of mining efforts is crucial for maintaining the blockchain ecosystem's integrity and accessibility. Bitaxe aims to lower the entry barriers for individual miners and promote a more distributed mining network by offering efficient, cost-effective, and user-friendly mining solutions. Through these efforts, Bitaxe aspires to contribute to a more inclusive and decentralized future for cryptocurrency mining.

Below is an illustrative timeline that encapsulates the journey of the Bitaxe project from its inception to its current state 2.2.

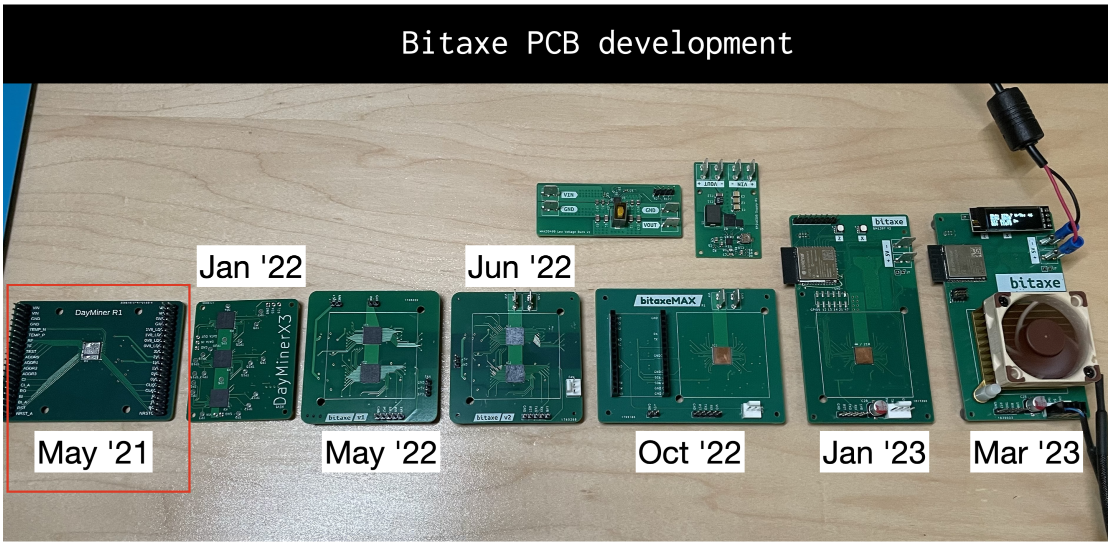

Figure 2.2: Bitaxe development [git]

2.5 Standards in the Mining Industry

While the Bitaxe project aims to transform the small-scale mining industry by empowering household mining operations, the current standard in the Bitcoin mining industry is predominantly driven by large scale operators. These operators typically fall into three different distinct categories:

1. Private Company-Driven Mining Operations: These are privately-owned enterprises that invest heavily in mining equipment and infrastructure. Their primary goal is to maximize profitability from Bitcoin mining. These companies often operate in regions with low electricity costs and favorable regulations to optimize their operations and minimize expenses.

2. Hosting Providers: These entities provide the necessary infrastructure for Bitcoin mining but do not engage in mining themselves. Instead, they lease their facilities to individual miners or small mining companies. This model allows clients to benefit from economies of scale in power and cooling without the need to manage and maintain the physical hardware themselves.

3. Public Company-Driven Mining Operations: These operations are managed by companies that are publicly traded and have access to the capital markets. They often rely on venture capital to scale their operations aggressively. They need to continuously expand their mining capabilities and ensure shareholder returns can drive significant investments in cutting-edge technology and strategic locations, influencing industry standards and practices.

Despite the diversity in the structure and scale of Bitcoin mining operations, one commonality persists across all forms: their reliance on jurisdictions and the regulations established by local and national governments. This dependency is a critical aspect of their operational strategy, as regulatory environments significantly influence the economic viability and legal standing of mining activities.

Mining operations must navigate a complex landscape of legal requirements, which can vary significantly from one jurisdiction to another. These may include licenses, tax obligations, and compliance with financial regulations, such as anti-money laundering (AML) and combating the financing of terrorism (CFT) standards.

Bitcoin mining companies must also be adept at navigating the global regulatory landscape. Changes in policies in one country can have ripple effects, influencing global Bitcoin supply and the distribution of mining power. For instance, a crackdown in a country with a significant share of the world's Bitcoin mining can lead miners to relocate to more accommodating environments, thereby shifting the geographical distribution of mining power and potentially affecting the decentralization of the Bitcoin network.

3 Requirements Analysis

This chapter will clarify the essential requirements for developing a comprehensive benchmarking framework for ASIC chips, as well as to identify the prerequisites for the potential influence of small-scale home miners on the Bitcoin network. The landscape of Bitcoin mining is predominantly controlled by large-scale mining operations and expansive mining pools, posing significant challenges for individual miners, often referred to as home miners. These challenges primarily stem from the difficulty in generating sufficient Bitcoin revenue to maintain operational feasibility.

This analysis will determine the technical and non-technical requirements and the important role of ASIC benchmarking in understanding and possibly enhancing the contributions of small-scale mining operations to the Bitcoin ecosystem.

3.1 Scenario

The scenario of the Bitcoin network is based on big mining facilities or public traded companies that do have an interest in making profit of the network and the usage of mining devices. This is in order to stay profitable and sustainable for their investors. The Bitcoin network is moving away from the basic idea of a decentralized network and is increasingly being dominated centrally by individual entities.

In order to understand the requirements, the scenario is divided into the different views of the mining industry: the view of decentralization, the mining industry in general and a potential change in the mining industry with another approach in order to decentralize the network.

3.1.1 Decentralization in the Bitcoin Network

The full decentralization of the Bitcoin network has only been implemented at the early stages of its development, largely because the concept of mining pools had not yet been developed. Initially, each miner was required to independently find a block to earn rewards, a process that yielded no compensation if unsuccessful. The development of mining pools revolutionized this approach by combining the computational power of multiple devices. This collective effort significantly increased the chances of finding blocks, ensuring more consistent rewards for individual miners, even if they did not personally solve the block puzzle. It's clear that the idea behind a merge of mining devices together to drive profitability makes sense. Eliminating the need for each miner to run their own node to be the only one to find the solution to the next Bitcoin block and still get a reward if they don't is a simple yet effective solution.

This shift not only enhanced profitability but also decreased the decentralization of mining, due to the inherent centralization of mining pools. These pools create block templates and gain control over them, which centralizes power within a few entities. To this day, joining a pool remains the most viable strategy for many miners aiming for profitability and consistent rewards. Mining pools offer a straightforward solution particularly beneficial for inexperienced users or operators of small-scale mining operations. As illustrated in Figure 3.1, the current distribution of mining pools shows that three major pools control over 60 percent of the network's total hash rate.

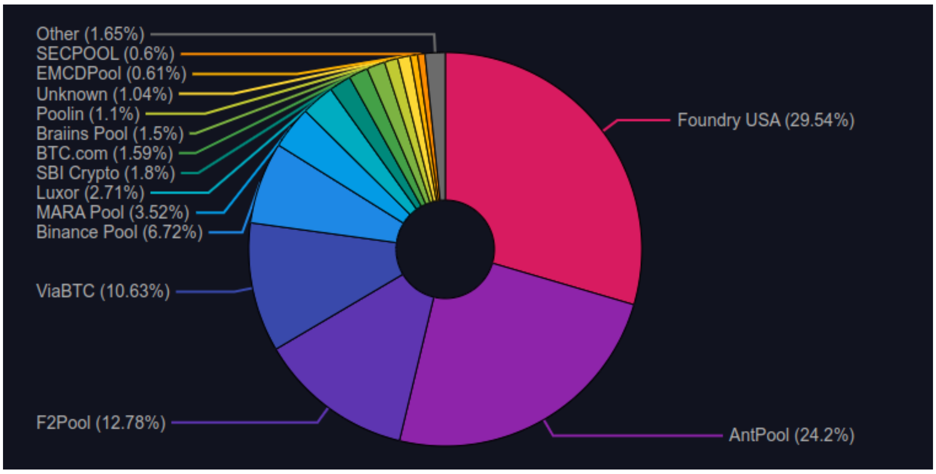

Figure 3.1: Mining Pool Dominance by [Mem]

The drive for profit persists. However, with this centralization, the Bitcoin network is deviating from its fundamental tenet of a decentralized solution.

3.1.2 The current Mining Industry

The mining industry is driven by a small number of manufacturers of ASIC chips and mining devices. Currently, there are four major Bitcoin ASIC manufacturers, all of which produce proprietary hardware. This complements the previous doubts about the decentralization of the network. As stated in Section 2, the Bitcoin network aims to eliminate the need for centralized entities, so this centralization in manufacturing and operation is counterintuitive.

This should not be taken in a judgmental way, but rather highlights the problem in this industry.

3.1.3 Eliminating the Need of Centralized Mining

The elimination of centralized mining facilities and pools is more of a theoretical aspect. No one can expect a company or any other entity to work for free. The so-called solo mining dilemma involves the critical aspect of not making a return on expenses and is therefore more of wishful thinking.

However, it is one approach to solving the centralized dilemma that the Bitcoin network faces with large mining pools. A more comprehensive approach would be to create a large number of small mining pools in order to increase the number of entities that run a mining pool and are still profitable, so that miners and companies do not face losses in the long run. It requires small-scale mining equipment, such as the open-source Bitaxe, which must therefore be operated as efficiently as possible to decentralize in every way, both on the pool side and on the operational side.

To achieve this drive for efficiency, it is necessary to understand how efficiency is calculated and what can be done to increase it.

3.2 Objectives

The following objectives will set out the core work of this thesis.

- 1. Benchmarking Tool Development for Bitaxe
- 2. Theoretical Analysis of small home miners impact on the Bitcoin network

The current state of the Bitaxe open-source miner features the ability to use an already developed ASIC chip manufactured by Bitmain, controlled by an ESP32, to mine Bitcoin. The software, that runs on the Bitaxe, allows a management of the frequency as well as the voltage provided to the ASIC chip. In order to use the ASIC chip as efficient as possible, the potential User would need to manually go through multiple different combinations of frequency and voltage assigned to the ASIC chip in order to find the most efficient setting for that specific ASIC chip. This approach allows us to calculate the required wattage per Terahash, a metric which is frequently employed. One such metric is J/Th (Joule per Terahash).

3.2.1 Benchmarking Framework Development

The Bitaxe Projects's benchmarking framework is an essential component designed to enhance the performance and efficiency of ASIC chips used in Bitaxe devices. This section dives into the framework's objective, the selection process for ASIC chips, the key benchmarking parameters, the development tools and techniques utilized, and the approach to testing and validation. This comprehensive framework ensures that Bitaxe devices operate at their optimum.

The primary objective of the Bitaxe benchmarking framework is to systematically evaluate the performance of various ASIC chips within the Bitaxe devices, identifying the most efficient configurations. This effort aims to maximize computational efficiency, reduce energy consumption, and ensure the scalability of Bitaxe technology.

The selection process for ASIC chips involves an exact evaluation of their performance characteristics, but will mostly be driven by the availability and usability of those in already created Bitaxe derivates that use such a chip.

The framework employs a comprehensive set of benchmarking parameters designed to evaluate the ASIC chips' performance thoroughly. These parameters include:

- Hashrate
- ASIC frequency
- ASIC voltage
- ASIC temperature

These parameters have been chosen in order to represent the most crucial for assessing their performance. The **hashrate** is a direct measure of the performance of a mining device. It allows for straightforward comparison between different ASIC models and configurations, providing a baseline for evaluating relative mining power. The **ASIC frequency** directly impacts the hashrate, as higher frequencies can potentially allow more hashes per second. Higher frequencies may yield higher hashrates but often at the cost of increased power consumption and heat production. Benchmarking frequency helps in finding the optimal balance for maximum efficiency. The **ASIC voltage** is the electrical power supplied to an ASIC, which influences its frequency and operational stability. Voltage levels directly correlate with energy consumption. Understanding how voltage affects power usage is vital for assessing the ASIC's cost-effectiveness. Lastly, the **ASIC temperature** is the operational temperature of the ASIC during mining. It is a critical parameter that affects the reliability and durability of ASIC hardware. Excessive heat can degrade performance over time and lead to hardware failure.

The benchmarking framework should feature the following aspects to ensure a thorough evaluation and continuous improvement of ASIC chips used in Bitaxe devices:

Comprehensive Evaluation Criteria
1. Performance Metrics: Include detailed metrics such as hashrate, frequency, voltage, and temperature, which provide an integrated view of each ASIC chip's capabilities and limitations.
2. Efficiency Indicators: Measuring energy efficiency ratios to assess the trade-offs between power consumption and output performance.

Advanced Analytical Tools
1. Automated Data Collection: Utilization of an automated system for data gathering to minimize human error and increase the reliability of the data collected.
2. Dynamic Testing Ranges: Testing and data gathering under a variety of environmental conditions and operational loads to identify potential performance issues under real-world stress conditions.

Open Source Collaboration
1. Community-Driven Development: Leveraging the Bitaxe development community for ongoing testing, feedback, and improvements. This ensures that the framework remains relevant and effective.
2. Transparency and Accessibility: The framework's methodology, data and results should be openly available to encourage transparency, peer review and broad participation.

Scalability and Flexibility
The framework should be able to handle increasing amounts of data and more complex

analysis as the number of Bitaxe users grows.

The testing and validation phase is critical to the benchmarking framework, ensuring that the findings are accurate and reflective of real-world conditions. Therefore, this will involve Field testing with the help of the development community of the Bitaxe project in order to gather device metrics under typical operational conditions.

The overall goal is to create this framework to prove or disprove the aspect of increasing the efficiency of these ASIC chips as well as to propose an open source approach to this specific topic. There is already developed propitiatory benchmarking software available, but it does not provide any insight into this, therefore an open source one needs to be developed.

3.2.2 Theoretical Analysis of Small-Scale Miners' Impact

This section states a theoretical requirement analysis of the impact small-scale miners have on the cryptocurrency ecosystem, particularly focusing on the Bitaxe Project. By examining various dimensions such as data collection methods, analytical models, underlying assumptions, and the expected impact areas, this analysis aims to clarify contributions and challenges posed by small-scale miners.

The primary objective of this theoretical analysis is to understand the role and influence of small-scale miners within the Bitaxe ecosystem. It seeks to evaluate both the quantitative and qualitative contribution of these miners, assessing how they affect network security and decentralization.

To conduct a comprehensive analysis, data collection will focus on several key areas:

- Hash Rate Contribution
- Geographical Distribution
- Economic Models

The analysis operates under several key assumptions, it presumes equal access to mining technologies and information, allowing small-scale miners to operate effectively. This analysis assume that small-scale miners are motived by both profit and participating in the small-scale miner ecosystem, contributing to its security and decentralization.

Technical and non-technical requirements from the backbone of any software developments project, guiding the creation, implementation, and evaluation of systems like the Bitaxe benchmarking framework. Understanding these requirements is crucial for this thesis to ensure the end product functions as intended but also meets the needs and expectations of its users and developers.

3.3 Technical Requirements

Technical requirements detail the specific technical specifications that software must meet to achieve its intended functionality. These include aspects related to software architecture, data management, security protocols, system integrations, performance benchmarks. In the Bitaxe project, technical requirements would outline how data aggregation should be implemented, the use of a relational database for storing inputs, and ensuring that the data aggregation processes does not interfere with other system tasks.

Technical requirements are as followed:

- FreeRTOS Task Implementation for Data Aggregation
- Relational Database Usage
- Anonymity in Data Aggregation
- Non-interferenece with other tasks

FreeRTOS is the Framework the Bitaxe Firmware is build on top of, therefore an implementation into this Framework would be needed. The data aggregation shall happen in a relational Database in order to ensure data integrity and reusability. To protect the data of each user or device, the data aggregation needs to be anonymous. It is important that these data items are stored and reused in a manner that ensures the confidentiality and anonymity of the individuals to whom they relate. To ensure the data aggregation does not interfere with other tasks or manipulates any outcome of the aggregated data, an examination of the impact is needed.

3.4 Non-technical Requirements

Non-technical requirements, on the other hand, focus on the user experience, accessibility, and overall impact of the software on its target audience. These might include requirements for user-friendliness, minimal impact on device performance, compliance with data privacy laws, and provisions for user documentation and support. For the Bitaxe project, ensuring that the framework is accessible to all users and does not noticeably affect the device's performance are key non-technical considerations.

- User-Friendly Usability
- Transparency and Control of Users
- Accessibility
- Documentation

Ensuring the benchmarking framework and any associated software are designed with a focus on user-friendliness. Users of all technical backgrounds should find the system intuitive and easy to navigate, encouraging widespread participation and reuse. While maintaining the invisibility of the data aggregation process to users, provide transparency regarding what data is collected and how it is used. Making the framework and implementation and its outputs accessible. The documentation should include instruction guides and the explanation of the implementation.

Both technical and non-technical requirements are needed to create a comprehensive framework that not only functions efficiently, but is also user-centric.

High Priority requirements were considered essential for the fundamental functionality and performances. These requirements were necessary to achieve the primary objectives of the project and to ensure that the devices could operate effectively within the specified parameters. It is evident that the achievement of the core goals of the project is contingent upon the fulfillment of these requirements.

Medium Priority requirements were identified as important elements that should be addressed to provide the fundamental usability of the anticipated outcome.

Low Priority requirements were considered optional features or enhancements which could add value but were not essential to the project's success.

Requirement	**Description**	**Priority**
Performance Metrics	Include detailed metrics such as hashrate, frequency, voltage, and temperature.	High
Efficiency Indicators	Measure energy efficiency ratios to optimize operational costs and environmental impact.	High
Anonymity in Data Aggregation	Anonymize data collected in order not to bias a specifc metric.	High
Automated Data Tools	Utilize automated systems for reliable data collection.	Medium
Transparency and Openness	Maintaining a high level of transparency and publish all data and code afterwards	High
Community Development	Leverage community feedback for ongoing framework improvements.	Low
Field Testing	Integrate field testing phases.	High
Analytical Simulation	Create analytical models to evaluate the impacts of small-scale mining on the Bitcoin network	High

Table 3.1: Prioritized Requirements for the ASIC Benchmarking Framework

Requirement	**Description**	**Priority**
User-Friendly Usability	How good it is usable for the User	Low
Transparency and Control of Users	Adjustable in every manner for the user and code openness	Medium
Accessibility	Transparency regarding what data is collected and how it is used	High
Documentation	Documentation should include instruction guides and the explanation of the implementation	Medium

Table 3.2: Non-Technical Requirements

Requirement	Description	Priority
FreeRTOS Task Implementation	Implementation into the FreeRTOS code basis for Data Aggregation	High
Relational Database Usage	Usage of a relational Database in order to assign data correctly	High
Anonymity	Store all the Data in a manner that there are no conclusion on who provided them	High
Non-interferenece with other tasks	The Task for the Data collection and sending shall not interfere with any other task	Medium

Table 3.3: Technical Requirements

4 State of Research

As Bitcoin continues to assert its relevance in both financial markets and the broader socio-economic landscape, understanding its underlying mechanisms-particularly bitcoin mining-has become a central area of academic and industrial research. This introduction provides an overview of the current state of research on bitcoin, focusing on the processes of bitcoin mining and the standards that govern the mining industry.

4.1 Standards in the Bitcoin Mining Industry

As the Bitcoin mining sector matures, it becomes increasingly influenced by a complex web of industry standards, regulatory requirements, and operational best practices. These elements not only dictate the sustainability and profitability of mining operations but also shape their strategic decisions and technological innovations. To gain deeper insights into these dynamics, an interview was conducted with the CEO of D-Central, a prominent mining hosting provider in Canada. The discussion provided valuable perspectives on how regulations, jurisdictions, power supply considerations, and security measures play pivotal roles in the industry [Wan24].

Based on insights from the CEO of D-Central, this section will explore the intricate standards that govern various aspects of their mining operations. These include general operational standards, regulatory compliance, security protocols, and the efficiency of mining hardware. Each category plays a vital role in shaping the practices and policies of mining entities, reflecting their adaptability to the technological, legal, and security challenges presented by the cryptocurrency mining industry.

4.1.1 General Standards

General standards in Bitcoin mining encompass best practices that guide daily operations, maintenance, and the overall management of mining facilities. These standards are more applicable to large mining operations and are only applicable in this area. Based on the insights from the interview [Wan24], there tend to be big differences from region to region. General standards don't seem so easy to define. Most standardizations come from regulatory areas. What are the requirements, for example in the area of power consumption or regulations in the area of noise volume, but also how revenues are to be treated. This would suggest that companies should implement best practices when operating in this area. Moreover, they need to stick to their social responsibilities. They rely heavily on the already built infrastructure and need to apply to their given rulesets.

While there seems to be no standards in the mining facility area, there are a couple of standards in the general Bitcoin mining ecosystem, from the protocol Bitcoin mining relies on to the payout scheme system of pools. Bitcoin's Stratum V1 protocol is a communications protocol designed primarily for pooled cryptocurrency mining. While individual Bitcoin miners could originally compute the proof of work independently, the increasing difficulty of mining made it nearly impossible for solo miners to compete with larger mining operations. The Stratum protocol was designed to allow miners to efficiently connect to a mining pool server [RC17]. Today, Stratum V1 is the protocol used by all mining devices to communicate with mining pools, it's the de facto standard in the mining industry. While there are potential improvements to be made, a proposal called Stratum V2 has been made, which will not be covered in this work.

Stratum V1 does feature the following:
Job Distribution: Efficiently distributes the work required for proof-of-work calculations from a central pool server to connected mining devices.
Minimized Bandwidth Usage: The protocol reduces bandwidth usage by minimizing the data required to start mining and the data sent for each share submission.
Work submission and results reporting: Facilitates communication from miners back to the pool regarding their progress on the current mining task and the shares they have completed.
Security: Originally, Stratum V1 did not focus heavily on security features, leading to vulnerabilities such as man-in-the-middle attacks. Subsequent enhancements and releases aim to address these security concerns.

The protocol operates over TCP or a similar connection and provides miners with continuous updates for block mining without the need for repeated polling. This efficiency is critical to ensuring that all miners in a pool are working with the most up-to-date block information, especially in a competitive mining environment where time to find a new block is critical.

Another standardized item in Bitcoin mining is the payout scheme used by pool mining operations. There are three main payout schemes that have been used to a greater or lesser extent and are commonly used today. There are a few other different payout schemes, but they never reached the broader community.
Bitcoin pool mining payout schemes are methods by which mining pools distribute rewards to their members based on their contributions to solving a block. These schemes are critical because they directly affect the profitability and incentive for miners to contribute their hashing power to the pool.

As expressed in: A Survey: Reward Distribution Mechanisms and Withholding Attacks in Bitcoin Pool Mining[ZLL+18] payout schemes do have advantages and disadvantages. The commonly used payout schemes are: Pay-Per-Share, Pay-Per-Last-N-Share and Full-Pay-Per-Share, as of 2024.

Pay-Per-Share Under the Pay-Per-Share (PPS) scheme, miners are paid a fixed amount for each share they submit, which represents a cryptographic proof of work that their mining hardware has solved. The payout is calculated based on the average probability of finding a block. Pay-Per-Share (PPS) was the most common distribution mechanism used in open pools a few years ago. In a PPS system, regardless of how many shares are submitted in a round, as long as a miner submits a share, he is immediately rewarded according to his expected contribution. [ZLL+18].

Pay-Per-Last-N-Share PPLNS is a more complex version of the proportional model. Miners are paid based on the last N shares, not just the current round. If a block is found, the reward is calculated based on the shares submitted during the window, regardless of round boundaries.

Full-Pay-Per-Share The Full Pay-Per-Share (FPPS) payout scheme is a more comprehensive adaptation of the traditional Pay-Per-Share (PPS) model. It has become increasingly popular among Bitcoin mining pools due to its balanced approach to reward distribution. The FPPS model extends the PPS approach by incorporating block transaction fees into the payouts. Under PPS, miners are typically only compensated for the block reward, which is the fixed amount of new bitcoins generated by mining a block. However, with FPPS, miners also receive a share of the transaction fees collected from the transactions included in the block. This approach provides a more comprehensive compensation that reflects the total actual earnings from both the block reward and the transaction fees [ZLL+18].

4.1.2 Regulatory Requirements

While Bitcoin mining presents some challenges, regulations can limit or impact operations and business models like D-Central's. One of the important factors about mining facilities is their use of already established infrastructure. This means that companies or mining operations in general have to work closely with the regulatory requirements and there is a certain degree of dependency as the CEO of D-Central stated [Wan24]. Some regions are oversaturated of their power limitations and with the example of D-Central their region does have issued a stop for new mining operations due to their limited capability power resource.

These regulations can substantially limit the growth of companies in the mining industry. Some regions also maintain a critical view in general about Bitcoin mining and its entail of their power consumption. As stated in The Current Status of Cryptocurrency Regulation in China and Its Effect around the World[Ril21], China banned most of the mining operations in 2018 in order to maintain a regulatory approach of cryptocurrency. Their official statement about this is the protection of private entities, and they refuse to accept cryptocurrencies as a legal tender.

Whether regulatory requirements may produce an impact on the mining industry differs from region to region. Therefore, is it necessary to view on mining operations that might be protected from such a regulatory approach.

4.1.3 Security Measures

In an industry where digital assets represent high-value targets for theft and cyber-attacks, robust security measures are indispensable. This part will outline the security protocols and systems D-Central employs to safeguard their operations and assets, both physical and digital.

While Bitcoin mining seems to be a profitable and easy to opt in business, these machines (miners) they have a physical value and therefore need to be protected against any harm.

D-Central implemented different security standards along the way to counter these parts. For example, they do not disclose their facility location in order to protect their mining hardware from theft. In addition, D-Central has various security systems that are designed redundantly. It plays an important role that these systems are both physical and digital in nature.

4.1.4 Efficiency of Hardware

One of the most important factors about Bitcoin mining is the efficiency of the hardware used. This is the driving factor for the sustainability to keep an operation in facilities, no matter what size, up and running.

The hardware itself tends to not disclose any sort of standard. As an individual or a mining company, you rely on the manufacture given standards and apply them. There is no real room for improvement, just plug these machines in and let them work. Whilst talking about efficiency, it is indeed possible to apply certain settings to those machines in order to drive them more efficiently. It is not necessary to delve deeply into the technical aspects of this process; rather, it can be viewed as a means of regulating the speed of the machine, which can be adjusted according to the parameters illustrated in Figure 4.1. This might not apply as a standard and is more of a tinkering process, as the CEO of D-Central disclosed, but it is a way a company or any other mining operator can apply in order to formalize their operation and the incurred costs of mining.

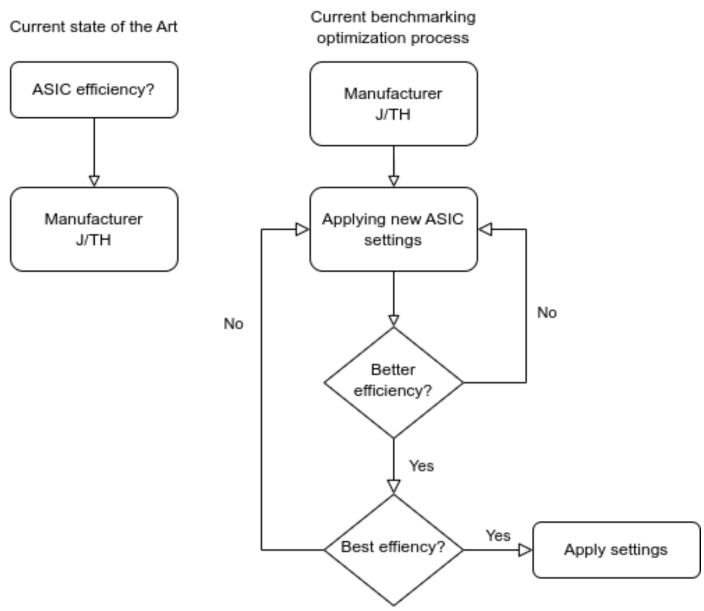

Figure 4.1: Current process of optimizing ASIC devices

Furthermore, the identification of potential alternative sources of energy represents a pivotal aspect in the advancement of companies such as D-Central. The dual-purpose utilization of surplus energy represents a significant driving factor in the necessity to adapt to the current market standards. As an example, D-Central does use stranded gas in order to mitigate the negative impact of gas companies and make use of an already but not used waste product.

Proprietary Software BRAIINS
Braiins is a company that produces proprietary control board hardware and software for these boards, offering more advanced functionalities than the standard firmware included with the original Antminer Bitcoin Miner Hardware. A key features of their *Braiins OS* is the *Autotune* functionality, which allows users to automatically tune each ASIC chip on their mining device individually to achieve maximum efficiency [Bra].

Braiins describes their autotune functionality as followes:

> "The idea behind autotuning is simple: if all the chips in a mining rig are unique, we should treat them as such. Rather than having uniform frequencies across all chips in the machine, we use a trial and error "tuning" process to determine the quality of each chip. Higher quality chips can perform well with higher frequencies and produce more hashrate.
>
> Lower quality chips don't produce as much hashrate per Watt, so we give those chips less work to do. By automatically finding the optimal settings for each chip, we help you utilize the full potential of your hardware at whatever power consumption level you set it to" [Bra].

This process is further visualized in the following graphic:

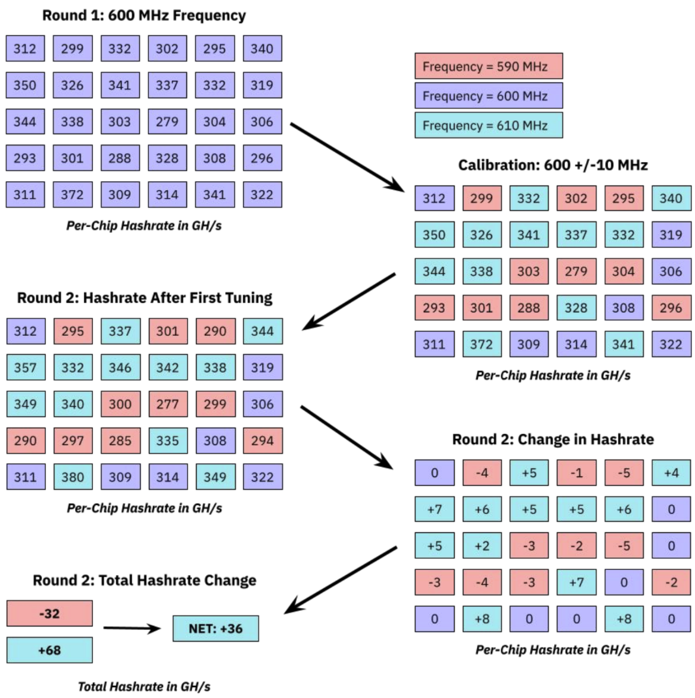

Figure 4.2: Braiins Autotuning Process [Bra]

> "In the illustration on the previous page, you can see the (oversimplified) logic of

> the autotuning process. It starts with some universal settings for frequencies and voltages to see how each chip performs, then begins calibrating per-chip settings based on those results. Now imagine that instead of just +/- 10 MHz frequency adjustments and a single round of tuning, you have possible adjustments of +/- 5, 10, 15, or 20 MHz per chip across hundreds of chips per machine.
>
> It's a process, and the results aren't going to be the same for every machine. Some machines will be in better condition, perhaps better located in the facility for cooling, and with higher quality chips. Those machines might see a 15percent+ improvement in J/TH efficiency while others will only improve by 5percent with the exact same configuration on Braiins OS+. Again, every ASIC is unique" [Bra].

The concept and process align with the previous manual optimization process, as represented in Figure 4.1. However, due to its proprietary nature, it is unclear if this software collects any information about the machines or the network to which they are connected. The Braiins software, which was previously a cornerstone of open-source Bitcoin mining, no longer aligns with many of the high-priority requirements, outlined in Section 3. Although Braiins continues to provide comprehensive performance metrics, efficiency indicators, and robust field testing capabilities, it is deficient in transparency and openness, given that it is no longer open-source. This transition constrains the user's control over settings and code, which is at odds with the Bitaxe project's requirement for complete transparency and community-driven development. Furthermore, while Braiins offers automated data tools and thorough documentation, its lack of emphasis on data anonymization and non-specific support for FreeRTOS and relational databases presents additional challenges. Consequently, while Braiins meets some technical requirements, its inability to fully comply with the core principles of transparency, user control, and community engagement necessitates the exploration of alternative or custom solutions for the Bitaxe project.

4.2 Small-Scale Mining Operations

A different approach to the large mining facilities or publicly traded bitcoin mining companies is to mine with small-scale in hash rate mining equipment. Therefore, anything below 1 Petahash is considered a small-scale mining operation in this thesis, due to a non-existence of any definition of small-scale mining operations.

Small mining operations are usually built and maintained by private individuals who either connect their small farm (all of these mining devices together are called a farm) to a pool to receive daily or weekly payouts to pay for electricity, or they try to solo mine (solve the next block puzzle by themselves), which has a low probability of success.

The distribution of the Bitcoin mining hashrate is a critical factor in understanding the network's resilience and vulnerability. Currently, a significant portion of Bitcoin's total computational power is concentrated within a few large mining pools as shown in Figure 3.1. This concentration poses potential risks to the network, including increased vulnerability to attacks and the influence of central entities on the protocol's decisions. Nevertheless, the emergence of small-scale mining farms offers a potential means of counterbalancing this trend and further decentralizing the network, thereby reinforcing the foundational principle of distributed control.

As expressed in [Pag18] potential attack scenarios may be denial of service or censorship. As yet, no successful large-scale attacks against Bitcoin have been recorded and, therefore, a full empirical description is not available [Pag18]. Nevertheless, it can be argued that the Bitcoin network is already facing some form of censorship, with the denial of transactions that contain additional data and are not directly linked to the transaction in- and output. The recent activation of the ordinals and runes protocol has prompted some individuals and large pool operators to attempt to censor this data. It can be argued whether this constitutes an enhancement for the blockchain, but censorship already occurs in this manner.

The potential attack scenario of major mining pool and facility operators is not yet fully understood. Consequently, this topic must be discussed in order to gain an appreciation of the risks involved in using and growing centralized mining operations.

In order to mitigate the potential impact of these attacks, small-scale mining operations may be able to adopt strategies to counteract this behavior. The decentralization of the network hashrate and the operation of numerous small-scale facilities may serve to mitigate the potential risk of censoring transactions. To date, no papers have been published on small-scale mining operations. This work introduces these operations in order to demonstrate their potential.

5 Conception of a Benchmarking Tool and Small-scale Miners Outcome

This chapter will examine the conceptualization of the idea of developing a Benchmarking Framework for small-scale miners and the conceptualization of a theoretical analysis of the potential impact small-scale miners might have on the ecosystem, decentralization, and security of the Bitcoin network.

The concept implies all previously defined basics of Section 2 about Bitcoin mining which also, among other things, defines the structure of this chapter. Moving onward, Section 5.1 will examine the specific Areas of Application for the Benchmarking framework. Further essential aspects include the benchmarking parameters in Section 5.2.1 as well as the data collection in Section 5.2.2 which will outline the content of data that's going to be stored. Section 5.2.3 will describe the process of storing the data, and Section 5.2.4 will be an aggregation approach to interpret the stored data.

The concept will not only clarify the technical aspects and parameters of the benchmarking framework but also present a theoretical analysis approach of the potential impact of small-scale mining farms and devices, such as the Bitaxe, on the bitcoin network. In Section 5.3 we will examine the potential capabilities of small-scale mining operations in terms of economical and hashrate implications. Additionally, we will explore the concept of decentralization, which is particularly relevant in the context of small-scale mining operations, in Section 5.3.1. Lastly, Section 5.3.2 will analyze the potential outcomes of such operations.

The primary objective of developing a benchmarking framework for the Bitaxe device is to establish standardized procedures and metrics for evaluating the performance and efficiency of this specific mining hardware. This framework will enable consistent, objective, and replicable testing of the device under various conditions, providing potential users with reliable data on its operational capabilities.

The objective of the theoretical analysis is to investigate the potential consequences of the widespread adoption of small-scale mining devices, such as the Bitaxe, on the larger Bitcoin mining ecosystem. This analysis will consider both the technical and economic implications, with a particular focus on the impact of such devices on the decentralization and security of the network.

5.1 Areas of Application

The rapid evolution and diversification of ASIC technologies necessitate the development of a robust framework to assess and compare their performance. This section outlines the application area of a benchmarking tool designed specifically for ASIC devices, focusing on its impact, utility, and alignment with open-source principles. The benchmarking tool is designed to adhere to open-source and non-proprietary software principles. This approach fosters a collaborative environment where developers and users can contribute to its improvement, adapt it to new needs, and share insights freely without the constraints of licensing fees or proprietary restrictions. This approach not only accelerates innovation but also promotes a more democratic and inclusive mining community.

The tool's provision of dependable and accessible performance data facilitates the creation of a more transparent and competitive market for mining hardware. This transparency serves to prevent market monopolies and ensures that advancements in ASIC technology benefit the broader community rather than a select few.

In light of the growing emphasis on sustainable mining practices, the tool can assist in identifying the most energy-efficient ASICs, thereby guiding miners towards choices that reduce their environmental footprint. This is becoming increasingly important as societal demand for environmentally responsible mining practices continues to grow.

Although the current application is limited to open-source developed Bitcoin mining hardware, it could potentially benefit the broader community by enhancing and adapting such a tool for other hardware in general. The current landscape of ASIC device benchmarking is largely dominated by simplistic metrics such as hashrate-to-wattage ratios. While this provides a basic measure of efficiency, it falls short of capturing the full spectrum of factors that influence ASIC performance and operational sustainability. Additionally, the de facto tools and software available for benchmarking are proprietary, developed by entities such as BRAIINS, which do not provide open access to their methodologies or software, limiting both transparency and collaborative improvements.

The area of application is therefore set to be around projects like the Bitaxe or QAxe (which is a derivate of the Bitaxe project with slight modifications and the use of 4 ASIC chips instead of only 1). By embracing open source values, it ensures wide accessibility and contributes to the ongoing decentralization of mining power.

5.2 Benchmarking

As explained in Section 4.1.4 the current state of optimization of ASIC chips is either a hard trial and error process, which has been illustrated in Figure 4.1 or the use of proprietary software such as BRAIINS auto-tune functionality, which is therefore not publicly available for the broader community. The efficiency of these chips is typically quantified as $\sum\left(\frac{J}{TH}\right)$, representing the energy efficiency ratio of joules to terahashes.

While the fundamental concept of the optimization process cannot be changed, given that it is the sole means of determining the efficiency of such hardware, it is possible to automate this process in order to achieve comparable outcomes in a significantly shorter timeframe. By reducing the time required and the overall procedure, this may be able to not only achieve quicker results but also greater accuracy, as automation can perform frequency and voltage changes with greater speed and reliability than a human being could.

At the most fundamental level, a benchmarking tool serves to enhance transparency within the cryptocurrency mining industry. The provision of objective and verifiable data on the performance of mining devices serves to clarify the capabilities of hardware sold to the public. This transparency is of paramount importance for the establishment of trust between manufacturers, miners, and consumers particularly in an industry that has been the subject of criticism for its opacity.

In a broader environmental context, the ability to measure and compare the energy efficiency of ASIC miners encourages a shift towards more sustainable mining practices. As energy consumption becomes a more visible and comparable metric, manufacturers and miners are motivated to prioritize efficiency in order to reduce both costs and environmental impact. In particular, allowing open-source developed mining devices, such as the Bitaxe, to gain access to the devices of small-scale miners and to measure their efficiency may potentially benefit the community and encourage more people to adopt a general approach to trust issues.

5.2.1 Benchmarking Parameters

Establishing clear and comprehensive benchmark parameters is not only a technical requirement but a strategic necessity. These parameters serve as the foundation for accurate assessments of the ASIC capabilities, guiding a potential user in their decision-making process. By quantifying key aspects such as efficiency, power consumption, stability, heat generation, voltage usage and current usage, benchmarks enable the ability to compare different ASICs objectively, and may drive innovations that meet the evolving demands of the market.

The utilization of these parameters will facilitate the formulation of informed decisions and enable the identification of the most optimal utilization for a specific ASIC. To clarify the need of these parameters, their importance will be described in the following.

Stability: One of the most crucial considerations in evaluating the suitability of a device is its stability. It is not beneficial if the device is highly efficient for a brief period of time but lacks stability and repeatedly reboots or experiences fluctuations in the power provided to the ASIC. Consequently, this parameter should be accorded the highest priority in the subsequent evaluation of all parameters.

Hashrate: The hashrate is one of the most crucial parameters for benchmarking an ASIC chip. It is desirable to achieve a high hashrate in order to optimise the performance of an ASIC chip. However, this comes at a cost in terms of power consumption, which will be given equal consideration alongside the power consumption of the chip itself. Furthermore, it is necessary to consider whether high hashrate and high power consumption result in an increase in temperature, which could have a negative impact on the efficiency of the chip itself.

To express this typically, higher hashrate H indicates greater computational power and hence higher power P usage, which can be express as:

$$P = f(H) \tag{5.1}$$

where f represents a function that models how power consumption increases with hashrate.

Power consumption and heat generation: The driving factors of stability and hashrate are inversely related to power consumption. This factor is likely to have been overlooked, yet it is of great importance to the overall operation and the efficiency and usability of an ASIC.

As expressed previously with higher hashrate comes greater power consumption which inevitable leads to higher heat generation. The relationship between power consumption P and heat generation Q can be modeled as:

$$Q = x \cdot P \tag{5.2}$$

where

- Q is the heat generation (measured in watts, W),
- x is a proportionality factor (dimensionless),
- P is the power consumption (measured in watts, W).

Frequency: In general, the hashrate output of an ASIC chip is directly proportional to the frequency of the chip's clock. Nevertheless, higher frequencies typically require higher voltages to maintain stability, and the relationship between voltage, frequency, and power consumption is non-linear.

The direct relationship between hashrate H and frequency f can be represented as:

$$H = k \cdot f \tag{5.3}$$

where k is a constant representing the hashrate per unit frequency.

Voltage: The voltage plays a crucial role in the stability of the frequency applied to the ASIC chip and is therefore a parameter that needs to be considered. Power consumption P in electronic circuits is often modeled by the equation:

$$P = V \cdot I \tag{5.4}$$

where

- P is the power consumption (measured in watts, W),
- V represents the voltage (measured in volts, V),
- I represents the current (measured in amperes, A).

Integrating these to model the hashrate output as a function of both frequency and voltage:

$$H = \chi(f \cdot V) \tag{5.5}$$

where

- H is the hashrate (measured in hashes per second, 1/s),
- $\chi(f, V)$ is a function representing the characteristics of the ASIC chip.

- f is the frequency (measured in hertz, Hz or 1/s),
- V is the voltage (measured in volts, V).

The characteristics of the ASIC are more on the hardware side and would require a more detailed examination of the manufacturing process of an actual ASIC chip. In this equation, however, they are simply represented as the characteristics and be given as a fact.

This set of equations provides a fundamental theoretical framework for understanding and optimizing the performance of ASIC chips based on their operating frequency and voltage.

5.2.2 Data Collection

The data collection process is the mandatory processes in order to gather data for later interpretations of such, the concept of that will be later discussed in Section 5.2.4.

The data collection process is divided into three primary phases: controlled laboratory tests, field deployments, and long-term performance monitoring. Initially, controlled laboratory tests will be conducted to determine the device's baseline performance characteristics, including power efficiency, hash rate, and thermal management under standardized conditions. Following laboratory assessments, the Bitaxe device will be subjected to field testing in real-world mining environments with the objective of evaluating its operational stability and robustness over extended periods. Finally, long-term performance monitoring will be implemented to track the device's endurance and efficiency over time. This will involve the collection of data on wear-and-tear, possible maintenance needs, and potential for performance degradation.

The process must be automated to prevent the user of a Bitaxe or QAxe from making any changes to the data independently. In order to achieve the desired outcome, an implementation into the existing Bitaxe code would be necessary.

5.2.3 Data Storage

The data storage needs to ensure its integrity, accessibility, and security. The choice of data storage solutions and the design of the data architecture are critical to the success of the benchmarking framework, as they directly impact the ability to analyze, share, and replicate findings.

The importance of robust data storage is crucial for several reasons:

- The reliability of the benchmarking results depends heavily on the accuracy of the data stored. Therefore any corruptions or loss of data could lead to false conclusions and flawed analyses
- It must be possible for others in the community to repeat and verify the results. This requires that the data must be stored in a manner that is accessible.
- As the potential volume of data grows, the storage solution must scale accordingly without loss of performance.

While these requirements need to be addressed, there are two potential solutions that achieve an optimal balance of accessibility, security, and cost-effectiveness.

Local Storage: This approach can be immediately used with high-speed access to raw data during testing phases. Local storage will reduce the expenses on a data collecting and storage system by the fact that the hardware already exists and doesn't need to be purchased or rented. On the other hand, adds complexity to the process as soon as field-testing will be used. The data must be sent to a specific IP address, which could cause issues, or does add up the complexity by the need of a dynamic-DNS service.

Cloud Storage: Cloud services offer robust disaster recovery capabilities, scalability, and remote access. This is particularly important for ensuring that data can be accessed by other researchers and for backing up data against local hardware failures. Cloud services therefore offer great flexibility and ease of use, no maintenance needs, but they come in at a cost.

Consequently, a comprehensive examination of the relevant factors is necessary in order to ascertain the optimal choice. Both options are viable and present a range of advantages and disadvantages.

5.2.4 Data Aggregation

The data aggregation process is crucial for this thesis to achieve reliable data based on raw data provided by others. This process requires a thoughtful consideration of the most effective approach for the data to achieve the intended outcome. Effective data aggregation not only enhances the quality and reliability of the data but also ensures that subsequent analyses are grounded in accurate and representative information.

The objective is to define a set of criteria that ensure data consistency, accuracy, and relevance. This includes considering how data from different sources might interact, the impact of aggregation techniques on data quality and the implications for the overall validity of the research findings.

5.3 Theoretical Analysis of Small-scale Miners

The second part of this thesis will focus on a theoretical analysis of small-scale miners such as the Bitaxe, or any derivates of it, as well as their potential impact on the overall Bitcoin network. Therefore, a theoretical analysis of collective hashrate of small-scale miners will be explored in order to create a rough expectation of what kind of hashrate would be needed to drive an impact on the network in order to influence block discovery within a reasonable amount of time.

Although this analysis will be conducted under a theoretical assumption, it will outline potential scenarios where varying numbers of such devices and their hashrate are deployed across diverse geographical and network conditions. Building on this foundation, a pro forma impact evaluation will be conducted to assess the impact of the Bitcoin mining ecosystem, with a particular focus on its ability to compete with large mining pools and its influence on the decentralization of the network.

Simulation Models: An analysis of this nature necessitates the utilization of simulation models, which may facilitate a comprehensive comprehension of the status quo of the Bitcoin mining ecosystem and the required hashrate to contribute in a specific manner to the solution of the next block. Consequently, a simulation may assist in understanding what would be needed to compete with larger operations in order to create a hypothetical thesis about the outcome of small-scale mining operations.

Comparative Analysis: The utilization of data already presented by larger mining operations, such as their hashrate, power consumption and estimated time to find a block, could potentially facilitate the identification of potential advantages and disadvantages associated with small-scale mining operations and their viability.

Scenario Testing: Finally, a series of hypothetical scenarios were tested to determine the threshold at which small-scale miners begin to have a noticeable impact on the network. A forecast can be made at which point decentralization begins to shift towards smaller entities.

The findings of this theoretical analysis will contribute to a more profound comprehension of the role that small-scale miners could potentially play in the broader Bitcoin mining landscape. The objective of this research is to provide a more comprehensive understanding of the collective impact of small-scale miners on the broader Bitcoin mining landscape. This knowledge is intended to inform both current and prospective miners in the Bitcoin ecosystem.

5.3.1 Decentralization

As already reflected in Section 3.1.1 decentralization introduces the concept of a network that fully exists without the need of centralized entities which therefore implicate a threat towards its own network. Bitcoin mining has seen a shift towards centralized entities such as mining pools, which tend to become larger over time. This section will outline a potential shift with the help of a theoretical analysis to determine if small-scale mining operations might be able to turnaround this shift towards a more decentralized bitcoin network in terms of the mining hashrate distribution.

By allowing pools to grow, the network becomes less and less decentralized and issues in terms of transaction censorship, as an example, might appear. Therefore, this analysis will conduct a theoretical the outcome of small-scale mining solutions and their possibility of decentralizing the network.

5.3.2 Impact Data

While small-scale mining operations may face significant disadvantages or advantages compared to the current network, it is crucial to idenitfy the potential impact such operations might offer. Therefore, this analysis should also consider a potential future outlook in conjunction with the current Bitcoin network hashrate. It is essential to determine the possible consequences of an enormous hashrate increment of small-scale mining operations, particularly in terms of the overall decentralization of the network.

The analysis of the hash rate contributions of small-scale mining solutions and their power consumption in relation to large-scale mining facilities could facilitate the development of a more decentralised network.

6 Implementation

The purpose of this chapter is to present the translation of all requirements into a functional code base and also provide a tangible demonstration of how small-scale mining could reshape the future of cryptocurrency mining. Each piece of code and every analysis conducted here is directly informed by our earlier discussions on decentralization, efficiency, and network security.

6.1 Implementation of Data Collection

The establishment of a code basis for the data collection is of critical importance for the subsequent analysis, which will determine the viability of collecting specific data.

The Bitaxe already possesses a user interface, which is web-based and provides a wealth of information. The raw data can be transformed and utilized in a metric collection system.

Figure 6.1: AxeOS the WebUI of Bitaxe

As shown in Figure 6.1 it's already possible to address needed information about the Bitaxe itself, in this Figure the BitaxeHex[1] is used as a reference. Information like the Power consumption, the ASIC Voltage and Temperature as well as the Frequency of the ASIC is readable. This information needs to be collected and sent to a data collecting unit.

To collect all the needed data the following code will be used to implement an automation.

Listing 6.1: Username Hashing

```
static bool isUsernameHashed = false;
static char hashedUsername[65] = {0};


if (!isUsernameHashed) {
    char *username = nvs_config_get_string(NVS_CONFIG_STRATUM_USER,
        STRATUM_USER);
    unsigned char hashOutput[32];
    mbedtls_sha256((const unsigned char *)username, strlen(username),
        hashOutput, 0);

    for (int i = 0; i < 32; i++) {
        sprintf(&hashedUsername[i * 2], "%02x", hashOutput[i]);
    }

    isUsernameHashed = true;
}
```

The first block of code ensures that the username used to identify the device or user in the database is securely hashed using SHA-256, a cryptographic hash function. This function uses the bitcoin address used by the mining device to create a unique identifier that can be used to populate the database without exposing any user-related information. Two static variables, isUsernameHashed and hashedUsername, track whether the username has been hashed and store the hashed value. If the username hasn't been hashed `!isUsernameHashed`, the code retrieves the username using a function (nvs_config_get_string()), hashes it, and then formats each byte of the hash into a hexadecimal string stored in hashedUsername. This conversion is typical for storing or transmitting hashes in a readable format.

Listing 6.2: Data Collection

```
esp_http_client_handle_t client = esp_http_client_init(&config);

while (1) {
    double uptime_in_minutes = (double)esp_timer_get_time() / (60.0 *
        1000000.0);
    int uptime_in_minutes_int = (int)uptime_in_minutes;
    ESP_LOGI(TAG, "Calculated␣uptime␣in␣minutes:␣%i",
        uptime_in_minutes_int);

    if (uptime_in_minutes_int > 5) {
    char data[1024];
    snprintf(data, sizeof(data),
```

[1]The BitaxeHex is a newer iteration of the Bitaxe which features 6 ASIC chips compared to just one.

```
                "system_info,id=%s,model=%s␣hashRate=%.1f,Freq=%f,
                    asicVoltage=%f,inputVoltage=%f,power=%f,temp=%f,uptime=%
                    i",
                hashedUsername,
                GLOBAL_STATE->asic_model,
                systemModule->current_hashrate,
                power_management->frequency_value,
                asic_voltage,
                power_management->voltage,
                power_management->power,
                power_management->chip_temp,
                uptime_in_minutes_int);

        esp_http_client_open(client, strlen(data));

        esp_http_client_write(client, data, strlen(data));

        esp_err_t err = esp_http_client_fetch_headers(client);

        if (err == ESP_OK) {
            ESP_LOGI(TAG, "HTTP␣POST␣Request␣succeeded,␣status␣=␣%d",
                esp_http_client_get_status_code(client));
        } else {
            ESP_LOGE(TAG, "HTTP␣POST␣Request␣failed:␣%s", esp_err_to_name(err
                ));
        }

        }
        vTaskDelay(pdMS_TO_TICKS(30000));
    }
```

The last part of the code sets up and continuously executes an HTTP POST request to periodically send the system's operational metrics.

- Metric Calculation: Calculates the system's uptime in minutes from the ESP32's high-resolution timer and then logs it.
- HTTP POST Preparation: Constructs a data string containing various system metrics (hashrate, frequency, voltages, power, temperature, and uptime). These are monitored continuously by the system, reflecting the current status of the ASIC miner.
- HTTP Communication: Initializes and opens an HTTP client session. Sends the prepared data string using an HTTP POST request. Checks for and logs the HTTP request's success or failure.

A process of frequent data transmission is employed in order to facilitate the generation of a decision-making base, which in turn enables the determination of the optimal settings to be used.

6.2 Implementation of Data Aggregation

In order to facilitate the aggregation of data from small-scale miners in an efficient and accessible manner, a robust system has been implemented that utilizes InfluxDB and Dynamic

DNS (DDNS). This configuration not only enhances the ability to collect and analyze data in an efficient manner, but also ensures that the findings are accessible in real-time.

InfluxDB, a time-series database, has been specifically designed to handle high write and query loads, rendering it an optimal choice for storing large volumes of mining data. Its capacity to efficiently store time-stamped data enables the tracking and analysis of trends over time, thereby providing insights into the performance and efficiency of small-scale mining operations. The system employs a data transmission architecture that is designed to facilitate secure and efficient transfer of data. The configuration comprises a number of interconnected system components, each responsible for a specific task, including data capture and storage. This ensures the integrity and accessibility of the data.

A Dynamic DNS service is crucial because it provides a stable hostname that resolves to the IP address of the home server, despite any dynamic changes in the IP provided by the internet service provider. Upon reaching the home server via the DDNS resolving, the data is received by a Telegraf instance running on the server. Telegraf acts as a data collection and forwarding agent, which is configured to parse and structure the incoming data to the locally running InfluxDB 6.2.

Telegraf processes the data by filtering, aggregating, and enhancing the metrics as needed. This step is crucial for reducing noise, ensuring relevance, and preparing the data for detailed analysis. Once processed, the data is forwarded from Telegraf to InfluxDB, the chosen time-series database. InfluxDB stores this data in an efficient manner, allowing for complex queries and real-time analytics, which are essential for ongoing monitoring and research into mining efficiency.

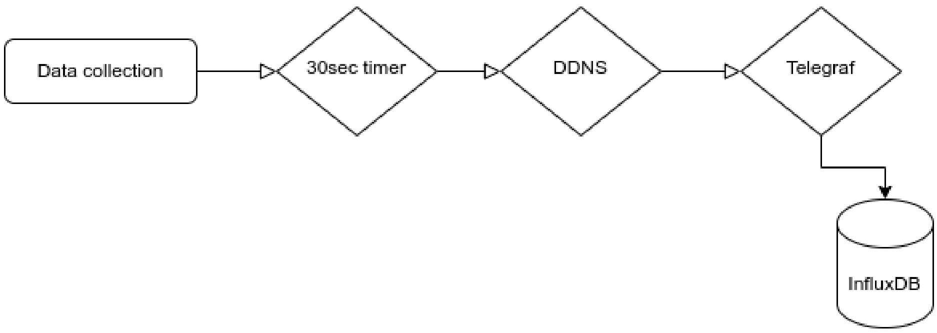

Figure 6.2: Data Path

Although there is no specific integration of data integrity built into it, it would be possible to handle such a scenario in Telegraf. This allows the user to specify which data is being passed through and which is not. Furthermore, only one device appeared to be off on the power consumption, which was subsequently handled later in the actual Python script that analyses the data 6.3.

6.3 Data Analysis

The goal of this data analysis is to extract meaningful insights that can answer key questions regarding the optimal operational settings for the Bitaxe device. Specifically, the analysis aims to determine which frequency provides the best efficiency, identify necessary adjustments, and recommend optimal settings for enhanced performance.

To analyze the collected data effectively, a structured approach is employed, comprising the following steps:

1. **Data Preprocessing**:
   - **Data Cleaning**: Removing any incomplete or erroneous data entries to ensure the accuracy of the analysis.
   - **Normalization**: Standardizing the data to facilitate comparison across different metrics and operational conditions.
2. **Descriptive Statistics**:
   - **Summary Statistics**: Calculating mean, median, standard deviation, and range for each metric to provide a basic understanding of the data distribution.
   - **Correlation Analysis**: Examining the relationships between different metrics to identify potential dependencies (e.g., correlation between hashrate and power consumption).
3. **Efficiency Analysis**:
   - **Hashrate per Watt (GH/W)**: Calculating the efficiency of the device at different frequencies by dividing the hashrate by power consumption.
   - **Optimal Frequency Identification**: Determining the frequency that provides the highest efficiency.
4. **Temperature Impact Assessment**:
   - **Temperature vs. Performance**: Analyzing how temperature variations impact hashrate and power consumption.
   - **Thermal Efficiency**: Evaluating the balance between performance and thermal management to avoid overheating while maintaining high efficiency.
5. **Settings Optimization**:
   - **Parameter Tuning**: Identifying which settings (e.g., frequency, voltage) need adjustment to achieve optimal performance
   - **Recommendations**: Providing actionable recommendations based on the analysis to improve the overall efficiency and reliability of the Bitaxe device.

In order to analyze the performance metrics of Bitaxe devices, it is first necessary to extract the data from the InfluxDB database. The InfluxDB database stores various metrics, including hashrate, power consumption, ASIC voltage, frequency, and temperature, which are each represented as a field within a measurement. In order to efficiently retrieve and export this data to CSV files, a Python script utilizing the InfluxDB client library was employed 6.3.

Listing 6.3: Data Extraction

```
# Function to query and export data for a single field
def export_field_data(field):
    query = f'''
    from(bucket: "{bucket}")
      |> range(start: -30d)
      |> filter(fn: (r) => r._field == "{field}")
      |> pivot(rowKey:["_time"], columnKey: ["_field"], valueColumn: "_value
         ")
    '''
    result = client.query_api().query_data_frame(query, org=org)

    # Export to CSV
    result.to_csv(f'{field}.csv', index=False)
    print(f"Data␣for␣field␣'{field}'␣exported␣successfully.")
    return field
```

The extraction process includes the following steps:

- **Connecting to InfluxDB:** The script connects to the InfluxDB instance using provided credentials.
- **Defining Fields:** The relevant fields are specified for extraction.
- **Querying Data:** For each field, a Flux query is constructed to retrieve data within the desired time range.
- **Exporting to CSV:** The queried data is converted into Pandas DataFrames and then exported to individual CSV files. This ensures that each metrics data is stored in a separate, easily accessible file.

The next step involves analyzing the extracted data into meaningful insights. The analysis focuses on understanding the distribution of various metrics, identifying patterns, and determining the optimal performance parameters for the Bitaxe device. This analysis process includes the following steps:

- **Loading Data:** Loading the CSV files containing the data for each metric.
- **Merging Data:** Individual DataFrames are merged based on common columns to create a comprehensive dataset.
- **Filtering Data:** Devices with unrealistic power consumption (less than 8W) are filtered out to ensure the analysis focuses on valid data.
- **Calculating efficiency:** The efficiency of each device is calculated as the ratio of hashrate to power consumption-
- **Computing Statistics:** Mean, median and standard deviation for each metric are computed to understand the overall performance distribution.
- **Identifying Optimal Device:** The device with the best average efficiency is identified.

- **Generating Graphs:** Histograms are generated for each metric 6.3.

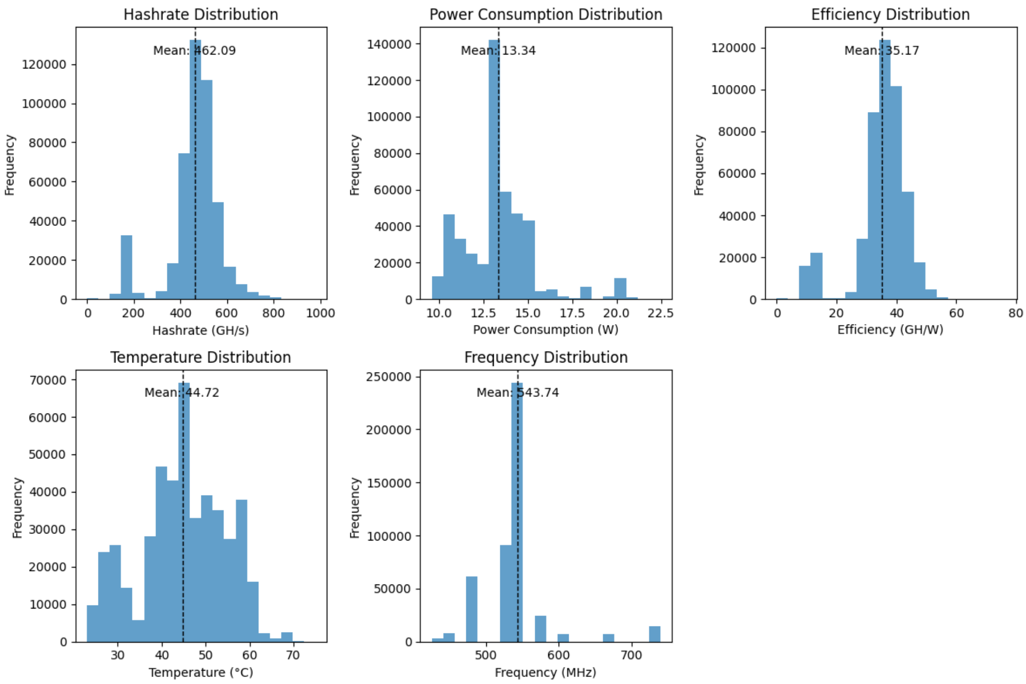

Figure 6.3: Analysis 1

The hashrate distribution graph shows that the majority of the Bitaxe devices have a hashrate clustered around the mean value of approximately 462.09 GH/s. This indicates that most devices are performing within a similar range. However, there are some outliers with significantly lower or higher hashrates, which could be due to various factors such as device condition, configuration differences, or operational environments.

Mean Hashrate: 462.09 GH/s

The power consumption distribution graph indicates that the power consumption of the devices is typically clustered around the mean value of approximately 13.34 W. There are fewer devices that consume significantly less or more power, which could be attributed to measurement errors, device issues, or variations in operational settings.

Mean Power Consumption: 13.34 W

The efficiency of the devices, as measured in GH/W (Gigahashes per Watt), is found to be approximately 35.17 GH/W, which is consistent with the mean value. This distribution indicates a consistent performance across the majority of devices, with some outliers demonstrating both higher and lower efficiency.

Mean Efficiency: 35.17 GH/W

The temperature distribution graph indicates that the operating temperatures of the devices are mostly centered around the mean value of 44.72°C. The spread of temperature values indicates that while the majority of devices operate within an acceptable temperature range, there are instances where temperatures are elevated, which could potentially impact performance and longevity.

Mean Temperature: 44.72°C

The frequency distribution graph indicates that the majority of devices operate at a frequency that is approximately equal to the mean value of 543.74 MHz. The presence of outliers suggests that some devices may be operating at different frequencies due to specific configurations or adjustments made for performance tuning.

Mean Frequency: 543.74 Mhz

Summary
The data analysis demonstrates that Bitaxe devices generally perform within the expected ranges for hashrate, power consumption, efficiency, temperature, and frequency. The mean values serve as a benchmark for optimal performance. Nevertheless, the presence of outliers in each distribution suggests that individual devices may require further investigation or optimization in specific areas.

- Most devices operate efficiently around the mean values of each metric.
- Outliers with lower efficiency, higher power consumption, or higher temperatures should be further examined to identify potential improvements in configurations or hardware maintanance.
- Continuous monitoring and analysis are essnetial to maintain optimal performance and identify issues early.

6.4 Implementation of Benchmarking

The development of a reliable benchmarking tool for testing Bitcoin mining ASICs is of critical importance for the evaluation of the performance, efficiency, and stability of mining hardware.

This section will present the developed benchmarking tool written in Python.

The provided code is a benchmarking tool designed to test the performance, efficiency, and stability of Bitcoin mining ASICs, specifically for the QAxe with four BM1366 ASIC. The script sets up logging, configures the miner, runs test jobs, and logs the results in order to determine the most efficient settings.

Listing 6.4: Benchmark.py

```
    random.seed(12345)

def testrun(config):
    piaxeMiner = miner.BM1366Miner(config, "
        bc1q7utau3qcy8hcjze9zsddg839sels90qyup5pv2", shared.BitcoinNetwork.
        MAINNET)
    piaxeMiner.init()
    piaxeMiner.set_difficulty(512)
    piaxeMiner.set_submit_callback(submit_cb)
    piaxeMiner.start_job(job)

    start_time = time.time()
    while True:
        with piaxeMiner.stats.lock:
            if time.time() - start_time > 15 * 60:
                break
#            if piaxeMiner.stats.valid_shares > 1000:
#                break
#
#            logging.info("left: %d", 1000-piaxeMiner.stats.valid_shares)

        time.sleep(1)

    elapsed = time.time() - start_time

    piaxeMiner.shutdown()

    return piaxeMiner.hash_rate(time_period=elapsed), elapsed

job={
    "job_id": "658dd1e40000ab91",
    "prevhash": "
        b064adaf22d7ac0ccc834a7fdcf88e55333a985b00010eda0000000000000000",
    "coinb1": "
        0100000001000000000000000000000000000000000000000000000000000000...",
    "coinb2": "0
        a636b706f6f6c0a2f736f6c6f206361742ffffffff027b441f2700000000160014
        ...",
    "merkle_branches": [
        "1eb4b7263d4cff7da31b12d229f5fff449a2b562b0125ad2d5fafd61553bb304",
        "cdf92795c97d3e605fa106b9fa0bb9117396285a17a5a712bfd185394c5e90d1",
        "df24f3058e2b27517e509959480dccd4d01109f302c82457125af158e02588c5",
```

```
        "1e325663cf83f80fb8e96a9003b7c6df511ecfae833e80fa4a7ce9821c9043ec",
        "86b131ccc80a41c7b6bb394d0f50172f39e821fd637f8614a3d38287d7dc7e42",
        "02224547803fc9afe7c1e9a54015a0c4165841e34117f08836f6dc7381757611",
        "637669c49a27971f7bb0b8ea9d06135070077c76878a1e4530d982fcc573ba10",
        "7af9a915bd396db4de93991ead88589be7704892d7e581a3b384f7bf7c418e0a",
        "f8e5d51530b415c31bc481b34035edaa820631e22507af682708231a5ea3be77",
        "35607c594892da344cbc0d0714ef3ab6fbdefc2b7c134bf3e73b0ca4563e48bd",
        "b4f6e62611b0be3d0147e39dfdbeb4c872c5b6a27a265b6eddc013573eee84a1",
        "024e88f023fd4f3b1de233e11afe5010af5fc0812dbceffc9cc76d7e65b20735"
    ],
    "version": "20000000",
    "nbits": "1703d869",
    "ntime": "65a1946b",
    "extranonce1": "63d38d65",
    "extranonce2_size": 8,
    "extranonce2": "000000000852f6ca",
    "merkle_root": "
       fbf0774adc895ea5e33b033fcadbf4f6f22ffd86751f4b12644502f78e8c8edf"
}
job = shared.Job.from_dict(job)

setup_logging(logging.DEBUG, "benchmark.log")
benchlog = setup_logging_benchy(logging.DEBUG, "benchmark_results.log")

# Load configuration from YAML
with open('config.yml', 'r') as file:
    config = yaml.safe_load(file)

def frequency_generator():
    for clock in range(460, 500, 5):
        yield [(clock, "asic_frequency")]

def enonce2_interval_generator():
    for enonce2_interval in range(3300, 10000, 100):
        yield [(enonce2_interval / 1000.0, "extranonce2_interval")]

def pwm1_generator():
    for pwm1 in range(0, 100, 5):
        yield [(pwm1 / 100.0, "fan_speed_1")]

def dummy_generator():
    while True:
        yield [(0, "unused")]

def chip_sweep_generator():
    for chips in [0, 1, 2, 3]:
        for clock in range(460, 480, 1):
            yield [(clock, "asic_frequency"), ([chips], 'chips_enabled')]

#modifier_func = enonce2_interval_generator
#modifier_func = frequency_generator
#modifier_func = pwm1_generator
modifier_func = dummy_generator
#modifier_func = chip_sweep_generator

for modifications in modifier_func():
    benchlog.info("==========================================================="
```

```
    )
benchlog.info("starting run ...")

for modified_setting in modifications:
    value = modified_setting[0]
    name = modified_setting[1]
    logging.info(f"modifying {name}, new value: {value}")
    config['qaxe'][name] = value

benchlog.info(yaml.dump(config['qaxe']))
hash_rate, elapsed = testrun(config)
benchlog.info("finished, elapsed: %s, hashrate: %.3fGH/s", elapsed,
    hash_rate)
```

The `testrun` function initializes the miner, sets the difficulty, starts a mining job, and runs the miner for a set period (15 minutes). It collects and returns the hash rate and elapsed time.

The `job details` for the mining task are provided as a dictionary and converted into a job object using `shared.Job.from_dict(job)`. The configuration settings for the miner are loaded from a YAML file.

The script runs a loop, modifying the miner's configuration with each iteration based on the selected parameter generator. It logs the modifications, runs the test, and logs the results.

This script is designed to automate the benchmarking process for Bitcoin mining ASICs, allowing for systematic testing of different parameters. It sets up comprehensive logging, runs the miner with varying configurations, and logs the performance metrics.

In order to facilitate the visualization of the logged metrics, a InfluxDB database and a Grafana dashboard have been established 6.4.

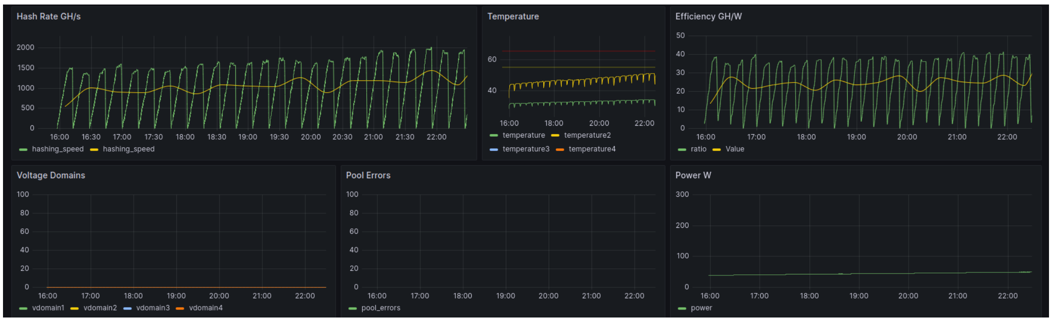

Figure 6.4: Benchmark Results Grafana

The following table 6.1 presents the benchmarking results on the QAxe testing at various different frequency settings, ranging from 400 to 545 MHz. The highlighted line represents the optimal setting, as determined through the process of benchmarking the device.

Frequency (MHz)	Efficiency (GH/W)	Power Consumption (W)	Hashrate (GH/s)
400	38.7	39.0	1458
405	35.2	39.0	1336
410	36.1	40.0	1414
415	38.4	40.0	1539
420	35.3	40.0	1390
425	36.1	40.0	1451
430	33.5	41.0	1394
435	35.4	41.0	1482
440	37.1	41.0	1531
445	38.3	42.0	1558
450	37.8	42.0	1575
455	37.5	43.0	1583
460	38.6	43.0	1678
465	38.9	44.0	1719
470	36.2	44.0	1641
475	36.3	44.0	1541
480	37.0	45.0	1658
485	37.7	45.0	1754
490	37.6	46.0	1758
495	41.0	46.0	1851
500	39.1	47.0	1807
505	41.1	47.0	1890
510	40.1	47.0	1994
515	38.5	48.0	1856
520	40.0	48.0	1890
525	37.6	48.0	1812
530	40.5	49.0	2003
535	39.5	49.0	1944
540	37.3	50.0	1829
545	39.0	50.0	1942

Table 6.1: Results of the Benchmarking Tool

6.5 Analysis for Small-scale Home Miners

As the landscape of Bitcoin mining continues to evolve, small-scale home miners represent a crucial demographic. Their ability to influence network decentralization and contribute to the overall security and robustness of the blockchain makes understanding their operations and efficiency vital. This section presents a theoretical implementation of an analysis, which is aimed at uncovering the unique challenges and opportunities faced by home miners.

While small-scale mining operations may present certain challenges, it is crucial to define the parameters of what constitutes a small-scale mining operation and what is more accurately classified as a farm. This distinction is important because it helps to differentiate between home mining, which is not primarily driven by profit, and mining operations that are designed for profit and utilize significantly higher levels of electricity.

The Bitaxe project represents a significant innovation in the realm of Bitcoin mining, particularly for small-scale operations. As an open-source ASIC standalone miner, the Bitaxe provides a cost-effective and accessible solution for individual miners and small mining farms. This section explores the potential impact of Bitaxe on the Bitcoin network and analyzes the scale of deployment required to drive a noticeable effect.

6.5.1 Hashrate Contribution

In the context of Bitcoin mining, the pure hashrate represents a crucial factor. The network hashrate is the sum of the hashrates of all devices, and it determines the network difficulty in processing the blockchain. Bitcoin difficulty adjustment occurs approximately every two weeks and is designed to ensure that new blocks are mined at an average rate of one every 10 minutes. If more miners join the network, the difficulty increases; if miners leave, the difficulty decreases, this is shown in Figure 6.5.

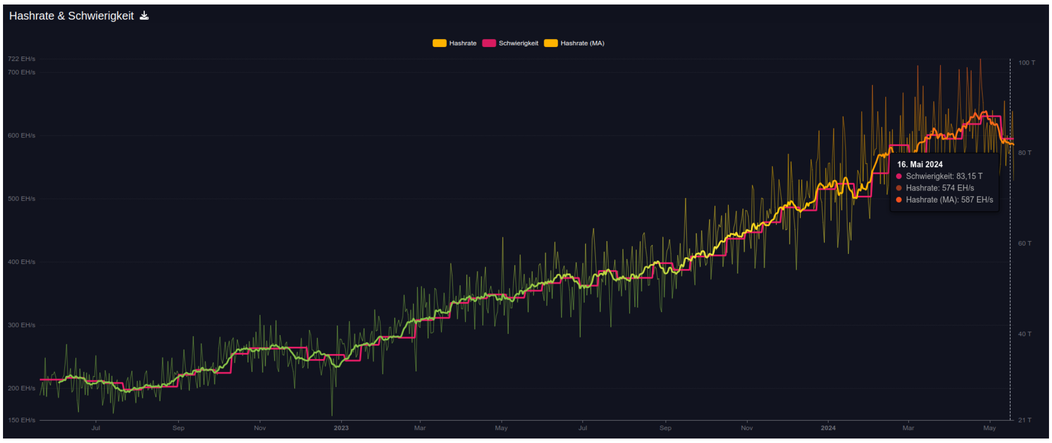

Figure 6.5: Network Hashrate and Difficulty (mempool.space)

Small-scale mining operations may be overshadowed by large, industrial-scale mining operations with high energy consumption and high hash rates. But in terms of the Bitcoin network, it only takes one correct hash to solve the next Bitcoin puzzle. Hence the argument that even a small mining operation can have an impact.

The Bitaxe Ultra, for instance, features the BM1366 ASIC chip, which provides a hash rate of approximately 0.5 TH/s per device. To analyze the potential impact, we need to understand the total hash rate of the Bitcoin network, which, as of May 2024, is approximately 690 EH/s (exahashes per second).

6.5.2 Network Hashrate Impact Calculation

To determine the number of Bitaxe devices needed to contribute significantly to the network, let's define a significant impact as contributing 0.1% to the total network hash rate. This is equivalent to:

$$\text{Desired Contribution} = 0.1\% \times 690 \text{ EH/s} = 0.69 \text{ EH/s} \tag{6.1}$$

Converting 0.69 EH/s to TH/s (terahashes per second):

$$0.69 \text{ EH/s} = 0.69 \times 10^6 \text{ TH/s} = 690,000 \text{ TH/s} \tag{6.2}$$

Given each Bitaxe Ultra provides 0.5 TH/s, the number of Bitaxe devices required is:

$$\text{Number of Bitaxe Devices} = \frac{690,000 \text{ TH/s}}{0.5 \text{ TH/s per device}} \approx 1,380,000 \text{ devices} \tag{6.3}$$

This amount of Bitaxe devices would contribute significantly to the network and it's hash rate. At about 0.69 EH/s, a bitcoin block would be found about every 6.94 days if the network difficulty doesn't increase.

To determine the expected number of days to find a Bitcoin block with a given hash rate contribution, we use the following steps:

1. The probability P of finding a block is:

$$P = \frac{H_{\text{contribution}}}{H_{\text{network}}} \tag{6.4}$$

Given:

- Total Network Hash Rate, $H_{\text{network}} = 690$ EH/s
- Miner Hash Rate Contribution, $H_{\text{contribution}} = 0.69$ EH/s

$$P = \frac{0.69 \text{ EH/s}}{690 \text{ EH/s}} = \frac{1}{1000} = 0.001 \tag{6.5}$$

2. The expected number of blocks E found per day is:

$$E = 144 \times P \tag{6.6}$$

$$E = 144 \times 0.001 = 0.144 \text{ blocks/day} \tag{6.7}$$

3. The expected number of days D to find one block is:

$$D = \frac{1}{E} \tag{6.8}$$

$$D = \frac{1}{0.144} \approx 6.94 \text{ days} \tag{6.9}$$

Therefore, with a hash rate contribution of 0.69 EH/s, it would take approximately 6.94 days to find one Bitcoin block.[2]

With its ease of deployment, the Bitaxe is a unique device that not only contributes to the Bitcoin network, but also requires little knowledge to set up and consumes as little as 12W per device.

6.5.3 Energy Consumption

The power consumption of each Bitaxe Ultra is approximately 12W. Therefore, the total energy requirement for 1,380,000 devices is:

$$\text{Total Power Consumption} = 1,380,000 \text{ devices} \times 12 \text{ W/device} = 16,560,000 \text{ W} \approx 16.56 \text{ MW} \tag{6.10}$$

This may sound like a significant amount of energy to solve one block every 6 days. But that power consumption is spread across the globe or across a country, not consumed by a single entity. This distribution helps decentralize the network hashrate, leveraging existing infrastructure without overburdening any single part of the grid. When distributed evenly, the grid can manage this consumption, supporting a decentralized and resilient network. Every household would in theory only add 12 watts to their household.

Each household would, in theory, only add 12 watts to their household consumption. To put this into perspective, many common household devices consume significantly more power:

- A typical LED light bulb consumes about 10-15W
- A standard refrigerator uses approximately 100-200W
- A desktop computer can consume between 200-600W

Given these comparisons, the additional 12W per household is relatively minimal. This minimal increase in power usage per household can be absorbed by the existing electrical infrastructure without requiring significant upgrades or causing strain on the grid. While the total energy consumption is considerable, it is important to evaluate the environmental impact. If a significant proportion of this energy is derived from renewable sources such as solar, wind, or hydroelectric power, the environmental impact of such a widespread mining operation can be minimized. The encouragement of the use of renewable energy for mining operations can serve to further enhance the sustainability of the network.

[2] This assumes that the hashrate and the difficulty does not change and persists at the same hight as of writing this thesis

6.5.4 Cost Analysis

When evaluating the viability of utilizing Bitaxe Ultra devices for small-scale Bitcoin mining, it is essential to assess both the initial investment and the ongoing operational costs. This section presents a comprehensive cost analysis, elucidating the total expenses associated with procuring and operating the devices.

The initial cost of acquiring Bitaxe Ultra devices varies depending on the retailer and country of purchase. To provide a clear picture of the potential expenses, a list of prices from 15 different stores across various countries has been compiled. The table below presents the name of each store, the country it is located in, and the corresponding price of the Bitaxe Ultra device 6.2.

Name of the Store	**Country**	**Price**
32Bitcoins	Australia	350AUD
ALtair	USA	149USD
Bitcoin Merch	USA	149USD
Bitronics	Spain	128EUR
D-Central	Canada	185CAD
Go Brrr	Austria	148EUR
JBP-3D	Europe	135EUR
Kaboomracks	USA	199USD
NerdMiner Store	Europe	249EUR
Open Source Miners	USA	134USD
RGZ Electronics	Spain	147EUR
Silexperience	France	188EUR
The Solo Mining Co.	UK	184GBP
Solo Satoshi	USA	189USD
TinyChipHub	China	169USD

Table 6.2: Comparison of Bitaxe Ultra Prices in Different Stores and Countries [Sko24]

If each Bitaxe Ultra costs around \$177, the total initial investment required would be:

$$\text{Total Cost} = 1{,}380{,}000 \text{ devices} \times \$177/\text{device} = \$244{,}260{,}000 \tag{6.11}$$

It is unlikely that any individual would be willing to expend this sum on mining equipment. However, the low price of entry into the market and the support provided to the network would result in the overall cost of distributing 0.1% more hashrate to the network and solving blocks on a more regular basis being this amount. A more intriguing aspect would be the cost analysis of power consumption. With an average power price per kilowatt-hour in Germany of 0.41 euros [(De24][ele24] :

$$\text{Daily Power Consumption} = 12 \text{ W} \times 24 \text{ H} = 288 \text{ Wh} = \frac{288 \text{ Wh}}{1000} = 0.288\text{kWh} \tag{6.12}$$

$$\text{Energy Cost} = 0.41 \text{ euros} \times 0.288\text{kWh} = 0.118 \text{ euros} \tag{6.13}$$

With this modest expenditure of 0.12 euros per day, even in Germany, which has one of the highest energy prices in Europe, it would be feasible to operate such a compact device. It is therefore possible to make the statement that it is quite possible to achieve a change in the network hashrate distribution with a large number of participants. To achieve an even greater decentralized distribution of the hashrate, it is necessary for a large number of individuals to participate in this process. However, this analysis shows that even with just 0.1% of participants, a change is possible. A more decentralized distribution of the hashrate is the initial step in achieving the objective of this thesis, namely the prevention of any single entity from exercising control over a significant proportion of the hashrate.

7 Evaluation

The evaluation chapter is designed to assess the extent to which the objectives and requirements of the benchmarking have been met. This chapter provides a systematic analysis of the benchmark performance, identifying areas of success and aspects that require improvement. The evaluation is based on the criteria established at the outset of the thesis, which include performance metrics, power consumption, efficiency, and overall usability of the ASIC chips.

7.1 Requirements and Objectives

At the beginning of the thesis, a number of key requirements and objectives were defined to guide the development and deployment of the Bitaxe Benchmarking Framework. These include:

- **Performance:** Achieving a high hashrate to optimize computational efficiency.
- **Power Consumption:** Maintaining reasonable power consumption levels to ensure cost-effectiveness and sustainability.
- **Efficiency:** Maximizing the efficiency of the chips, measured as the ratio of hashrate to power consumption, adjusted for heat-related losses.
- **Anonymity:** The collection of anonymous data is employed in order to prevent the introduction of bias in the evaluation of a specific user.
- **Automation in Data Gathering:** Utilization of automated Data Gathering systems.
- **Transparency and Openness:** Maintaining transparency and publish all data and code afterwards.
- **Analytical Simulation:** Create analytical models to evaluate the impacts of small-scale mining on the Bitcoin network

7.2 Performance Evaluation

7.2.1 Hashrate Achievement

The primary goal was to achieve a high hashrate to maximize the mining efficiency. The hashrate of the Bitaxe chips was measured under various conditions, and the results were as follows:

The percentage increase can be calculated using the formula:

$$\text{Percentage Increase} = \left(\frac{\text{New Hashrate} - \text{Old Hashrate}}{\text{Old Hashrate}}\right) \times 100$$

- The previous average hashrate achieved was 462.09 GH/s
- the new hashrate with applied configurations is 472.5 GH/s which is an increase of 2.27%.

7.2.2 Power Consumption Analysis

The power consumption was a critical factor in the evaluation. The target was to maintain power consumption below a specific threshold while achieving the desired hashrate.

The percentage decrease in power consumption can be calculated using the formula:

$$\text{Percentage Decrease} = \left(\frac{\text{Old Power Consumption} - \text{New Power Consumption}}{\text{Old Power Consumption}}\right) \times 100$$

- The previous average power consumption recorded was 13.34 W.
- The power consumption decreased to 11.75 W which is an percentage optimization of 11.92%.

7.2.3 Efficiency Assessment

The efficiency of the chips, defined as the ratio of hashrate to power consumption, was a key metric. The percentage increase in efficiency (measured in W/GH) can be calculated using the formula:

$$\text{Percentage Increase} = \left(\frac{\text{New Efficiency} - \text{Old Efficiency}}{\text{Old Efficiency}}\right) \times 100$$

- The efficiency with a mean of 35.17 GH/W which results in 28.43J / TH. This represents a reduction of 8W per Terashash in comparison to the official 21J/TH figure provided by Bitmain for their S19XP models.
- The new efficiency increased from 35.17 GH/W to 41.1 GH/W which is an percentage increase of 16.86% and a efficiency of 24.86 J/TH.

7.2.4 Technical Requirements

The technical requirements for the implementation of the data aggregation into the Bitaxe firmware constituted a pivotal requirement.

- **FreeRTOS Implementation:** The data aggregation and forwarding of the collected data were incorporated into the Bitaxe firmware code.

- **Relation Database:** In order to facilitate the storage of the collected data, InfluxDBv2 was employed. This was done in order to ensure that the data could be processed in a manner that would be conducive to the desired outcome.
- **Anonymity:** The anonymity was achieved by utilizing the mining Bitcoin address and hashing it in order to generate a unique, unidentifiable number.
- **Non-interference:** Prior to implementation, the data collection task was tested to ensure that it would not interfere with other tasks or trigger any system halts.

7.2.5 Non-Technical Requirements

The non-technical requirements for the implementation were primarily concerned with the usability and openness of this thesis.

- **User-Firendly Usability:** The data collection was configured and programmed as an opt-in button in the Bitaxe firmware, thereby enabling the user to easily decide whether or not to enable it.
- **Transparency and Control:** The code basis and all data collected are available for public access at an open GitHub repository: `https://github.com/WantClue/Master-Thesis`.
- **Accessibility:** The data collection process was designed to yield data that would be necessary for the data analysis.
- **Documentation:** All source code is available for review and verification in the GitHub repository. Which also features a documentation.

7.3 Summary of Findings

Based on the evaluation, the following conclusions can be drawn about the Bitaxe project:

The implementation of a benchmarking framework and the data analysis of this possessed data showed a successful outcome to determine potential improvements for the ASIC chip used in the Bitaxe device. Furthermore, does it highlight that a future outlook of the heat generation impact is needed in order to evaluate this data precisely.

Furthermore, the following conclusions can be drawn about small-scale mining solutions and their potential outcome:

- **Hashrate Contribution:** Small-scale miners, although individually contributing a relatively small portion of the overall network hashrate, collectively have the potential to significantly influence the network. Approximately 1,380,000 Bitaxe Ultra devices would be required to achieve a 0.1% contribution to the total network hashrate.
- **Energy Consumption:** The total power consumption for 1,380,000 devices amounts to approximately 16.56 MW. While this is a significant amount of energy, the impact is mitigated by the distributed nature of small-scale mining. Each device consumes about 12W, which is minimal compared to common household appliances. This makes

it feasible for individuals to participate in mining without placing undue strain on household electrical infrastructure or the wider grid.

- **Environmental Considerations:** The environmental impact of widespread small-scale mining can be mitigated if a significant portion of the energy used is derived from renewable sources. The utilisation of solar, wind, or hydroelectric power can enhance the sustainability of such mining operations.
- **Operational Costs:** The daily energy cost of operating a Bitaxe Ultra device is approximately 0.12 euros in Germany, making it economically viable even in regions with high electricity prices. Despite the low chance of finding a block, the low operational cost of the Bitaxe device makes it a viable option for individuals engaged in small-scale mining.

8 Summary and Future Outlook

In this chapter, the key findings and insights gained from the analysis of the Bitaxe project are consolidated, with a particular emphasis placed on its application in the context of small-scale home mining solutions. This summary is intended to provide an overview of the research conducted, the outcomes achieved, and the implications of these results.

8.1 Summary

The Bitaxe project represents a significant advance in the accessibility of Bitcoin mining to small-scale home miners. By analyzing the hashrate contribution, energy consumption, and economic feasibility, it is evident that small-scale mining can have a meaningful impact on the Bitcoin network. Future developments should focus on enhancing the technical capabilities of the Bitaxe devices, improving heat management, and fostering collaboration with larger mining operations in order to fully realize the potential of decentralized mining.

8.2 Key Objectives and Achievements

The primary objectives of the Bitaxe project were to:

- Analyze the performance metrics, including hashrate, power consumption and efficiency.
- Assess the potential impact of small-scale mining on the Bitcoin network.
- Propose future improvements and collaborations to enhance mining efficiency and decentralization.

Through a process of rigorous analysis and testing, it was able to achieve a significant milestone in the development and evaluation of the Bitaxe ASIC miner. The performance metrics indicated that the Bitaxe Ultra, with its BM1366 ASIC chip, could provide a viable solution for small-scale miners. Furthermore, the theoretical models and empirical data yielded insights into the network impact and energy consumption of the device.

8.3 Future Outlook

This section will be devoted to the exploration of potential future developments and areas for further research and implementations. The advancements discussed here aim to enhance the performance, efficiency, and scalability of the Bitaxe ASIC chips, and to provide a more comprehensive understanding of their impact on the Bitcoin mining ecosystem.

Implementation of an Auto-adjust Tool One of the key areas for future work is the development and implementation of an auto-adjust tool for the Bitaxe. Such a tool would enable precise overclocking or underclocking automatically and analysis of various performance metrics, right on the Bitaxe device itself. In contrast to the conventional manual process and the benchmarking process presented in this thesis, the device would be capable of identifying the optimal settings required for operation, taking into account the full range of available options, without the need for manual interception.

- **Hashrate**: Accurate real-time monitoring of the hashrate under different operational conditions.
- **Power Consumption**: Detailed tracking of power consumption to optimize energy efficiency.
- **Temperature**: Continuous measurement of chip temperature to study the effects of heat generation on performance.
- **Efficiency**: Calculation of the efficiency ratio (hashrate per watt) adjusted for heat-related losses.

The auto-adjust tool could provide valuable insights for automatically adjusting the operational parameters of the Bitaxe, thereby enhancing their overall performance and usability even more and potentially implementing the currently missing functionality of adjusting the ASIC frequency on the fly.

Determining the Impact of Heat on Performance:
A further area of significant potential for future research is the detailed study of the impact of heat generation on the performance of the Bitaxe ASIC chips. Although theoretical models have been developed to describe the relationship between power consumption and heat generation, empirical data is required to validate these models and quantify the actual performance degradation due to heat.

Future work should focus on:

- **Empirical Data Collection**: Conducting controlled experiments to gather data on how heat affects the hashrate and efficiency of the chips.
- **Heat Management Solutions**: Developing and testing cooling solutions to mitigate the detrimental effects of heat on chip performance.
- **Refinement of Models**: Using the empirical data to refine existing models and improve predictions of chip performance under various thermal conditions.

Collaboration with Large Mining Facilities:
To gain a broader understanding of the impact of small-scale mining solutions on the overall Bitcoin mining network, it is essential to collaborate with large mining facilities. Such collaborations can provide extensive data and insights that are otherwise difficult to obtain.

Future research could explore:

- **Data Sharing**: Establishing partnerships with large mining facilities to share data on hashrate, power consumption, and network contributions.

- **Comparative Analysis**: Conducting comparative studies to assess the impact of integrating small-scale mining solutions with large-scale operations.
- **Scalability Studies**: Evaluating the scalability of Bitaxe chips in different mining environments and their potential to decentralize the network hashrate.

Such collaborative efforts can help in understanding the broader implications of small-scale mining solutions and contribute to more sustainable and efficient mining practices.

8.4 Conclusion

The future outlook for the Bitaxe project is promising, with several potential advancements and areas for further research. Implementing an auto-adjustment tool, determining the actual impact of heat on chip performance, and collaborating with large mining facilities can significantly enhance the understanding and optimization of Bitaxe devices. These efforts will contribute to the development of more efficient, scalable, and sustainable Bitcoin mining solutions and the decentralization of the mining hashrate.

Abbreviations

FOSS Free and open source software

ASIC Application-Specific Integrated Circuit

OSMU Open Source Miners United

OSS Open Source Software

AML Anti Money Laundering

CFT Combating the financing of terrorism

ECDSA Elliptic Curve Digital Signature Algorithm

UTXO Unspend Transaction Output

List of Figures

List of Tables

Bibliography

[ÅF08] Ågerfalk, Pär J ; Fitzgerald, Brian: Outsourcing to an unknown workforce: Exploring opensurcing as a global sourcing strategy. In: *MIS quarterly* (2008), S. 385–409

[B+02] Back, Adam u. a.: Hashcash-a denial of service counter-measure. (2002)

[BBH+13] Becker, Jörg ; Breuker, Dominic ; Heide, Tobias ; Holler, Justus ; Rauer, Hans P. ; Böhme, Rainer: Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In: *The economics of information security and privacy* (2013), S. 135–156

[BHP+12] Brügge, Bernd ; Harhoff, Dietmar ; Picot, Arnold ; Creighton, Oliver ; Fiedler, Marina ; Henkel, Joachim: *Open-Source-Software: eine ökonomische und technische Analyse.* Springer-Verlag, 2012

[Bra] Braiins: *BraiinsOS*. `https://academy.braiins.com/en/braiins-os/about/`

[BT17] Bedford Taylor, Michael: The Evolution of Bitcoin Hardware. In: *Computer* 50 (2017), Nr. 9, S. 58–66. `http://dx.doi.org/10.1109/MC.2017.3571056`. – DOI 10.1109/MC.2017.3571056

[CV17] Coelho, Jailton ; Valente, Marco T.: Why modern open source projects fail. In: *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering.* New York, NY, USA : Association for Computing Machinery, 2017 (ESEC/FSE 2017). – ISBN 9781450351058, 186–196

[Dai98] Dai, Wei: b-money, 1998. In: *URL http://www. weidai. com/bmoney. txt* (1998)

[(De24] (Destatis), Statistisches B.: *Strompreise für Haushalte: Deutschland, Halbjahre.* 2024

[ele24] *Average monthly electricity wholesale price in Germany from January 2019 to May 2024 (in euros per megawatt-hour) [Graph].* `https://www.statista.com/statistics/1267541/germany-monthly-wholesale-electricity-price/`. Version: 2024

[Fit06] Fitzgerald, Brian: The Transformation of Open Source Software. In: *MIS Quarterly* 30 (2006), Nr. 3, 587–598. `http://www.jstor.org/stable/25148740`. – ISSN 02767783

[fre] *Free Software Foundation.* `https://www.fsf.org/`. – Access: 2024-02-18

[git] *Bitaxe.* `https://github.com/skot/bitaxe`. – Access: 2024-03-01

[KDF13] Kroll, Joshua A. ; Davey, Ian C. ; Felten, Edward W.: The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In: *Proceedings of WEIS* Bd. 2013 Citeseer, 2013

[Mem] *Mempool*. `https://mempool.space`

[MFH00] Mockus, Audris ; Fielding, Roy T. ; Herbsleb, James: A case study of open source software development: the Apache server. In: *Proceedings of the 22nd international conference on Software engineering*, 2000, S. 263–272

[Nak08] Nakamoto, Satoshi: Bitcoin whitepaper. In: *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)* (2008)

[Pag18] Pagnotta, Emiliano: Bitcoin as decentralized money: prices, mining, and network security. In: *SSRN (3264448)* (2018)

[RC17] Recabarren, Ruben ; Carbunar, Bogdan: *Hardening Stratum, the Bitcoin Pool Mining Protocol*. 2017

[Ril21] Riley, John: The current status of cryptocurrency regulation in China and its effect around the world. In: *China and WTO Review* 7 (2021), Nr. 1, S. 135–152

[Sko24] Skot: *Bitaxe Webpage*. `https://bitaxe.org`. Version: 2024

[VBP+17] Vendome, Christopher ; Bavota, Gabriele ; Penta, Massimiliano D. ; Linares-Vásquez, Mario ; German, Daniel ; Poshyvanyk, Denys: License usage and changes: a large-scale study on github. In: *Empirical Software Engineering* 22 (2017), S. 1537–1577

[Wan24] WantClue: *Interview with @DCentralTech a BTC hosting provider*. `https://youtu.be/NwJkUm56PA8`. Version: April. 2024

[ZLL+18] Zhu, Saide ; Li, Wei ; Li, Hong ; Hu, Chunqiang ; Cai, Zhipeng: A survey: Reward distribution mechanisms and withholding attacks in Bitcoin pool mining. In: *Math. Found. Comput.* 1 (2018), Nr. 4, S. 393–414