

Evaluation eines Crypto Mining Systems

Studienarbeit

für die Prüfung zum

Bachelor of Science

des Studienganges Informatik mit Schwerpunkt Informationstechnik

an der Dualen Hochschule Baden-Württemberg Karlsruhe

von

Dominik Klein und Robin Weisenburger

Abgabedatum

06.06.2022

Bearbeitungszeitraum

26 Wochen

Matrikelnummer

Klein: 3180051 / Weisenburger: 9883215

Kurs

TINF19B3

Ausbildungsfirma

dmTECH GmbH, Karlsruhe

Betreuer

Prof. Dr. Kai Becher

Gutachter der Studienakademie

Prof. Dr. Jürgen Vollmer

Eidesstattliche Erklärung

gemäß § 5 (3) der „Studien- und Prüfungsordnung DHBW Technik“ vom 01. August 2019.
Ich versichere hiermit, dass ich die Studienarbeit mit dem Titel

„Evaluation eines Crypto Mining Systems“

selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ort, Datum

Dominik Klein und Robin Weisenburger

Inhaltsverzeichnis

Abbildungsverzeichnis	VI
Tabellenverzeichnis	VII
Listingverzeichnis	VIII
Abkürzungsverzeichnis	IX
1 Einleitung	1
1.1 Motivation	1
1.2 Ziel	2
1.3 Vorgehensweise	2
2 Grundlagen	3
2.1 Kryptowährungen	3
2.2 Wallets	4
2.3 Blockchain	8
2.4 Difficulty	10
2.5 Transaktionen	11
2.6 Generierung digitaler Währungen	13
2.7 Sicherheit und Anonymität	18
3 Kryptowährungen	22
3.1 Handel von Kryptowährungen	22
3.2 Bitcoin	23
3.3 Ethereum	24
3.4 Tether	25
3.5 Chia	26
3.6 Monero	27
3.7 Vergleich	29

4 Kryptomining	30
4.1 Hardware	30
4.2 Software	32
4.3 Solo- & Pool-Mining	35
4.4 Stratum Protokoll	36
5 Vorbereitung	39
5.1 Konzept	39
5.2 Hardware	40
5.3 Software	42
5.4 Kosten	45
5.5 Ermittlung der Effizienz	46
5.6 Verbesserungsmöglichkeiten	46
5.7 Ziele	47
6 Umsetzung	48
6.1 Einrichtung Wallet	48
6.2 Ermittlung des Stromverbrauchs	50
6.3 Einrichtung Mining-Rig (Hardware)	51
6.4 Einrichtung Mining-Rig (Software)	53
6.5 Durchführung der Test-Szenarien	60
6.6 Windows Szenarien	62
6.7 Linux Szenarien	84
6.8 Mining-OS Szenarien	93
6.9 Leistungssteigerung	102
6.10 Auto Switching	116
7 Auswertung & Analyse	123
7.1 Allgemeine Analyse	123
7.2 Windows Ergebnisse	125
7.3 Linux-Ergebnisse	126
7.4 Hive-OS-Ergebnisse	127
7.5 Overclocking-Ergebnisse	128
8 Fazit	130
8.1 Bewertung	130
8.2 Empfehlung	135

9 Ausblick	136
9.1 Ethereum 2.0	136
9.2 Energiekosten in Zukunft	137
9.3 Mining in der Zukunft	139
A Anhang	XI
A.1 Anhang Bewertungsmatrix	XI
A.2 Anhang Break-even-Point Matrix	XII
A.3 Anhang Bewertungsschwellenwerte	XIII
Literaturverzeichnis	XXI

Abbildungsverzeichnis

2.1	HD Wallet Aufbau [1]	6
2.2	Funktionsweise einer Blockchain [2]	9
2.3	Funktionsweise digitaler Signaturen [1]	12
2.4	Ablauf einer BTC Transaktion [1]	13
2.5	Funktionsweise Proof of Work [2]	14
2.6	Funktionsweise Proof of Stake [2]	16
2.7	51% Attacke [3, S.403]	20
2.8	Ethereum Blockchain Explorer Beispiel [4]	21
3.1	Umsatzstärkste Kryptowährungen [5, S.67]	22
3.2	Funktionsweise ETH2 [6]	25
3.3	Funktionsweise einer Ring Signatur [7]	28
4.1	Ablauf der Kommunikation über das Stratum Protokoll	38
5.1	Privat Mining-Rig für zu Hause [8]	40
6.1	Ledger Nano S	48
6.2	Ledger Apps	49
6.3	Ledger Ethereum Wallet	50
6.4	Web-Oberfläche zur Leistungsmessung (Auszug)	51
6.5	Mininig-Rig (1)	52
6.6	Mining-Rig (2)	52
6.7	Awesome Miner Konfiguration	56
6.8	Awesome Miner Pool Konfiguration	57
6.9	Awesome Miner: entfernte Miner Einrichtung	58
6.10	Aufbau 01	63
6.11	Aufbau 02	64
6.12	Aufbau 03	66
6.13	Aufbau 04	67

6.14	Aufbau 05	69
6.15	Aufbau 06	70
6.16	Aufbau 07	72
6.17	Aufbau 08	73
6.18	Aufbau 09	75
6.19	Aufbau 10	76
6.20	Aufbau 11	78
6.21	Aufbau 12	79
6.22	Aufbau 13	81
6.23	Aufbau 14	82
6.24	Aufbau 15	85
6.25	Aufbau 16	86
6.26	Aufbau 17	88
6.27	Aufbau 18	89
6.28	Aufbau 19	91
6.29	Aufbau 20	92
6.30	Aufbau 21	94
6.31	Aufbau 22	95
6.32	Aufbau 23	97
6.33	Aufbau 24	98
6.34	Aufbau 25	100
6.35	Aufbau 26	101
6.36	Aufbau 27	108
6.37	Aufbau 28	109
6.38	Aufbau 29	111
6.39	Aufbau 30	112
6.40	Aufbau 31	114
6.41	Aufbau 32	115
6.42	NiceHash Übersicht	118
6.43	BetterHash Benchmark Übersicht	121
9.1	Zusammensetzung der Stromkosten im April 2022 in Deutschland [9]	137
9.2	Strompreisentwicklung von 2000 bis 2022 [9]	138
9.3	Industriestrompreis Deutschland im Januar 2022 [10]	139

Tabellenverzeichnis

3.1	Vergleich Kryptowährungen [11]	29
5.1	NiceHash Mining-Plugins	43
5.2	Kosten des Mining-Rigs	45
6.1	Auswertung Windows Test-Szenarien	83
6.2	ASUS RX 580 Leistungsparameter vor/nach Übertaktung	104
6.3	PowerColor RX 580 Leistungsparameter vor/nach Übertaktung	105
6.4	ZOTAC RTX 2070 SUPER Leistungsparameter vor/nach Übertaktung . .	105
7.1	Ergebnisse Windows Test-Szenarien	125
7.2	Ergebnisse Linux Test-Szenarien	126
7.3	Ergebnisse Hive-OS Test-Szenarien	127
7.4	Ergebnisse Overclocking Test-Szenarien	129

Listingverzeichnis

6.1	Parametrisierung der Mining-Software PhoenixMiner	53
6.2	Parametrisierung der Mining-Software lolMiner	53
6.3	Ausgabe PowerShell Skript: Switch Compute Mode	54
6.4	HiveOS Konfigurationsdatei (rig.conf)	59
6.5	HiveOS FlightSheet (lolMiner)	60
6.6	BetterHash AutoSwitching Log (Auszug)	122

Abkürzungsverzeichnis

AMD	Advanced Micro Devices, Inc.
API	Application Programming Interface
APT	Advanced Packaging Tool
ASIC	Application Specific Integrated Circu
BIOS	Basic Input/Output System
BTC	Bitcoin
BURST	Burstcoin
CLI	Command Line Interface
CPU	Central Processing Unit
CUDA	Compute Unified Device Architecture
dApps	dezentralen Anwendungen
ETH	Ethereum
ETH2	Ethereum 2.0
FIL	Filecoin
FPGA	Field Programmable Gate Array
GPU	Graphics Processing Unit
GUI	Graphical User Interface

HD Wallet	Hierarchisch Deterministisches Wallet
HDD	Hard Disk Drive
JSON	JavaScript Object Notation
LAN	Local Area Network
LTS	Long Time Support
Nvidia	Nvidia Corporation
NXT	Nextcoin
OpenCL	Open Computing Language
OpenGL	Open Graphics Library
PCIe	Peripheral Component Interconnect Express
PIN	Persönliche Identifikationsnummer
PoA	Proof of Activity
PoC	Proof of Capacity
PoS	Proof of Stake
PoSpace	Proof of Space
PoT	Proof of Time
PoW	Proof of Work
RAM	Random-Access-Memory
RDP	Remote Desktop Protocol
RHEL	Redhat Enterprise Linux
RPC	Remote Procedure Call
SATA	Serial Advanced Technology Attachment

SHA	Secure Hash Algorithm
SSD	Solid State Drive
SSH	Secure Shell
TBW	total Bytes written
TCP	Transmission Control Protocol
TRX	Tron
URL	Uniiform Resource Locator
USB	Universal Serial Bus
USD	US-Dollar
USDT	Tether
XCH	Chia
XMR	Monero

1 Einleitung

In der Einleitung werden das Ziel sowie die Motivation dieser Arbeit erläutert. Außerdem werden die Vorgehensweisen beschrieben.

1.1 Motivation

Der Markt von Kryptowährungen wächst immer weiter und gewinnt zunehmend an Aufmerksamkeit. Mit dem Wachstum des Marktes für Kryptowährungen einhergehend, wird das Mining dieser Währungen ebenfalls immer beliebter. Der rasante Anstieg innerhalb kurzer Zeit zeigt sich anhand der Marktkapitalisierung beliebter Währungen wie dem Bitcoin (BTC) oder Ethereum (ETH) sehr deutlich. Innerhalb von 60 Tagen stieg die Marktkapitalisierung von BTC um circa 43% und um circa 59% bei ETH. [12] Noch deutlicher wird der schnelle Anstieg bei Vergleich des Preises für einen BTC in den Jahren 2017 und 2021. Kostet im Januar 2017 ein BTC ca. 930 €, ist er im Januar 2021 bereits ca. 24.110 € wert. Einen historischen Hochpunkt erreicht der BTC im Oktober 2021 mit einem Wert von ca. 58.650 €. [13] Jedoch ist diese Dynamik nicht ausschließlich auf den Wert solcher Währungen, wie BTC beschränkt. Insbesondere bei Hardware zur Generierung von Kryptowährungen besteht eine hohe Nachfrage. Dies lässt sich bei Grafikkarten der Firma Nvidia Corporation (Nvidia) und Advanced Micro Devices, Inc. (AMD) beispielhaft beobachten. Eine Folge der hohen Nachfrage ist eine sinkende Verfügbarkeit und eine Erhöhung der Preise von Grafikkarten. [14] Aus der hohen Dynamik in den Themenfeldern Kryptomining und Kryptowährungen sowie dem Konzept einer dezentralen digitalen Währung wie beispielsweise dem BTC und deren Generierung ergibt sich die Motivation für diese Studienarbeit.

1.2 Ziel

Ziel dieser Studienarbeit ist es, ein Kryptomining System zu konzipieren und zu realisieren. Außerdem soll das Kryptomining System unter wissenschaftlichen Gesichtspunkten analysiert werden. Jedoch ist nicht nur die reine Realisierung des Systems und dessen Analyse Ziel, sondern auch einen umfassenderen Blick auf verschiedenste Währungen zu erlangen. Die Erläuterung grundlegender Konzepte von Kryptowährungen ist ebenfalls Teil dieser Arbeit. Des Weiteren stellt sich die Frage der Optimierung und der Rentabilität, insbesondere in Bezug auf den Stromverbrauch solcher Systeme. Letztlich ist diese Arbeit nur eine Momentaufnahme der Themenbereiche Kryptowährung und Kryptomining. Die bereits in 1.1 erläuterten schnellen Veränderungen lassen keine vollständige und abschließende Betrachtung des Themas zu.

1.3 Vorgehensweise

In Kapitel 2 werden die Grundlagen zum Verständnis dieser Arbeit erläutert. Dazu werden Kryptowährungen sowie deren Aufbewahrung und Verwaltung in Wallets näher betrachtet. Ebenfalls sind Grundlagen zur Blockchain Technologie Teil dieses Kapitels. Die Konzepte zur Generierung von digitalen Währungen werden vorgestellt sowie abschließend die Sicherheit von Wallets und Kryptowährungen beleuchtet. Das darauffolgende Kapitel 3 führt in den Markt der Kryptowährungen ein und stellt die bekanntesten Währungen vor. Diese werden im Anschluss in einem Vergleich gegenübergestellt. Kapitel 4 befasst sich mit der Generierung von Kryptowährungen durch Mining. Dies wird sowohl auf Hardwareebene als auch auf Softwareebene näher beleuchtet. Außerdem werden die Unterschiede zwischen Solo- und Pool-Mining vorgestellt sowie ein für den Kryptomining Prozess wichtiges Protokoll erläutert. Mit dem Kapitel 5 wird die Vorarbeit für die spätere Umsetzung eines Mining-Rigs geleistet. Dafür wird ein Konzept erstellt sowie die verschiedenen notwendigen Komponenten ausgewählt und analysiert. Die Kosten werden dabei ebenfalls berücksichtigt. Die Realisierung sowie die Leistungssteigerung des konzipierten Mining-Rigs ist Teil von Kapitel 6. Eine umfassende Analyse und Auswertung der durch die Umsetzung erlangten Daten findet in Kapitel 7 statt. In Kapitel 8 wird ein Fazit in Form einer Bewertung anhand festgelegter Kriterien gezogen sowie eine Empfehlung gegeben. Schließlich findet im letzten Kapitel ein Ausblick statt. Insbesondere zu Ethereum 2.0 sowie den Energiekosten und Mining in der Zukunft.

2 Grundlagen

In diesem Kapitel werden die zum Verständnis dieser Arbeit notwendigen Grundlagen erläutert. Dazu wird zu Beginn näher auf Kryptowährungen eingegangen. Darauf folgen Erklärungen zu Blockchains und zu Wallets. Transaktionen und die Difficulty sind ebenfalls Teil dieses Kapitels. Außerdem werden verschiedene Möglichkeiten aufgezeigt, wie digitale Währungen generiert werden können. Die Sicherheit von Wallets und Kryptowährungen wird ebenfalls thematisiert.

2.1 Kryptowährungen

Kryptowährungen sind digitale Zahlungsmittel, die auf Grundlage eines Blockchain-Systems arbeiten. Guthaben wird durch eine Transaktion in Form von Daten von einem Teilnehmer zu einem anderen übertragen. [15] Die Regulierung und jede Regel werden dabei in kryptografischen Algorithmen gefasst. Der Name leitet sich aus der Kombination der Begriffe „Kryptografie“ und „Währung“ ab: Kryptowährung. Diese Währung wird durch Kryptografie gesichert und rar gemacht, diese Aufgabe übernimmt beim Euro die Europäische Zentralbank. [16, S.41] Alle Verifizierungen der Transaktion (Signaturprüfung) werden im Netzwerk von Rechnern (Miner) übernommen. Wer einen passenden Signaturschlüssel besitzt, kann Transaktionen einstellen und über das dahinterstehende Guthaben verfügen. Der Schlüssel wird in einer digitalen Geldbörse (Wallet) hinterlegt und gespeichert. Bei einem Zahlungsvorgang wird der Zahlungsempfänger durch eine abstrakte, generierte Adresse (eine Art Kontonummer) repräsentiert. Durch dieses Verfahren werden Kryptowährungen pseudonym verwendet. Sogenannte Miner überwachen und führen dann die Transaktionen aus. [15] Laut Bundesamt für Finanzdienstleistungsaufsicht stellen Kryptowährungen keine Währung, sondern Finanzinstrumente dar. [17] Nach Einschätzung des Bundesministeriums der Finanzen werden sie als Wirtschaftsgüter eingestuft, sodass im Umgang mit Kryptowährungen steuerliche Aspekte zu beachten sind. [18] Für Kryptowährungen gibt es keine staatlichen Regulierungen, dies kann zu

verschiedensten negativen Folgen führen, zum Beispiel kann der Ausschluss eigener Transaktionen aufgrund von einer Mehrheitsentscheidung der Miner die Folge sein. Außerdem sind Kryptowährungen durch das aufwendige Miningverfahren zur Verwaltung der Block-chain oft wenig effizient und erfordern einen großen Hardwareaufwand und einen hohen Stromverbrauch. BTC ist die bekannteste Währung, allerdings gibt es mittlerweile mehr als 1000 verschiedene Kryptowährungen am Markt. [15]

2.2 Wallets

Mithilfe von Wallets können Bestände von Kryptowährungen verwaltet werden. Sie funktionieren dabei nach dem Prinzip einer Geldbörse. Wallets bestehen aus einem Public-Key und einem Private-Key. Der Public-Key ist nicht geheim und wird von der Gegenseite zur Überweisung von Coins auf das eigene Wallet genutzt. Dies ist vergleichbar mit einer Kontokennung. Der Public-Key besteht aus einer Zeichenkette mit 34 Zeichen. Den anderen Teil des Wallets bildet der Private-Key. Dieser ist geheim, darf nicht geteilt werden und ist bestmöglich zu schützen. Am Beispiel von BTC besteht dieser Private-Key aus einer 52-stelligen Zeichenkette. Public-Key und Private-Key sind stets einander zugeordnet und im gesamten BTC Netzwerk eindeutig. Ein Wallet kann mehrere Schlüsselpaare und damit auch Adressen zum Empfangen von Coins beinhalten. Zusätzlich wird für jedes Wallet eine *Mnemonische Passphrase* oder auch *seed recovery phrase* genannt, erstellt. Diese besteht aus 12 oder 24 Wörtern. Mithilfe dieser Wörter können alle im Wallet gespeicherten Schlüsselpaare wiederhergestellt werden. Diese *recovery phrases* werden bei hierarchischen, deterministischen Wallets eingesetzt. Gehen Wallet und die *seed recovery phrase* verloren, besteht keine Möglichkeit auf das Wallet zuzugreifen oder es wiederherzustellen. Damit stellt die *seed recovery phrase* eine Option zur Sicherung von Wallets dar. In der Praxis wird pro Transaktion ein Schlüsselpaar und somit auch eine Adresse verwendet, d.h. für jede Transaktion sollte eine neue Adresse generiert werden. [19, 20, 21]

Es gibt verschiedene Wallet Architekturen, die im folgenden kurz vorgestellt werden.

Nichtdeterministische Wallets

Nichtdeterministische Wallets basieren auf der zufälligen Generierung von Private-Keys. Die Schlüssel stehen untereinander in keiner Beziehung. Da pro Transaktion eine neue Adresse verwendet werden soll, setzt dies auch einen neuen Private-Key voraus. Folglich müssen viele Schlüssel generiert werden. Geht ein Schlüssel verloren, so ist der Betrag an Coins auf diesem Wallet verloren. Der Aufwand, jeden privaten Schlüssel zu sichern, ist hoch. [22, S.96]

Deterministische Wallets

Deterministische Wallets werden als *Seed Wallets* bezeichnet. Bei *Seed Wallets* werden alle Private-Keys des Wallets aus einem *Seed* abgeleitet. Somit muss für die Sicherung des gesamten Wallets nicht jeder private Schlüssel gesichert werden, sondern lediglich der *Seed*. Aus diesem sind die Private-Keys wiederherstellbar. Außerdem können die Public-Keys aus den Private-Keys errechnet werden. Die in 2.2 bereits erwähnte *Mnemonische Passphrase* findet bei diesem Wallet Typ Anwendung. Die Kette von 12 bzw. 24 Wörtern dient zum Wiederherstellen des *Seeds* und damit letztlich allen Private-Keys. Somit ist für die Sicherung eines deterministischen Wallets nur der *Seed* oder die *Mnemonische Passphrase* notwendig. [20][22, S.97f]

Hierarchisch deterministische Wallets

Hierarchisch Deterministisches Wallets (HD Wallets) sind eine Erweiterung des ursprünglichen deterministischen Wallets. Die einzelnen Schlüssel sind in einer Baumstruktur angeordnet. Dabei kann immer nur der in der Hierarchie weiter unten gelegene Schlüssel abgeleitet werden. Aus dem *Seed* wird in der Regel ein Master-Key erstellt, mit welchem dann weitere Schlüssel, sogenannte Parent Schlüssel, abgeleitet werden können. Diese Architektur ermöglicht es beispielsweise, neue Public-Keys zu erstellen, ohne selbst im Besitz des Private-Keys sein zu müssen. Wie auch bei deterministischen Wallets wird eine *mnemonische Passphrase* erstellt, mit der bei Verlust des Wallets der *Seed* und damit alle Schlüssel wiederhergestellt werden können. Abbildung 2.1 zeigt den Aufbau eines solchen Wallets. [22, S.98f]

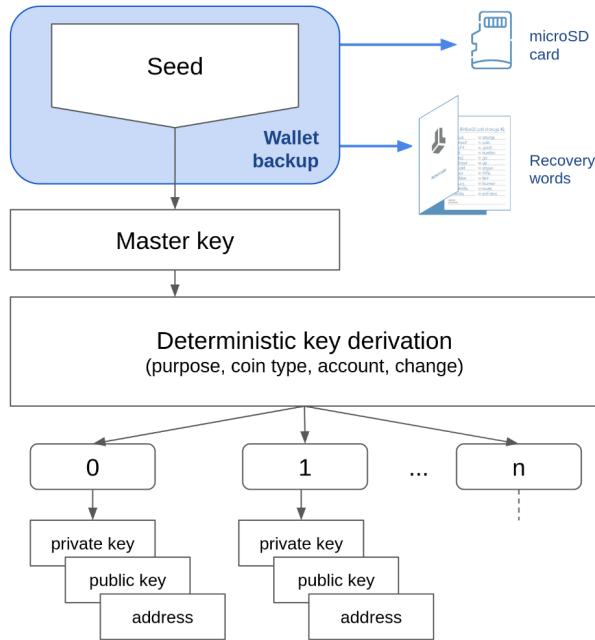


Abbildung 2.1: HD Wallet Aufbau [1]

Die Nutzung eines HD Wallets mit entsprechender *Mnemonische Passphrase* entspricht dem heute gängigen Standard. Durch die vereinfachten Sicherungsmöglichkeiten sowie der Flexibilität, die HD Wallets bieten, sind sie den nichtdeterministischen Wallets überlegen. [22, S.99f]

In der Praxis unterscheiden sich Wallets in zwei grundlegende Arten. Im Folgenden werden beide mit zugehörigen Beispielen erläutert.

Cold-Wallets

Cold-Wallets sind Wallets, die nicht mit dem Internet verbunden sind. Sie können somit nicht aus der Ferne angegriffen werden. Oft werden Cold-Wallets in Tresoren oder an anderen sicheren Orten aufbewahrt, um zusätzliche Sicherheit zu erreichen. [23] Die Generierung eines solchen Wallets erfolgt optimalerweise auf einem System ohne Netzwerkzugriff. So soll sichergestellt werden, dass die Private-Keys zu keinem Zeitpunkt über das Internet erreichbar sind. Um Kryptowährungen auf diesem vom Netzwerk getrennten Wallet empfangen und Transaktionen überprüfen zu können, kann zusätzlich ein *watch-only* Wallet eingerichtet werden. Dabei wird der Public-Key des Cold-Wallets auf ein System mit Internetverbindung übertragen. Somit lassen sich Transaktionen überprüfen

und Währungen auf dieses Wallet empfangen. Jedoch können keine Kryptowährungen an andere Wallets gesendet werden. Die Signierung von Transaktionen ist ebenfalls nicht möglich, da der Private-Key ausschließlich offline im Cold-Wallet vorhanden ist.[24] Ein solches Cold-Wallet mit zusätzlichem *watch-only* Wallet lässt sich auf gängigen Computern mit einer Wallet Software realisieren. Paper-Wallets sind ein Beispiel für Cold-Wallets. Das Prinzip von Paper-Wallets besteht darin, alle relevanten Informationen auszudrucken und sicher aufzubewahren. Auch bei einem Paper-Wallet lässt sich ein zusätzliches *watch-only* Wallet realisieren. Dazu werden lediglich der Public-Key des Paper-Wallets sowie ein mit dem Internet verbundenes System mit entsprechender Wallet Software benötigt. [25, 26, 27]

Hot-Wallets

Hot-Wallets sind das Gegenteil von Cold-Wallets. Sie sind mit dem Internet verbunden oder werden über das Internet dem Nutzer bereitgestellt. Die Private-Keys sind dabei über das Internet erreichbar und liegen entweder auf dem Gerät des Besitzers oder auf den Servern eines Anbieters. Online-Wallets, mobile App Wallets und Desktop-Wallets sind Beispiele für Hot-Wallets. Wobei bei Online-Wallets die Private-Keys auf den Servern des entsprechenden Anbieters gespeichert sind und nicht beim Besitzer des Wallets. Dies hat zur Folge, dass insbesondere Online-Wallets eine große Angriffsfläche für Attacken und den Diebstahl von Private-Keys bieten. Auch bei mobilen App-Wallets und Desktop-Wallets besteht die Gefahr eines Angriffes und Diebstahls der zugehörigen Private-Keys, beispielsweise durch Viren auf den Geräten des Wallet-Besitzers. Dem gegenüber steht die einfache Benutzung für den Anwender. Es können ohne weiteres Transaktionen signiert und Kryptowährungen an andere Wallets gesendet werden. [23, 25, 27]

Weitere Arten von Wallets sind Multi-Signature-Wallets und Hardware-Wallets. Da diese im Umgang mit der Verwahrung von Kryptowährungen Anwendung finden, werden sie kurz vorgestellt.

Multi-Signature-Wallets

Im Gegensatz zu Paper-Wallets oder Online-Wallets, die i.d.R. *Single-Key* Wallets sind, werden bei Multi-Signature-Wallets mehrere Private-Keys zur Bestätigung von Transaktionen benötigt. Für den Zugriff auf die vorhandenen Währungen des Wallets bedarf es allen

zugehörigen Private-Keys des Wallets. Mit einem einzelnen Private-Key können keine Kryptowährungen an andere Wallets versendet werden. Die Signierung von Transaktionen ist ebenfalls nur mit allen Private-Keys möglich. Die Aufteilung, wie viele Private-Keys zu einem Multi-Signature-Wallet gehören und wie viele von diesen für den Zugriff benötigt werden, kann frei definiert werden. Beispielsweise können aus insgesamt drei Schlüsseln nur die Signatur von zwei benötigt werden. Dies wird als *2-of-3* bezeichnet. [25, 28]

Hardware-Wallets

Um die Wallet-Sicherheit zu erhöhen, werden Wallets auch in Form von Hardware bereitgestellt. Sie besitzen oft die Form eines Universal Serial Bus (USB)-Sticks und werden an einen Computer angeschlossen, der über eine entsprechende Software des Herstellers verfügt. Die Private-Keys sind in einem besonders gesicherten Bereich des Hardware-Wallets gespeichert. Damit bei einer Transaktion nicht der Private-Key offenbart werden muss, wird die Transaktion an das Hardware-Wallet übertragen, von diesem intern signiert und entsprechend wieder zurückgegeben. So ist zu keinem Zeitpunkt der direkte Zugriff auf Private-Key möglich. Zusätzlich sind Hardware-Wallets mit Passwörtern oder Persönliche Identifikationsnummer (PIN) gesichert, um zu verhindern, dass der reine Besitz des Wallets für den Zugriff auf die Währungen ausreicht. Da der Verlust des Hardware-Wallets zum Verlust des Zugriffs auf die Private-Keys und damit auf die Vermögenswerte des Wallets führt, sollte die *Mnemonische Passphrase* an einem anderen sicheren Ort aufbewahrt werden. Nur so kann ein Hardware-Wallet wiederhergestellt werden. [29, 25]

2.3 Blockchain

In der Welt der Kryptowährungen ist die sogenannte Blockchain eine bedeutsame Technologie. „Die Blockchain Technologie bietet die Grundlage zur Existenz einer dezentralen digitalen Währung.“ [16, S.41] Es sind damit Vermögensübertragungen ohne ein Finanzinstitut oder sonstige Kontrollinstanzen möglich. Ziel der Blockchain ist es, Daten in einer verteilten Infrastruktur ohne zentrale Instanz nachvollziehbar und manipulationssicher zu machen. Die Blockchain ermöglicht es ohne zentrale Instanz, vertrauensvoll und transparent Transaktionen mit Kryptowährungen zu verifizieren. [15]

Der Name Blockchain leitet sich vom Aufbau der Daten ab. Es werden Blöcke aus Datensätzen gebildet und Blöcke werden wiederum zu einer wachsenden Blockkette (engl.

Blockchain) miteinander verknüpft. [15] Die Datensätze enthalten Transaktionen und somit bildet die Blockchain eine Kette, bestehend aus einer chronologischen Reihenfolge von Transaktionen. Die Blockchain kann dadurch mit einem Kontenbuch verglichen werden. Mithilfe von Kryptografie wird diese zu einer unveränderlichen Transaktionshistorie. [16, S.64] Im Vergleich zu einem zentralisierten System ist es möglich, die Blockchain von jeder Person und zu jeder Zeit öffentlich einzusehen. [30, S.20] Auf der Webseite bitcoin.org kann die vollständige Blockchain für den BTC heruntergeladen und nachvollzogen werden. [31] Diese ist allerdings sehr groß und wächst immer weiter an. Es ist als Teilnehmer nicht notwendig, die komplette Transaktionshistorie zu speichern. Dieser Vorgang wäre umständlich, es kommt daher die Blockstruktur zum Tragen. [30, S.20] In jedem Block werden mehrere Transaktionen vereint und verkettet. Jeder neue Block baut unwiderruflich auf seinen direkten Vorgänger auf, dadurch kann dieser als vertrauensvollen Beweis für die Teilnehmer angesehen werden für die Geschehnisse der Blöcke davor. [16, S.64/65] Die Abbildung 2.2 verdeutlicht nochmals die Funktionsweise einer Blockchain. Nach Jörg

Was ist eine Blockchain

und wie funktioniert sie?

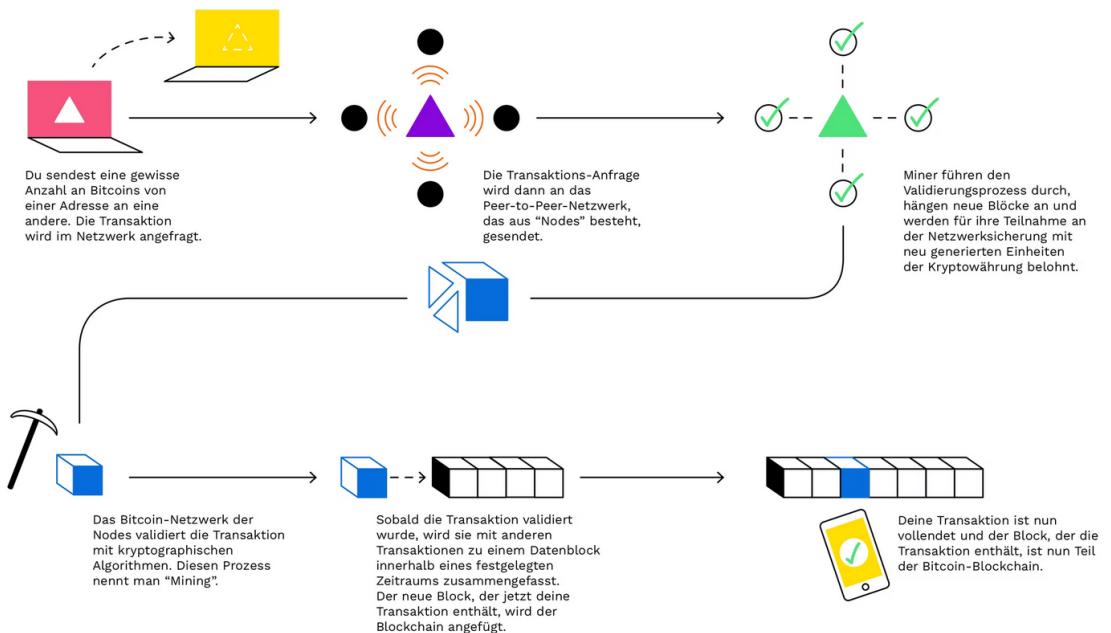


Abbildung 2.2: Funktionsweise einer Blockchain [2]

Platzer enthält jeder Block folgende Informationen:

1. Transaktionen, die seit der Erstellung des letzten Blocks vollzogen wurden
2. Proof of Work (PoW) (Arbeitsbeweis): Das Ergebnis des Bitcoin-Minings
3. Eine Nonce, mit einem mathematischen Bezug auf den Vorgängerblock. Dieser beweist den Teilnehmern, dass der neue Block auf dem bisherigen Stand der gemeinsamen Buchhaltung (bisherige Blöcke) aufbaut.

Es ist die Sprache einer gemeinsamen Buchhaltung, da alle Teilnehmer seit der ersten Transaktion der Blockchain das gleiche Kontenbuch als Wahrheit akzeptieren. Jede Transaktion wird außerdem mit einem Zeitstempel versehen. [31, S.21] Das hat zur Folge, dass die Transaktionshistorie in der chronologischen Reihenfolge und unveränderlich festgehalten wird. Alle Transaktion werden im Netzwerk von sogenannten Minern überwacht. Da Transaktionen entweder ganz oder gar nicht durchgeführt werden müssen und ein Zahlungsempfänger jederzeit die aktuelle Version des Kontenbuches (Blockchain) kennt, ist es nicht möglich, einen BTC „doppelt“ auszugeben (Double Spending Problem). [16, S.38]

2.4 Difficulty

Beim Konsensverfahren PoW 2.6.1 findet ein Wetteifern auf das Lösen der Blöcke statt, um eine Belohnung zu erhalten. Je nach Komplexität der Aufgabe wird mehr oder weniger Zeit beansprucht. Diese Komplexität wird auch Difficulty(dt. Schwierigkeit) genannt. Genauer betrachtet geht es darum, einen Hash zu erzeugen.

Ein Hash ist ein alphanumerischer Code, der zur Darstellung von Wörtern oder Daten verwendet wird. Miner nehmen einen Stapel Transaktionsdaten und lassen ihn durch einen Hash-Algorithmus laufen, eine Einwegfunktion, die - bei einem bestimmten Datensatz - immer dasselbe Ergebnis liefert, dessen Ausgabe aber nicht umgekehrt werden kann, um die ursprünglichen Daten anzuseigen. Zur Erstellung dieser zufälligen Hash-Codes werden Hash-Algorithmen verwendet. Bevor neue Daten zu einer Blockchain hinzugefügt werden können, müssen Miner darum wetteifern, einen Hash zu erzeugen, der kleiner oder gleich einem numerischen Wert ist, der als Ziel-Hash bezeichnet wird.

Die Miner führen den Hashing-Prozess durch, indem sie einen einzigen Wert ändern, der als Nonce betitelt wird - oder eine Zahl, die nur einmal verwendet wird - und jedes Mal,

wenn die Nonce geändert wird, wird ein neuer Hash mit einer eigenen Reihe von Zahlen erstellt. Es gibt keine Möglichkeit, vorherzusagen, wie ein Hash aussehen wird und da jeder Datensatz nur eine Ausgabe für eine bestimmte Hash-Funktion hat, müssen die Miner den Prozess des Hinzufügens einer neuen Nonce zu den Daten wiederholen, bis sie die Hash-Anforderung erfüllen.

Die Anforderung, die ein Hash erfüllen muss, entspricht der Schwierigkeit. Ein gültiger Hash muss unter einem bestimmten Zielwert liegen, der vom Protokoll der Kryptowährung automatisch festgelegt (und in regelmäßigen Abständen angepasst) wird. Je niedriger der Zielwert ist, desto mehr Wiederholungen der Hash-Funktion muss ein Miner durchlaufen, um ein akzeptables Ergebnis zu erhalten - mit anderen Worten, desto höher ist die Schwierigkeit. Ein Schürfer kann theoretisch Glück haben und beim ersten Versuch einen gültigen Hash für einen bestimmten Block erhalten. Im Laufe der Zeit bedeutet ein höherer Schwierigkeitsgrad jedoch, dass die Schürfer im Durchschnitt mehr Nonces pro Block durchprobieren müssen. [32]

2.5 Transaktionen

Transaktionen basieren neben der in Kapitel 2.3 bereits beschriebenen Blockchain Technologie auf digitalen Signaturen. Mit digitalen Signaturen können Nachrichten oder Daten von einer Person unterschrieben werden. Diese Unterschrift lässt sich auf ihre Echtheit überprüfen. Eine Manipulation, beispielsweise durch Veränderung der unterschriebenen Nachricht, kann ebenfalls festgestellt werden. Um Nachrichten zu signieren, wird ein sogenanntes Schlüsselpaar benötigt. Dieses Schlüsselpaar umfasst einen Private- und einen Public-Key. Mit dem Private-Key wird die zu signierende Nachricht verrechnet. Im Anschluss kann mithilfe des zugehörigen Public-Keys diese Signatur überprüft werden. Die Sicherheit von digitalen Signaturen ist dadurch gewährleistet, dass die Berechnung des Private-Keys aus dem Public-Key sehr aufwändig ist. Außerdem lassen sich Manipulationen der Nachricht mithilfe von digitalen Signaturen erkennen. Dazu wird aus der ursprünglichen Nachricht mittels eines Hash-Algorithmus ein Wert fester Länge gebildet. Dieser Wert wird mithilfe des Private-Keys signiert. Der Empfänger der Nachricht bildet aus dieser ebenfalls mittels des Hash-Algorithmus den Hash Wert und vergleicht ihn mit dem vom Sender signierten Hash Wert. Sind die Werte unterschiedlich, kann von einer Manipulation der Nachricht ausgegangen werden. Abbildung 2.3 verdeutlicht die Funktionsweise von digitalen Signaturen.

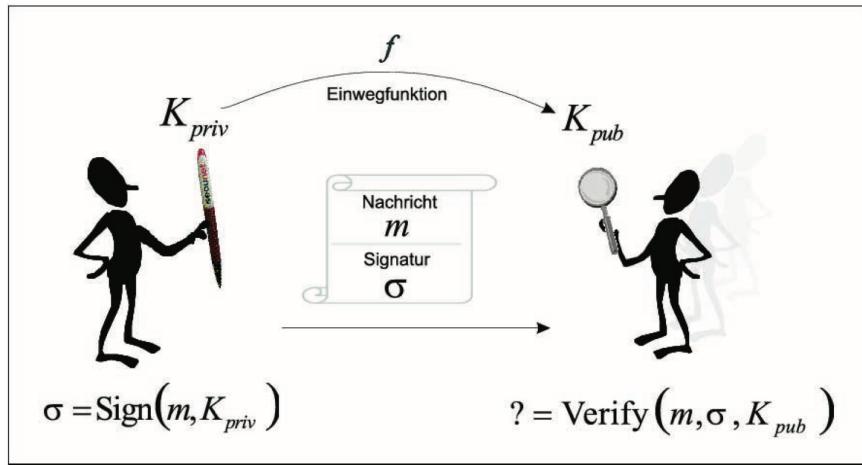


Abbildung 2.3: Funktionsweise digitaler Signaturen [1]

Im Folgenden wird der Ablauf einer BTC Transaktion erläutert. Um eine bestimmte Anzahl an BTCS an ein anderes Wallet überweisen zu können, wird dessen Public-Key benötigt. Der Public-Key ist dabei letztlich die Adresse des Wallets.

Eine BTCS Transaktion besteht aus drei Informationen:

1. Input
2. Menge
3. Output

Der Input beinhaltet die Adresse, von der zuvor die BTCS an den jetzigen Sender gesendet wurden. Somit ist der Ursprung der in der aktuellen Transaktion zu versendenden BTCS bekannt. Die Menge wird durch den Sender bestimmt. Der Bestand des Sender-Wallets ist gleichzeitig auch die maximale Menge an BTCS, die transferiert werden können. Der Output entspricht der Empfängeradresse, an die überwiesen werden soll. Die Transaktionen mit den genannten Informationen werden vom Sender mit dem Private-Key seines Wallets signiert. Die signierte Transaktion wird im BTCS Netzwerk veröffentlicht und bestätigt. Die Bestätigung erfolgt am Beispiel BTC mittels Proof of Work (siehe 2.6.1). Ist die Transaktion in der Blockchain (siehe 2.3) und im Netzwerk bestätigt, ist die Menge an transferierten BTCS dem Empfänger Wallet zugeordnet und für den Empfänger in dessen Wallet sichtbar. Abbildung 2.4 zeigt anschaulich den Ablauf einer BTCS Transaktion.

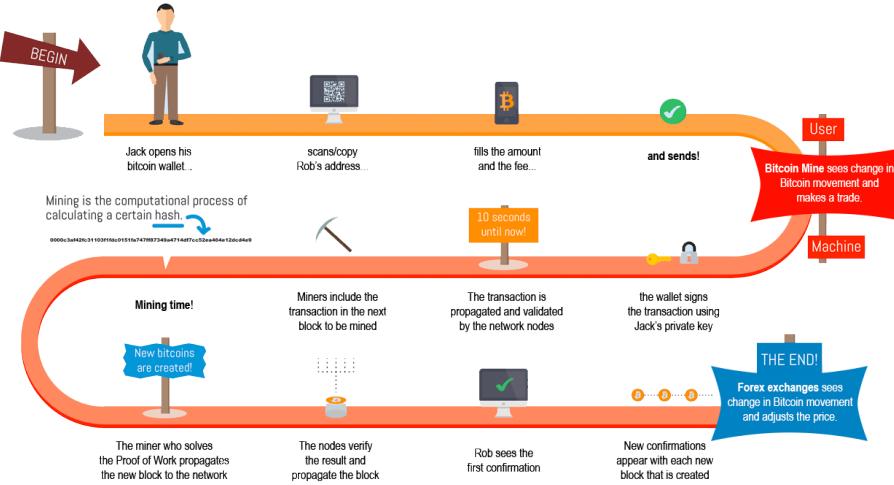


Abbildung 2.4: Ablauf einer BTC Transaktion [1]

2.6 Generierung digitaler Währungen

Um die Dezentralität der Kryptowährungen zu sichern, müssen alle Teilnehmer des Netzes die getätigten Transaktionen verifizieren und speichern. Für die Struktur der Blockchain muss sichergestellt sein, welcher Teilnehmer den nächsten Block berechnet (löst). Die Lösung eines Blockes wird in der jeweiligen Währung belohnt, daher muss die Lösung eine gewisse Hürde darstellen, die von allen Teilnehmern akzeptiert wird. Für das Beweisverfahren, das Konsensverfahren, gibt es mehrere Ansätze. Der bekannteste und meistgenutzte Ansatz ist Proof of Work, der sogenannte Arbeitsbeweis. Ein weiterer und immer populärer werdender Ansatz ist Proof of Stake. Proof of Stake setzt eine gewisse Menge an Kryptowährung voraus, um Lösungen durchführen zu dürfen. Immer häufiger werden auch Kombinationen aus diesen Verfahren, also Hybridverfahren, eingesetzt.

2.6.1 Proof of Work

Aus dem Englischen übersetzt bedeutet proof of work: Arbeitsbeweis. Dieser Nachweis über die Lösung eines Blocks kommt bei vielen Coins zum Einsatz, der bekannteste hierfür ist der BTC. Die Lösung eines Blocks wird mit der verwendeten Währung belohnt. Aus wirtschaftlicher Sicht muss es [...] etwas kosten, einen Block zu kriegen, ansonsten kann Information kostenlos kreiert, verändert oder gelöscht werden.“ [16, S.59] Dadurch entsteht ein Rennen zur Lösung und auf die damit verbundene Belohnung. Die Höhe der Belohnung ist davon abhängig, wie viele Blöcke bereits erzeugt wurden. Dies stellt letztlich

einen Mechanismus dar, um die Kryptowährung zu stabilisieren. Im Falle des Bitcoins wurde ein Block bei seiner Einführung im Januar 2009 mit 50 neuen BTC belohnt. Nach 210.000 geschriebenen Blöcken kommt das Bitcoin-Halving zum Tragen. Das bedeutet, der darauffolgende Block wird nur noch mit 25 BTC entlohnt. Eine Bitcoin-Halving Periode dauert etwa vier Jahre an. Aktuell im Jahr 2022 beträgt die Entlohnung eines gelösten Blockes 6,25 BTC. [33] Bei einem Eurowechselkurs von 36.000 € zu einem BTC entspricht die Lösung eines Blocks 225.000 €. [34] Das nächste Bitcoin-Halving wird für das Jahr 2024 erwartet. Die Abbildung 2.5 verdeutlicht die Arbeitsweise des Konsensverfahrens PoW.

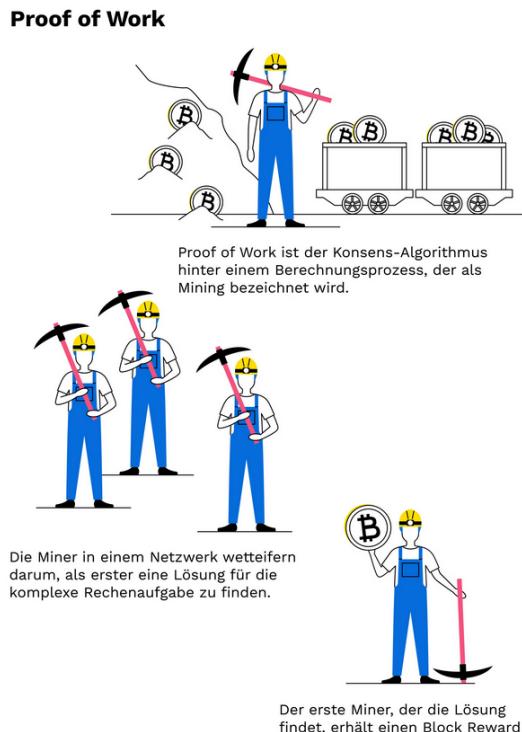


Abbildung 2.5: Funktionsweise Proof of Work [2]

Die Lösung eines Blocks basiert auf einem komplexen kryptografischen Algorithmus. [16, S.62] Diese „Rechenaufgaben“ sind einerseits sehr schwer und anderseits rechenintensiv, aber ist die Lösung erfolgt, kann diese von anderen Teilnehmern einfach und schnell überprüft und akzeptiert werden. [30, S.23] Die Lösung des Problems kann nicht direkt errechnet werden, sondern muss durch Probieren von Millionen verschiedener Möglichkeiten erraten werden. Dieser Rateprozess hat zur Folge, dass Miner mit einer großen Rechenleistung eine höhere Wahrscheinlichkeit zur Lösung aufweisen. Üblich ist auch der Zusammenschluss von Minern zu einem Miner-Pool, mit gebündelter Rechenleistung, um das Rennen zu gewinnen und die Belohnung unter den Minern aufzuteilen. Der Rateprozess

erlaubt es zudem mit einer unwahrscheinlich geringen Wahrscheinlichkeit von eins zu einer Million (1:1.000.000), dass auch einzelne Miner das Rennen zur Lösung eines Blocks gewinnen können. Zuletzt wurde ein solcher Erfolg Anfang des Jahres 2022 erzielt. [35]

2.6.2 Proof of Stake

Der zweite populäre Nachweis verfolgt einen anderen Ansatz. Stake bzw. staken bedeutet übersetzt einen Anteil einlegen und tatsächlich ist ein Anteil an der jeweiligen Währung Voraussetzung, um sich für die Lösung eines Blocks zu verifizieren. Neben dem Besitz der Währung ist es weiterhin entscheidend, wie lange diese schon „eingelegt“ wurde. Wer mehr Geld im System kontrolliert, wird auch automatisch eine größere Bedeutung zugemessen. Das Prinzip basiert auf einem Social Media Phänomen. Das Vertrauen in eine Freundschaftsanfrage ist größer, wenn der anfragende Account selbst viele Freunde hat und schon lange existiert. Das Vorgehen bringt allerdings auch Kritiker hervor und wirft die Frage auf, wie ein solches Netzwerk dezentralisiert bleiben kann, denn letztendlich kontrollieren wenige Reiche den Konsens. [16, S.60] Neben der Kritik gibt es aber auch einen entscheidenden Vorteil zum Thema Nachhaltigkeit. Der Energieverbrauch ist im Vergleich zu PoW deutlich geringer, da das „Rennen“ auf die Lösung wegfällt. Außerdem wird ein Zufalls-Algorithmus eingesetzt, um einen Teilnehmer zu ziehen, der den nächsten Block lösen darf. Die Folge daraus ist, wer einen höheren Stake hält, hat automatisch eine höhere Wahrscheinlichkeit, gezogen zu werden. [34] Allerdings wird dieser Blockchain Mechanismus bisher von wenigen Kryptowährungen genutzt. Bei jenen, die diesen Mechanismus nutzen, funktioniert er allerdings überraschend gut. Das Problem, dass nur wenige den Konsens beherrschen, wird laut Julian Hosp mit folgenden Mitteln eingedämmt:

- Eine Stimmabstimmung lässt sich wie folgt errechnen: Wer 1000 Coins in einer Gemeinschaft staked, in der 100.000 Coins gestaked werden, hat ein Stimmrecht von einem Prozent und bekommt gleichzeitig ein Prozent der ausgeschütteten Belohnung. Wichtig dabei ist, wenn jemand viel Geld hat, hat er nicht unbedingt ein großes Stimmrecht. Dies steht ihm nur dann zu, wenn das Vermögen gestaked und nicht im Umlauf gehalten wird.
- Da Geld in einem Blockchain-System nicht aus dem Nichts entstehen kann, ist die Wahrscheinlichkeit von betrügerischen Angriffen gering.
- Die Belohnungen der Blockchain werden gleichmäßig auf die Staker aufgeteilt, sodass sich eine Rendite berechnen lässt. Es ist zum Beispiel möglich, dass die Blockchain

rund fünf Prozent des gestakten Kapitals pro Jahr auszahlt. Wer über das Jahr 1000 Coins staked wird also mit 50 Coins belohnt.

Während sich im PoW Konzept der Begriff Mining etabliert hat, spricht man beim PoS Ansatz vom Minting, zu Deutsch: Prägen. Ein weiterer Punkt, der für den Erhalt des dezentralen Systems spricht, ist, dass es bei PoS nicht möglich ist, konzentrierte Mining-Pools zu erstellen. Einer der bekanntesten Vertreter dieses Systems ist der Nextcoin (NXT). Die Abbildung 2.6 untermauert die Funktionsweise des PoS Verfahrens.

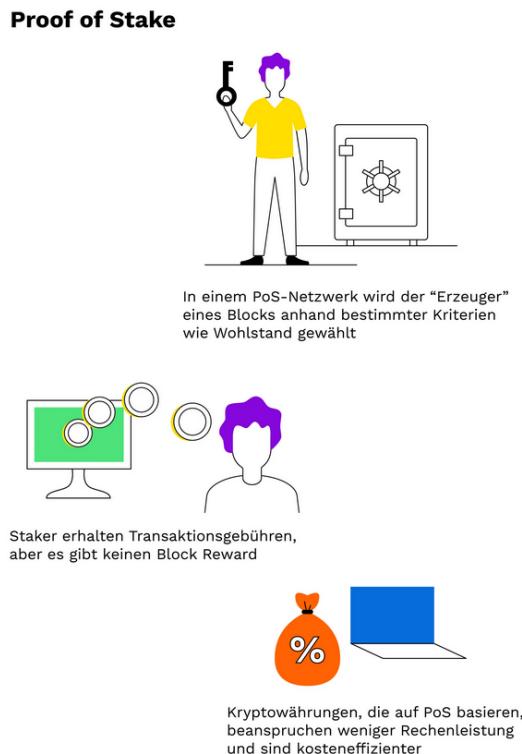


Abbildung 2.6: Funktionsweise Proof of Stake [2]

2.6.3 Proof of Activity

Die Hybridversion aus PoW und PoS wird auch als Proof of Activity (PoA) bezeichnet. Das PoA-System ist ein Versuch, die besten Aspekte des PoW- und des PoS-Systems zu kombinieren. Bei PoA beginnt der Mining-Prozess auf die gleiche Weise wie bei einem PoW-Prozess, wobei verschiedene Miner versuchen, sich gegenseitig mit höherer Rechenleistung zu übertreffen, um einen neuen Block zu finden. Wenn ein neuer Block gefunden (oder geschürft) wurde, schaltet das System auf PoS um, wobei der neu gefundene Block nur einen Header und die Belohnungsadresse des Schürfers enthält. [36] [37]

Anhand der Header-Details wird eine neue, zufällige Gruppe von Validatoren aus dem Blockchain-Netzwerk ausgewählt, die den neuen Block validieren oder signieren muss. Je mehr Münzen ein Prüfer besitzt, desto größer sind seine Chancen, als Unterzeichner ausgewählt zu werden. [37]

Sobald alle Validierer den neu gefundenen Block signiert haben, erhält er den Status eines vollständigen Blocks, wird identifiziert und dem Blockchain-Netzwerk hinzugefügt und die Transaktionen werden auf ihm aufgezeichnet. Sollten einige der ausgewählten Unterzeichner nicht in der Lage sein, den Block vollständig zu unterzeichnen, geht der Prozess zum nächsten Gewinnerblock über, wobei eine neue Gruppe von Validierern nach dem Zufallsprinzip ausgewählt wird (abhängig von ihrem Münzeinsatz). Dieser Prozess wird so lange fortgesetzt, bis ein Siegerblock die erforderliche Anzahl von Unterzeichnern erhält und zu einem vollständigen Block wird. Die Mining-Gebühren/Belohnungen werden zwischen dem Miner und den verschiedenen Validierern aufgeteilt, die in ihrer jeweiligen Rolle dazu beigetragen haben, den Block zu validieren. [37] [38]

2.6.4 Proof of Space / Proof of Capacity

Proof of Space (PoSpace) (auch Proof of Capacity (PoC)) ist eine Konsensmethode zum Nachweis eines berechtigten Interesses an einem Dienst (z. B. dem Versenden einer E-Mail) durch Zuweisung einer nicht trivialen Menge an Datenspeicher zur Lösung einer vom Dienstanbieter gestellten Aufgabe. Das Konzept wurde 2013 von Dziembowski et al. und Ateniese et al. formuliert. PoSpace ist dem PoWs sehr ähnlich. Der Unterschied besteht jedoch darin, dass anstelle von Berechnungen Speicher verwendet wird, um Blöcke in der Blockchain zu erstellen und z. B. Kryptowährung zu verdienen. PoSpace unterscheidet sich von speicherintensiven Funktionen dadurch, dass der Engpass nicht in der Anzahl der Speicherzugriffe, sondern in der Menge des benötigten Speichers liegt.

Nach der Veröffentlichung von Bitcoin wurden Alternativen zum PoW-Mining-Mechanismus erforscht und PoSpace wurde im Zusammenhang mit Kryptowährungen untersucht. PoSpace werden als ressourceneffizientere Alternative angesehen, da sie weniger Energiekosten für die Speicherung erfordern. Auf der anderen Seite werden sie wegen des steigenden Bedarfs an Speicherhardware kritisiert. Es wurden mehrere theoretische und praktische Implementierungen von PoSpace veröffentlicht und diskutiert, z. B. von Chia (XCH).

Das PoC-Protokoll umfasst einen zweistufigen Prozess, der Plotten und Mining beinhaltet. Zunächst wird die Festplatte geplottet: Die Liste aller möglichen Nonce-Werte wird durch wiederholtes Hashing von Daten, einschließlich des Kontos eines Miners, erstellt. Jeder dieser Nonce-Werte enthält 8192 Hashes, die von 0 bis 8191 durchnummieriert sind. Alle Hashes werden in "Scoops", zu Deutsch "Schaufelen" gepaart, das bedeutet, benachbarte Hashes werden zu einem Zweierpaar zusammengefasst. So bilden beispielsweise Hash 0 und 1 die Schaufel 0, Hash 2 und 3 die Schaufel 1 und so weiter. [39] [40]

Der zweite Schritt ist der eigentliche Mining-Vorgang, bei dem ein Miner eine Scoop-Zahl berechnet. Wenn ein Schürfer beispielsweise mit dem Schürfen beginnt und eine Schaufelnummer 38 generiert, geht er zur Schaufelnummer 38 der Nonce 1 und verwendet die Daten dieser Schaufel, um einen Terminwert zu berechnen. Der Vorgang wird für die Berechnung der Frist für jede auf der Festplatte des Schürfers gespeicherte Nonce wiederholt. Nach der Berechnung aller Fristen wird diejenige mit der geringsten Frist vom Miner ausgewählt. Eine Frist ist die Zeitspanne in Sekunden, die seit dem letzten gelösten Block vergehen muss, bevor ein Schürfer einen neuen Block lösen darf. Wenn innerhalb dieser Zeit kein anderer einen Block gelöst hat, kann der Schürfer einen Block lösen und die Blockbelohnung beanspruchen. [40] [41]

Wenn Miner X unter anderem eine Mindestfrist von 36 Sekunden einhält und kein anderer Miner den Block innerhalb der nächsten 36 Sekunden lösen kann, sichert sich X die Chance, den nächsten Block zu lösen und eine Belohnung zu erhalten. [40] [41]

2.7 Sicherheit und Anonymität

Sicherheit und Anonymität spielen bei Kryptowährungen eine große Rolle. Daher werden diese beiden Aspekte im Folgenden differenziert und näher betrachtet.

2.7.1 Sicherheit

Unter Sicherheit können verschiedenste Gesichtspunkte herangezogen werden. Neben der Sicherheit in Bezug auf den Wert der Kryptowährung stellt sich ebenfalls die Frage nach der Sicherheit des Netzwerkes, der Blockchaintechnologie und der Dezentralisierung, da diese den Kern von Kryptowährungen darstellen.

Sicherheit des Wertes

Kryptowährungen wie der BTC unterliegen ständigen Preisschwankungen. Ähnliches ist auf dem Aktienmarkt zu beobachten. Der Wert des BTCS ist wie bei allen anderen Kryptowährungen somit nicht konstant. Der Tiefpunkt von BTC im Jahr 2021 lag bei ca. 25.300 €. Der Hochpunkt erreichte im selben Jahr ca. 58.300 €.[42] Diese enormen Kursschwankungen des BTCS stellen ein entsprechendes Verlustrisiko dar. Die Sicherheit des Wertes beispielsweise eines BTCS ist daher zu keinem Zeitpunkt gewährleistet.

Sicherheit durch Dezentralisierung

Bei PoW (siehe 2.6.1) Netzwerken wie beispielsweise dem Bitcoin (BTC) Netzwerk besteht die Möglichkeit einer 51% Attacke. Ein Angreifer, der mindestens 51% der gesamten Mining-Rechenleistung des Netzwerkes besitzt oder kontrollieren kann, ist technisch in der Lage, Transaktionen zu manipulieren und Coins mehrfach auszugeben. Dies wird auch als *double spend problem* bezeichnet. Der Angreifer berechnet mithilfe seiner Rechenleistung weitere Blöcke der Blockchain. Die selbst berechneten Blöcke werden an die öffentliche Blockchain angehängt, ohne diese jedoch im Netzwerk zu veröffentlichen. Somit ergibt sich eine private Blockchain des Angreifers. Veröffentlicht nun der Angreifer seine private Blockchain, wird diese vom Netzwerk als gültig akzeptiert, da immer die längste Blockchain als valide Version der Blockchain angenommen wird. Dies ist auf die *Longest Chain Rule* zurückzuführen. Der Angreifer hat somit erreicht, dass seine eigens errechneten Blöcke vom Netzwerk anerkannt werden und damit auch die Transaktionen innerhalb dieser Blöcke gültig sind. Abbildung 2.7 verdeutlicht die Funktionsweise der 51% Attacke. [43, 44][3, S.402f]

Die theoretische Möglichkeit, dass ein Angreifer mindestens 51% der gesamten Mining-Leistung eines Netzwerks besitzen könnte und damit entsprechend fähig ist, die Historie der Blockchain zu manipulieren, gefährdet die Sicherheit enorm und widerspricht dem Konzept der Dezentralisierung.

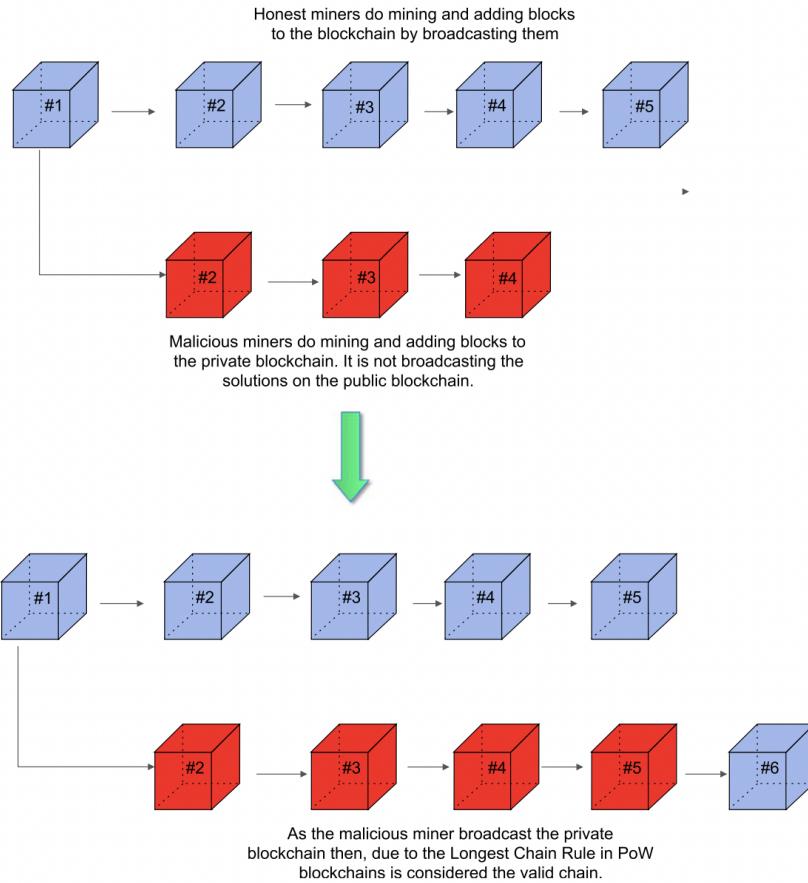


Abbildung 2.7: 51% Attacke [3, S.403]

2.7.2 Anonymität

Kryptowährungen werden entweder in einem Wallet aufbewahrt oder über eine Transaktion an ein anderes Wallet übertragen. Diese beiden Fälle sollen unter dem Aspekt der Anonymität betrachtet werden.

Anonymität von Transaktionen

Da alle Transaktionen in der Blockchain festgehalten werden, können Transaktionen überprüft und nachverfolgt werden. Dies ist beispielsweise mithilfe eines Blockchain Explorers möglich. Es wird eine Wallet Adresse oder eine Transaktions-ID benötigt, um eine entsprechende Suche durchzuführen. So lassen sich zu jeder beliebigen Transaktion das Sender-Wallet und das Empfänger-Wallet herausfinden. Jedoch lassen die in der Blockchain gespeicherten Daten selbst keinen Rückschluss auf die Identität von Sender oder Empfänger

zu. Damit sind Transaktionen pseudonym und nicht anonym. Kryptowährungen wie beispielsweise Monero (XMR) besitzen jedoch Funktionen, um die Anonymität der Nutzer weiter zu erhöhen und Rückschlüsse auf Personen zu erschweren. [45]

Anonymität von Wallets

Neben der Nachverfolgbarkeit von Transaktionen über die Blockchain, lassen sich ebenfalls Informationen über Wallets herausfinden. Mit einer Wallet Adresse ist sowohl der aktuelle Bestand an Coins auf diesem Wallet öffentlich, als auch alle eingehenden und ausgehenden Transaktionen. Abbildung 2.8 zeigt einen Auszug aus dem Ethereum Blockchain Explorer. Jedoch gibt auch hier die Blockchain keine Auskunft über den Eigentümer des Wallets. Eine Identifikation gelingt i.d.R. beispielsweise durch Zahlungen einer Person mit den Coins des Wallets. Werden z.B. Waren mit BTCs bezahlt, lässt sich der Wallet Besitzer über die Versandadresse ermitteln. Außerdem lässt sich beispielsweise im BTCs Netzwerk die Identität eines Nutzers über dessen IP-Adresse ermitteln, da BTC ein Peer-to-Peer-Netzwerk ist. Ist die Identität eines Wallet Besitzers bekannt, können über empfangene oder gesendete Transaktionen von diesem Wallet weitere Identifizierungen erfolgen. Damit ist ein Wallet pseudonym und aufgrund der Informationen in der Blockchain nicht anonym. [45]

The screenshot shows a detailed view of a Ethereum wallet address (0x0A161C1D37545e77B193681686808E0026b6ebbB). The top navigation bar includes links for Address, Buy, Exchange, Earn, and Gaming. The main interface is divided into several sections:

- Overview:** Displays the balance (0.266219034773100899 Ether) and value (\$471.05) in USD.
- More Info:** Shows the "My Name Tag" field as "Not Available" with a link to update it.
- Transactions:** A table showing the latest 25 transactions from a total of 80. The columns include Txn Hash, Method, Block, Age, From, To, Value, and Txn Fee. The table lists three recent transactions, all of which are "Public Mint" operations.

Abbildung 2.8: Ethereum Blockchain Explorer Beispiel [4]

3 Kryptowährungen

3.1 Handel von Kryptowährungen

Kryptowährungen zu handeln, ist auf verschiedensten Wegen möglich. Neben dem Handel auf offiziellen Marktplätzen und Börsen, besteht die Möglichkeit, auf Angebote von privaten Anbietern zurückzugreifen oder die Währung gegen eine andere Kryptowährung zu tauschen und nicht in Euro oder US-Dollar (USD). Bei Betrachtung der umsatzstärksten Kryptowährungen zeigt sich die Dimension, die zwei Kryptowährungen auf dem gesamten Markt besitzen. [46, S.20] Bitcoin (BTC) und Ethereum sind die umsatzstärksten Währungen. Abbildung 3.1 zeigt die umsatzstärksten Kryptowährungen im Jahr 2017.

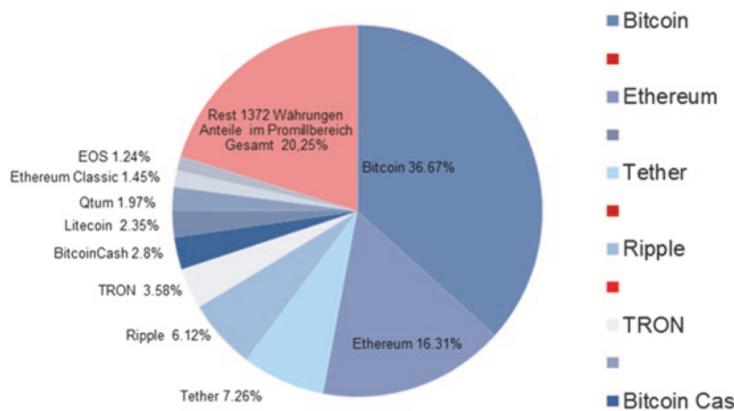


Abbildung 3.1: Umsatzstärkste Kryptowährungen [5, S.67]

Börsen

Der Handel von Kryptowährungen über Börsen ist rund um die Uhr möglich. Häufig bieten diese Plattformen im Rahmen eines Nutzerkontos zum Handeln, ebenfalls mit diesem verknüpft, Online-Wallets (vgl. 2.2) an. So kann der Nutzer die gekauften Währungen

direkt auf dem Wallet, das von der Börse bereitgestellt wird, speichern. Da mehrere verschiedene Währungen handelbar sind, werden i.d.R. auch für all diese entsprechenden Wallets angeboten. Neben dem Kauf von Kryptowährungen mit einer Fiatwährung wie beispielsweise Euro, können auch Kryptowährungen gegen andere Kryptowährungen getauscht werden. [5, S. 65f]

Handelsplätze

Auf Handelsplätzen wird in der Regel von Privatpersonen gekauft. Dabei stellt eine Person, die Kryptowährungen besitzt, ein Angebot auf die Plattform und bietet eine bestimmte Menge einer Währung zum Kauf an. Potenzielle Käufer können mit dem Verkäufer in Kontakt treten und den Verkauf abwickeln. Auch in diesem Fall kann die Bezahlung entweder in einer Fiatwährung stattfinden oder mit einer anderen Kryptowährung bezahlt werden. Diese Entscheidung liegt bei Käufer und Verkäufer. Anders als bei Börsen ist die Plattform in diesem Fall nur Vermittler. Folglich ist diese bei Betrugsfällen nicht oder nur sehr eingeschränkt haftbar. Der Großteil des Risikos liegt bei dem Käufer der Kryptowährungen. [5, S. 69f]

3.2 Bitcoin

Bitcoin (BTC) ist nicht nur eine Währung, sondern umfasst ein ganzes Netzwerk sowie mehrere Protokolle. Mit BTC können Werte in Form von Coins generiert und über das Netzwerk an andere übertragen werden. Ein Whitepaper aus 2008 erläutert die Vorstellung eines Peer-to-Peer Geldsystems ohne zentrale Stelle. Dies ist der Anfang des Bitcoins (BTCs). Ziel ist es, ein Geldsystem zu schaffen, in dem die Ausgabe von Geld, die Überprüfung von Transaktionen sowie Abrechnungen ohne zentrale Stelle möglich sind. Den Kern des gesamten Konzepts bildet dabei der PoW-Algorithmus. Technisch ist PoW dank des BTC Protokollstapels möglich. Somit kann jeder Nutzer, auf dessen Gerät der BTC Protokollstapel betrieben werden kann, am Mining mit der Leistung seiner Hardware teilnehmen. Der Schweregrad der Berechnung wird immer wieder angepasst, wobei nach jeweils vier Jahren die Mininggeschwindigkeit halbiert wird. Dies ist so im Protokoll definiert. Außerdem ist die Gesamtmenge an Bitcoins festgelegt. Sie wird voraussichtlich im Jahr 2140 erreicht. Durchschnittlich werden alle zehn Minuten Transaktionen verifiziert

und an die entsprechenden Miner die Belohnung in Form von Bitcoins ausgeschüttet. [47, S.41-44]

Zusammenfassend besteht BTC aus [47, S.41]:

1. dem Peer-to-Peer BTC Netzwerk
2. der Blockchain
3. Regeln und kryptografischen Verfahren zur Validierung von Transaktionen und zur Ausgabe von Coins
4. dem PoW-Algorithmus zur Berechnung der gültigen Blockchain

3.3 Ethereum

Ethereum (ETH) ist eine dezentralisierte Open-Source-Plattform, die auf der Blockchain-Technologie basiert. Es ist bei ETH auch die Rede von der Blockchain der zweiten Generation. [16, S.140] Die Kryptowährung ist seit 2015 am Markt vertreten. Das Whitepaper für die Blockchain wurde bereits im Jahr 2013 von seinem Erfinder und Mitbegründer Vitalik Buterin veröffentlicht. Streng genommen heißt die Währung des Ethereum-Netzwerks Ether, aber in der Fachwelt ist der Begriff Ethereum ebenso geläufig. Die Open-Source-Plattform ermöglicht das Entwickeln von dezentralen Anwendungen (dApps) für jedermann. Diese dApps finden bereits Einsatz bei Finanzanwendungen, Social-Media-Plattformen, Messengern, Spielen und vieles mehr. [48] ETH ist aktuell die zweitstärkste Kryptowährung mit einem Marktwert von knapp 265 Mrd. Euro. [49]

Wie beim BTC setzt ETH auf das Konsensverfahren PoW und somit auch auf die Miningtechnologie. Das Hashverfahren für den Miningprozess heißt Ethash und ist eine Abwandlung der Secure Hash Algorithm (SHA)-3 Hashfunktion. Der Ethash kommt auch bei unzähligen anderen Kryptowährungen zum Einsatz. [50] Aufgrund des stark kritisierten PoW Ansatzes in Bezug auf Umwelt und Nachhaltigkeit, will die Ethereum Foundation im Jahr 2022 einen neuen Weg einschlagen. Bis in jüngster Vergangenheit unter dem Namen Ethereum 2.0 (ETH2) bekannt, soll der PoW Ansatz mit einem PoS Ansatz kombiniert werden. Die Foundation gab bekannt, dass man auf den Namen ETH2 verzichtet, um klarzumachen, dass es sich um ein Update handelt und nicht um eine neue Währung. Die bisherige PoW Struktur wird nun als Execution-Layer bezeichnet und kann mit einem "Motor" verglichen werden. Der PoS Ansatz wird Consensus Layer genannt und ist dann

ein darüberliegender Layer und steuert die darunter liegende Schicht als "Hirn". Um die bisher entwickelte Client-Software weiterhin mit minimalen Anpassungen nutzen zu können, findet die Kommunikation zwischen Execution-Layer (PoW) und Consensus Layer (PoS) über RPC statt. [6] Abbildung 3.2 verdeutlicht die Funktionsweise von ETH2.

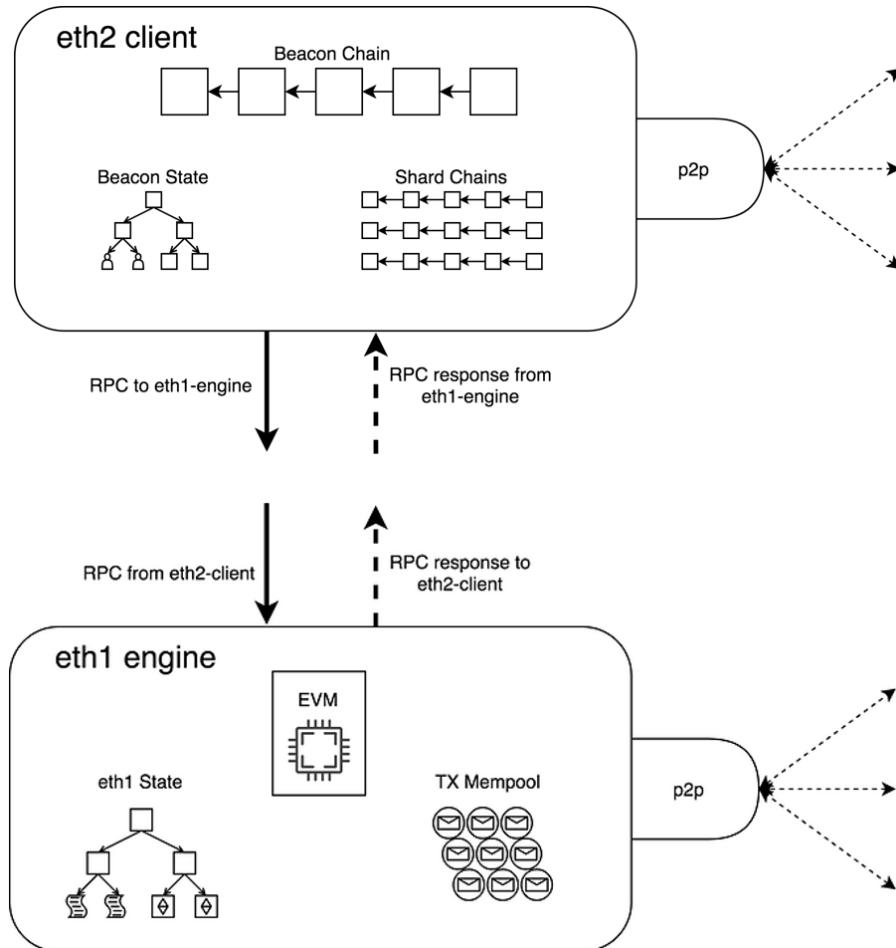


Abbildung 3.2: Funktionsweise ETH2 [6]

3.4 Tether

Tether (USDT) wurde von Brock Pierce, Reeve Collins und Craig Sellars erfunden und ist 2015 auf dem Markt erschienen. Ursprünglich sollte die Währung Realcoin heißen, aber USDT sollte nicht als Alternativwährung zum BTC angesehen werden. Das Besondere am USDT ist, dass dieser vom USD gedeckt ist. Eine Einheit USDT verbrieft einen USD. Bei dieser Art von Kryptowährung spricht man von sogenannten Stablecoins. Es wird ein fester Wechselkurs zum USD von 1:1 angestrebt. [51]

USDT ist der stärkste Stablecoin am Markt mit einem Wert von etwa 70 Mrd. [49] Euro. Stablecoins sind auf Blockchain-Technologie basierende Token, deren Wert an eine andere Währung oder einen anderen Vermögenswert gekoppelt ist. USDT kann als eine hybride Währung beschrieben werden, da der Token an sich eine Kryptowährung, aber der Wert eines einzelnen Tokens an den USD gebunden ist. Julian Hosp, großer Fan der Tokenisierung, schreibt in seinem Buch darüber: "Tokenisierung bedeutet, dass reale Vermögenswerte wie Aktien, Anleihen, Immobilien, Gold usw. auf die Blockchain gebracht werden." [16, S.146]

USDT wird vom Unternehmen Tether Labs herausgegeben. Dabei soll jeder USDT-Token 1:1 durch die Reserve von USDT gedeckt sein. Während Tether Labs ursprünglich angab, für jeden USDT einen USD als Barreserve zu halten, verwendet Tether mittlerweile auch andere Rücklagen für die Deckung von USDT. Steigt der Bedarf an USDT, werden frische Einheiten geprägt. Werden USDT wieder bei Tether Labs gegen USD getauscht, werden die USDT-Einheiten verbrannt. Tether hat keine eigene Blockchain, sondern kann auf jeder Blockchain herausgeben werden. Derzeit sind die beliebtesten Blockchains für die Herausgabe von USDT, ETH und Tron (TRX). USDT kann ausgegeben, gehandelt oder transferiert werden wie Bitcoin oder andere Kryptowährungen. [51]

Der weltweit größte Stablecoin wurde erfunden, um zwei grundlegende Probleme im Krypto-Space zu lösen. Zum einen soll der grenzüberschreitende Transfer einer stabilen Währung mit niedrigen Gebühren ermöglicht werden. Zum anderen soll der blitzschnelle Handel mit Kryptowährungen erleichtert werden: Tether ermöglicht es, Trading-Gewinne in USDT zu parken, ohne dazu das Krypto-Ökosystem verlassen zu müssen. [51]

3.5 Chia

Chia (XCH) ist eine der jüngsten Kryptowährungen, sie wurde im August 2017 vom BitTorrent Erfinder Bram Cohen erfunden. Das offizielle Whitepaper wurde im Februar 2021 verabschiedet und die Markteinführung begann im März 2021. Die Entwickler selbst bezeichnen XCH als das erste digitale Geld in Unternehmerqualität. [52] [53]

"Wir glauben, dass Kryptowährung einfacher zu benutzen sein sollte als Bargeld, schwieriger zu verlieren und fast unmöglich zu stehlen. Jeder, der Transaktionen validieren möchte, sollte in der Lage sein, ohne Einweg-Hardware oder eine hohe Stromrechnung zu farmen" - Das Chia Team [52]

Die Entwickler von XCH bezeichnen ihre Kryptowährung als grün. Das liegt am gewählten Konsensverfahren. Während das PoW Verfahren sehr in der Kritik steht und als klimaschädlich gilt, setzt XCH auf die PoSpace und Proof of Time (PoT) Verfahren. Dabei weisen Nutzer nach, dass auf einer bestimmten Festplatte oder einem anderen Speicher im Netzwerk ausreichend Speicherplatz zur Verfügung steht. Mit der Installation der Chia-Software belegen Chia-Farmer (Blockchain Nutzer) den Speicherplatz und stellen diesem dann dem Chia-Netzwerk zur Verfügung. XCH ist allerdings nicht der erste Coin, der "Storage Farming" betreibt, so gibt es das Konzept selbst schon länger z.B. beim Burstcoin (BURST) oder Filecoin (FIL). Allerdings hat die neue XCH einen regelrechten Hype entfacht, der eben auch den Speichermedien-Markt beeinflusst. Das grüne Image des XCH Coins bröckelt, wenn man genauer hinsieht. Zum einen umfasst das XCH Netzwerk mehr als 32 Exabytes an Datenspeicher (Stand: 14.01.2021)[54], ein Exabyte entsprechen 1.152.921.504.606.846.976 Bytes. Das bedeutet, wer mitverdienen will, hat als Privatperson mit wenigen Terabyte wenig Chancen. Nicht nur die Anschaffung der Hardware kostet Geld und verbraucht Ressourcen in der Herstellung. Auch der Betrieb selbst ist stromhungrig, weniger stark als beim Graphics Processing Unit (GPU)-Mining, aber trotzdem immens. Des Weiteren werden Festplatten stark beansprucht, sodass diese nur eine kurze Lebenserwartung aufweisen und oft getauscht werden müssen. Wer also kein Rechenzentrum betreibt und günstig an Strom kommt, hat kaum eine Chance wirtschaftlich XCH Coins zu farmen. [52] [53] [54]

3.6 Monero

Monero (XMR) ist eine im Jahr 2014 veröffentlichte Kryptowährung mit Fokus auf sicheren und privaten Transaktionen. XMR basiert wie BTC auf PoW. (vgl. 2.6.1) Der zugrundeliegende Algorithmus für das Mining von XMR ist *RandomX*. Gekennzeichnet ist dieser Algorithmus durch die Optimierung auf Central Processing Unit (CPU)-Mining. Außerdem ist ein Ziel der XMR Entwickler, das Mining auf spezieller Hardware bestmöglich zu erschweren oder unmöglich zu machen. XMR ist im Gegensatz zu BTC in der Gesamtmenge nicht gedeckelt. Somit ist das Mining von XMR theoretisch ohne zeitliche Begrenzung möglich. Um die Privatsphäre zu verbessern, werden sogenannte *Schattenadressen* eingesetzt. Diese werden automatisch bei der Transaktion erstellt und nur einmalig genutzt. Ein weiteres Grundkonzept von XMR, um die Privatsphäre der Nutzer zu gewährleisten, ist der Einsatz von *Ring Signaturen*. Diese *Ring Signaturen* erschweren die Zuordnung einer Transaktion zu einem Nutzer. Dazu wird die Transaktion nicht vom Absender selbst

signiert, sondern eine Signatur aus der des Absenders sowie aus den Signaturen anderer Nutzer gebildet. Das Ergebnis ist eine Signatur bestehend aus mehreren gleichwertigen Signaturen verschiedener Nutzer. Durch die Gleichwertigkeit der einzelnen Signaturen ist der eigentliche Absender unklar. Letztlich werden alle privaten Schlüssel der an dem Ring beteiligten Nutzer miteinander XOR verrechnet. [55, 56] Abbildung 3.3 verdeutlicht die Funktionsweise von *Ring Signatures*.

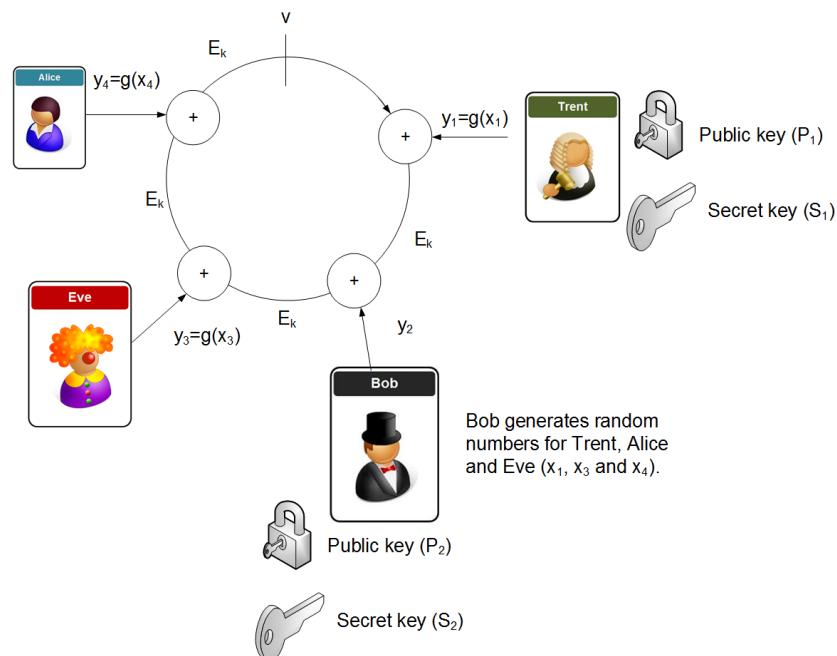


Abbildung 3.3: Funktionsweise einer Ring Signatur [7]

3.7 Vergleich

Dieses Kapitel beinhaltet einen kurzen Vergleich, der im Rahmen dieser Arbeit betrachteten Kryptowährungen. Damit soll ein Überblick über die Kryptowährungen mit der größten Marktkapitalisierung gegeben werden. Jedoch sind nur die betrachteten Kryptowährungen in der Tabelle 3.1 aufgeführt.

Rang	Name	Abkürzung	Marktkapitalisierung	Mining
1	Bitcoin	BTC	1,17 Bio. Euro	Ja, SHA-256
2	Ethereum	ETH	521 Mrd. Euro	Ja, Ethash
3	Tether	USDT	70 Mrd. Euro	Nein
4	Monero	XMR	4 Mrd. Euro	Ja, RandomX

Tabelle 3.1: Vergleich Kryptowährungen [11]

Die Kryptowährung XCH ist nicht in der Tabelle aufgeführt, da sie nicht wie die anderen Währungen auf PoW, sondern auf Proof of Space basiert und eine deutlich geringere Marktkapitalisierung aufweist.

4 Kryptomining

4.1 Hardware

Die folgenden Punkte beschreiben in Kürze, welche Möglichkeiten es aus Hardwaresicht gibt, Kryptomining zu betreiben. Dabei ist die Hashrate eine Einheit, die angibt, wie gut sich die entsprechende Hardware zum Mining eignet. Die Hashrate beschreibt die Anzahl der Versuche pro Sekunde eine Nonce auszuprobieren.

CPU-Mining

Beim Central Processing Unit (CPU)-Mining werden handelsübliche Desktop- oder Laptop-CPUs zum Lösen der Hashes genutzt. Diese Idee stammt aus der Anfangszeit der Kryptowährungen, als es noch keine anderen Wege gab, Mining zu betreiben. Die Hashrate einer durchschnittlichen CPU liegt im Bereich von ein bis drei Millionen Hashes pro Sekunde, abhängig von der Taktung der CPU. [16, S.70] Die Gesamthashrate liegt allerdings bei mehreren Tera-Hashes, was die Leistung einer CPU verschwindend gering wirken lässt. Aus diesem Grund müsste man für die Hardware und den Strom viel mehr Geld ausgeben als für die zu erwartende Belohnung in Form von Geld, daher ist CPU-Mining heutzutage praktisch ausgestorben. [57]

GPU-Mining

Nachdem das Kryptomining immer populärer wurde und wie im Absatz davor beschrieben, dass CPUs-Mining nicht mehr profitabel ist, führte dies zu einem neuen Ansatz. Die neue Herangehensweise zielt auf Grafikkarten (GPUs) ab. Sie wurden in der Wissenschaft immer attraktiver, da wissenschaftliche Berechnungen in kürzerer Zeit damit ausgeführt werden konnten. Der gleiche Effekt kann auch bei der Hashrate beobachtet werden. GPUs sind im Grunde keine besseren CPUs, sie funktionieren einfach anders. GPUs sind dafür ausgelegt,

mit wenigen Einheiten (Kerne) komplexe Aufgaben zu lösen. Dagegen können GPUs wiederkehrende Aufgaben "lernen" und schnell abarbeiten. Diese Eigenschaft macht GPUs zur besseren Mininghardware. [57] Aktuelle Grafikkarten im Mittelklassebereich haben eine Hashrate von 20 bis 50 Millionen pro Sekunde und sind mindestens um den Faktor 20 effizienter als CPUs. Allerdings ist der Einsatz der Hardware auch davon abhängig, welche Kryptowährung damit geschürft werden soll. Der Hash-Algorithmus des Bitcoins macht ein GPU-Mining nutzlos, wohingegen ETHs sich besonders gut mit GPUs schürfen lässt. [16, S.71]

ASIC-Mining

Application Specific Integrated Circu (ASIC) Miner sind im Gegensatz zu anderer Mining-Hardware nicht zweckentfremdet, sondern speziell für Kryptomining entwickelt und konzeptioniert. Die ersten ASIC-Miner sind seit 2013 auf dem Markt und enthalten spezielle Mikrochips, die im Vergleich zu Standard Computer-Hardware sehr viel leistungsfähiger in Bezug auf Kryptomining sind. Ein ASIC-Miner aus dem Jahr 2018 im Wert von 2500 USD hat etwa eine Miningpower von 400 GPUs oder 12000 CPUs. Allerdings können ASIC-Miner nur für diesen einen Zweck genutzt werden, wenn diese nicht gerade schürfen, sind sie wertlose Hardware. Es gibt mittlerweile milliardenschwere Unternehmen, die sich auf die Herstellung dieser Miner spezialisiert haben. Dieser Geschäftszweig ist sehr risikobehaftet und könnte von heute auf morgen wegbrechen, wenn Kryptowährungen auf andere Verfahren umstellen und das bisherige Mining entfällt. [16, S.71] Solange Strom ein begrenztes Gut und dessen Erzeugung klimaschädigend ist, wird das Ziel sein, das traditionelle Mining zu unterbinden. [57]

Der Hardwareaufbau ist fix und nicht veränderbar, während bei sogenannten programmierbaren Logikgattern (Field Programmable Gate Array (FPGA)-Miner) Veränderungen an der Schaltung möglich sind. Das bedeutet, dass die Schaltung fest in Silizium verklebt werden kann, dadurch können ASIC-Miner kosteneffizienter und in großer Stückzahl produziert werden. Außerdem kann die Stromzufuhr gesteuert und optimiert werden, das macht ASIC-Miner oft sehr viel energieeffizienter als andere Miner. [57]

Mit dem Aufkommen der ASIC-Miner wurde es zunehmend schwerer, als Privatperson mit herkömmlicher Computerhardware einen Block in der Blockchain zu lösen. Das Mining mit CPU und GPU in geringer Stückzahl ist daher wenig profitabel. Das spielt Unternehmen in die Karten, die große thermisch regulierte Rechenzentren betreiben und Zugang zu günstigem Strom haben. Außerdem zentralisiert sich das Mining auf wenige Pools, die

durch hohe Rechenpower gefährlich nahe an die kritischen 51% Gesamtrechenleistung gelangen können. [57]

Festplatten-Mining

Die Kryptowährung XCH löste einen Hype und einen Run auf Festplatten aus. Die Währung erlaubt ein Kryptomining mit Festplatten. Es kommt das PoSpace Konsensverfahren zum Einsatz. Entscheidend dabei ist, Speicherplatz für das Miningnetzwerk bereitzustellen. Da das Chia-Netzwerk über drei Exabyte Speicherkapazität umfasst, sind Platten mit besonders viel Speicherkapazität gefragt. Der Speicher wird mit Plots gefüllt. Ein K-32 Plot erzeugt 256 Gigabyte große Dateien, die für die XCH Blockchain bereitgestellt werden. [58] Für die Erstellung von Plots sind eine schnelle CPU, viel Arbeitsspeicher und eine Solid State Drive (SSD) von Vorteil. Der Plotvorgang kann somit deutlich beschleunigt oder sogar mehrere Plots parallel erzeugt werden. Der Vorgang selbst dauert dennoch mehrere Stunden bis Tage, je nach Hardwareleistung. Ist der Plot dann erzeugt, wird dieser auf eine Hard Disk Drive (HDD) ausgelagert und kann zum Farmen (Coin erneten) genutzt werden. Je größer die Speicherkapazität und die darauf enthaltenen Plots, desto größer die Chancen beim Farmen der Coins. Beim Erzeugen des Plots ist die SSD einer enormen Schreiblast ausgesetzt. Standardfestplatten sind dafür nicht ausgelegt und stoßen bei einer solchen Schreiblast schnell an die TBW Grenze. Diese gibt an, für welche Auslastung (Schreibvorgänge) die Festplatte konzeptioniert wurde. Ist diese erreicht, ist das Ableben der Festplatte gewiss und sie muss getauscht werden. [59]

4.2 Software

Im Folgenden werden zu Beginn die Software-Schnittstellen der beiden Grafikkartenhersteller Nvidia und AMD vorgestellt. Im Anschluss wird erläutert, welche Software benötigt wird, um auf Windows sowie auf Linux Mining zu betreiben. Außerdem wird das Konzept von Mining-Betriebssystemen vorgestellt.

4.2.1 Schnittstellen und Treiber

CUDA

Compute Unified Device Architecture (CUDA) ist eine von Nvidia entwickelte Schnittstelle, mit der Rechenoperationen oder Programmteile auf Nvidia Grafikkarten ausgeführt werden können. Sie stellt dem Programmierer eine Schnittstelle bereit, die dieser in seinem Programm implementieren kann. CUDA umfasst dabei mehrere Bibliotheken, Compiler sowie weitere Tools und ist beispielsweise für C++ oder Python verfügbar. CUDA ist im Gegenteil zur Open Graphics Library (OpenGL) oder anderen Schnittstellen nicht ausschließlich auf Video- oder Bildanwendungen beschränkt. Der Vorteil, bestimmte Operationen über die CUDA Schnittstelle zu implementieren und damit auf der Grafikkarte auszuführen, liegt beispielsweise in der hohen Anzahl an Cores. Damit ist eine hohe Parallelisierung möglich. Da CUDA die meisten Nvidia Grafikkarten unterstützt, sind in der Regel weitere Treiber nicht notwendig. [60]

OpenCL

Open Computing Language (OpenCL) ist ebenfalls eine Schnittstelle, um auf unterstützten Geräten bestimmte Rechenoperationen oder Programmteile ausführen zu können. OpenCL setzt eine auf dem System installierte OpenCL Umgebungslaufzeit voraus. Neben AMD wird OpenCL auch von Nvidia und anderen Herstellern unterstützt. Neben Grafikkarten kann OpenCL Code auch auf CPUs ausgeführt werden. OpenCL ist für Sprachen wie C++, Java oder auch Python verfügbar. [61, 62]

4.2.2 Betriebssystem

Grundsätzlich lässt sich sowohl auf Windows als auch auf Linux Mining betreiben. Jedoch sollte je nach Art des Minings entschieden werden, welches Betriebssystem für die entsprechende Art am besten geeignet ist.

Windows

Grafikkartentreiber der Hersteller AMD und Nvidia werden in der Regel primär für Windows implementiert. Da die Zielgruppe der Grafikkarten häufig Windows nutzt, ist

das Mining mit Grafikkarten auf Windows mit den entsprechenden Treibern möglich. Hierzu wird bei Nvidia CUDA und bei AMD Grafikkarten der entsprechende Treiber benötigt. Zu beachten ist jedoch, dass Windows ein Graphical User Interface (GUI) basiertes Betriebssystem ist und damit Grafikressourcen, die für das Mining genutzt werden könnten, selbst benötigt. Neben dem Grafikkarten-Mining ist das Mining mit dem Prozessor ebenfalls auf Windows möglich. Hierzu sind keine weiteren Treiber notwendig. In diesem Fall gilt Ähnliches wie bei Grafikkarten-Mining. Das Windows Betriebssystem benötigt selbst Prozessorressourcen, die dadurch nicht für den Miningprozess zur Verfügung stehen. Insbesondere durch die GUI werden mehr Prozessorressourcen verbraucht als bei einem kommandozeilenbasiertem Betriebssystem. Außerdem wird bei Windows eine Lizenzgebühr fällig. Festplatten-Mining, insbesondere XCH-Mining (siehe Abschnitt 4.1), lässt sich ebenfalls auf Windows realisieren. Die benötigte Software von XCH ist auf Windows verfügbar. Außerdem unterstützt Windows eine hohe Anzahl an Festplatten mit entsprechend viel Speicherplatz.

Linux

Unter Linux muss zu Beginn zwischen einem Desktop basierten und einem kommandozeilenbasierten System unterschieden werden. Desktop basierte Linux Systeme weisen in den bereits genannten Punkten ähnliches Verhalten auf. Bei einem kommandozeilenbasierten Linux System stehen vermeintlich zusätzliche Ressourcen für den Miningprozess zur Verfügung, da sowohl die Grafikkarte als auch der Prozessor keine grafische Oberfläche bereitstellen müssen. Ob diese genutzt werden können, zeigen die Tests. CPU-Mining auf Linux Systemen ist vergleichbar mit dem Mining auf Windows. Bei Grafikkarten Mining werden ebenfalls die entsprechenden Treiber benötigt. CUDA Treiber sind unter den gängigen Linux Distributionen wie Ubuntu oder Fedora verfügbar. Von AMD werden die Distributionen Ubuntu und Redhat Enterprise Linux (RHEL) unterstützt. Grundsätzlich entfallen bei Linux Lizenzkosten für das Betriebssystem. Festplatten-Mining ist ebenfalls mit XCH möglich. Die entsprechende Software wird von XCH auch für Linux bereitgestellt. ASIC-Miner werden in der Regel auf Linux betrieben. Oft sind ASIC-Miner ein vollständiges System mit bereits installiertem Linux Betriebssystem und entsprechender Mining-Software.

4.2.3 Mining-Betriebssystem

Mithilfe von Mining-Betriebssystemen wird eine möglichst auf das Mining ausgerichtete optimale Nutzung der Hardware angestrebt. I.d.R basieren Mining-Betriebssysteme auf Linux. Zum einen, um die für das Betriebssystem notwendigen Systemressourcen gering zu halten und zum anderen, da die Systeme primär über eine Web-Oberfläche verwaltet werden und damit eine GUI auf dem System selbst überflüssig ist. Außerdem sind die Betriebssysteme auf das notwendige Minimum an Software reduziert. Grundlegend bestehen sie aus:

- dem Betriebssystem Kern
- Treibern für Mining-Hardware (bei Grafikkarten beispielsweise CUDA und OpenCL)
- Mining-Software
- Remote Management Dienste

Des Weiteren sind die Übertaktung oder Leistungssteigerung der Mining-Hardware sowie Überwachung der Leistungsdaten ebenfalls mit dem Mining-Betriebssystem möglich. Das Linux Betriebssystem ist grundsätzlich ein kostenfreies Betriebssystem, jedoch werden für die namhaften Mining-Betriebssysteme monatliche Gebühren fällig. Diese sind gestaffelt nach Größe und Anzahl der Mining-Systeme.

4.3 Solo- & Pool-Mining

Miner, die für sich selbst schürfen und keinem Pool angehören, werden als Solo-Miner bezeichnet. Beim Lösen eines Blocks wird die Belohnung für das Lösen des gesamten Blocks an den Miner ausgeschüttet und muss nicht aufgeteilt werden. Am Beispiel von BTC beträgt die Entlohnung 6,25 BTC, was je nach Marktwert eine hohe Summe darstellt. Dadurch entsteht ein regelrechtes Rennen um die Lösung der Blöcke, sodass es enorm unwahrscheinlich ist, dieses Rennen als Solo-Miner zu gewinnen. Je größer die Rechenleistung des Miners, desto größer wird die Wahrscheinlichkeit, das Rennen zu gewinnen. Daraus ergibt sich die Unwahrscheinlichkeit, als Solo-Miner einen Block zu lösen, da ein solcher in der Regel nicht über die notwendige enorme Miningleistung verfügen. Angesichts dessen schließen sich Solo-Miner zu Mining-Pools zusammen und erhöhen dadurch ihre Chance um ein Vielfaches, einen Block zu lösen. Wer einem großen anerkannten Pool beitritt,

trägt zur Lösung eines Blocks bei, allerdings muss die Entlohnung für den gelösten Block unter allen beteiligten Minern aufgeteilt werden. In der Regel geschieht diese Aufteilung anteilig der Rechenleistung, die dem Pool von den Minern zur Verfügung steht. Außerdem erheben die Pool-Betreiber Abgaben, die sogenannten "Fees". Somit stellt sich die Frage, welche der beiden Formen wirtschaftlich mehr Sinn ergibt. Solo-Miner forcieren das Glück, selbstständig einen Block zu lösen, außer sie verfügen über Unmengen an Rechenpower, um in absehbarer Zeit einen Block lösen zu können. Beim Pool-Mining hingegen gibt es kontinuierliche Auszahlungen, allerdings sind die Energiekosten oft höher als die Belohnungen und daher nicht immer wirtschaftlich. Erst wer genug Rechenleistung zu günstigen Energiekosten in den Pool bereitstellt, zieht daraus einen Nutzen [63].

4.4 Stratum Protokoll

Das Stratum Protokoll ist ein Protokoll zur Kommunikation zwischen Minern und Servern, die Jobs an die teilnehmenden Miner vergeben. Diese Server werden von Pools betrieben und dienen der Koordination der Teilnehmer des Pools. Ursprünglich ist das Stratum Protokoll nur für BTC entwickelt worden, jedoch heute Standard für andere Kryptowährungen wie beispielsweise ETH. Grundsätzlich liegt dem Stratum Protokoll ein Transmission Control Protocol (TCP) Socket zugrunde. Über diesen Socket werden Daten bidirektional über JavaScript Object Notation (JSON) Remote Procedure Call (RPC) ausgetauscht. Um Anfragen und zugehörige Antworten zuordnen zu können, werden in der Anfrage sowie in der Antwort entsprechende einzigartige Identifikatoren hinzugefügt. Die Anfrage besteht aus einer ID, der aufzurufenden Methode und Parametern. Die Antwort besteht ebenfalls aus einer ID sowie einem Result-Feld und einem Error-Feld. Die ID der Antwort entspricht dabei der ID der Anfrage. [64, 65]

Von der Anmeldung eines Miners bei einem Pool bis hin zur Bestätigung seiner Lösung durch den Pool lässt sich die Kommunikation über das Stratum Protokoll in fünf Schritte gliedern. Die Schritte werden im Folgenden kurz erläutert.

1 Subscription

Um mit einer Miningsession zu beginnen oder eine bestehende fortzusetzen, muss die *subscribe* Methode aufgerufen werden. Diese Methode wird ausschließlich von Clients aufgerufen. Unter anderem werden bei diesem Aufruf der Name sowie die Version der

Mining-Software des Clients, die IP-Adresse und der Port des Servers über Parameter im Aufruf der Methode an den Server übermittelt. [64, 65]

2. Mining-Rig login

Um die Ergebnisse der Berechnungen an den Server schicken zu können und letztlich dafür vergütet zu werden, ist die Autorisierung des Workers gegenüber dem Pool notwendig. Dazu wird die RPC Methode *authorize* aufgerufen. Als Parameter sind dabei, der Worker-Name sowie ein entsprechendes Passwort anzugeben. Dieses wird vom Server geprüft und entsprechend mit einer Antwort, in der *true* für eine erfolgreiche und *false* für eine fehlgeschlagene Autorisierung als Parameter enthalten sind, an den Client übermittelt. [64, 65]

3. Difficulty adjustment

Nachdem der Worker erfolgreich autorisiert wurde, wird die aktuelle Difficulty der Block-chain vom Server an den Client gesendet. Dies wird über die RPC Methode *set_difficulty* realisiert. [64, 65]

4. Task delivery

Über die Methode *notify* werden alle für das Mining eines Blocks relevanten Informationen als Parameter vom Server an den Client gesendet. Dazu gehören die Job-ID, die Block Version sowie diverse Hashes. Die *notify* Methode erwartet keine Antwort. [64, 65]

5. Mineral Submission

Wurde der Job durch den Miner ausgeführt und beendet, wird das Ergebnis über die *submit* Methode zurück an den Server gesendet. Als Parameter werden hier unter anderem die Job-ID, sowie der Worker Name angegeben. Die Antwort des Servers umfasst das Result *true*, falls die Lösung korrekt ist. Wird die Lösung abgelehnt, wird im Result-Feld *false* angegeben. [64, 65]

Abbildung 4.1 zeigt den beschriebenen Ablauf. Während einer Miningsession werden kontinuierlich über die *notify* Methode Jobs an den Client geschickt. Ebenso werden gelöste Jobs zur Bestätigung an den Server übermittelt.

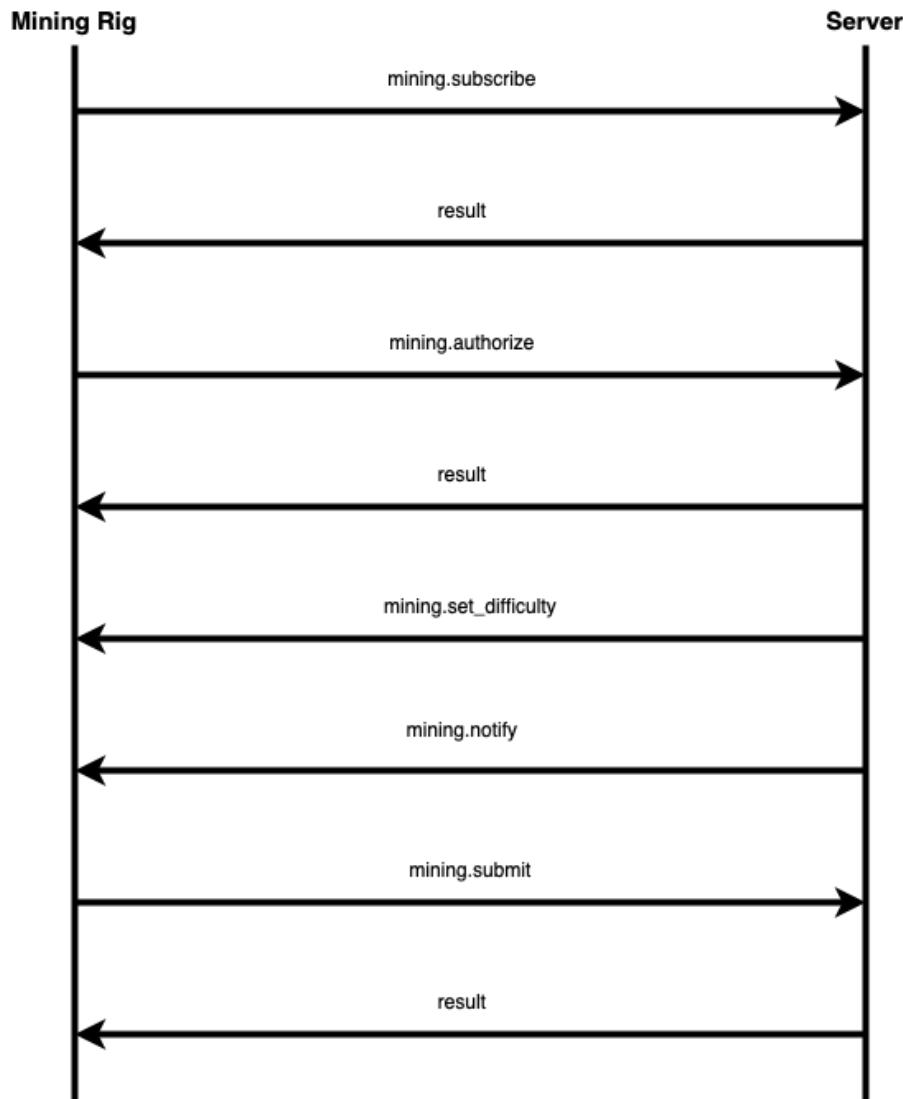


Abbildung 4.1: Ablauf der Kommunikation über das Stratum Protokoll

5 Vorbereitung

Im folgenden Kapitel werden die Vorbereitungen für die Umsetzung der Studienarbeit getroffen. Dazu zählen die Erläuterung des Konzepts, die benötigte Hardware sowie deren Beschaffungskosten. Des Weiteren werden die Herangehensweise in Bezug auf Hardware und Software vorgestellt sowie Ziele definiert.

5.1 Konzept

Für die Evaluierung eines Kryptosystems wird im Rahmen dieser Studienarbeit ein GPU Mining-Rig realisiert, analysiert und die Ergebnisse schließlich bewertet. Das Rig soll nach gängigen Standards aufgebaut werden und orientiert sich am Beispiel, das in Abbildung 5.1 zu sehen ist. Das Grundgerüst stellt dazu der Aluminium-Rahmen, der für Standard-Computerhardware passend ist. Auf dem Rahmen werden alle benötigten Komponenten mit Schrauben befestigt. Für die Evaluierung kommen drei Grafikkarten zum Einsatz. Für deren Einbau im Rahmen sind sogenannte Riser-Karten erforderlich. Die Riser-Karten ermöglichen einen größeren Abstand zum Mainboard und somit eine bessere Kühlung der einzelnen Grafikkarten. Durch zusätzliche Lüfter an der Front des Rahmens werden die Kanäle zwischen den Grafikkarten mit Luft durchströmt. Das Mainboard kann im unteren Teil des Rahmens befestigt und mit RAM, CPU und CPU-Kühler bestückt werden. Daneben bietet der Rahmen Platz für ein Netzteil und Festplatten. Außerdem ist der Einsatz von einem Live-Betriebssystem mittels USB-Stick geplant. Neben den Hardwarekosten entstehen Betriebskosten in Form von verbrauchtem Strom. Dieser Strom wird mit einem Kilowattstundenzähler ermittelt. In Betrieb sollen dann die Leistungsmerkmale ermittelt und später analysiert und ausgewertet werden. Details zu den Leistungsmerkmalen werden im Kapitel 5.7 Ziele definiert. Das Mining-Rig soll aufgrund der entstehenden Geräuschkulisse in einem separaten Raum aufgebaut und Remote verwaltet werden.



Abbildung 5.1: Privat Mining-Rig für zu Hause [8]

5.2 Hardware

Im Folgenden wird die verwendete Hardware vorgestellt. Grundlage des gesamten Mining-Rigs bildet ein Mining-Frame, welcher für sechs Grafikkarten ausgelegt ist. Ein Mining-Frame ist ein aus Metall bestehendes Gerüst, auf dem alle Komponenten des Rigs platziert werden. Durch die offene Bauweise soll eine optimale Kühlung der Komponenten gewährleistet werden. Als Mainboard kommt ein MSI Z87-G45 GAMING zum Einsatz. Dieses Mainboard zeichnet sich durch sieben PCI-Express Steckplätze aus und ist daher ideal für den Miningbetrieb geeignet. Als Prozessor wird ein Intel i7-4770k der 4. Generation genutzt. Da der Fokus des Rigs auf Mining mit Grafikkarten liegt, ist die Leistung des gewählten Prozessors ausreichend. Gleicher gilt für den RAM. Die gewählten 16 GB sind auch für ein Live-Betriebssystem ausreichend. Als Grafikkarten kommen zwei AMD Radeon RX 580 8 GB sowie eine Nvidia ZOTAC GAMING GeForce RTX 2070 SUPER AMP Extreme zum Einsatz. Beide Grafikkarten-Typen sind im mittleren Preissegment angesiedelt, wobei sich die Nvidia Grafikkarte am oberen Ende des mittleren Preissegments befindet. Die vorgestellten Grafikkarten eignen sich für das Mining bekannter Währungen wie ETH. Der Prozessor wird von einer Kompaktwasserkühlung gekühlt. Die Stromversorgung erfolgt über ein Corsair Netzteil mit 850 Watt Leistung. Dieses Netzteil ist 80

Plus Gold zertifiziert. [66] Daraus ergibt sich ein Mindestwirkungsgrad bei maximaler Last von 89%. Bei 50% Last wird ein Mindestwirkungsgrad von 92% erreicht. [67] Daher sollte das Netzteil nicht bei 100% Last betrieben werden. Um die notwendige Größe des Netzteils zu bestimmen, werden im Folgenden die im System verwendeten Komponenten mit entsprechender von dem Hersteller angegebener maximaler Leistung aufgelistet:

- Intel i7-4770k: 84 Watt [68]
- Asus Radeon RX 580 8 GB Strix: 200-299 Watt [69]
- Power Color Radeon RX 580 8 GB: 185 Watt [70]
- ZOTAC GAMING GeForce RTX 2070 SUPER AMP Extreme: 215 Watt [71]
- SSD, Lüfter, Wasserkühlung: circa 30 Watt

Daraus ergibt sich eine maximale Leistung von 813 Watt. Da der Prozessor jedoch im Betrieb nicht Teil des Miningprozesses und damit auch nicht zu 100% ausgelastet ist, wird die Leistung im Praxisbetrieb unter 813 Watt liegen. Um die Grafikkarten in einem Mining-Frame betreiben zu können, werden Riser Karten benötigt. Diese bestehen aus einer Platine mit einem x16 Peripheral Component Interconnect Express (PCIe) Sockel sowie einem USB A Anschluss und einem Anschluss zur Stromversorgung. Die Stromversorgung erfolgt je nach Modell der Riser Karte über Serial Advanced Technology Attachment (SATA) oder Molex. Auf diese Riser Karte wird die Grafikkarte gesteckt. Mit einem USB A zu USB A Kabel und einer weiteren Platine wird die Grafikkarte mit dem Mainboard verbunden. Diese weitere Platine besteht aus einem x1 PCIe Stecker, welcher über einen USB-Anschluss verfügt und in einen PCIe Slot auf dem Mainboard gesteckt wird. Somit muss die Grafikkarte nicht direkt in den PCIe Slot auf dem Mainboard gesteckt werden, sondern lässt sich flexibel am Mining-Frame anbringen. Für eine entsprechende Kühlung der Grafikkarten sorgen 120 mm Lüfter, die ebenfalls am Mining-Frame angebracht werden. Zur Installation des Betriebssystems oder zum Live-Betrieb eines Systems kommt ein 32 GB USB-Stick bei der Installation zum Einsatz. Der Stromverbrauch sowie die aktuelle Gesamtleistung werden über ein TP-Link Kasa HS110 Strommessgerät erfasst.

Die folgende Liste umfasst alle Komponenten, die für das Mining-Rig vorgesehen sind:

- Mining-Rig: Frame für 6 Grafikkarten
- Mainboard: MSI Z87-G45 GAMING
- CPU: Intel i7-4770k 4.Generation
- RAM: Corsair 16 GB DDR3
- Festplatte: 128 GB SSD
- Grafikkarte 1: Asus Radeon RX 580 8 GB Strix
- Grafikkarte 2: Power Color Radeon RX 580 8 GB
- Grafikkarte 3: ZOTAC GAMING GeForce RTX 2070 SUPER AMP Extreme
- Wasserkühlung: Kompaktwasserkühlung CPU
- Netzteil: Corsair RM850 850 Watt
- Riser-Cards: KOLINK x1 PCIe zu x16 PCIe Adapter auf USB 3.0 Basis
- Lüfter: 3x Arctic F12 120 mm
- USB-Stick: SanDisk 32 GB
- KWh-Zähler: TP-Link Kasa HS110

5.3 Software

Im Rahmen dieser Arbeit wird Software zum Grafikkarten Mining auf Windows oder auch auf Linux eingesetzt. Da der Markt für Mining-Software groß ist und entsprechend viele Mining-Programme erhältlich sind, werden die in der Umsetzung eingesetzten Programme in diesem Abschnitt vorgestellt.

5.3.1 Windows

Unter Windows können Softwares wie NiceHash, AwesomeMiner oder auch BetterHash eingesetzt werden. Jedes dieser drei Programme stellt selbst keine Miningalgorithmen oder Funktionen bereit, sondern umfasst mehrere Miningprogramme und infolgedessen mehrere Algorithmen. Dies lässt sich als eine Sammlung von Miningprogrammen verstehen. Damit die darunterliegenden Miningprogramme nicht einzeln durch den Nutzer konfiguriert werden müssen, übernimmt dies NiceHash, AwesomeMiner oder BetterHash. Außerdem stellen die Miningprogramme ein lokales Application Programming Interface (API) zur Verfügung. Über diese API können der aktuelle Status oder Leistungsdaten der Hardware abgefragt werden. NiceHash, AwesomeMiner und BetterHash nutzen diese Schnittstelle zu den Miningprogrammen, um entsprechende Daten abzufragen und dem Nutzer in der eigenen Oberfläche darzustellen. NiceHash beinhaltet bereits einige Miningprogramme, diese werden als NiceHash Plugins bezeichnet. Tabelle 5.1 gibt einen Überblick über die in NiceHash enthaltenen Miningprogramme, die mit Nvidia als auch mit AMD Grafikkarten kompatibel sind. [72] Da das in dieser Arbeit evaluierte Rig aus AMD Grafikkarten und einer Nvidia Grafikkarte besteht, werden ausschließlich Miningprogramme mit Kompatibilität für beide Hersteller betrachtet.

Programm	Algorithmus	Plattform
BMiner	Ethash, Etchash, Equihash 144_5, Cuckatoo32	Nvidia, AMD
ClaymoreDual	Ethash	Nvidia, AMD
GMiner	Ethash, ProgPoW, KAWPOW, Equihash, CuckooCycle	Nvidia, AMD
Phoenix	Ethash, Etchash	Nvidia, AMD
LolMiner	Ethash, Etchash, CuckooCortex, Equihash 144_5, CuckooCycle, Equihash 125_4, BeamHash, Cuckatoo31, Cuckatoo32, Autolykos2	Nvidia, AMD
NanoMiner	Ethash, Etchash, CuckooCortex, KAWPOW, RandomX, Autolykos2	Nvidia, AMD

Tabelle 5.1: NiceHash Mining-Plugins

Die Software AwesomeMiner unterstützt unter anderem die in NiceHash enthaltenen Plugins. Zusätzlich umfasst AwesomeMiner noch weitere Miningprogramme und damit Algorithmen. [73] Mit BetterHash hingegen lassen sich nur folgende Kryptowährungen schürfen:

- Bitcoin
- Ethereum
- Monero
- ZCash
- Ethereum Classic
- Bitcoin Gold
- GrinCoin
- Ravencoin
- Firo

Mit BetterHash lassen sich weniger Algorithmen und damit auch weniger Währungen als beispielsweise mit dem AwesomeMiner schürfen. [73, 74] Der Vorteil aller drei vorgestellten Softwares liegt in der Zusammenfassung einzelner Miner zu einem Programm mit entsprechender GUI. So wird die Konfiguration erleichtert und ein Wechsel des Miningprogramms oder des Algorithmus unkompliziert möglich.

5.3.2 Linux

Unter Linux ist die Nutzung von NiceHash und BetterHash nicht möglich, da diese ausschließlich für Windows verfügbar sind. AwesomeMiner und die zugrundeliegenden Miningprogramme selbst können jedoch ebenfalls auf Linux betrieben werden. So kann Mining beispielsweise mit folgenden Programmen auf Linux betrieben werden:

- lolMiner
- NanoMiner
- NBMiner
- GMiner

Die aufgelisteten Programme können auf Linux und auf Windows mittels AwesomeMiner oder eigenständig verwendet werden und unterstützen Nvidia und AMD Grafikkarten. [73]

5.4 Kosten

Tabelle 5.2 listet alle Positionen, die im Rahmen dieses Studienprojekts Kosten verursacht haben, auf. Eine Ausnahme sind die Stromkosten. Wie diese ermittelt werden, wird in Kapitel 6.2 näher erläutert.

Pos.	Komponente	Anzahl	Stückpreis	Gesamt
1	Frame für 6 Grafikkarten	1	33,90 €	33,90 €
2	MSI Z87-G45 GAMING	1	113,99 €	113,99 €
3	Intel i7-4770k 4.Generation	1	290,00 €	290,00 €
4	Corsair XMS3 2x 8 GB DDR3	1	89,99 €	89,99 €
5	Asus Radeon RX 580 8 GB	1	300,00 €	300,00 €
6	Power Color Radeon RX 580	1	254,11 €	254,11 €
7	Zotac GeForce RTX 2070 Super	1	583,99 €	583,99 €
8	Kompaktwasserkühlung CPU	1	57,90 €	57,90 €
9	Corsair RM850 850 Watt	1	124,00 €	124,00 €
10	KOLINK Riser Card	3	12,90 €	38,70 €
11	Arctic F12 120 mm	3	7,59 €	22,77 €
12	SanDisk 32 GB USB-Stick	1	6,32 €	6,32 €
13	Crucial BX500 120 GB	1	52,51 €	52,51 €
14	TP-Link Kasa HS110	1	21,75 €	21,75 €
15	Awesome Miner (Monate)	2	4,00 €	8,00 €
16	Ledger Nano S (Wallet)	1	59,00 €	59,00 €
Gesamt				2056,93 €

Tabelle 5.2: Kosten des Mining-Rigs

Die Hardware zur Realisierung dieser Studienarbeit wurde ausschließlich über den Online-versandhändler Amazon bezogen. Die Summe aller oben genannten Positionen ergeben einen Gesamtpreis von 2056,93 €.

5.5 Ermittlung der Effizienz

Die Effizienz wird in Bezug auf die Wirtschaftlichkeit betrachtet. Es wird ein Verhältnis zwischen den aufgebrachten Kosten (Aufwand) und dem erwirtschafteten Betrag (Ertrag) errechnet. Dabei werden initiale Kosten zur Anschaffung der Hardware außen vor gelassen. Die Formel für diese Berechnung ist nach Günter Wöhe [75, S.38] wie folgt definiert:

$$(5.1) \quad \text{Wirtschaftlichkeit(Effizienz)} = \frac{\text{Ertrag}}{\text{Aufwand}}$$

Die verbrauchte Energie in Form von Strom wird mithilfe des Kilowattstundenzählers ermittelt und mit dem aktuellen Strompreis verrechnet. Der Strompreis liegt zum Zeitpunkt der Durchführung der Studienarbeit bei 0,26 € pro kWh und ist vertraglich für das Jahr 2022 festgeschrieben, sodass dieser Wert für alle Berechnungen genutzt werden kann. Der Ertrag hingegen hängt von zwei Faktoren ab. Zum einen wie viel Kryptowährung das System schürft und zum anderen wie der Wechselkurs zum Euro der geschürften Währungen steht. So wäre es theoretisch möglich, eine gute Effektivität in Bezug auf eine Kryptowährung zu erzielen. Hat diese Währung gerade oder generell einen schlechten Wechselkurs zum Euro, ist die Effektivität bzw. Wirtschaftlichkeit allerdings schlecht.

5.6 Verbesserungsmöglichkeiten

Um die Effizienz zu verbessern, muss entweder der Ertrag gesteigert oder der Aufwand vermindert werden. Zur Minderung des Aufwands wäre es möglich, den Stromanbieter zu wechseln, um einen günstigeren Stromtarif zu bekommen, allerdings liegt der durchschnittliche Strompreis in Deutschland bei 32,62 € pro Kilowattstunde [76] und somit weit über dem im Kapitel zuvor genannten. Eine weitere Option wäre es, ein Netzteil mit höherem Wirkungsgrad zu nutzen. Netzteile arbeiten am effektivsten bei einer Belastung von etwa 80%, allerdings kann diese bei der Umsetzung nicht für jedes Testszenario erreicht werden. Auch leistungsfähigere Grafikkarten mit weniger Energieaufnahme würden zur Leistungssteigerung beitragen. Ist es allerdings erwünscht, die Effizienz mit der gleichen Hardware zu steigern, bleibt die Möglichkeit, den Ertrag zu steigern. Dies wird in erster Linie durch die richtige Nutzung erreicht, wie in Kapitel 5.3 beschrieben. Außerdem sind Firmware-Updates oder das Übertakten der Hardware möglich. Beim generellen

Übertakten der Hardware muss allerdings darauf geachtet werden, dass in der Regel die Erhöhung der Taktrate mit einer höheren Spannung am Bauteil erzeugt wird und somit eben auch die Stromaufnahme steigt.

5.7 Ziele

Das Ziel dieser Arbeit ist die Evaluation eines Kryptominingsystems. Dazu wird das Mining-Rig in verschiedenen Konfigurationen aufgebaut, getestet und ausgewertet. Dabei werden die drei Grafikkarten einzeln oder in verschiedenen Kombination eingebaut, unterschiedliche Betriebssysteme und Miner getestet. Zu den Betriebssystemen zählen Windows, Linux und ein ausgewähltes Mining-Betriebssystem HiveOS. Außerdem wird versucht, die Hardware mit Übertaktungsmaßnahmen profitabler zu machen. Für die Einschätzung der Leistungsfähigkeit wird mithilfe eines Kilowattstundenzählers der Energieverbrauch ermittelt. Weitere Leistungsmerkmale sind die geschürfte Kryptowährung, die Hashrate der Hardware sowie die erzeugte Wärme. Die erhobenen Daten werden dann ausgewertet und gegenübergestellt. Dadurch wird versucht, die effizienteste Konfiguration zu finden und schließlich auf dieser Basis eine Empfehlung abzugeben.

6 Umsetzung

Das Kapitel Umsetzung beschäftigt sich mit dem Aufbau und der Einrichtung des Mining-Rigs nach den in Kapitel 5 geschaffenen Rahmenbedingungen. Des Weiteren werden in diesem Kapitel alle Testszenarien durchgeführt und die Leistungsdaten erhoben. Leistungssteigerung sowie die Evaluierung von Auto Switching ist ebenfalls Teil dieses Kapitels.

6.1 Einrichtung Wallet

Wie im Kapitel Grundlagen 2 beschrieben, ist der erste Schritt die Erstellung eines Wallets. Dazu wird ein Hardware-Wallet der Firma Ledger verwendet. Die Abbildung 6.1 zeigt den Ledger Nano S.



Abbildung 6.1: Ledger Nano S

Die Einrichtung des Hardware-Wallets ist denkbar einfach, zuerst muss ein PIN-Code festgelegt werden. Anschließend zeigt der Ledger eine 24 Wörter Phrase an, die unbedingt sicher aufbewahrt werden sollte. Diese dient zur Wiederherstellung des Wallets, sollte der PIN verloren gehen oder die Hardware beschädigt werden. Im nächsten Schritt kann der Ledger mit dem Computer verbunden und die Ledger Live Sofware installiert werden. Damit die Software Zugriff auf die im Ledger gespeicherten Informationen erhält, muss auf dem Hardware-Wallet mit einem Tastendruck die Zugriffsanfrage bestätigt werden. Die Software erlaubt nun über einen Manager Wallets, welche von Ledger als Apps bezeichnet werden, passend zum geschürften Coin zu installieren. Dies erfolgt über einen

App Catalog, welcher alle von Ledger unterstützten Apps enthält. Da im Rahmen dieser Arbeit ausschließlich Ethereum geschürft wird, muss die Ethereum App installiert werden. Abbildung 6.2 zeigt dies. Die Installation einer oder mehrere dieser Apps muss ebenfalls mit der Bestätigung am Ledger verifiziert werden.

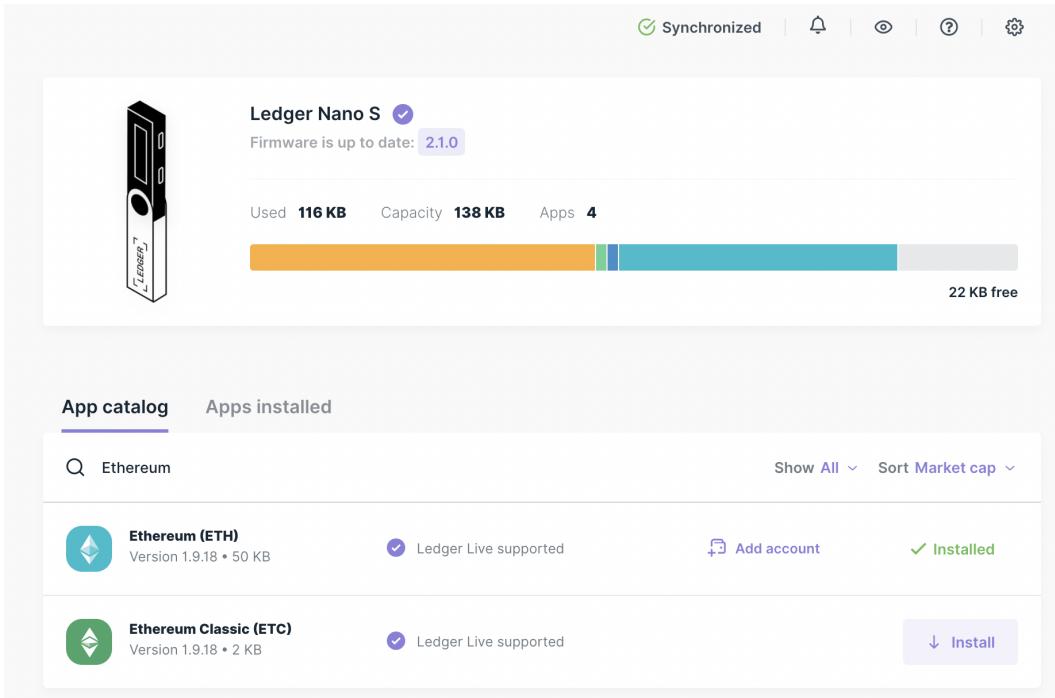


Abbildung 6.2: Ledger Apps

Nach der Installation muss ein sogenannter Account angelegt werden. Ein Account entspricht einem Wallet mit einer Wallet Adresse. Dies kann direkt aus dem App Catalog erfolgen. Nachdem ein Account angelegt wurde, kann die Adresse dieses Accounts angezeigt werden. Abbildung 6.3 zeigt die Anzeige der Adresse über die Receive Funktion in der Ledger Live Software. Zu diesem Zeitpunkt können bereits Einzahlungen auf das Wallet erfolgen.

Da in den folgenden Testszenarien unterschiedliche Programme zum Kryptomining evaluiert werden, ist nicht in allen Fällen die Nutzung des Ledger Wallets im wirtschaftlichen Sinne sinnvoll, denn einige Anbieter erheben bei der Nutzung eigener Wallets und nicht deren integrierter zusätzliche Gebühren. Um diese zu vermeiden, werden in den integrierten Wallets genutzt. Beispielsweise erhebt NiceHash für die Nutzung eigener Wallets im Mining-Prozess zusätzliche Gebühren. [77] Angesichts dessen werden in diesen Fällen die integrierten Wallets eingesetzt. In allen anderen Fällen wird das Wallet des Ledgers genutzt. Details dazu finden sich in den entsprechenden Testszenarien.

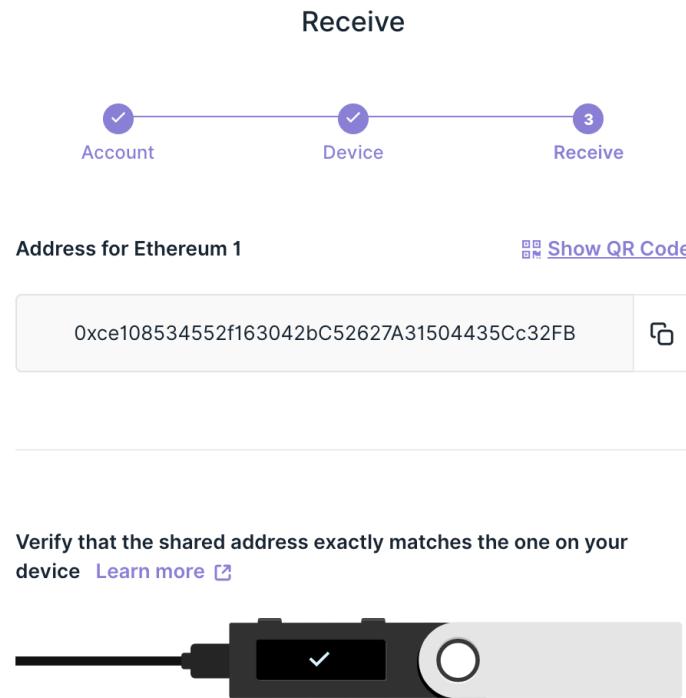


Abbildung 6.3: Ledger Ethereum Wallet

6.2 Ermittlung des Stromverbrauchs

Um den Stromverbrauch des Rigs zu ermitteln, wird wie bereits erwähnt eine TP-Link Kasa HS110 Steckdose verwendet. Diese Steckdose besitzt einen integrierten Leistungsmesser und kann daher zur Ermittlung der aktuell benötigten Leistung sowie des Verbrauchs eingesetzt werden. Die vom Hersteller bereitgestellte App ermöglicht jedoch nur die Anzeige des aktuellen Verbrauchs, ohne diesen zeitlich aufzuschlüsseln. Um den Stromverbrauch des Rigs möglichst korrekt zu ermitteln, ist die zeitliche Aufschlüsselung der aktuell benötigten Leistung notwendig. Damit keine Verfälschung durch kurzzeitige Leistungsschwankung bei der Ermittlung der benötigten Leistung auftritt, wird der Mittelwert aus 10 einzelnen Werten gebildet. Die eingesetzte Web-Applikation protokolliert die aktuelle Leistung pro Minute. Damit ergibt sich der Mittelwert von 10 Minuten, der als benötigte Leistung im weiteren Verlauf dieser Arbeit je Szenario angenommen wird. Ermöglicht wird dies durch die freie Web-Applikation *TPLink Energy Monitor*. [78] Abbildung 6.4 zeigt einen Auszug aus der Web-Oberfläche des *TPLink Energy Monitors*.

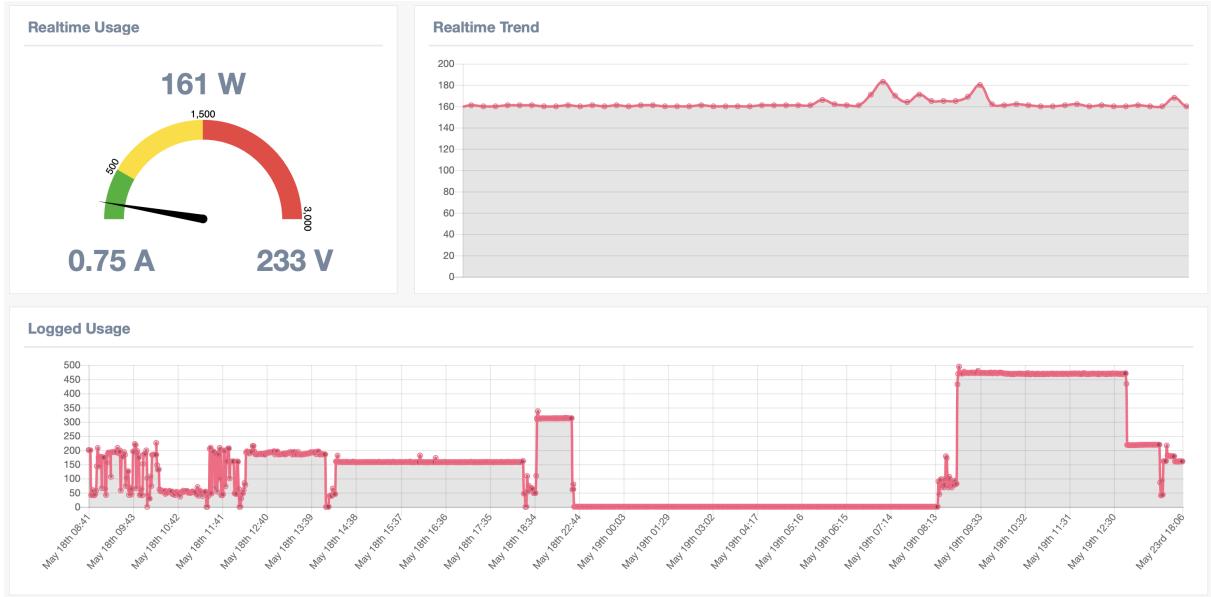


Abbildung 6.4: Web-Oberfläche zur Leistungsmessung (Auszug)

6.3 Einrichtung Mining-Rig (Hardware)

Das nach dem Konzept aus dem Kapitel 5 realisierte Mining-Rig ist in der Abbildung 6.5 und 6.6 dargestellt. Das Mainboard wird in den Rahmen eingesetzt und verschraubt, daneben sind das Netzteil und eine Festplatte platziert und fest mit dem Rahmen verschraubt. Die Riser-Karten stecken in den vorhandenen PCIe-Slots auf dem Mainboard und die Gegenstücke sind an der darüberliegenden Querstrebe fixiert. Beide Teile der Riser-Karten sind mittels eines USB-Kabels verbunden. Die Grafikkarten sind wiederum in die Riser-Karten gesteckt und mit dem Rahmen verschraubt. Die Lüfter sind an der Frontseite zu den Grafikkarten montiert, um die Zwischenräume der Karten mit kühler Luft zu versorgen und um die Abwärme abzuführen. Die Lüfter sind mit dem Mainboard verbunden und auf System-Fan 1-3 angesteckt. Außerdem ist der CPU-Kühler am Steckplatz CPU-Fan angeschlossen. Alle Komponenten sind zudem für die Stromversorgung mit dem Netzteil verbunden. Diese Verbindungen sind mit Molex 4-Pol-Kabeln und mit 6/8-Pol PCIe-Kabeln realisiert. Das Rig kann mit einem Schließerkontakt über die Power-SW-Pins am Mainboard gestartet werden. Um den Start zu vereinfachen, wird der Schließerkontakt durch einen Taster ersetzt. Es verfügt zudem über eine LAN-Anbindung und damit auch einen Zugang ins Netzwerk. Administriert wird das Rig über eine Remote Verbindung mittels Remote Desktop Protocol (RDP) von Microsoft und unter Linux über Secure Shell (SSH).



Abbildung 6.5: Mininig-Rig (1)



Abbildung 6.6: Mining-Rig (2)

6.4 Einrichtung Mining-Rig (Software)

Nun wird die Einrichtung des Mining-Rigs unter dem Aspekt Software erläutert. Da im Rahmen dieser Arbeit sowohl das Betriebssystem Windows als auch Linux sowie ein Mining-Betriebssystem, welches auf Linux basiert, evaluiert werden, unterscheidet sich die Einrichtung je nach Betriebssystem. Auf allen wird jedoch die Software *PhoenixMiner* und *lolMiner* eingesetzt. Die notwendigen Informationen zum Mining wie die Pool-Adresse, Port, Worker Name und Passwort müssen als Parameter an die Mining-Software übergeben werden. Dabei ist die Parametrisierung abhängig von der Software. Grundsätzlich werden jedoch die gleichen Parameter übergeben. Listing 6.1 und 6.2 zeigen beispielhaft, wie die in dieser Arbeit eingesetzten Miner zu parametrisieren sind.

```
1 PhoenixMiner.exe -pool eu1.ethermine.org:4444 -pool2 us1.
    ethermine.org:4444 -wal
    ce108534552f163042bC52627A31504435Cc32FB -proto 3
```

Listing 6.1: Parametrisierung der Mining-Software PhoenixMiner

```
1 lolMiner.exe --algo ETHASH --pool eu1.ethermine.org:4444 --
    user ce108534552f163042bC52627A31504435Cc32FB
```

Listing 6.2: Parametrisierung der Mining-Software lolMiner

6.4.1 Windows

Zu Beginn der Umsetzung werden die Tests auf Windows mit der Software Awesome Miner durchgeführt. Dazu wird im ersten Schritt Windows 10 Pro auf dem System installiert. Im nächsten Schritt werden entsprechende Treiber für die Grafikkarten installiert. Um auf AMD Grafikkarten schürfen zu können, muss die entsprechende Grafikkarte in den *compute Mode*, oder auch Berechnungs-Modus genannt, umgeschaltet werden. Ab Werk befinden sich die Grafikkarten im Grafikmodus. Ohne Umschalten in den Berechnungs-Modus würden die Grafikkarten nur circa ein Drittel der Leistung im Miningprozess erbringen. Der *compute Mode* kann entweder über die von AMD mitgelieferte Software, in der unter anderem auch das Übertragen der Grafikkarten möglich ist, oder über ein frei erhältliches PowerShell Skript aktiviert werden. Die Ausgabe des Skripts ist in Listing 6.3 dargestellt.

Letztlich werden die entsprechenden Einträge in der Windows Registry durch das Skript angepasst.

```

1 AMD Compute Mode Toggle Script v2.0
2
3 Choose between:
4 (1) Turn ON Compute Mode - Adds mining power to AMD GPUs
5 (2) Turn OFF Compute Mode - Back to default registry
   settings
6 (9) Check the Compute Mode status of all AMD GPUs
7 (X) Any other selection will exit the script
8
9 Make a choice and press ENTER: 1
10
11      GPU #0 is AMD, modifying settings...
12      GPU #0 MOD - Compute Mode is now ENABLED
13      GPU #0 is SET FOR MINING
14
15      GPU #1 is Microsoft, no mods needed!
16
17      GPU #2 is AMD, modifying settings...
18      GPU #2 MOD - Compute Mode is now ENABLED
19      GPU #2 is SET FOR MINING
20
21      GPU #3 is Intel Corporation, no mods needed!
22
23      GPU #4 is NVIDIA, no mods needed!
24
25 -> 4 changes were made to your registry; 4 succeeded and 0
   failed.
26 RESTART YOUR PC FOR THE NEW REGISTRY SETTINGS TO BE APPLIED

```

Listing 6.3: Ausgabe PowerShell Skript: Switch Compute Mode

Bei Grafikkarten von Nvidia ist die Umstellung nicht notwendig. Nach der Umstellung der AMD Grafikkarten in den *compute Mode* folgt die Installation von Awesome Miner. Wie bereits in vorherigen Kapiteln erwähnt, umfasst Awesome Miner diverse Miningprogramme.

Konkret werden die beiden Miningprogramme *lolMiner* und *PhoenixMiner* im Rahmen der Durchführung dieser Arbeit verwendet. Beide Miningprogramme unterstützen sowohl Grafikkarten von Nvidia als auch von AMD. Das Miningprogramm *lolMiner* ist primär auf AMD Grafikkarten ausgelegt, unterstützt jedoch auch gängige Nvidia Karten. Die Entwicklergebühr liegt dabei bei 1%. Der *PhoenixMiner* zeichnet sich durch eine geringe Entwicklergebühr von 0,65% aus. Außerdem ist dieses Miningprogramm primär für den Ethash Algorithmus und damit für das Schürfen von Ethereum ausgelegt. Sowohl *lolMiner* als auch *PhoenixMiner* unterstützen Windows wie auch Linux und bieten darüber hinaus das sogenannte Dual-Mining an. Dual-Mining ermöglicht das gleichzeitige Ausführen von zwei Algorithmen auf einer Grafikkarte und damit das gleichzeitige Schürfen von zwei Währungen. Nach der Installation von Awesome Miner muss ein Miner angelegt werden. Dies kann als Profil mit einer festgelegten Miningkonfiguration verstanden werden. Grundsätzlich besitzt Awesome Miner verschiedene Möglichkeiten, einen Miner zu erstellen. Neben der Anbindung an die API eines bestehenden Miningprogramms bietet Awesome Miner die Möglichkeit eines *Managed-Miner* oder eines *Managed-Profit-Miner*. In beiden Fällen werden die Verwaltung und Konfiguration der eigentlichen Miningprogramme durch Awesome Miner realisiert. Daher wird dies auch als managed bezeichnet. Der Unterschied zwischen *Managed Miner* und *Managed Profit Miner* liegt in der Funktionsweise. Wird ein *Managed Miner* erstellt, so wird ausschließlich der festgelegte Algorithmus unabhängig von der Profitabilität geschürft. Wird hingegen ein *Managed Profit Miner* verwendet, so wird automatisch zwischen verschiedenen Algorithmen je nach Profitabilität gewechselt. Dies wird auch als Auto-Switching bezeichnet (siehe Kapitel 6.10). Ziel ist es, den Gewinn durch das Wechseln von Mining-Algorithmen zu maximieren. Unter Windows kommt ausschließlich ein *Managed Miner* zum Einsatz. Abbildung 6.7 zeigt die Einrichtung eines *Managed Miners* in Awesome Miner. Zu den notwendigen Angaben gehören der Algorithmus, eine kompatible Mining-Software sowie ein Pool. Zusätzlich kann optional Dual-Mining konfiguriert oder der Pfad zu einer bereits installierten Mining-Software angegeben werden.

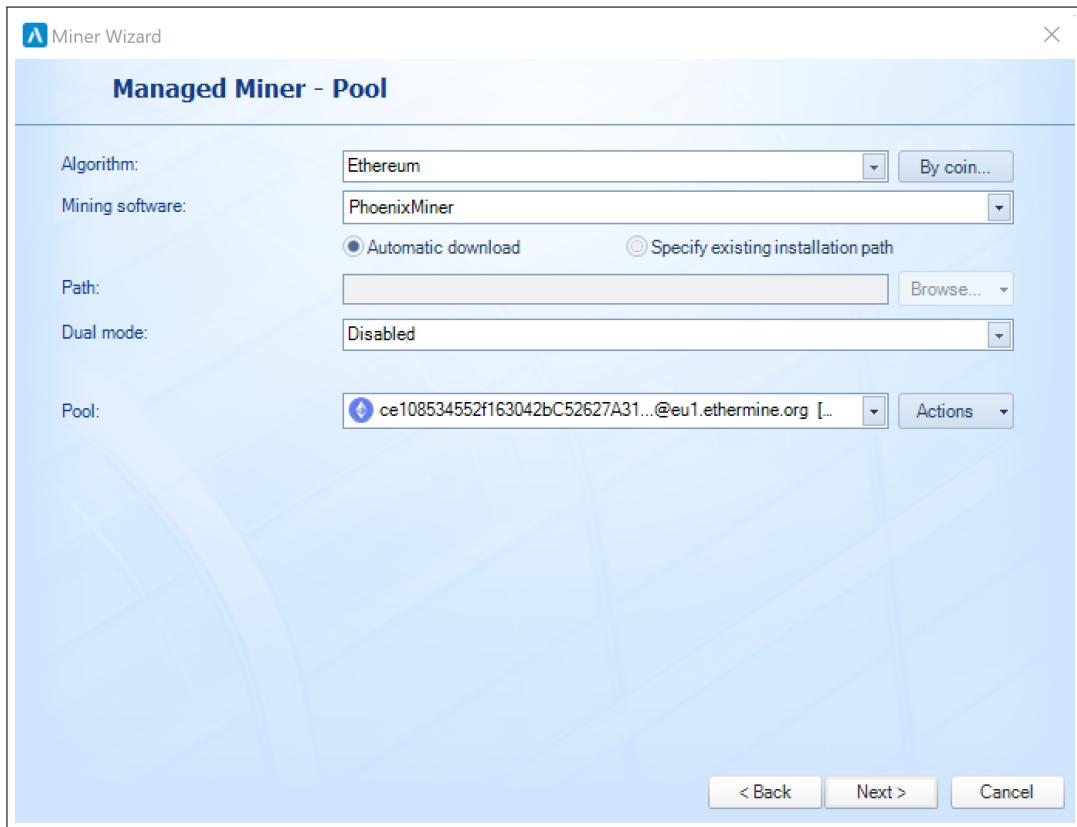


Abbildung 6.7: Awesome Miner Konfiguration

Um in der *Managed Miner* Konfiguration den gewünschten Pool angeben zu können, muss dieser zuerst konfiguriert werden. Pools werden über eine IP-Adresse oder einen Hostname und einen Port spezifiziert. Kommuniziert wird über das Stratum Protokoll (siehe Kapitel 4.4). Zusätzlich sind noch ein sogenannter Worker Name sowie ein Passwort notwendig. I.d.R. bieten Pools Server auf verschiedenen Kontinenten der Erde an, weshalb stets der nächstgelegene Server gewählt werden sollte. In dieser Arbeit wird der Ethermine Pool verwendet. Dieser bietet einen Server in Europa an. Die Uniform Resource Locator (URL) sowie der Port lassen sich von der Website des Pools entnehmen. Grundsätzlich gibt es zwei verschiedene Möglichkeiten, wie Pool Betreiber die Miner identifizieren. Zum einen bieten einige Pools eigene Benutzerkonten an. In diesem Benutzerkonto werden dann entsprechende Wallet-Adressen für die Auszahlung der geschürften Kryptowährungen hinterlegt. Letztlich wird in der Mining-Software als Worker Name der Benutzername des Pool-Kontos angegeben. Die zweite Möglichkeit ist, direkt die Wallet Adresse als Worker Name anzugeben. Pools wie Ethermine bieten keine eigenen Benutzerkonten an, sondern nutzen direkt die Wallet-Adressen. Somit muss kein zusätzliches Konto angelegt werden.

und die Auszahlung erfolgt auf das Wallet, mit dem sich der Worker beim Pool anmeldet. Abbildung 6.8 zeigt die Konfiguration eines Pools in Awesome Miner.

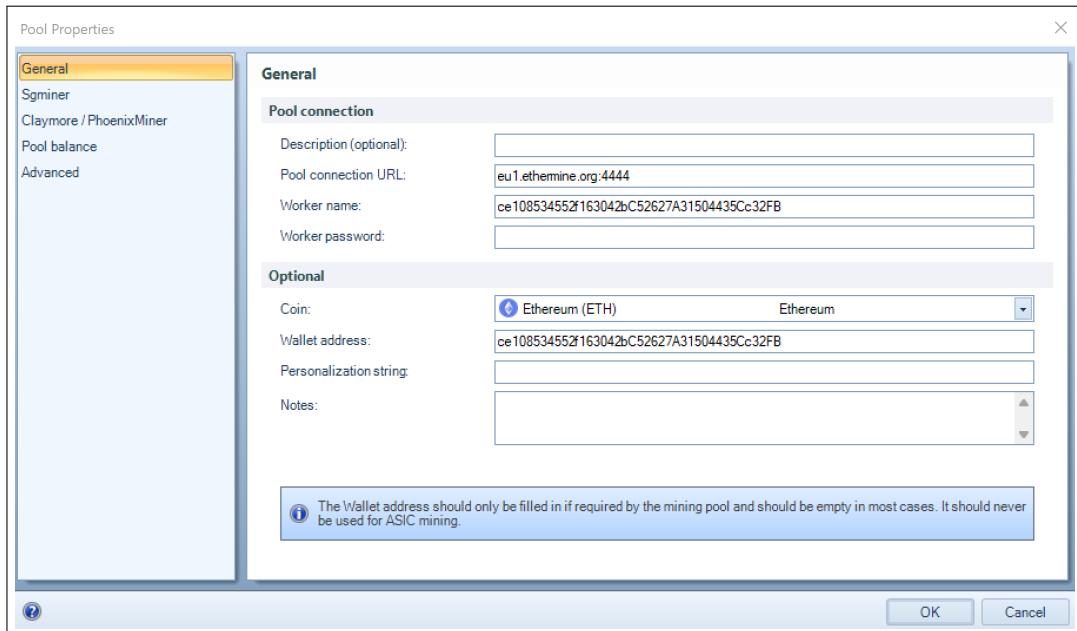


Abbildung 6.8: Awesome Miner Pool Konfiguration

Durch das Erstellen eines *Managed Miners* und dem entsprechenden Pool in Awesome Miner, wird die Parametrisierung der Mining-Software automatisch von Awesome Miner übernommen. So kann einfach zwischen verschiedenen Minern gewechselt werden, ohne dass die Parametrisierung verändert werden muss.

6.4.2 Linux

Für die Umsetzung und die Durchführung der Tests im Rahmen dieser Arbeit wird das Betriebssystem Ubuntu Server 21.04 Long Time Support (LTS) eingesetzt. In Bezug auf die Verfügbarkeit von Treibern für Grafikkarten als auch die Einfachheit der Bedienung ist Ubuntu für den Einsatzzweck dieses Projekts geeignet. Da eine GUI Grafikressourcen benötigt, wird die Server Version von Ubuntu verwendet. Damit entfällt die GUI und die gesamte Leistung der Grafikkarten steht für das Mining zur Verfügung. Nach der Installation des Betriebssystems werden Treiber für die Grafikkarten benötigt. Treiber für Nvidia Grafikkarten werden über den Advanced Packaging Tool (APT) Paketmanager installiert. AMD Treiber müssen vom Hersteller heruntergeladen und installiert werden. Wie auch bei Windows ist es notwendig, die AMD Grafikkarten in den *compute mode*

zu versetzen. Dies kann entweder manuell oder über ein Skript ähnlich wie bereits in Abschnitt 6.4.1 umgesetzt werden. Um eine Grafikkarte in den *compute mode* zu versetzen, ist die Anpassung von zwei Werten notwendig. Zum einen muss in ”/sys/class/drm/-card0/device/power_dpm_force_performance_level” der Wert ”manual” geschrieben werden und zum anderen in ”/sys/class/drm/card0/device/pp_power_profile_mode” der Wert ”5”. Fünf steht dabei für *compute mode*. Diese beiden Werte sind für jede Karte einzeln anzupassen. Im Pfad ändert sich dabei in Abhängigkeit der gewählten Grafikkarte der Ordner ”card0”. Außerdem muss dies bei jedem Startvorgang des Systems wiederholt werden. [79] Um die Vergleichbarkeit zu gewährleisten, wird auf Linux ebenfalls Awesome Miner eingesetzt. Der Aufbau unterscheidet sich jedoch von Windows. Auf dem Linux System wird der Awesome Miner Remote Agent installiert. Ein zweites System mit Windows dient zur Entfernten-Verwaltung des Linux Mining-Systems. Auf dem Windows System wird ein *External Miner* angelegt. Über diesen kann im Anschluss das Linux System verwaltet werden. Die Konfiguration eines entfernten Miners entspricht der eines *Managed Miners*. Die Mining-Software sowie die Parametrisierung werden automatisch durch den Awesome Miner Remote Agent lokal umgesetzt. Abbildung 6.9 zeigt die Einrichtung eines *External Miners*.

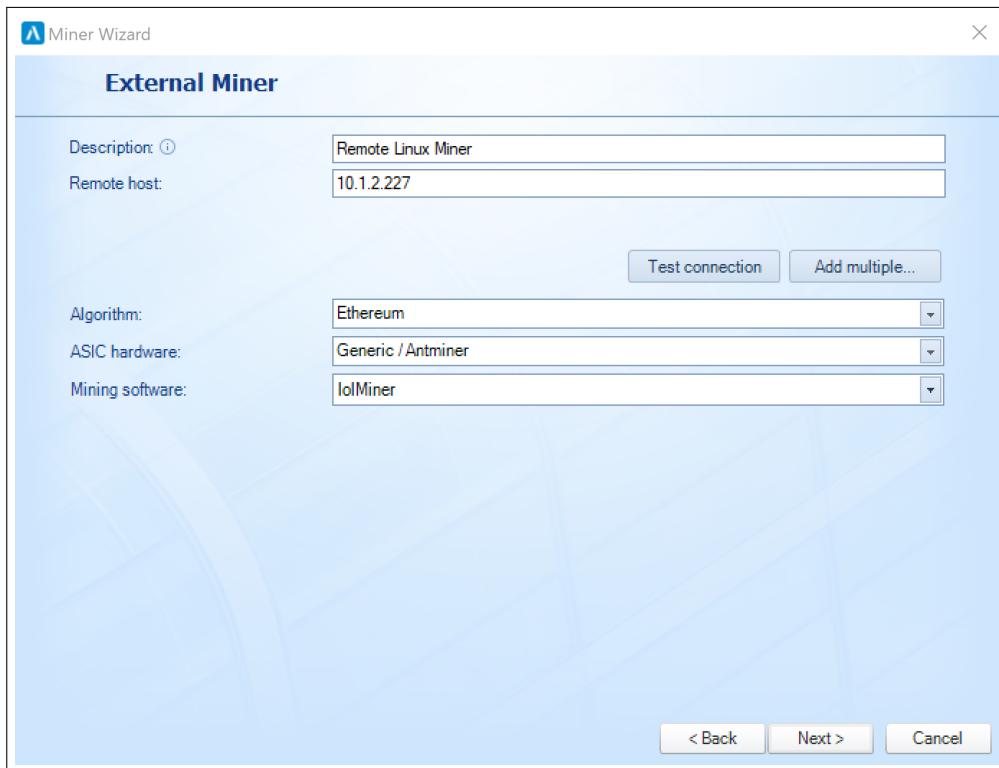


Abbildung 6.9: Awesome Miner: entfernte Miner Einrichtung

6.4.3 Mining-OS

Als Mining-OS wird HiveOS eingesetzt. HiveOS ist ein auf Mining optimiertes Ubuntu 18.04 LTS Server System, das bereits alles für den Mining-Betrieb Notwendige beinhaltet. Es sind bereits Treiber für Nvidia und für AMD Grafikkarten enthalten, sowie diverse Mining-Software und Tools zur Verwaltung. Außerdem bietet HiveOS eine entfernte Verwaltung des Systems und Möglichkeiten zur Übertaktung. Auto-Switching und Dual-Mining sind ebenfalls mit HiveOS möglich. Zur Installation muss das HiveOS Image auf einen USB-Stick geschrieben werden. Im Anschluss muss eine Konfigurationsdatei auf den USB-Stick in das Wurzelverzeichnis kopiert werden. Sie wird über die HiveOS Website heruntergeladen. In dieser Datei ist eine eindeutige ID hinterlegt, mit der das Rig dem HiveOS Nutzeraccount zugeordnet wird. Listing 6.4 zeigt diese Datei.

```

1 # This is unique ID of your farm
2 FARM_HASH="50ae8869ca309ed4c3963553e764df59f246e47d"
3 #URL where hive server is
4 HIVE_HOST_URL="http://api.hiveos.farm"
5 API_HOST_URLs="http://api.hiveos.farm http://api2msk.hiveos.
farm"
```

Listing 6.4: HiveOS Konfigurationsdatei (rig.conf)

Das System wird von dem erstellten USB-Stick gestartet. HiveOS ist ein LiveSystem. Daher ist keine Installation notwendig. Nach dem Start registriert sich das System über die HiveOS API und kann im Anschluss über die HiveOS Weboberfläche verwaltet werden. Die Mining-Konfiguration befindet sich in sogenannten *flight sheets*. In ihnen werden ähnlich wie bei Aweseome Miner alle Parameter für die Mining-Software definiert. Zusätzlich muss neben dem *flight sheet* auch ein Wallet im HiveOS Konto hinzugefügt werden. Das Wallet besteht aus einem frei wählbaren Namen und der entsprechenden Wallet-Adresse. Das angelegte Wallet wird im *flight sheet* ausgewählt und dient als Worker Name für den Ethermine-Pool. Wie bereits erwähnt, erfolgt die Zuordnung und die Auszahlung des Pools an die Miner über die Ethereum Wallet-Adresse als Worker Name. Listing 6.5 zeigt das verwendete *flight sheet* für die Software lolMiner.

```

1  {
2      "name": "lolMiner Ethermine",
3      "isFavorite": false,
4      "items": [
5          {
6              "coin": "ETH",
7              "pool": "ethermine",
8              "pool_geo": [
9                  "EU"
10             ],
11             "pool_ssl": false,
12             "pool_urls": [
13                 "eu1.ethermine.org:4444",
14                 "eu1.ethermine.org:14444"
15             ],
16             "wal_id": 6068246,
17             "dpool_ssl": false,
18             "miner": "lolminer",
19             "miner_config": {
20                 "algo": "ETHASH",
21                 "pass": "x",
22                 "port": "%URL_PORT%",
23                 "server": "%URL_HOST%",
24                 "template": "%WAL%.%WORKER_NAME%"
25             }
26         }
27     ]
28 }
```

Listing 6.5: HiveOS FlightSheet (lolMiner)

6.5 Durchführung der Test-Szenarien

Das Mining-Rig ist auf GPU-Mining ausgelegt, sodass nur entsprechende Coins infrage kommen, die dies unterstützen. Der größte Vertreter davon ist ETH. Ziel ist es, ETH

oder verwandte Coins innerhalb eines Pools zu schürfen. Dieser Vorgang soll in einigen Test-Szenarien untersucht werden. Die Test-Szenarien werden nach Betriebssystem gegliedert und in verschiedenen Aufbauten durchgeführt. Das bedeutet, die Tests werden mit unterschiedlicher Anzahl an GPUs und verschiedener Mining-Softwares betrachtet. Eine Testmatrix zu allen Test-Szenarien kann im Anhang eingesehen werden. Um anschließend eine Evaluation durchzuführen, werden bei jedem Durchgang Daten erhoben. Für einen möglichen Vergleich wird versucht, einen möglichst gleichbleibenden Datensatz zwecks Vergleichbarkeit zu erzeugen. Er umfasst folgende Daten:

- Dauer
- Ø Hashrate
- Ø Temperatur GPU
- Ø Leistung GPU
- Ø Leistung System
- benötigte Energie
- geschürfte Bitcoin
- Bilanz

Täglich ändernde Wechselkurse der Währungen machen einen Vergleich der einzelnen Szenarien schwierig und wenig aussagekräftig. Aus diesem Grund wurden folgende Voraussetzungen für die Testszenarien getroffen, um die erhobenen Daten möglichst gut vergleichen zu können:

- In der Regel wird bei Mining-Pools die Menge der geschürften Kryptowährung in Bitcoin umgerechnet. Da mehrere Miner sowie Softwares zum Einsatz kommen, wird der Bitcoin als Referenz genommen und alle Ergebnisse in **BTC** angegeben.
- Ein fester Wechselkurs vom Dollar zum Euro mit dem Faktor **0,92**. Stand 06.03.2022.
- Ein fester Wechselkurs vom Bitcoin zum Euro mit dem Faktor **44000**. Durchschnittswert der letzten 6 Monate. Stand 06.03.2022.
- Ein fester Kilowattstundenpreis von **0,26 €** (beschrieben in Kapitel 5.5).

6.6 Windows Szenarien

Die Test-Szenarien 1 bis 14 werden mit dem Betriebssystem Windows 10 Pro durchgeführt. Eingesetzte Mining-Softwares: Awesome Miner mit den Mineren lolMiner und PhoenixMiner.

6.6.1 Szenario 1

Hardware-Aufbau:

In diesem Test-Szenario werden ausschließlich die Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 31 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgegloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 26,65 MH/s
- Ø max. Temperatur: 55,14 °C
- Ø Leistung aller GPUs: 177 W
- Ø Leistung System: 200 W
- benötigte Energie: 4,80 kWh ~ 1,25 €
- Bitcoin: 0,000028 BTC ~ 1,23 €
- Bilanz: Verlust **0,02 €**

Die Abbildung 6.10 veranschaulicht dieses Ergebnis.

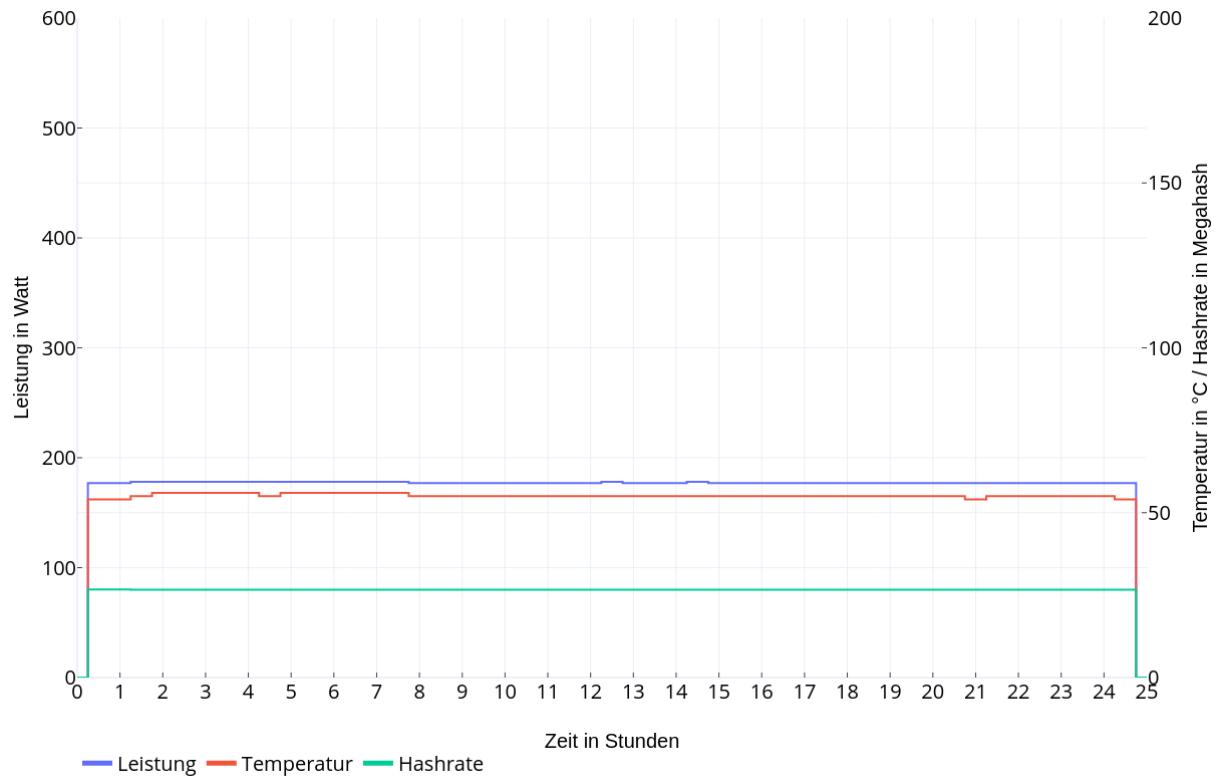


Abbildung 6.10: Aufbau 01

6.6.2 Szenario 2

Aufbau:

In diesem Test-Szenario wird ausschließlich die Power Color Radeon RX580 8 GB Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 30 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggert und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 22,91 MH/s
- Ø max. Temperatur GPU: 66,04 °C
- Ø Leistung aller GPUs: 156 W
- Ø Leistung System: 197 W
- benötigte Energie: 4,73 kWh ~ 1,23 €
- Bitcoin: 0,000024 BTC ~ 1,06 €
- Bilanz: Verlust **0,17 €**

Die Abbildung 6.11 veranschaulicht dieses Ergebnis.

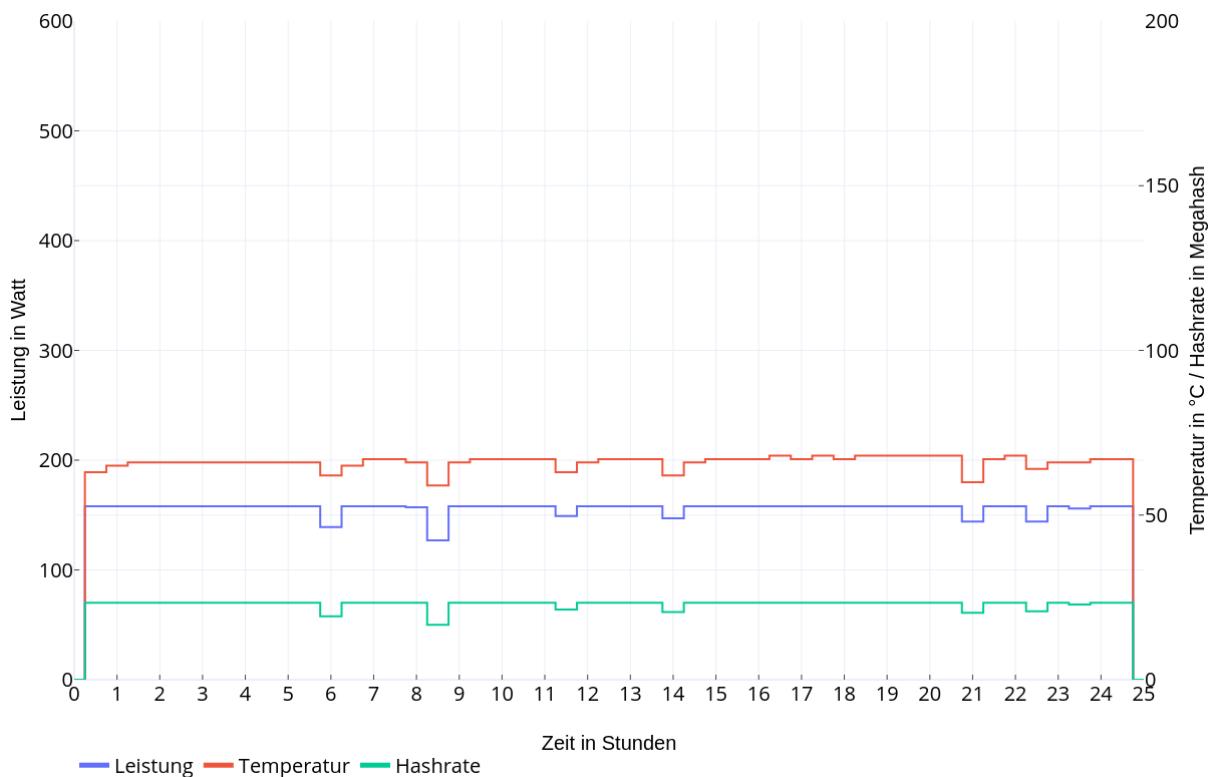


Abbildung 6.11: Aufbau 02

6.6.3 Szenario 3

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 38 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 36,87 MH/s
- Ø max. Temperatur: 58,35 °C
- Ø Leistung aller GPUs: 172 W
- Ø Leistung System: 206 W
- benötigte Energie: 4,94 kWh ~ 1,28 €
- Bitcoin: 0,000038 BTC ~ 1,67 €
- Bilanz: Gewinn 0,39 €

Die Abbildung 6.12 veranschaulicht dieses Ergebnis.

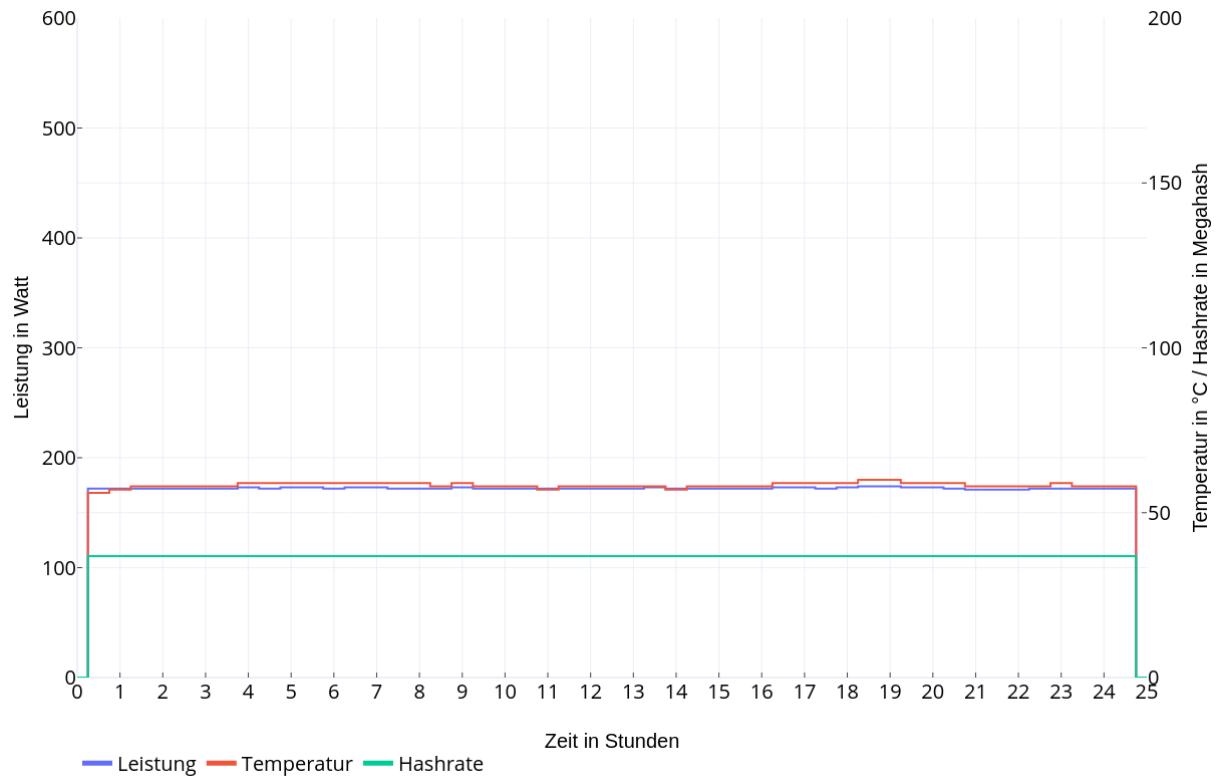


Abbildung 6.12: Aufbau 03

6.6.4 Szenario 4

Aufbau:

In diesem Test-Szenario wird die Power Color Radeon RX580 8 GB Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 45 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggert und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 49,99 MH/s
- Ø max. Temperatur: 69,00 °C
- Ø Leistung aller GPUs: 337 W
- Ø Leistung System: 370 W
- benötigte Energie: 8,88 kWh ~ 2,31 €
- Bitcoin: 0,000052 BTC ~ 2,29 €
- Bilanz: Verlust **0,02 €**

Die Abbildung 6.13 veranschaulicht dieses Ergebnis.

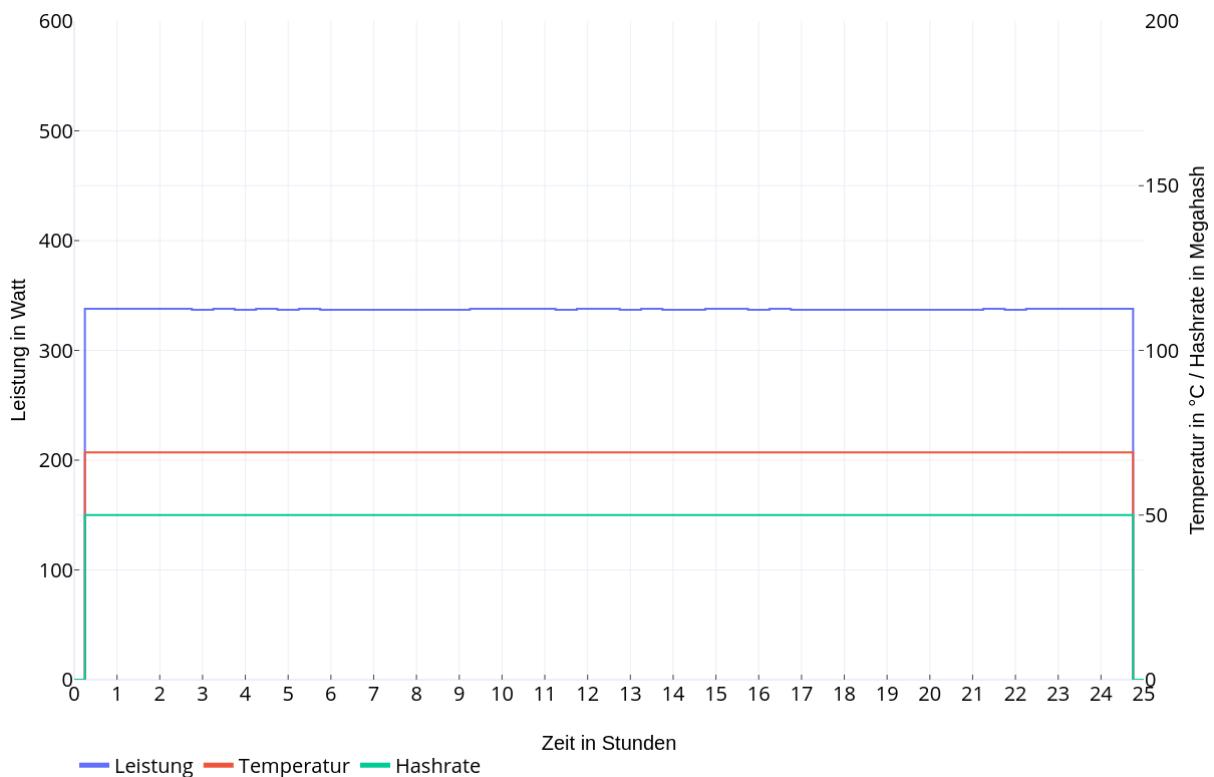


Abbildung 6.13: Aufbau 04

6.6.5 Szenario 5

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 47 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 63,51 MH/s
- Ø max. Temperatur: 57,86 °C
- Ø Leistung aller GPUs: 350 W
- Ø Leistung System: 379 W
- benötigte Energie: 9,10 kWh ~ 2,37 €
- Bitcoin: 0,000066 BTC ~ 2,90 €
- Bilanz: Gewinn 0,53 €

Die Abbildung 6.14 veranschaulicht dieses Ergebnis.



Abbildung 6.14: Aufbau 05

6.6.6 Szenario 6

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 41 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggert und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 60,22 MH/s
- Ø max. Temperatur: 66,16 °C
- Ø Leistung aller GPUs: 330 W
- Ø Leistung System: 375 W
- benötigte Energie: 9,00 kWh ~ 2,34 €
- Bitcoin: 0,000063 BTC ~ 2,77 €
- Bilanz: Gewinn 0,43 €

Die Abbildung 6.15 veranschaulicht dieses Ergebnis.

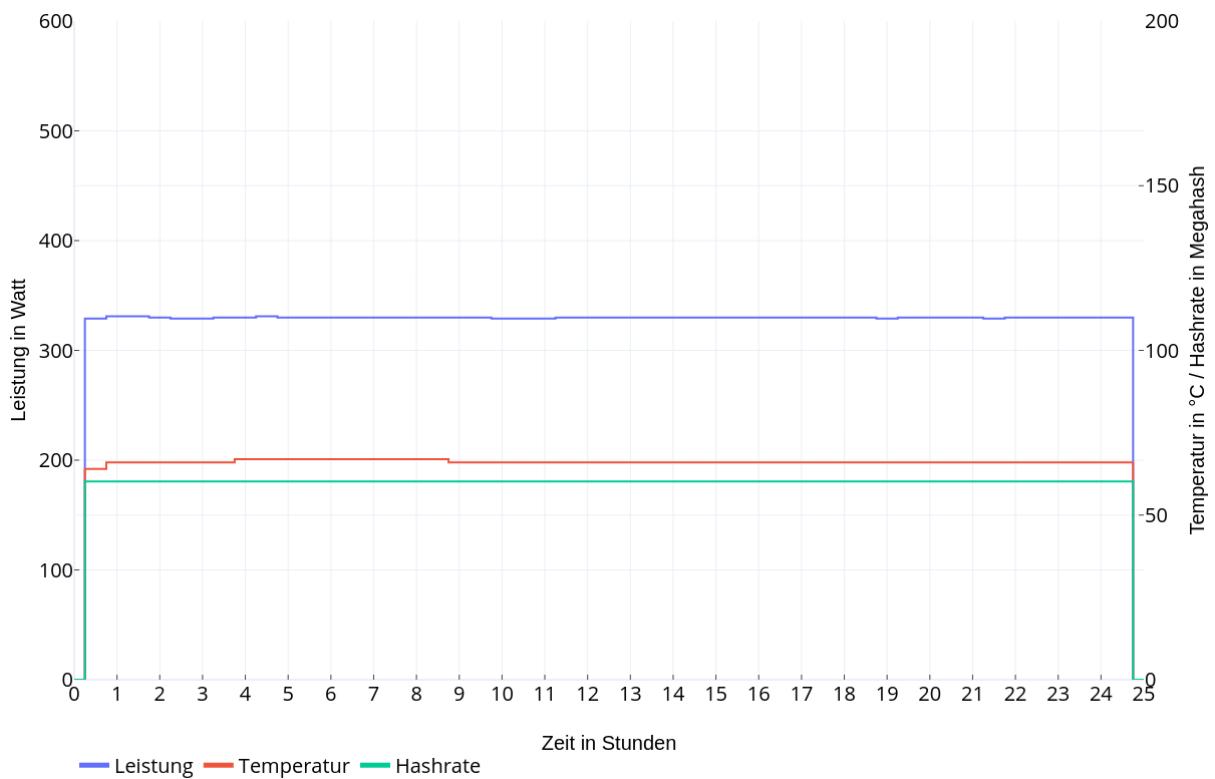


Abbildung 6.15: Aufbau 06

6.6.7 Szenario 7

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 55 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 86,85 MH/s
- Ø max. Temperatur: 68,47 °C
- Ø Leistung aller GPUs: 512 W
- Ø Leistung System: 553 W
- benötigte Energie: 13,27 kWh ~ 3,45 €
- Bitcoin: 0,000090 BTC ~ 3,96 €
- Bilanz: Gewinn 0,51 €

Die Abbildung 6.16 veranschaulicht dieses Ergebnis.

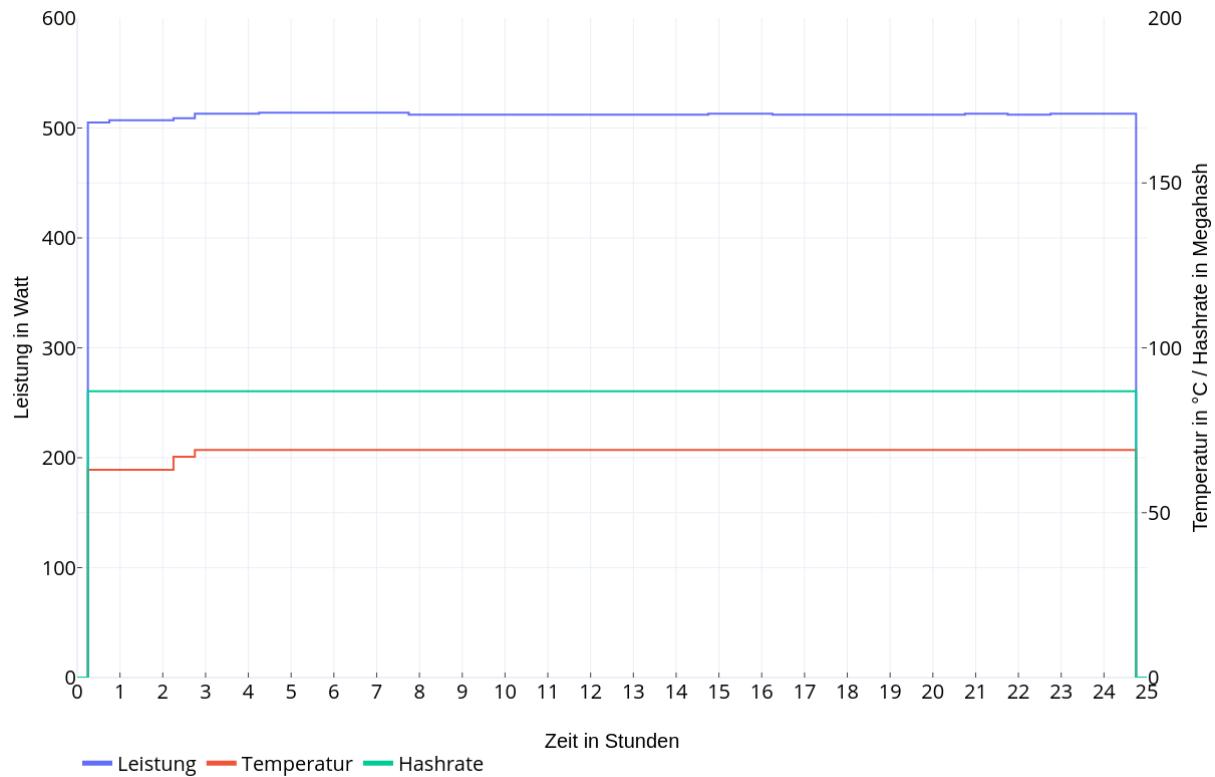


Abbildung 6.16: Aufbau 07

6.6.8 Szenario 8

Aufbau:

In diesem Test-Szenario wird ausschließlich die Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 31 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 27,70 MH/s
- Ø max. Temperatur: 56,94 °C
- Ø Leistung aller GPUs: 185 W
- Ø Leistung System: 205 W
- benötigte Energie: 4,92 kWh ~ 1,28 €
- Bitcoin: 0,000029 BTC ~ 1,28 €
- Bilanz: Gewinn 0,00 €

Die Abbildung 6.17 veranschaulicht dieses Ergebnis.

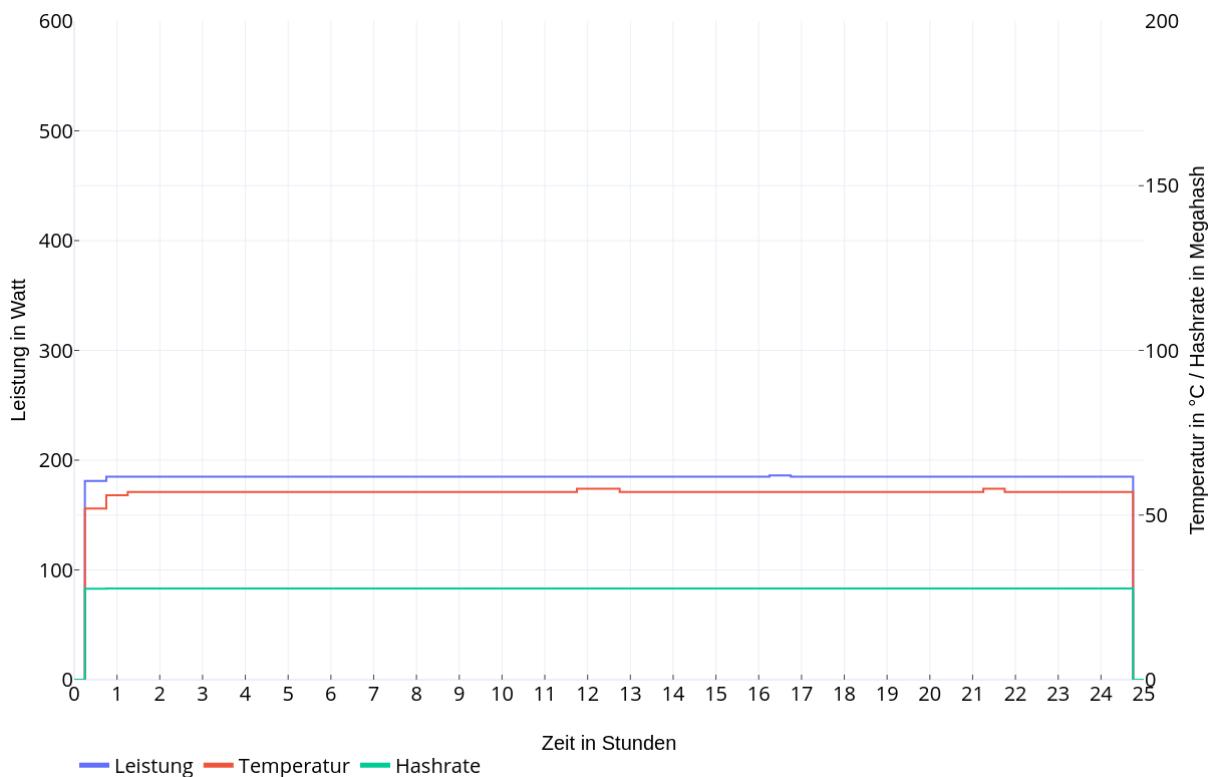


Abbildung 6.17: Aufbau 08

6.6.9 Szenario 9

Aufbau:

In diesem Test-Szenario wird ausschließlich die Power Color Radeon RX580 8 GB Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 30 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 24,62 MH/s
- Ø max. Temperatur: 68,57 °C
- Ø Leistung aller GPUs: 164 W
- Ø Leistung System: 208 W
- benötigte Energie: 4,99 kWh ~ 1,30 €
- Bitcoin: 0,000026 BTC ~ 1,14 €
- Bilanz: Verlust 0,16 €

Die Abbildung 6.18 veranschaulicht dieses Ergebnis.

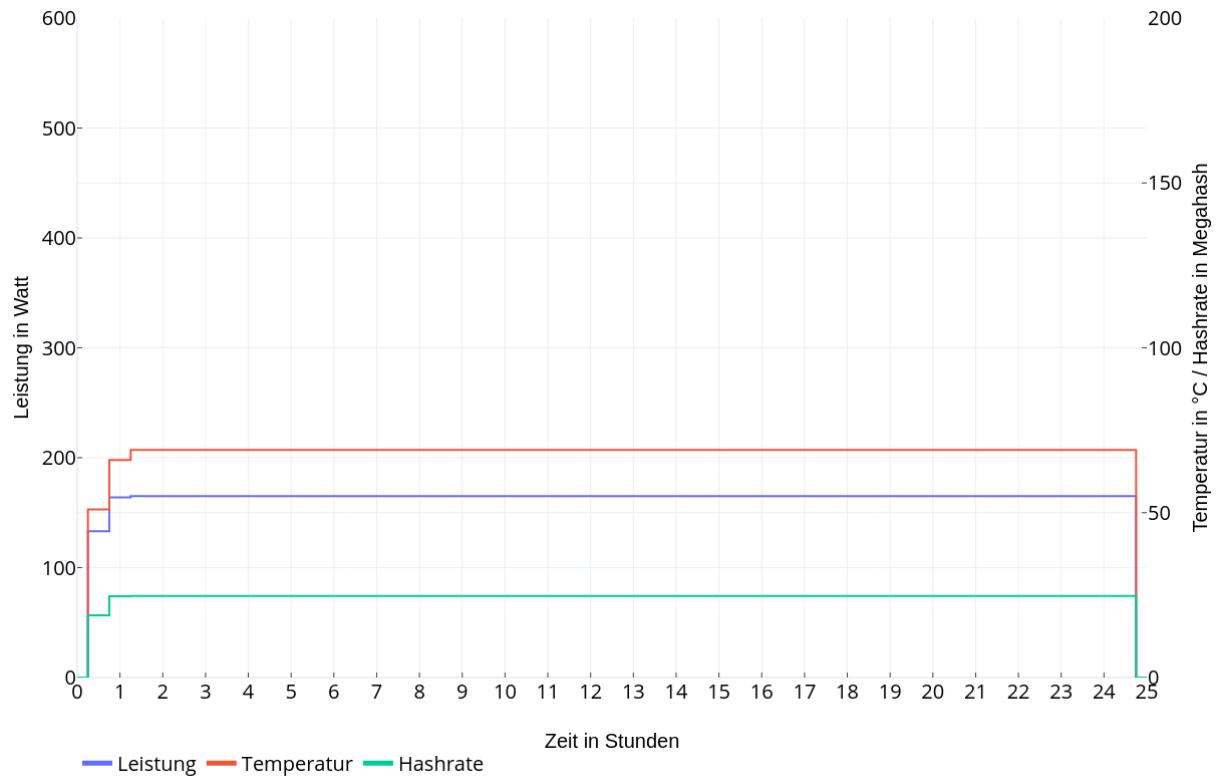


Abbildung 6.18: Aufbau 09

6.6.10 Szenario 10

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 38 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 37,17 MH/s
- Ø max. Temperatur: 60,41 °C
- Ø Leistung aller GPUs: 175 W
- Ø Leistung System: 207 W
- benötigte Energie: 4,97 kWh ~ 1,29 €
- Bitcoin: 0,000039 BTC ~ 1,72 €
- Bilanz: Gewinn 0,43 €

Die Abbildung 6.19 veranschaulicht dieses Ergebnis.

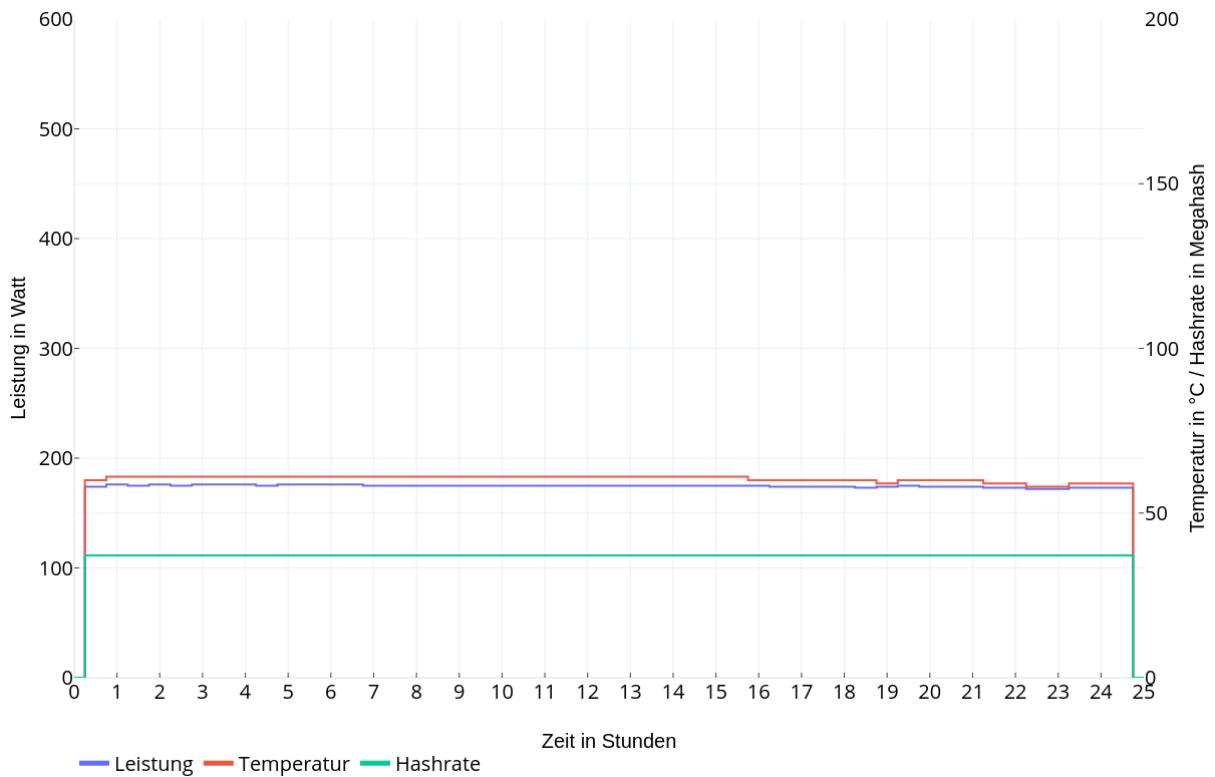


Abbildung 6.19: Aufbau 10

6.6.11 Szenario 11

Aufbau:

In diesem Test-Szenario wird die Power Color Radeon RX580 8 GB Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 45 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 52,40 MH/s
- Ø max. Temperatur: 68,84 °C
- Ø Leistung aller GPUs: 349 W
- Ø Leistung System: 386 W
- benötigte Energie: 9,26 kWh ~ 2,41 €
- Bitcoin: 0,000054 BTC ~ 2,38 €
- Bilanz: Verlust **0,03 €**

Die Abbildung 6.20 veranschaulicht dieses Ergebnis.

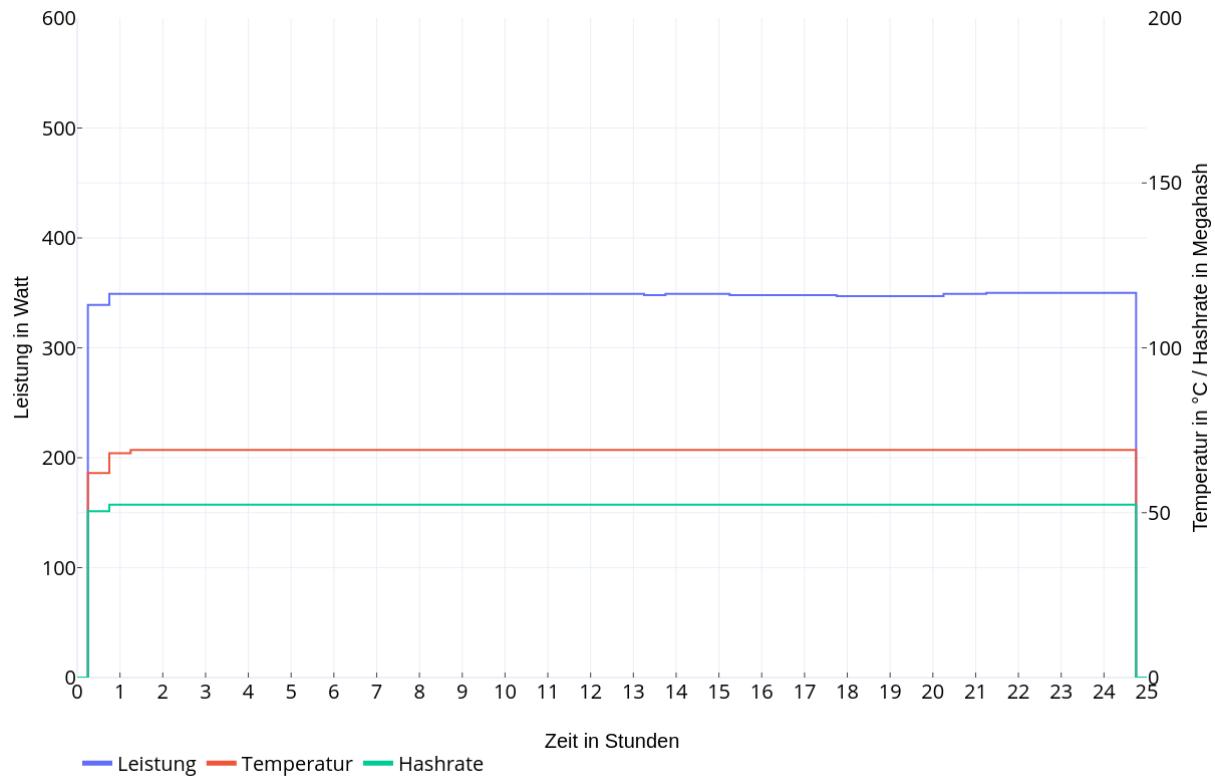


Abbildung 6.20: Aufbau 11

6.6.12 Szenario 12

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 47 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 64,87 MH/s
- Ø max. Temperatur: 58,65 °C
- Ø Leistung aller GPUs: 357 W
- Ø Leistung System: 385 W
- benötigte Energie: 9,24 kWh ~ 2,40 €
- Bitcoin: 0,000067 BTC ~ 2,95 €
- Bilanz: Gewinn 0,55 €

Die Abbildung 6.21 veranschaulicht dieses Ergebnis.

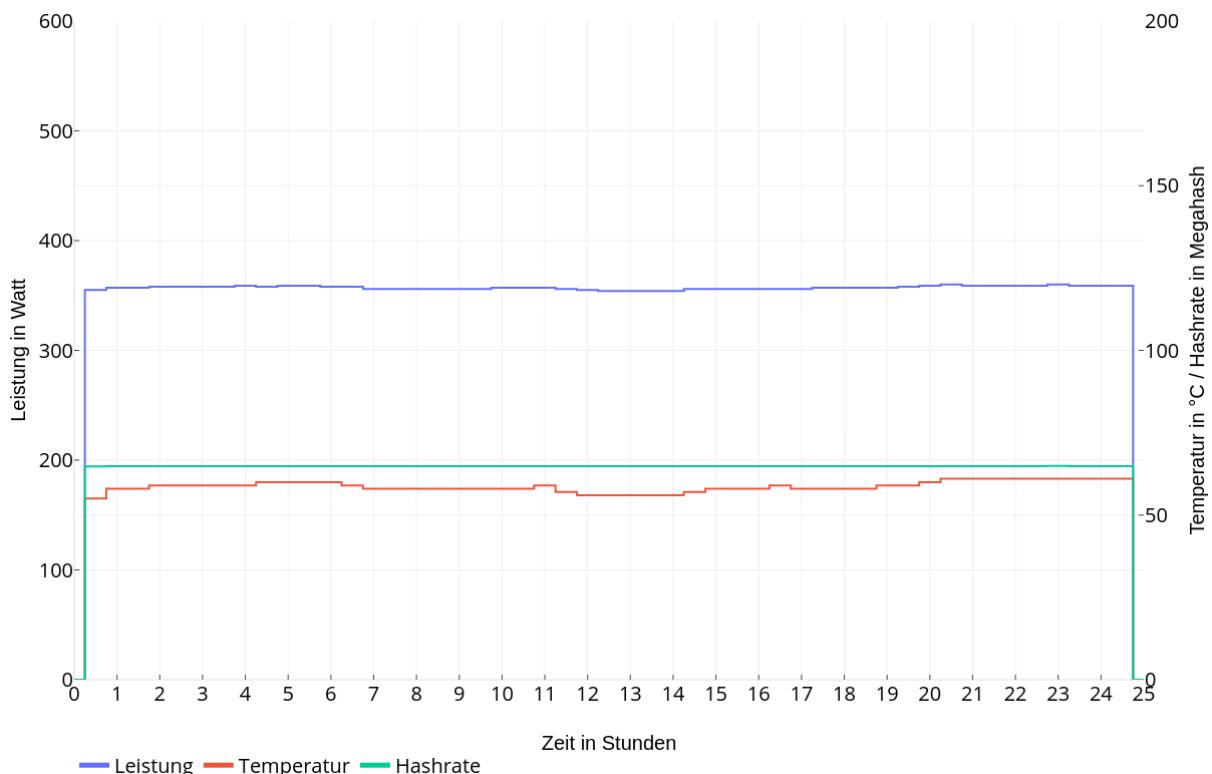


Abbildung 6.21: Aufbau 12

6.6.13 Szenario 13

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 41 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 61,83 MH/s
- Ø max. Temperatur: 68,73 °C
- Ø Leistung aller GPUs: 340 W
- Ø Leistung System: 380 W
- benötigte Energie: 9,12 kWh ~ 2,37 €
- Bitcoin: 0,000064 BTC ~ 2,82 €
- Bilanz: Gewinn 0,45 €

Die Abbildung 6.22 veranschaulicht dieses Ergebnis.

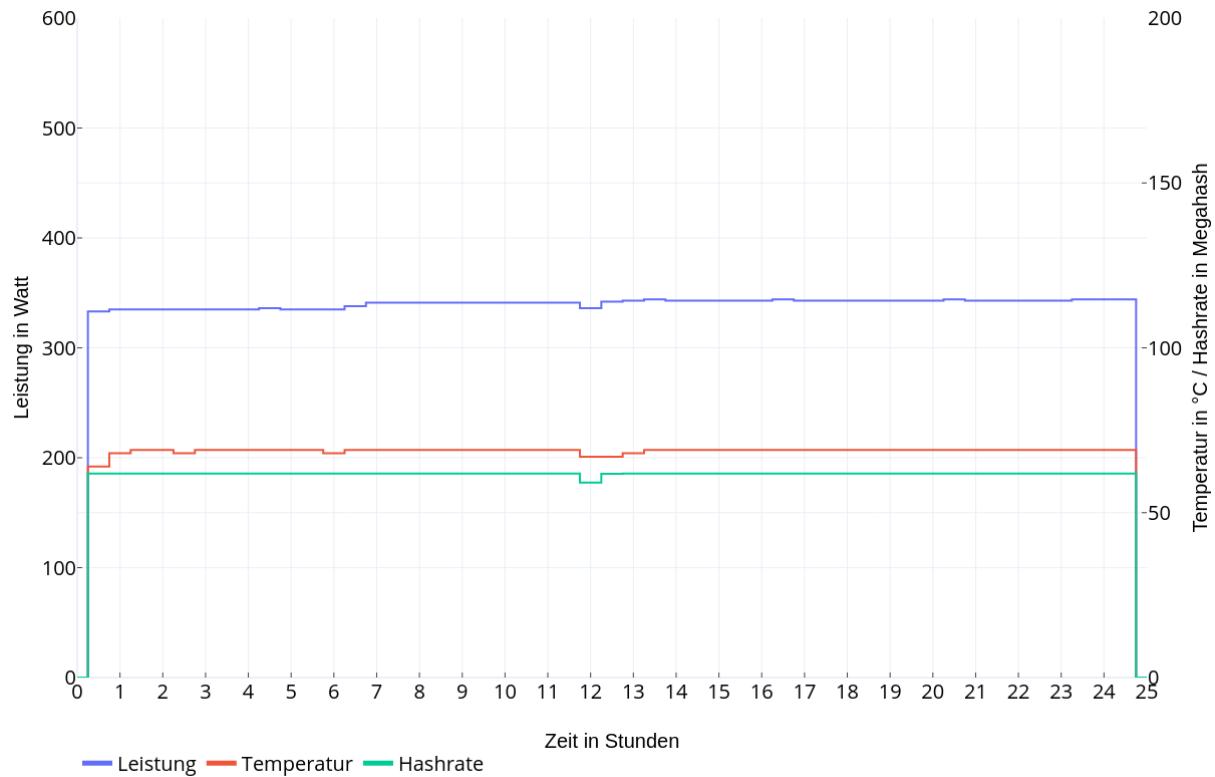


Abbildung 6.22: Aufbau 13

6.6.14 Szenario 14

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 55 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 89,48 MH/s
- Ø max. Temperatur: 68,84 °C
- Ø Leistung aller GPUs: 520 W
- Ø Leistung System: 564 W
- benötigte Energie: 13,54 kWh ~ 3,52 €
- Bitcoin: 0,000093 BTC ~ 4,09 €
- Bilanz: Gewinn **0,57 €**

Die Abbildung 6.23 veranschaulicht dieses Ergebnis.

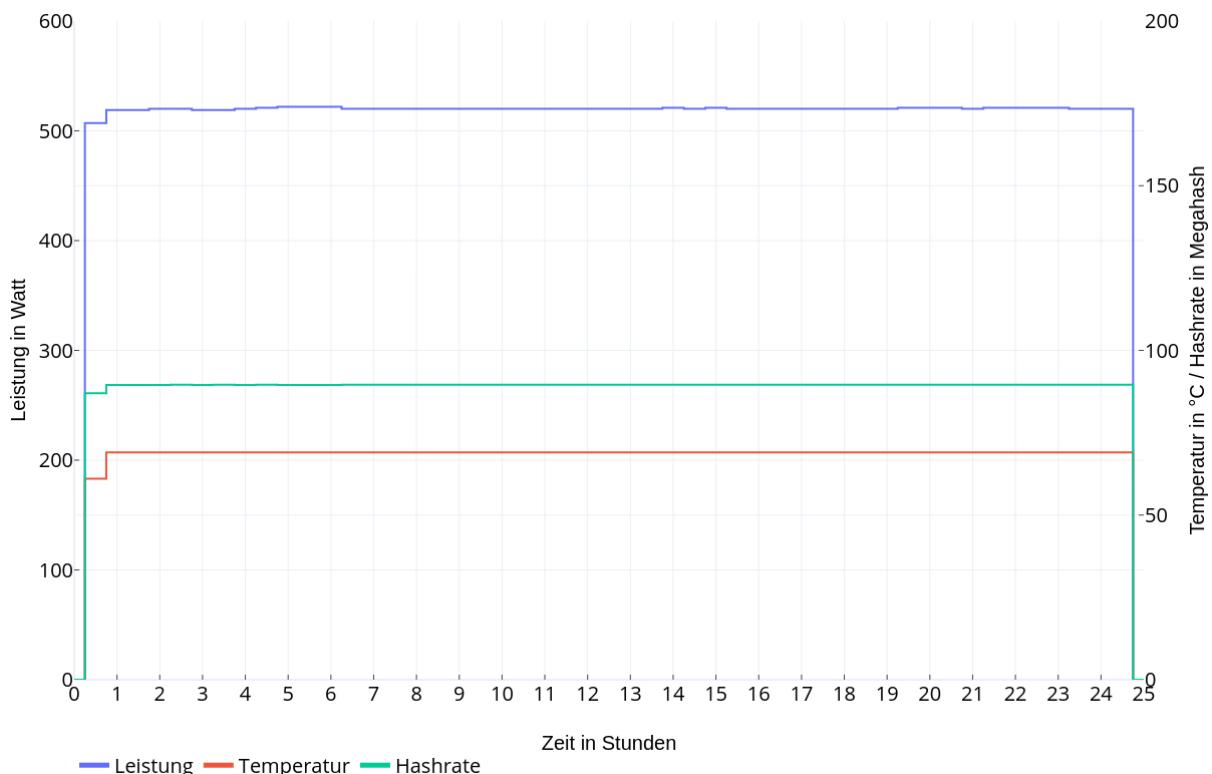


Abbildung 6.23: Aufbau 14

6.6.15 Zwischenfazit und Vorauswahl

Die durchgeföhrten Windows-Szenarien erlauben das Ziehen eines Zwischenfazits. Dadurch soll eine Vorauswahl getroffen werden, um die Testszenarien im weiteren Verlauf einzuschränken. Die folgende Tabelle 6.1 zeigt alle Testszenarien, geordnet nach dem Gewinn absteigend:

Szenario	Hashrate	BTC	Umsatz	Verlust	Gewinn
Szenario 14	89,48 MH/s	0,000093	4,09 €	3,52 €	0,57 €
Szenario 12	64,87 MH/s	0,000067	2,95 €	2,40 €	0,55 €
Szenario 5	63,51 MH/s	0,000066	2,90 €	2,37 €	0,53 €
Szenario 7	86,85 MH/s	0,000090	3,96 €	3,45 €	0,51 €
Szenario 13	61,83 MH/s	0,000064	2,82 €	2,37 €	0,45 €
Szenario 6	60,22 MH/s	0,000063	2,77 €	2,34 €	0,43 €
Szenario 10	37,17 MH/s	0,000039	1,72 €	1,29 €	0,43 €
Szenario 3	36,87 MH/s	0,000038	1,67 €	1,28 €	0,39 €
Szenario 8	27,70 MH/s	0,000029	1,28 €	1,28 €	0,00 €
Szenario 4	49,99 MH/s	0,000052	2,29 €	2,31 €	-0,02 €
Szenario 1	26,65 MH/s	0,000028	1,23 €	1,25 €	-0,02 €
Szenario 11	52,40 MH/s	0,000054	2,38 €	2,41 €	-0,03 €
Szenario 9	24,62 MH/s	0,000026	1,14 €	1,30 €	-0,16 €
Szenario 2	22,91 MH/s	0,000024	1,06 €	1,23 €	-0,17 €

Tabelle 6.1: Auswertung Windows Test-Szenarien

Die Tabelle veranschaulicht die bislang effektivsten Testszenarien. Mit den drei Grafikkarten und den zwei verwendeten Minern haben sich 14 Möglichkeiten ergeben. Da die Szenarien sehr zeitaufwendig sind, werden im weiteren Verlauf nur die drei gewinnbringendsten Kartenkombinationen weiter betrachtet. Das sind Szenario 7/14 mit allen drei Grafikkarten, Szenario 5/12 mit der Zotac 2070 Super und der Asus RX590, Szenario 3/10 mit der Zotac 2070 Super alleine. Sofern möglich werden auch weiterhin der lolMiner sowie der PhoenixMiner eingesetzt. Die Szenarien 6/13 werden nicht weiter berücksichtigt, da die Kombination aus zwei Grafikkarten aus den Szenarien 5/12 bessere Werte liefert.

6.7 Linux Szenarien

Die Test-Szenarien 15 bis 19 werden mit dem Betriebssystem Linux Ubuntu 20.04 LTS Server durchgeführt. Eingesetzte Mining-Softwares: Awesome Miner mit den Mineren *lolMiner* und *PhoenixMiner*.

6.7.1 Szenario 15

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 36 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgelogggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24h
- Ø Hashrate: 36,93 MH/s
- Ø max. Temperatur: 60,51 °C
- Ø Leistung aller GPUs: 174 W
- Ø Leistung System: 206 W
- benötigte Energie: 4,94 kWh ~ 1,28 €
- Bitcoin: 0,000038 BTC ~ 1,67 €
- Bilanz: Gewinn **0,39 €**

Die Abbildung 6.24 veranschaulicht dieses Ergebnis.

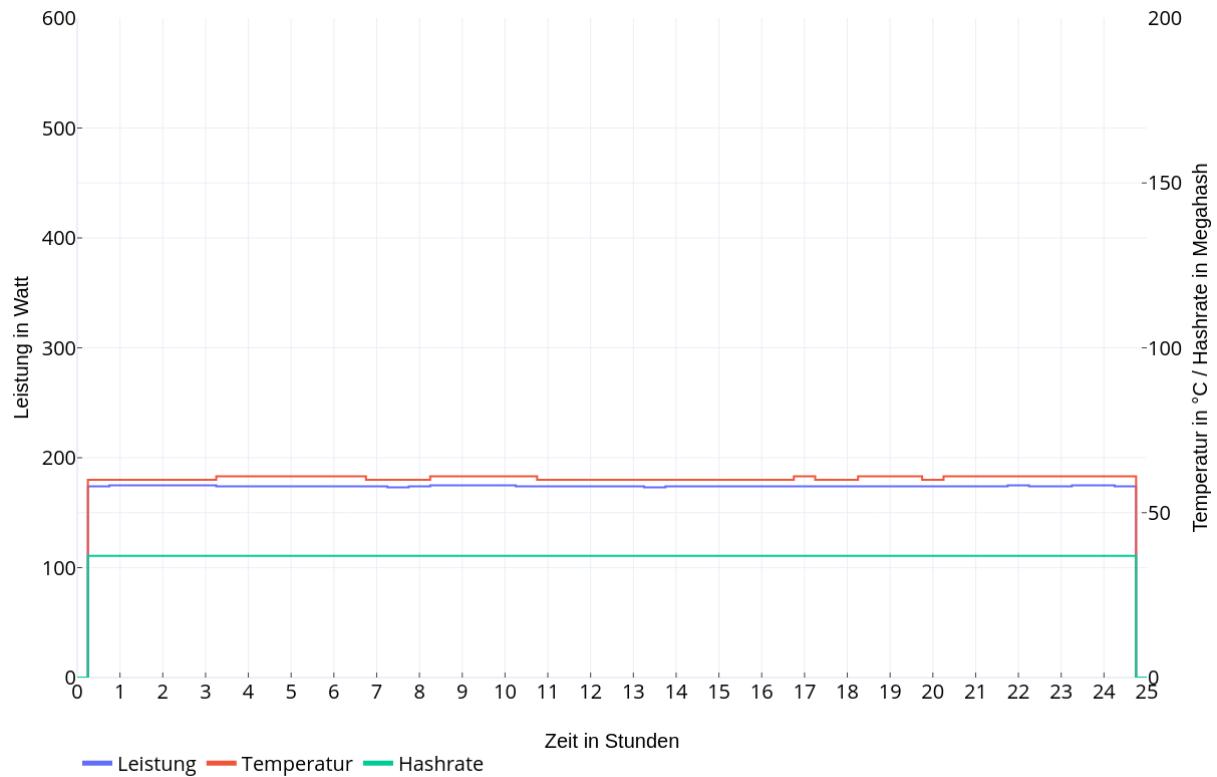


Abbildung 6.24: Aufbau 15

6.7.2 Szenario 16

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 50 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggert und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 63,65 MH/s
- Ø max. Temperatur: 60,78 °C
- Ø Leistung aller GPUs: 361 W
- Ø Leistung System: 388 W
- benötigte Energie: 9,31 kWh ~ 2,42 €
- Bitcoin: 0,000066 BTC ~ 2,90 €
- Bilanz: Gewinn 0,48 €

Die Abbildung 6.25 veranschaulicht dieses Ergebnis.

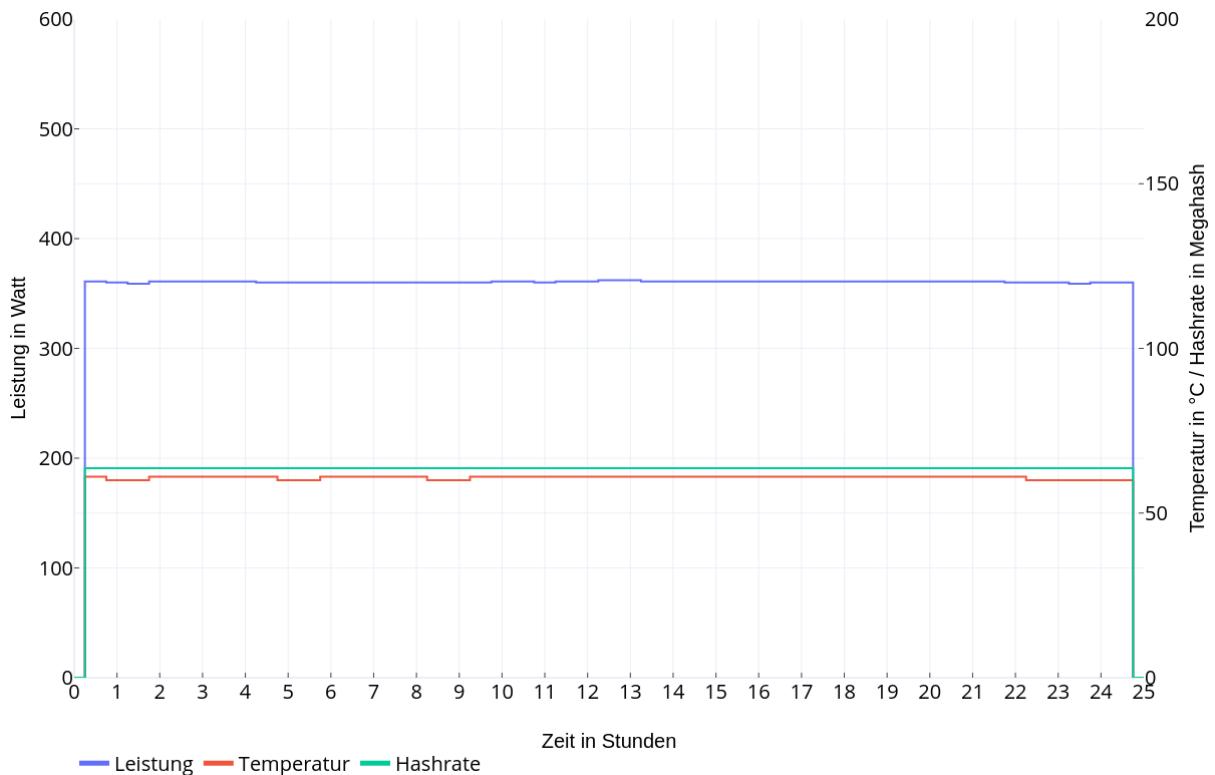


Abbildung 6.25: Aufbau 16

6.7.3 Szenario 17

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 69 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 87,07 MH/s
- Ø max. Temperatur: 68,96 °C
- Ø Leistung aller GPUs: 527 W
- Ø Leistung System: 577 W
- benötigte Energie: 13,85 kWh ~ 3,60 €
- Bitcoin: 0,000090 BTC ~ 3,96 €
- Bilanz: Gewinn 0,36 €

Die Abbildung 6.26 veranschaulicht dieses Ergebnis.

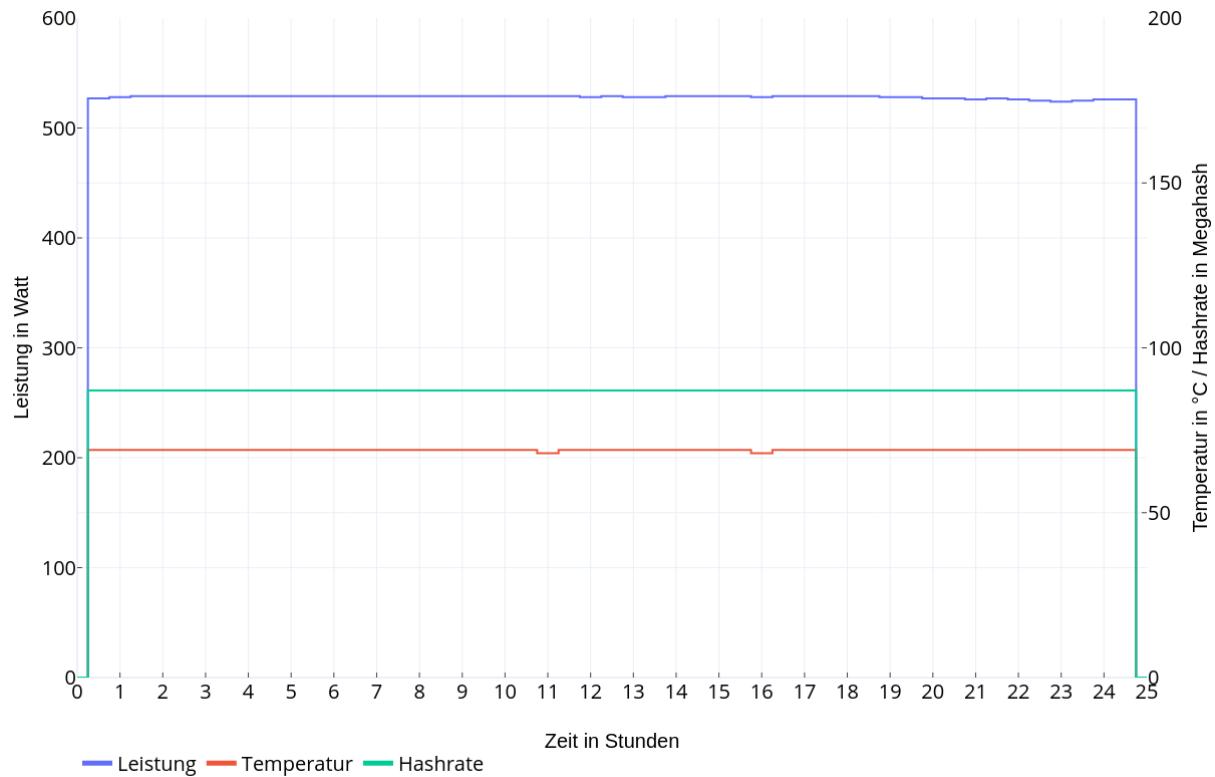


Abbildung 6.26: Aufbau 17

6.7.4 Szenario 18

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 37 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 37,15 MH/s
- Ø max. Temperatur: 60,41 °C
- Ø Leistung aller GPUs: 175 W
- Ø Leistung System: 207 W
- benötigte Energie: 4,97 kWh ~ 1,29 €
- Bitcoin: 0,000039 BTC ~ 1,72 €
- Bilanz: Gewinn **0,43 €**

Die Abbildung 6.27 veranschaulicht dieses Ergebnis.

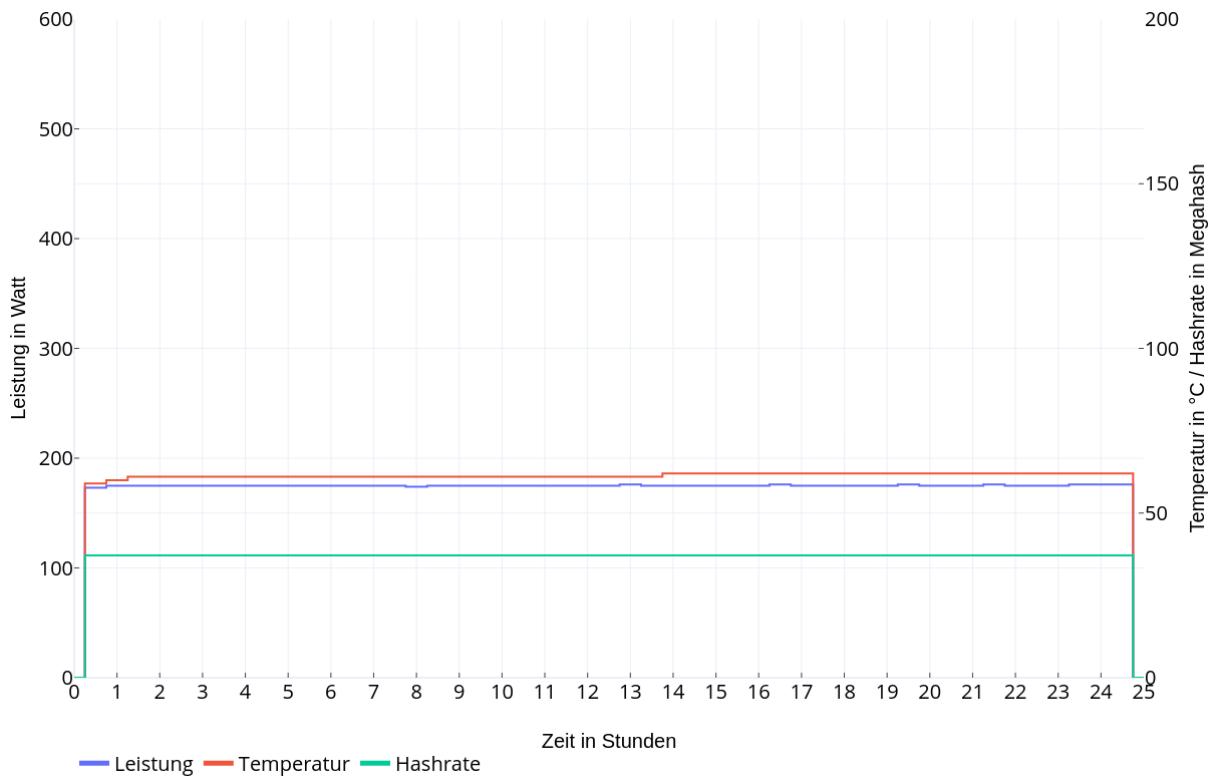


Abbildung 6.27: Aufbau 18

6.7.5 Szenario 19

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 50 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 65,19 MH/s
- Ø max. Temperatur: 61,35 °C
- Ø Leistung aller GPUs: 362 W
- Ø Leistung System: 389 W
- benötigte Energie: 9,34 kWh ~ 2,43 €
- Bitcoin: 0,000068 BTC ~ 2,99 €
- Bilanz: Gewinn 0,56 €

Die Abbildung 6.28 veranschaulicht dieses Ergebnis.

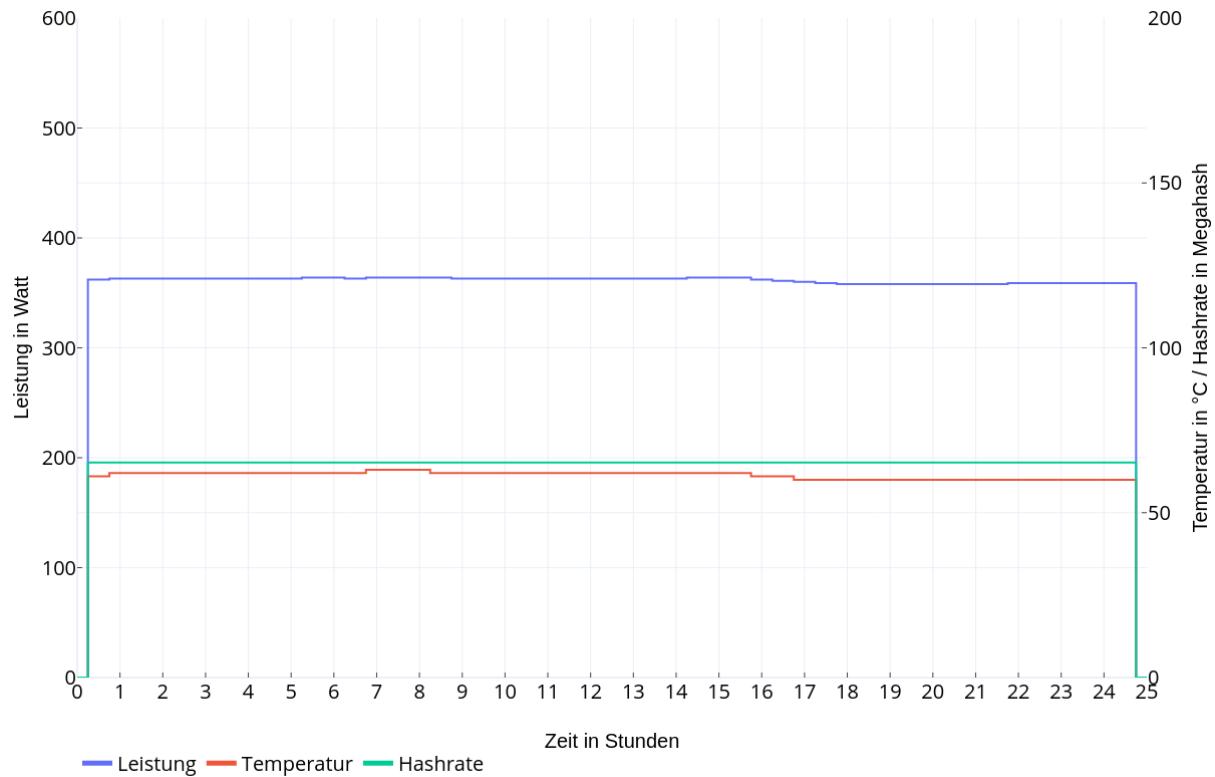


Abbildung 6.28: Aufbau 19

6.7.6 Szenario 20

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 70 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 90,11 MH/s
- Ø max. Temperatur: 69,00 °C
- Ø Leistung aller GPUs: 530 W
- Ø Leistung System: 575 W
- benötigte Energie: 13,80 kWh ~ 3,59 €
- Bitcoin: 0,000094 BTC ~ 4,14 €
- Bilanz: Gewinn 0,55 €

Die Abbildung 6.29 veranschaulicht dieses Ergebnis.

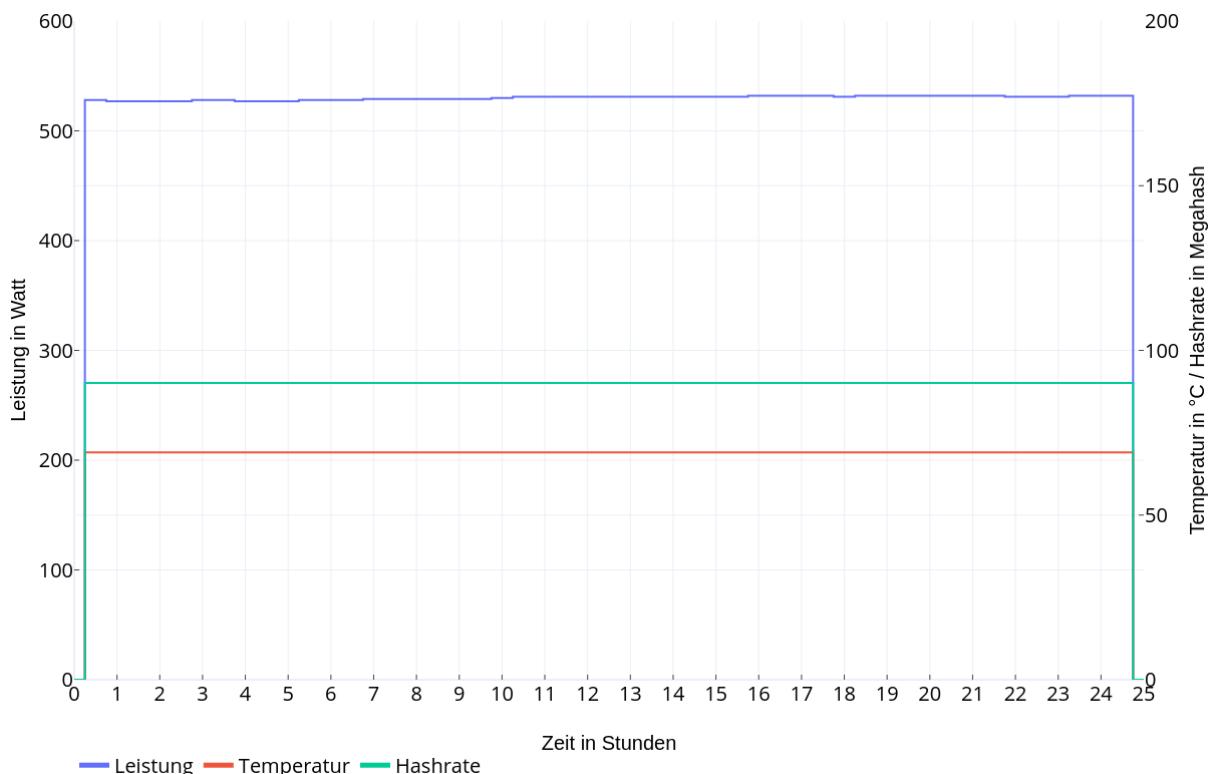


Abbildung 6.29: Aufbau 20

6.8 Mining-OS Szenarien

Die Test-Szenarien 21 bis 26 werden mit dem Live-Mining-Betriebssystem HiveOS durchgeführt. Eingesetzte Miner sind lolMiner und PhoenixMiner.

6.8.1 Szenario 21

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 38 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeologt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 36,93 MH/s
- Ø max. Temperatur: 60,71 °C
- Ø Leistung aller GPUs: 174 W
- Ø Leistung System: 208 W
- benötigte Energie: 4,99 kWh ~ 1,30 €
- Bitcoin: 0,000038 BTC ~ 1,67 €
- Bilanz: Gewinn 0,37 €

Die Abbildung 6.30 veranschaulicht dieses Ergebnis.

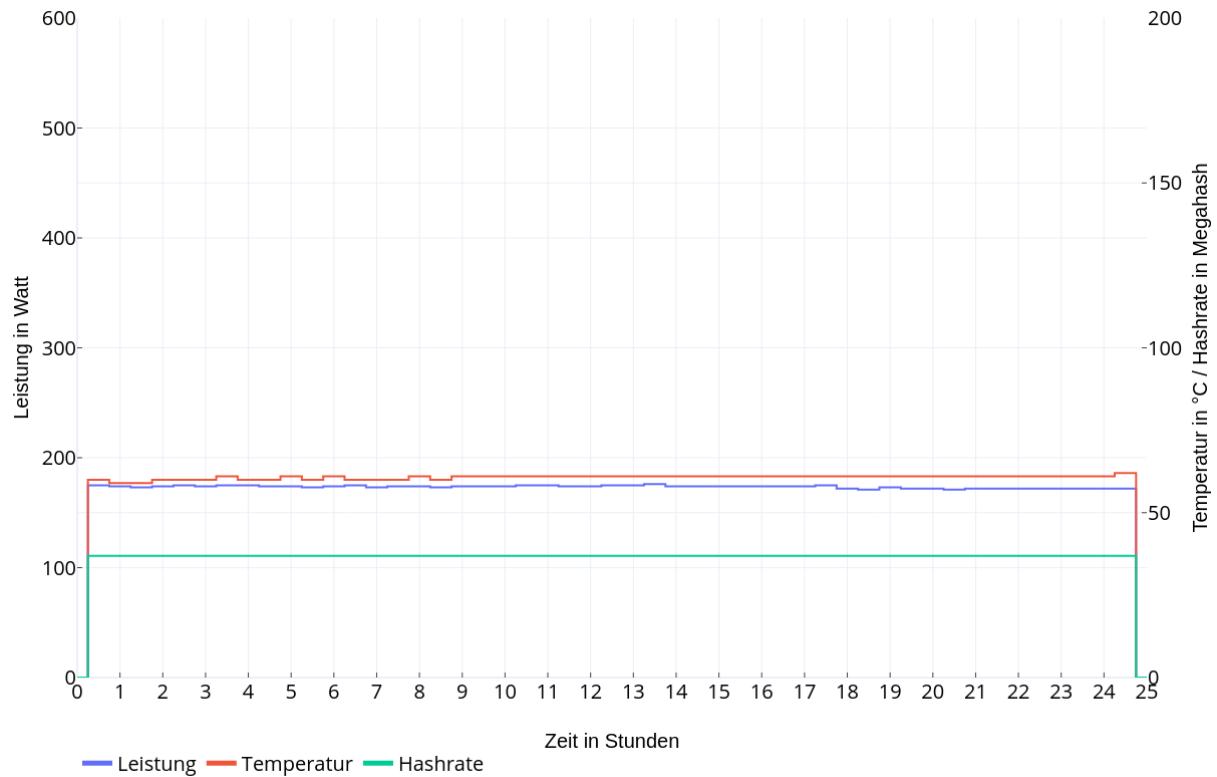


Abbildung 6.30: Aufbau 21

6.8.2 Szenario 22

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 53 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggert und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 63,67 MH/s
- Ø max. Temperatur: 68,47 °C
- Ø Leistung aller GPUs: 363 W
- Ø Leistung System: 395 W
- benötigte Energie: 9,48 kWh ~ 2,46 €
- Bitcoin: 0,000066 BTC ~ 2,90 €
- Bilanz: Gewinn 0,44 €

Die Abbildung 6.31 veranschaulicht dieses Ergebnis.

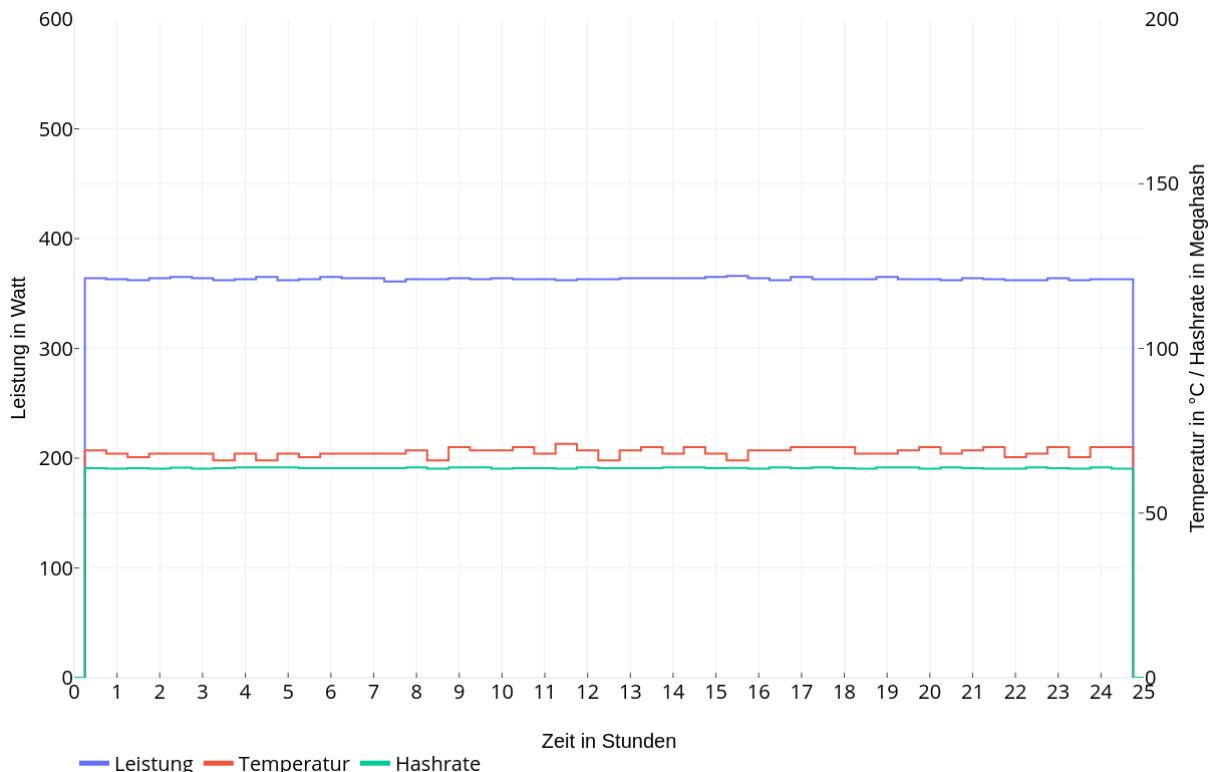


Abbildung 6.31: Aufbau 22

6.8.3 Szenario 23

Hardware-Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 73 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

• Dauer:	24 h		
• Ø Hashrate:	87,10 MH/s		
• Ø max. Temperatur:	68,31 °C		
• Ø Leistung aller GPUs:	527 W		
• Ø Leistung System:	583W		
• benötigte Energie:	13,99 kWh	~	3,64 €
• Bitcoin:	0,000090 BTC	~	3,96 €
• Bilanz:	Gewinn		0,32 €

Die Abbildung 6.32 veranschaulicht dieses Ergebnis.

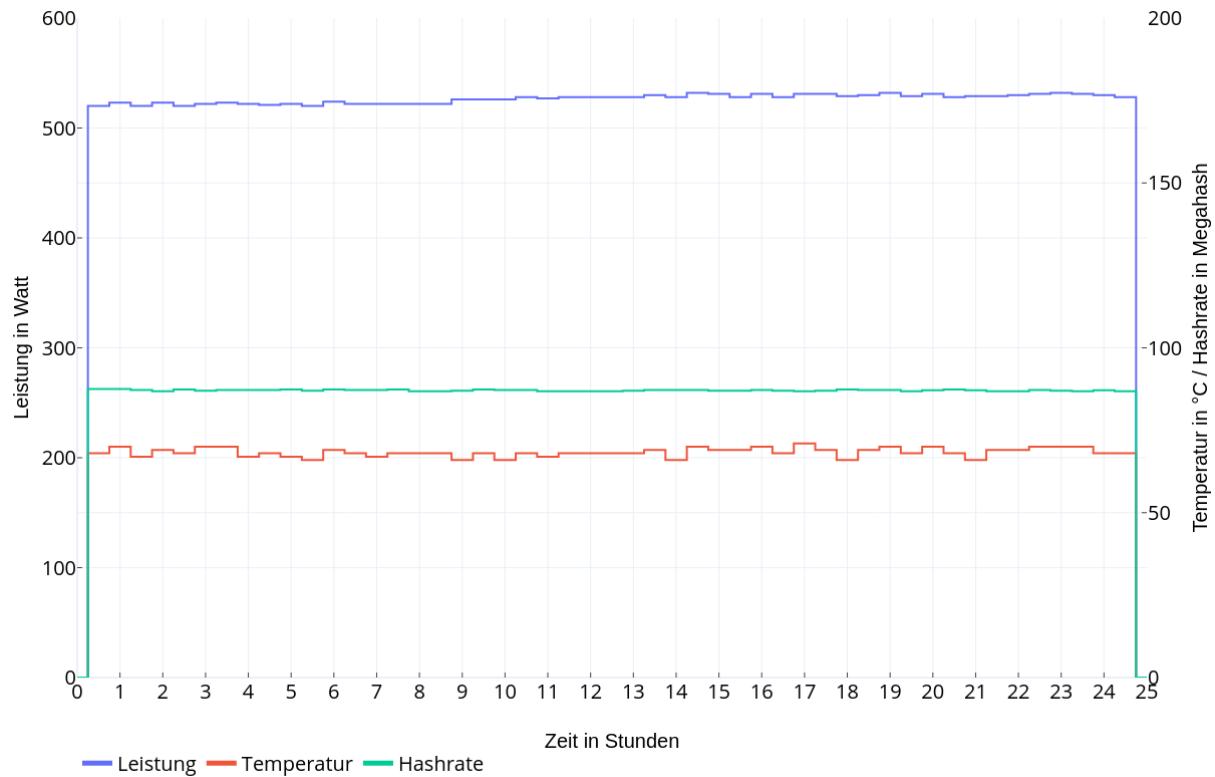


Abbildung 6.32: Aufbau 23

6.8.4 Szenario 24

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 38 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 37,15 MH/s
- Ø max. Temperatur: 63,47 °C
- Ø Leistung aller GPUs: 175 W
- Ø Leistung System: 209 W
- benötigte Energie: 5,02 kWh ~ 1,31 €
- Bitcoin: 0,000039 BTC ~ 1,72 €
- Bilanz: Gewinn **0,41 €**

Die Abbildung 6.33 veranschaulicht dieses Ergebnis.

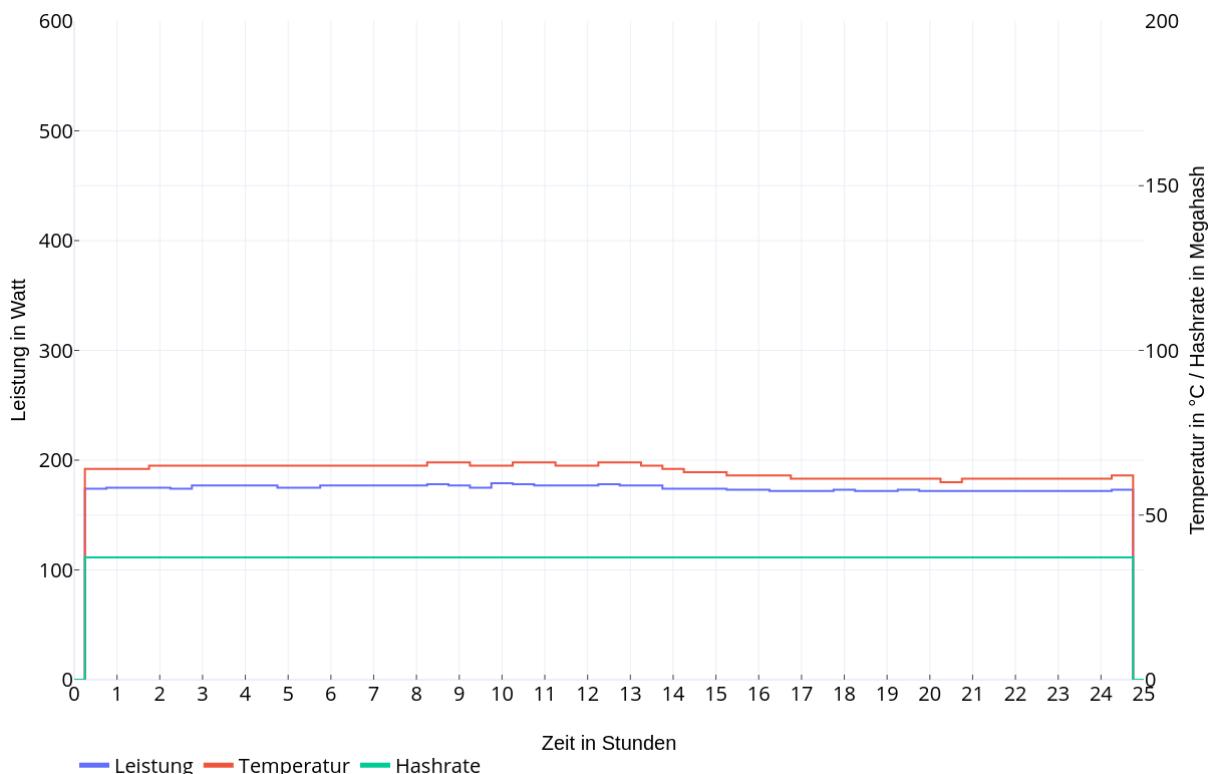


Abbildung 6.33: Aufbau 24

6.8.5 Szenario 25

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 54 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 65,19 MH/s
- Ø max. Temperatur: 68,98 °C
- Ø Leistung aller GPUs: 364 W
- Ø Leistung System: 396 W
- benötigte Energie: 9,50 kWh ~ 2,47 €
- Bitcoin: 0,000068 BTC ~ 2,99 €
- Bilanz: Gewinn 0,52 €

Die Abbildung 6.34 veranschaulicht dieses Ergebnis.

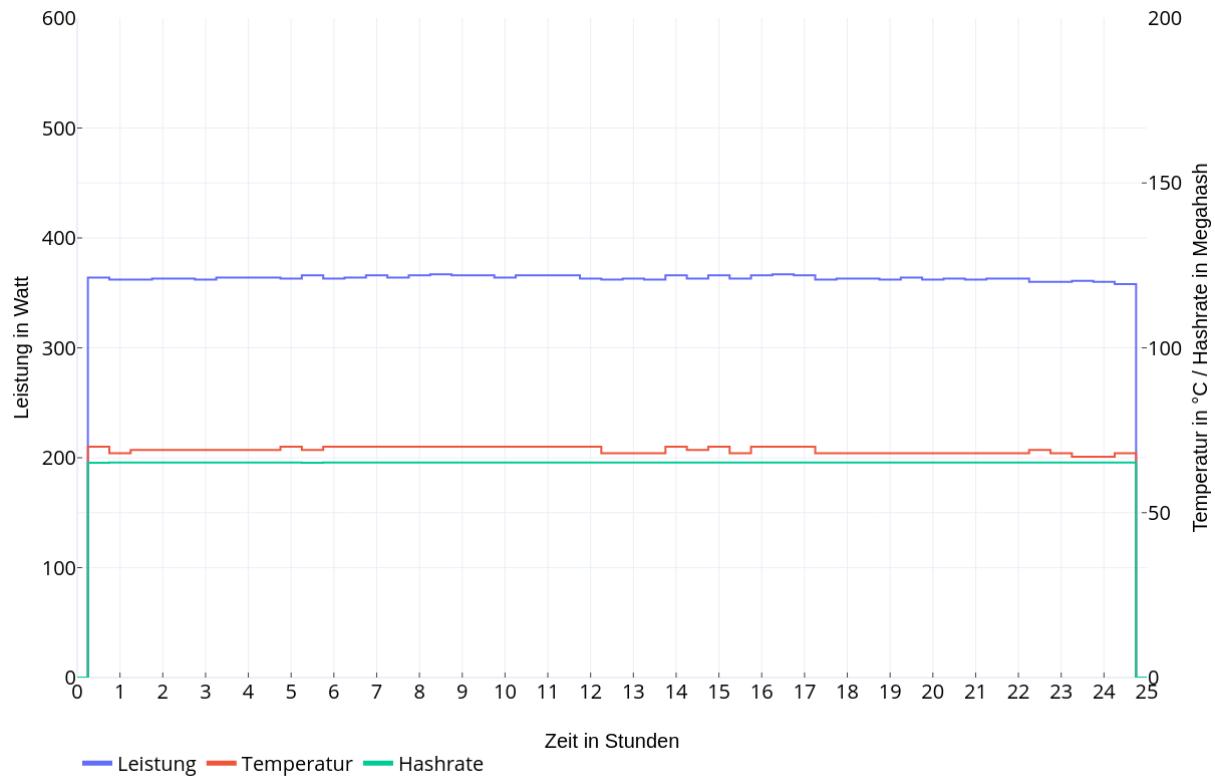


Abbildung 6.34: Aufbau 25

6.8.6 Szenario 26

Hardware-Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 75 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 90,11 MH/s
- Ø max. Temperatur: 69,69 °C
- Ø Leistung aller GPUs: 530 W
- Ø Leistung System: 584 W
- benötigte Energie: 14,02 kWh ~ 3,65 €
- Bitcoin: 0,000094 BTC ~ 4,14 €
- Bilanz: Gewinn 0,49 €

Die Abbildung 6.35 veranschaulicht dieses Ergebnis.

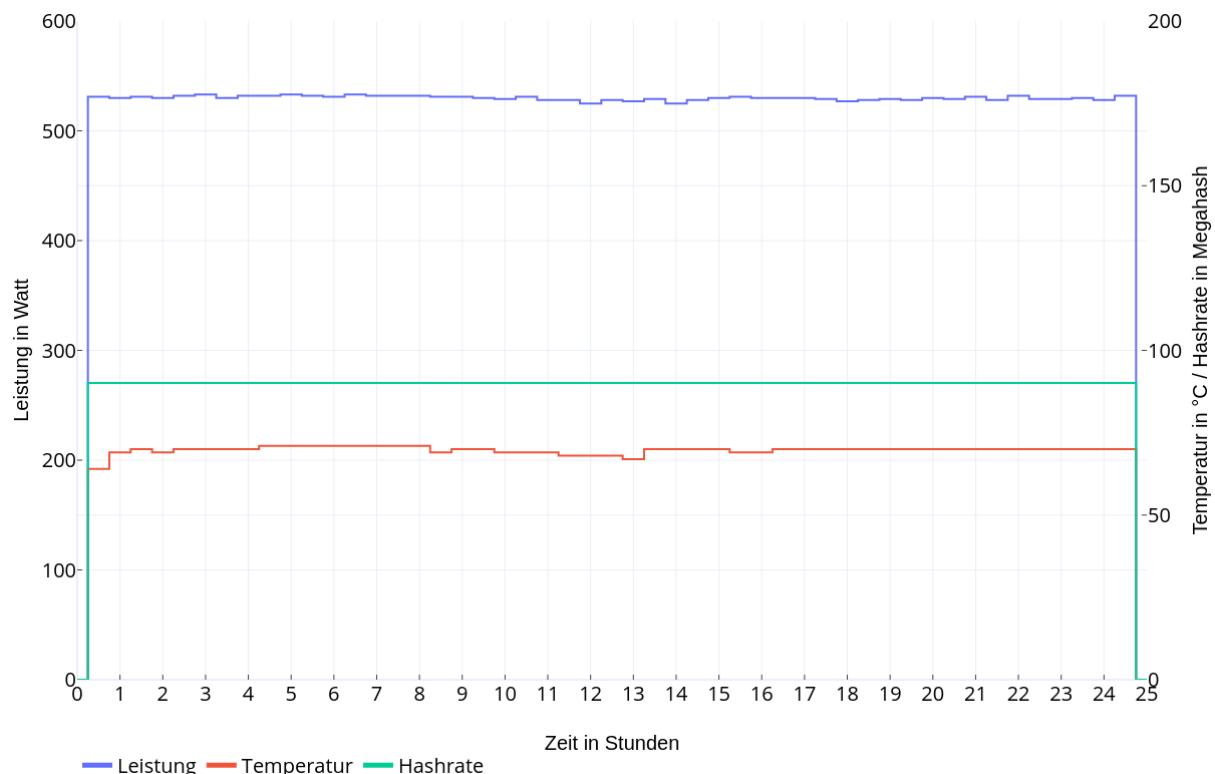


Abbildung 6.35: Aufbau 26

6.9 Leistungssteigerung

In diesem Kapitel werden Möglichkeiten betrachtet, die Leistung der Grafikkarten zu steigern. Leistungssteigerung in Bezug auf Mining bedeutet, eine höhere Hashrate bei gleichem oder geringerem Stromverbrauch zu erzielen. Hierzu bestehen zwei Möglichkeiten. Eine Möglichkeit ist, mithilfe von Übertaktung der Grafikkarte mit entsprechenden Parametern die Hashrate zu erhöhen, wobei gleich oder weniger Strom verbraucht wird. Eine weitere Möglichkeit ist die Modifikation des Basic Input/Output System (BIOS) der Grafikkarten. Hersteller von Grafikkarten limitieren die Möglichkeiten für Nutzer, Leistungsparameter zu verändern. Mithilfe von Modifikationen im BIOS der Grafikkarten lassen sich diese Limitierungen teilweise aufheben und damit die Übertaktung umfangreicher durchführen.

6.9.1 Leistungssteigerung durch Übertaktung

Für das Übertakten von Grafikkarten sind Anpassungen verschiedener Parameter notwendig. Diese werden nun kurz erläutert.

Core voltage

Die Core voltage ist die Spannung der Grafikkarten Kerne. Bei einer Übertaktung dieser Kerne muss die Spannung ebenfalls angepasst werden. Jedoch ist zu beachten, dass eine Erhöhung der Spannung eine stärkere Wärmeentwicklung zur Folge hat.

Core clock

Der Core clock gibt die Taktfrequenz der Grafikkarten Kerne an. Core clock wird auch als Base clock bezeichnet. Eine Erhöhung führt zu mehr Zyklen pro Sekunde und damit zu einer schnelleren Berechnung. Auch bei der Taktfrequenz führt eine zu große Anpassung zu Instabilitäten des Systems.

Memory clock

Ähnlich wie die Taktfrequenz der Grafikkarten Kerne modifiziert werden kann, lässt sich die Taktrate des Random-Access-Memorys (RAMs) anpassen. Eine Erhöhung des Memory clocks steigert die Zugriffszeiten auf dem RAM.

Memory voltage

Die Memory voltage ist die Spannung des Grafikkarten RAMs. Bei einer Übertaktung des RAMs muss die Spannung ebenfalls angepasst werden. Jedoch ist zu beachten, dass eine Erhöhung der Spannung eine stärkere Wärmeentwicklung zur Folge hat.

Power level

Mithilfe des Power Levels wird die Leistungsaufnahme der gesamten Grafikkarte beschränkt. Wird das Power Level abgesenkt, wird weniger Leistung aufgenommen, jedoch kann dies zur Instabilität des gesamten Systems führen. Eine Erhöhung hingegen führt zu einer höheren Leistungsaufnahme und damit zu einer stärkeren Wärmeentwicklung.

Die Anpassung jedes einzelnen Parameters geht mit der Frage nach der Stabilität des Systems einher. Neben dem Ziel, die Leistung zu erhöhen, spielt die Stabilität des Systems eine zentrale Rolle. Je nach Mining Algorithmus unterscheidet sich, welche Parameter zu erhöhen oder zu verringern sind. Da Ethash ein RAM intensiver Algorithmus ist, sollte bei Ethereum Mining die Geschwindigkeit des RAMs der Grafikkarte erhöht werden. Der Core clock hingegen kann leicht abgesenkt werden. Im Folgenden werden für alle drei Grafikkarten Parameter ermittelt, unter denen die Grafikkarte stabil betrieben werden kann und die Hashrate möglichst hoch ist. Außerdem wird dies unter dem Aspekt der Leistungsaufnahme bewertet. Die Übertaktung wird auf Windows mit der Mining-Software PhoenixMiner durchgeführt. Zum einen sind gängige Übertaktungstools wie beispielsweise MSI-Afterburner nur auf Windows verfügbar und zum anderen ergibt sich aus den bereits durchgeföhrten Tests, dass mit dem Windows Betriebssystem sowie der PhoenixMiner Software, die bisher besten Mining-Ergebnisse erzielt werden. Zur Übertaktung der Grafikkarten werden folgende Werte verändert: Core clock, Memory clock, und Power level. Core Voltage sowie Memory Voltage werden nicht modifiziert. Sie werden in Abhängigkeit der Taktfrequenzen von der Übertaktungssoftware automatisch

angepasst. Als Übertaktungssoftware für Grafikkarten von AMD wird die *AMD Software: Adrenalin Edition* verwendet.

ASUS RX 580 8 GB OC

Wie bereits erwähnt, wird bei ETH Mining der Ansatz verfolgt, die RAMs Geschwindigkeit möglichst zu maximieren, wohingegen die Taktfrequenz der Kerne leicht abgesenkt werden kann. Im Ausgangszustand ohne jegliche Optimierung oder Übertaktung liefert die Grafikkarte im Durchschnitt 27,70 MH/s bei einer Leistungsaufnahme von 185 Watt (siehe Abschnitt 6.6.8). Daraus ergibt sich eine Effizienz von circa 149730 H/s/W. Mit der Absenkung des Core clocks um 10% sowie eines Memory Clocks von 2250 MHz und einem Power level von -15% ergibt sich eine Hashrate von 31,62 MH/s. Dabei beträgt die Leistung 154 Watt. Eine weitere Erhöhung des Memory Clocks ist mit der verwendeten Software nicht möglich. Aus der gesteigerten Hashrate und der gesenkten notwendigen Leistung ergibt sich eine Effizienz von 205325 H/s/W. Dies entspricht einer Leistungssteigerung von 37,13%, errechnet aus Hash pro Watt vor und nach der Übertaktung. Die Tabelle 6.2 zeigt die Leistungsparameter vor und nach der Übertaktung mit entsprechender Hashrate und Leistung gegenübergestellt. Die erste Zeile der Tabelle stellt dabei den Ausgangszustand dar. In der zweiten Zeile sind die Übertaktungsparameter dargestellt.

Core clock	Memory clock	Power level	Hashrate	Leistung
1224 MHz	2000 MHz	100%	27,70 MH/s	185 W
-10%	2250 MHz	90%	31,62 MH/s	154 W

Tabelle 6.2: ASUS RX 580 Leistungsparameter vor/nach Übertaktung

PowerColor RX 580 8 GB

Da es sich bei dieser Grafikkarte ebenfalls um eine RX 580 handelt, wird der gleiche Ansatz, wie im vorherigen Abschnitt vorgestellt, verfolgt. Im Ausgangszustand, d.h. ohne Optimierung und ohne Übertaktung erreicht die Grafikkarte eine durchschnittliche Hashrate von 24,65 MH/s bei einer Leistungsaufnahme von 164 Watt (siehe Abschnitt 6.6.9). Daraus ergibt sich eine Effizienz von 150122 H/s/W. Der Core clock wird um 8% abgesenkt. Memory clock und Power level entsprechen den Werten der ASUS RX 580 Grafikkarte. Mit diesen Parametern ergibt sich eine Hashrate von 28,40 MH/s bei einer

Leistung von 154 Watt. Daraus ergibt sich eine Effizienz von 184416 H/s/W. Die entspricht einer Leistungssteigerung von 22,84%. Eine Absenkung des Core clocks von über 8% ist nicht möglich, da dies zu Instabilitäten führt. Tabelle 6.3 zeigt die Leistungsparameter dieser Grafikkarte vor und nach der Übertaktung.

Core clock	Memory clock	Power level	Hashrate	Leistung
1340 MHz	2000 MHz	100%	24,65 MH/s	164 W
-8%	2250 MHz	90%	28,40 MH/s	139 W

Tabelle 6.3: PowerColor RX 580 Leistungsparameter vor/nach Übertaktung

ZOTAC RTX 2070 SUPER

Um eine Übertaktung der ZOTAC RTX 2070 SUPER vornehmen zu können, wird eine andere Software benötigt. Daher wird das von ZOTAC für die Grafikkarte bereitgestellte Übertaktungs-Tool *FireStorm* eingesetzt. Ohne Übertaktung und Optimierung wird eine Hashrate von 37,17 MH/s erreicht. Dabei wird eine Leistung von 175 Watt benötigt (siehe Abschnitt 6.6.10). Daraus ergibt sich eine Effizienz von 212400 H/s/W. Die Taktfrequenz der Kerne wird um 25% verringert, wobei die Taktfrequenz des RAMs von 6800 MHz auf 7700 MHz erhöht wird. Außerdem wird das Power level auf 58% abgesenkt. Dadurch wird eine Hashrate von 43,03 MH/s bei einer Leistungsaufnahme von 125 Watt erreicht. Dies entspricht einer Effizienz von 344240 H/s/W. Durch die vorgestellten Leistungsparameter ergibt sich eine Leistungssteigerung im Vergleich zum Ausgangszustand ohne Anpassungen von 62,07%. Tabelle 6.4 zeigt die Leistungsparameter vor und nach der Übertaktung.

Core clock	Memory clock	Power level	Hashrate	Leistung
1995 MHz	6800 MHz	100%	37,17 MH/s	175 W
-25%	7700 MHz	58%	43,03 MH/s	125 W

Tabelle 6.4: ZOTAC RTX 2070 SUPER Leistungsparameter vor/nach Übertaktung

Die ermittelten Leistungsparameter stellen keinesfalls die optimalen Parameter dar, unter denen die maximal mögliche Hashrate bei minimaler Leistungsaufnahme erreicht wird. Aus diversen Tests ergeben sich die vorgestellten Werte für jede einzelne Grafikkarte. Im Rahmen dieser Ermittlung stellt sich die Frage nach der Stabilität. Um diese Frage der Stabilität unter den modifizierten Leistungsparametern zu beantworten und um die

Abhängigkeit in Bezug auf die Mining-Software festzustellen, werden im Folgenden die Szenarien 3 (siehe Abschnitt 6.6.3), 5 (siehe Abschnitt 6.6.5) und 7 (siehe Abschnitt 6.6.7) mit der Mining-Software *lolMiner* und der Übertaktung der jeweils beteiligten Grafikkarten sowie die Szenarien 10 (siehe Abschnitt 6.6.10), 12 (siehe Abschnitt 6.6.12), und 14 (siehe Abschnitt 6.6.14) unter der Mining-Software *PhoenixMiner* und ebenfalls mit Übertaktung der Grafikkarten erneut durchgeführt.

6.9.2 Szenario 27

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 38 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 42,63 MH/s
- Ø max. Temperatur: 48,78 °C
- Ø Leistung aller GPUs: 124 W
- Ø Leistung System: 160 W
- benötigte Energie: 3,84 kWh ~ 1,00 €
- Bitcoin: 0,000044 BTC ~ 1,94 €
- Bilanz: Gewinn **0,94 €**

Die Abbildung 6.36 veranschaulicht dieses Ergebnis.

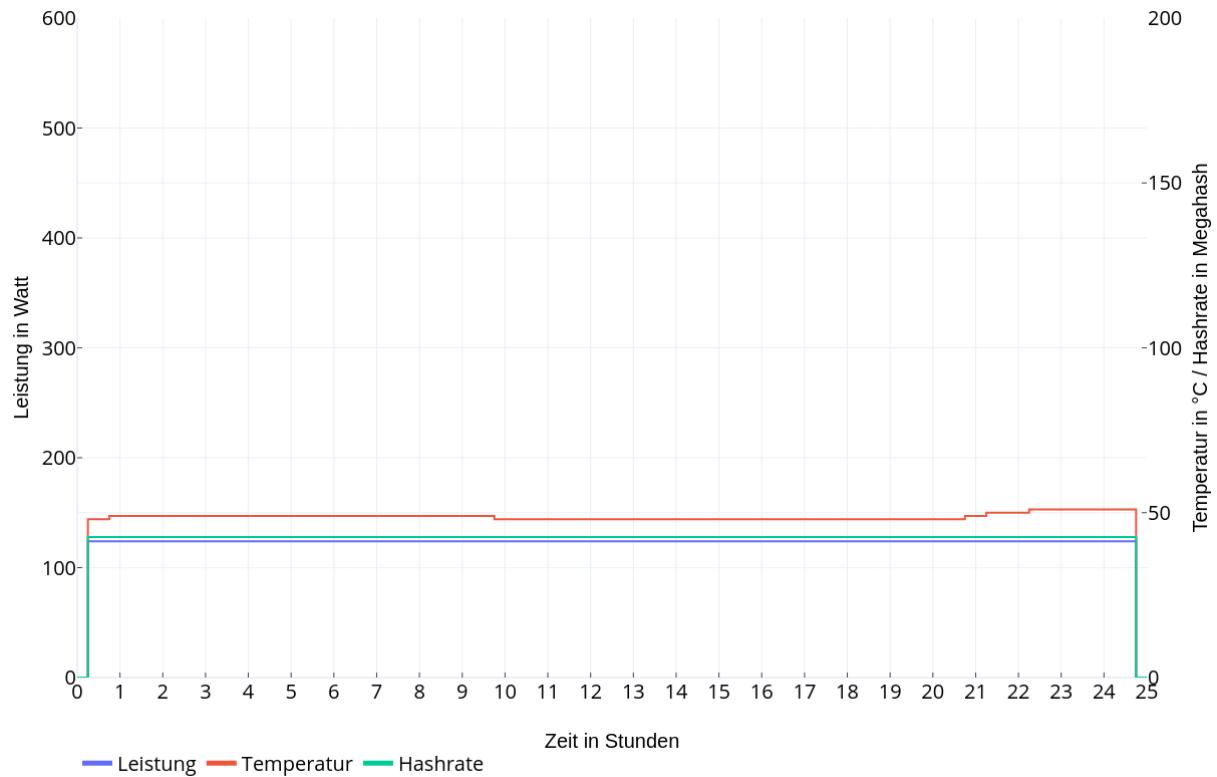


Abbildung 6.36: Aufbau 27

6.9.3 Szenario 28

Aufbau:

In diesem Test-Szenario wird die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 49 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggert und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 73,70 MH/s
- Ø max. Temperatur: 53,65 °C
- Ø Leistung aller GPUs: 278 W
- Ø Leistung System: 312 W
- benötigte Energie: 7,49 kWh ~ 1,95 €
- Bitcoin: 0,000077 BTC ~ 3,39 €
- Bilanz: Gewinn **1,44 €**

Die Abbildung 6.37 veranschaulicht dieses Ergebnis.

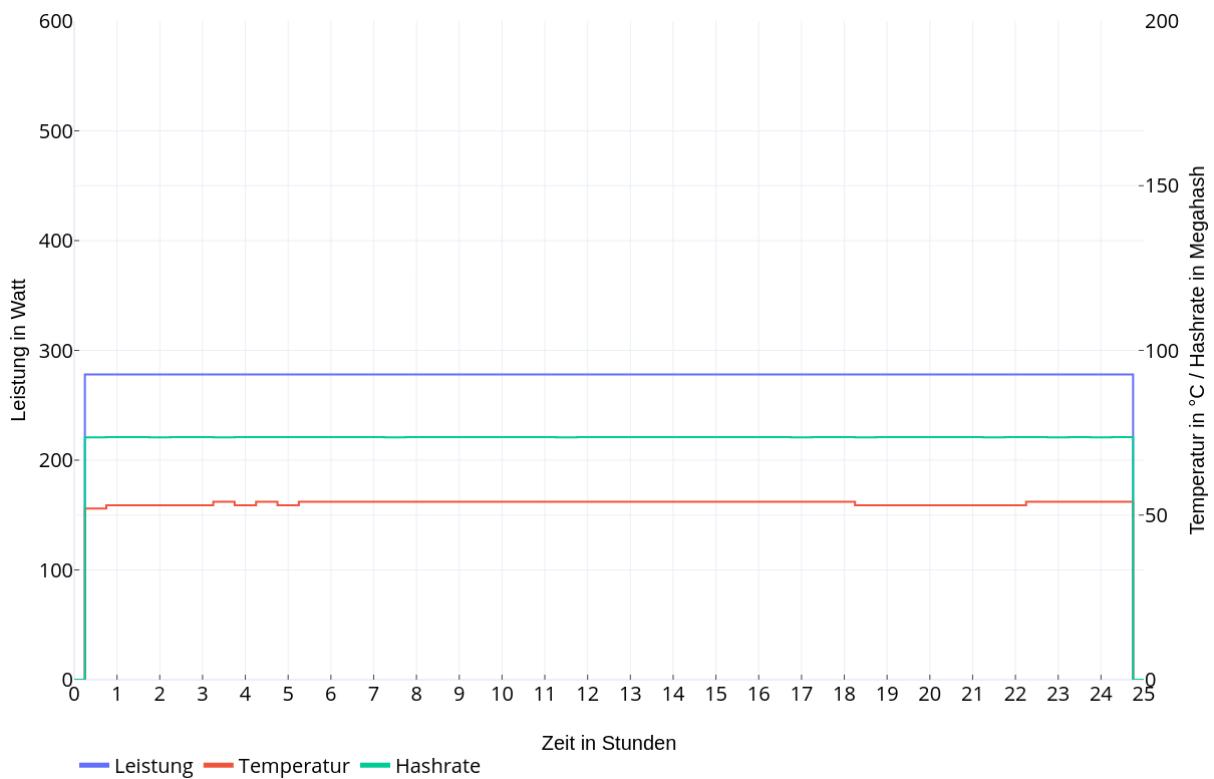


Abbildung 6.37: Aufbau 28

6.9.4 Szenario 29

Hardware-Aufbau:

In diesem Test-Szenario werden die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 57 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *lolMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

• Dauer:	24 h		
• Ø Hashrate:	101,08 MH/s		
• Ø max. Temperatur:	57,14 °C		
• Ø Leistung aller GPUs:	421 W		
• Ø Leistung System:	470 W		
• benötigte Energie:	11,28 kWh	~	2,93 €
• Bitcoin:	0,000105 BTC	~	4,62 €
• Bilanz:	Gewinn		1,69 €

Die Abbildung 6.38 veranschaulicht dieses Ergebnis.

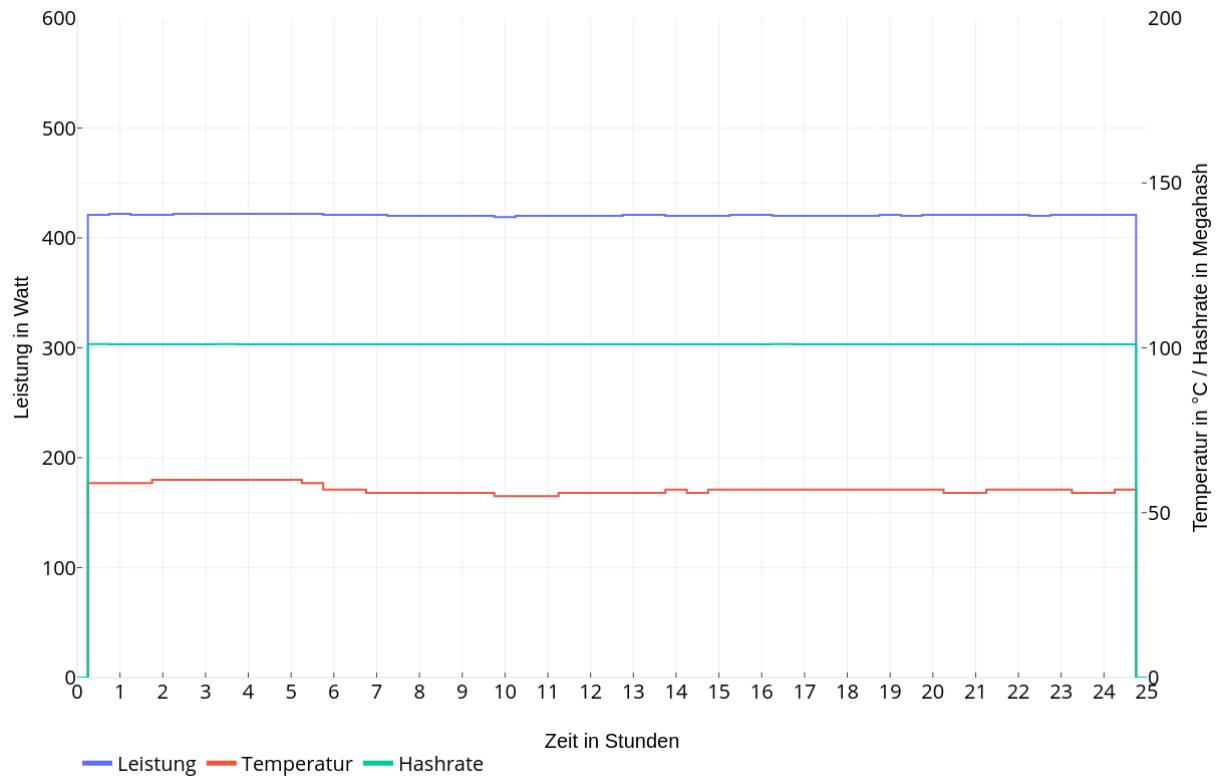


Abbildung 6.38: Aufbau 29

6.9.5 Szenario 30

Hardware-Aufbau:

In diesem Test-Szenario wird ausschließlich die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, werden die beiden anderen Grafikkarten für dieses Szenario entfernt. Das System benötigt im Ruhezustand 38 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 42,98 MH/s
- Ø max. Temperatur: 53,00 °C
- Ø Leistung aller GPUs: 125 W
- Ø Leistung System: 160 W
- benötigte Energie: 3,84 kWh ~ 1,00 €
- Bitcoin: 0,000045 BTC ~ 1,98 €
- Bilanz: Gewinn 0,98 €

Die Abbildung 6.39 veranschaulicht dieses Ergebnis.

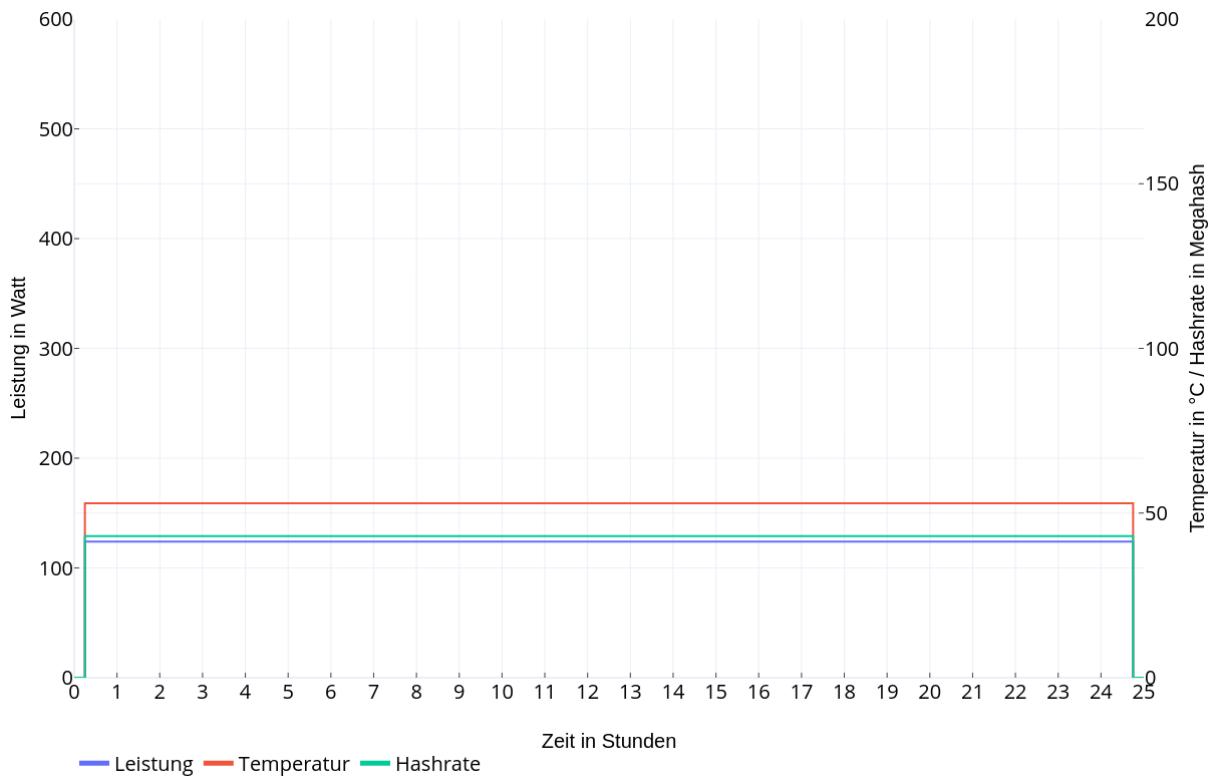


Abbildung 6.39: Aufbau 30

6.9.6 Szenario 31

Aufbau:

In diesem Test-Szenario werden die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Um die Messungen nicht zu verfälschen, wird die dritte GPU entfernt. Das System benötigt im Ruhezustand 47 Watt.

Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 74,60 MH/s
- Ø max. Temperatur: 56,96 °C
- Ø Leistung aller GPUs: 279 W
- Ø Leistung System: 315 W
- benötigte Energie: 7,56 kWh ~ 1,97 €
- Bitcoin: 0,000078 BTC ~ 3,43 €
- Bilanz: Gewinn **1,46 €**

Die Abbildung 6.40 veranschaulicht dieses Ergebnis.

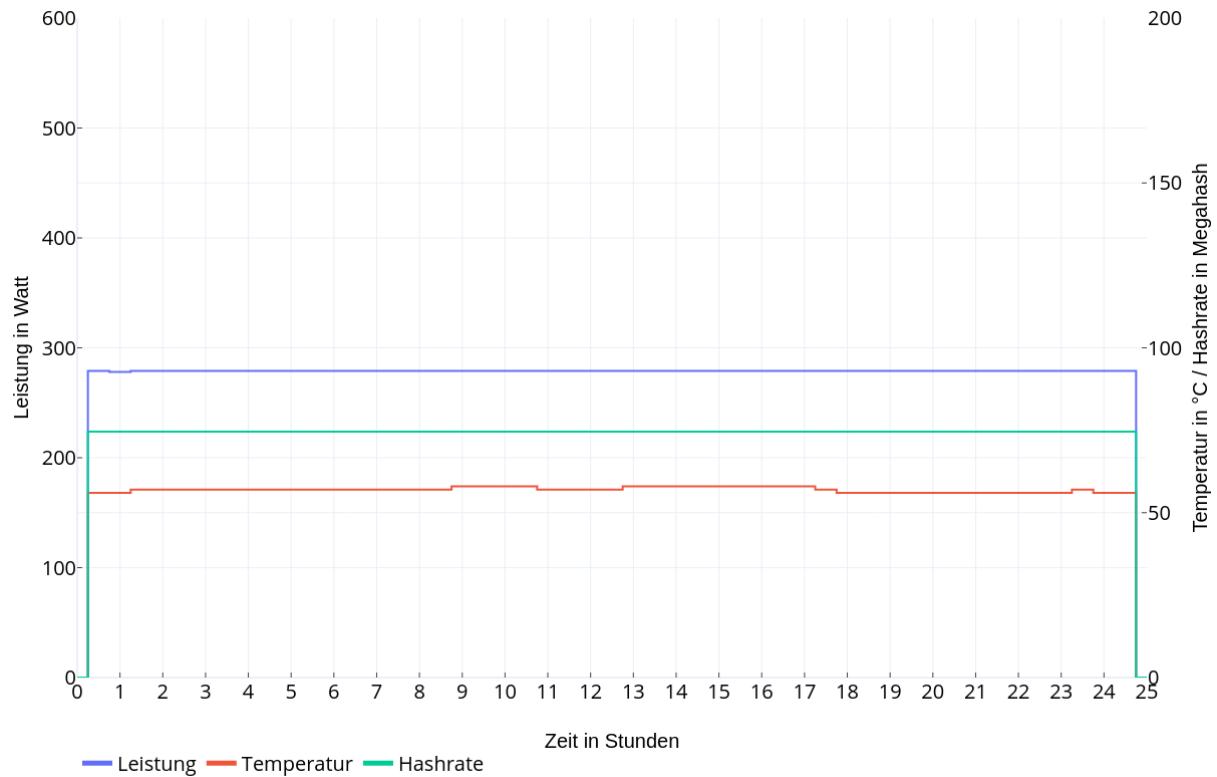


Abbildung 6.40: Aufbau 31

6.9.7 Szenario 32

Hardware-Aufbau:

In diesem Test-Szenario werden die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte zusammen mit der Power Color Radeon RX580 8 GB Grafikkarte und der Asus Radeon RX580 8 GB Strix Grafikkarte in das Mining-Rig eingebaut. Das System benötigt im Ruhezustand 57 Watt.

Software und Durchführung:

Zum Einsatz kommt die Software Awesome-Miner mit der darunterliegenden Mining-Software *PhoenixMiner*. Das Schürfen findet über den Ethermine-Pool statt und die Ausschüttung erfolgt ab einem Ether direkt auf das Hardware-Wallet. Die Testdauer umfasst 24 Stunden und es werden alle Daten aus dem Unterkapitel 6.5 mitgeloggt und gemessen.

Ergebnis:

Der Mining-Vorgang ergab folgende Daten:

- Dauer: 24 h
- Ø Hashrate: 103,11 MH/s
- Ø max. Temperatur: 62,00 °C
- Ø Leistung aller GPUs: 422 W
- Ø Leistung System: 473 W
- benötigte Energie: 11,35 kWh ~ 2,95 €
- Bitcoin: 0,000107 BTC ~ 4,71 €
- Bilanz: Gewinn **1,76 €**

Die Abbildung 6.41 veranschaulicht dieses Ergebnis.

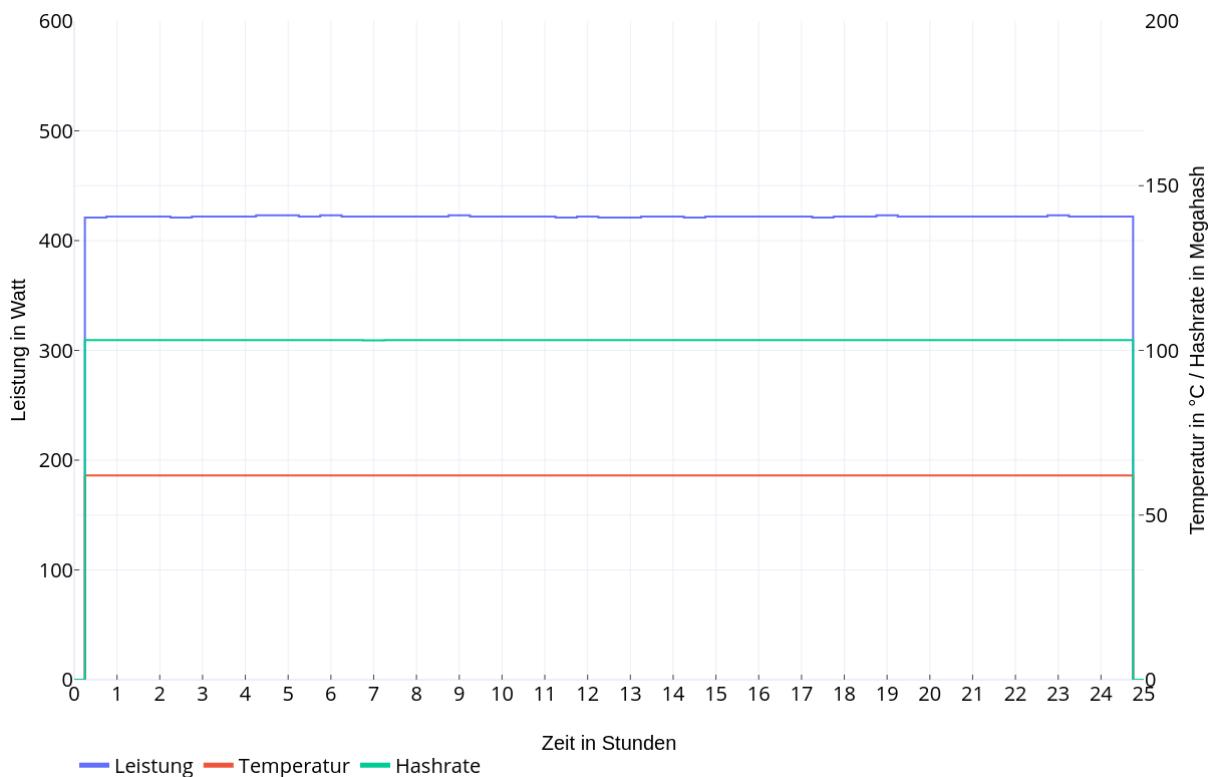


Abbildung 6.41: Aufbau 32

6.10 Auto Switching

Als Auto-Switching wird der automatische Wechsel zwischen verschiedenen Mining-Algorithmen und damit auch zwischen verschiedenen Kryptowährungen je nach Rentabilität bezeichnet. Ziel ist es, die zur Verfügung stehende Hardware des Mining-Rigs optimal zu nutzen. Optimal bedeutet dabei, den größtmöglichen Gewinn zu erzielen. Die auf dem Markt erhältlichen Programme, welche Auto-Switching unterstützen, unterscheiden sich grundlegend in den Anpassungs- und Konfigurationsmöglichkeiten durch den Nutzer. Die Softwares NiceHash und BetterHash bieten für den Nutzer keine Möglichkeit, die Parameter und damit letztlich die Kriterien für das Auto-Switching selbst festzulegen. Hier entscheidet ausschließlich die Software des Anbieters, wann auf welchen Algorithmus gewechselt wird. Dem gegenüber steht die Profit-Switching Funktion von Awesome Miner. Neben einer Funktion zur automatischen Ermittlung der passenden Parameter für das entsprechende System, kann durch den Nutzer festgelegt werden, ab welchen Schwellenwerten auf welchen Algorithmus automatisch gewechselt werden soll. Im Folgenden werden die Auto-Switching Funktionalität von NiceHash und Betterhash hinsichtlich ihrer Wirtschaftlichkeit evaluiert. Dazu werden alle drei Grafikkarten des Rigs eingesetzt, um möglichst viel Potenzial für den Wechsel zwischen Algorithmen zu bieten. Dabei wird das Rig jeweils 24 Stunden betrieben. Die Auto-Switching Funktion von Awesome Miner wird nicht evaluiert.

6.10.1 NiceHash Auto Switching

NiceHash führt vor dem eigentlichen Mining ein sogenanntes *Mining-Benchmarking* durch. Dies dient zur Ermittlung, welche Grafikkarte bei welchem Algorithmus welche Hashrate erzielt. Auf Basis dieser Daten wird im eigentlichen Mining-Prozess zwischen den Algorithmen gewechselt. Die Festlegung, zwischen welchen Algorithmen gewechselt wird, erfolgt automatisch durch NiceHash. Außerdem wird ebenfalls automatisch festgelegt, welcher Algorithmus mit welcher Mining-Software auf der Grafikkarte ausgeführt wird. NiceHash unterstützt auf der ZOTAC RX 2070 SUPER folgende Algorithmen:

- DaggerHashimoto (Ethereum, Ethereum Classic)
- GrinCuckatoo32 (GRIN)
- ZHash (Bitcoin Gold, ZelCash)

- BeamV3 (Beam)
- Autolykos (Ergo)
- ZelHash (Flux)
- KAWPOW (Raven)
- Octopus (Octopus Network)
- CukooCycle (Aeternity)

NiceHash unterstützt bei einigen Algorithmen zwei verschiedene Mining-Tools. Auf beiden AMD RX 580 Grafikkarten werden folgende Algorithmen unterstützt:

- DaggerHashimoto (Ethereum, Ethereum Classic)
- GrinCuckatoo31 (GRIN)
- GrinCuckatoo32 (GRIN)
- ZHash (Bitcoin Gold, ZelCash)
- BeamV3 (Beam)
- Autolykos (Ergo)
- ZelHash (Flux)
- KAWPOW (Raven)

Somit kann auf der ZOTAC RX 2070 SUPER zwischen neun Algorithmen und auf beiden AMD RX 580 Grafikkarten zwischen acht Algorithmen Auto-Switching betrieben werden. Welche Kryptowährung mit den aufgelisteten Algorithmen geschürft werden kann, ist irrelevant, da NiceHash grundsätzlich und ausschließlich in BTC vergütet. Wird Mining mit NiceHash betrieben, so wird zwar ein Algorithmus, mit dem eine entsprechende Kryptowährung geschürft werden kann auf dem Rig ausgeführt, jedoch wird diese Rechenleistung auf NiceHash vermietet, d.h. die eigene Leistung wird auf dem NiceHash Marktplatz zur Miete angeboten. Daher erfolgt die Vergütung wie bereits erwähnt in BTC. Außerdem wird für die Auszahlung ein von NiceHash bereitgestelltes Wallet genutzt. Für den Transfer auf eigene Wallets werden entsprechend Gebühren fällig. Andere Nutzer können sich die Rechenleistung des Rigs ebenfalls für Bitcoin mieten. Abbildung 6.42 zeigt die NiceHash Oberfläche.

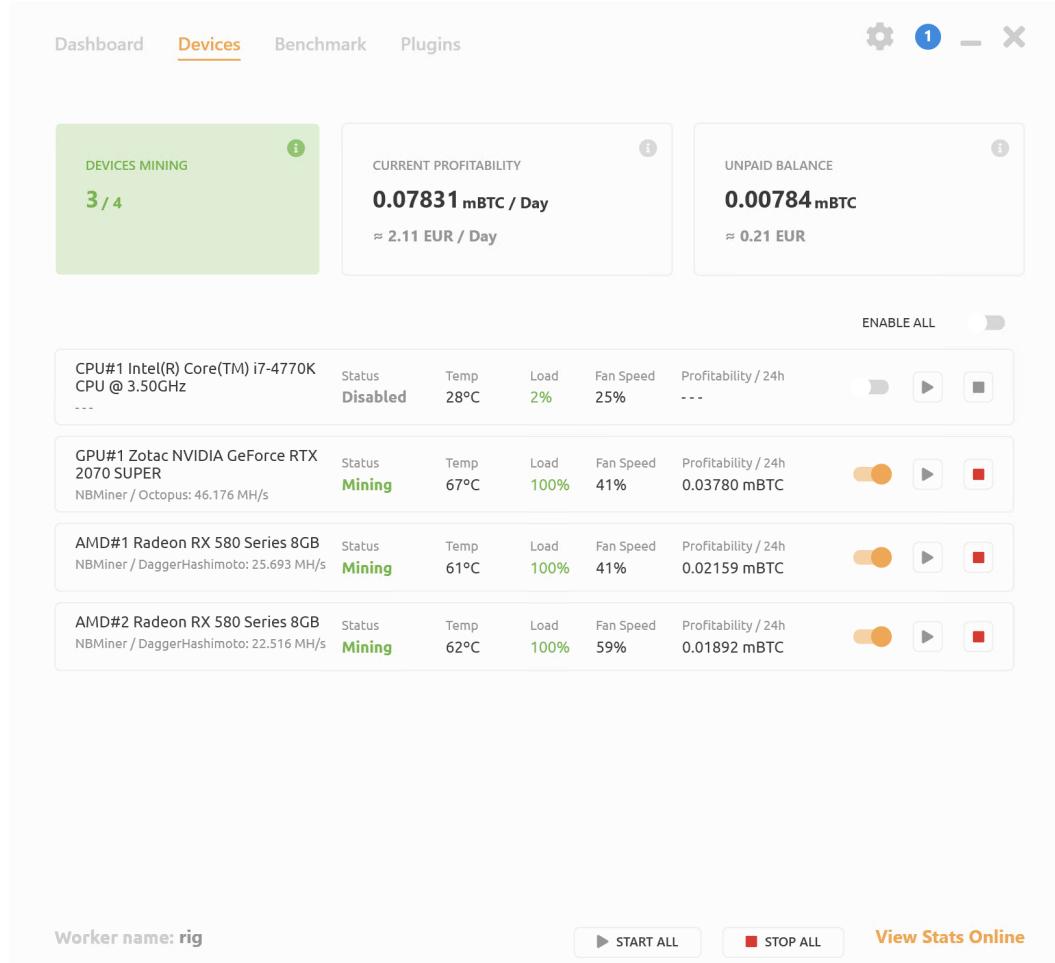


Abbildung 6.42: NiceHash Übersicht

Auswertung

Im Rahmen des 24 Stunden NiceHash-Tests wurden 0,0000757 BTC geschürft und verdient. Dies entspricht nach festgelegtem Kurs 3,34 €. Bei einer gemessenen Systemleistung von 620 W stehen diesem Wert allerdings 3,87 € Stromkosten gegenüber. Das bedeutet, innerhalb von 24 Stunden werden 0,53 € Verlust gemacht.

Die Zahlen sprechen klar gegen den Einsatz von NiceHash im Auto-Switching Modus. Bei genauerer Betrachtung fällt auf, dass nicht das volle Potenzial genutzt wurde. Zum einen verbraucht das System deutlich mehr Leistung als bei vergleichbaren Tests mit drei Grafikkarten, sodass die geschürfte Menge höher ausfallen müsste, um das zu rechtfertigen. Das Problem ist, dass der Auto-Switching Vorgang nicht reibungslos zwischen den Schürf-Algorithmen hin und her wechselt. Sobald NiceHash einen "besseren" Algorithmus findet, wird der aktuelle Mining-Prozess gestoppt. Um mit dem neuen Algorithmus schürfen zu

können, durchläuft NiceHash erneut einen Benchmark-Test und setzt neue Parameter der Hardware entsprechend, sodass es immer beim Wechsel zu Unterbrechungen kommt, die ebenfalls stromhungrig sind, da die Hardware getestet wird. Die Unterbrechungen machen etwa 18% des Mining-Prozesses aus. Mit Bereinigung dieser Unterbrechungen wäre ein potenzieller Wert von 0,00009 BTC möglich, was 3,96 € entsprechen würden. Damit wäre ein Gewinn von 0,09 € am Tag möglich. Das Problem der hohen Leistungsaufnahme bleibt allerdings bestehen. Ein weiteres Problem ist, dass nicht immer alle drei Grafikkarten genutzt werden. So kommt es immer wieder vor, dass nur die NVIDIA 2070 Super genutzt wird, da diese zum Teil andere Algorithmen unterstützt als die anderen beiden Karten. Zum Einsatz kamen laut Logs folgende Algorithmen:

• DAGGERHASHIMOTO	0,0000317 BTC	~	42%
• OCTOPUS	0,0000235 BTC	~	31%
• KAWPOW	0,0000158 BTC	~	21%
• CUCKOO CYCLE	0,0000031 BTC	~	4%
• BEAMV3	0,0000016 BTC	~	2%

Im realen Betrieb macht das Mining-Rig Verlust und selbst ohne Unterbrechungen wäre das Mininig-Rig nur wenig profitabel. Die Auto-Switching Funktion von NiceHash kann aus diesen Gründen nicht empfohlen werden. Es ist stehts besser, sich für eine Kryptowährung zu entscheiden und den Mining-Vorgang dahin gehend zu optimieren, insbesondere die Leistungsaufnahme zu senken. Während der Benchmarks sowie des Mining-Prozesses sind Instabilitäten des Systems aufgetreten. Zu Beginn eines Benchmarks fror das System vollständig ein und musste neu gestartet werden. Nach einer Wiederholung konnte dieser jedoch ohne Weiteres durchgeführt werden. Außerdem protokollierte das von NiceHash erstellte Log File einige Neustarts der Mining-Software aufgrund von aufgetretenen Fehlern.

6.10.2 BetterHash Auto Switching

BetterHash führt ebenfalls vor Beginn des Minings-Benchmarks durch, um die Leistung der Hardware des Rigs bei verschiedenen Algorithmen zu ermitteln. Auf Basis dieser Daten wird wie bei NiceHash vollautomatisch zwischen den von BetterHash unterstützten Algorithmen gewechselt. Jedoch unterscheidet sich BetterHash in zwei Punkten grundlegend

von NiceHash. Zum einen existiert kein Marktplatz, auf dem Mining-Leistung vermietet und gemietet wird. Zum anderen erfolgt die Auszahlung der geschürften Kryptowährungen nicht zwingend in BTC. BetterHash bietet die Möglichkeit eines *BTC Auto-Exchanges*. Ist diese aktiviert, werden alle geschürften Kryptowährungen automatisch in BTC getauscht. Somit erfolgt auch die Auszahlung in BTC. Ist die Funktion nicht aktiviert, so muss für jede Kryptowährung ein eigenes Wallet bei BetterHash hinterlegt werden. Um die Vergleichbarkeit mit NiceHash zu gewährleisten, wird die *BTC Auto-Exchanges* Funktion aktiviert. BetterHash bietet außerdem zwei Arten des Auto-Switchings. Der Nutzer kann auswählen, ob das Auto-Switching auf Basis von Server Empfehlungen von BetterHash oder auf Basis von lokalen Benchmarks durchgeführt werden soll. Da NiceHash auf Basis von Benchmarks arbeitet, wird dies entsprechend bei BetterHash konfiguriert, um die Vergleichbarkeit wahren.

BetterHash unterstützt auf der ZOTAC RX 2070 SUPER Grafikkarte folgende Algorithmen:

- ZHash (Bitcoin Gold, ZelCash)
- Ethash (Ethereum, Ethereum Classic)
- FiroPow (Firo)
- KAWPOW (Raven)
- Equihash (Zcash, Beam, Bitcoin Gold)

Auf beiden AMD RX 580 Grafikkarten stehen folgende Algorithmen für das Mining mit BetterHash zur Verfügung:

- ZHash (Bitcoin Gold, ZelCash)
- Ethash (Ethereum, Ethereum Classic)
- RandomX (Monero)
- KAWPOW (Raven)

Abbildung 6.43 zeigt die Benchmark Ergebnisse des Mining-Rigs. Die auf der rechten Seite ausgewählten Algorithmen sind von BetterHash automatisch auf Basis der Benchmark Ergebnisse ausgewählt.

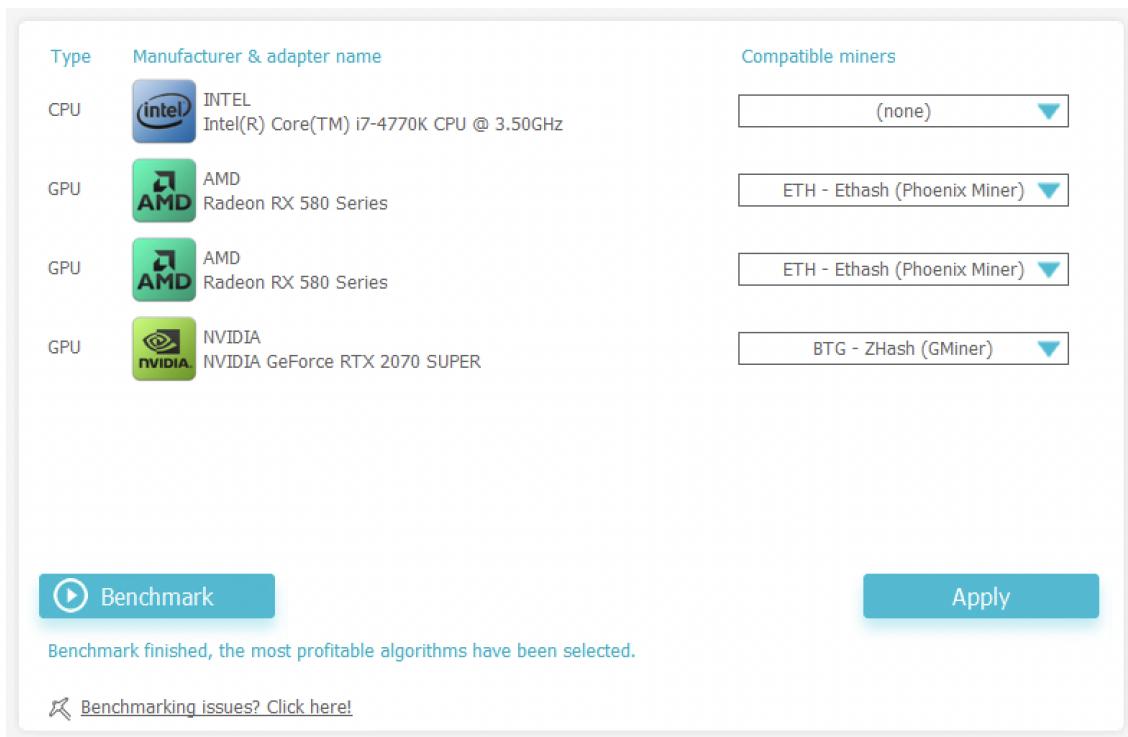


Abbildung 6.43: BetterHash Benchmark Übersicht

Auswertung

Innerhalb von 24 Stunden können so 0,00008 BTC erwirtschaftet werden und das entspricht 3,52 €. Die Stromkosten belaufen sich bei 560 W Systemleistung auf 3,49 €, das ergibt einen Gewinn von 0,03 €. Das folgende Listing 6.6 zeigt einen Auszug aus dem Mining-Log. Aus dem Auszug ist zu erkennen, dass der Algorithmus nicht geändert wurde, dies entspricht dem Großteil des Logs, sodass bei BetterHash insgesamt weniger Algorithmus-Wechsel vollzogen werden. Weniger Wechsel bedeuten demnach auch weniger Unterbrechungen des Mining-Vorgangs. BetterHash braucht im Vergleich zu NiceHash weniger Systemleistung. Daraus ergeben sich automatisch geringere Stromkosten. Durch die insgesamt weniger Algorithmus-Wechsel wird auch effektiver geschürft, sodass nach 24 Stunden ein höherer Ertrag erwirtschaftet wurde. BetterHash schneidet im Vergleich deutlich besser ab, allerdings auch nicht wirklich gut. Auto-Switching Verfahren sind auf den ersten Blick eine vielversprechende Funktion, jedoch in der Praxis nicht wirtschaftlich und unprofitabel.

```
1 20:19:36 Local profitability test
2 20:19:36 Tested Radeon RX 580 Series [1] and ETH - Ethash (
   Phoenix Miner) remains the most profitable.
3 20:19:36 Tested Radeon RX 580 Series [2] and ETH - Ethash (
   Phoenix Miner) remains the most profitable.
4 20:19:36 Tested NVIDIA GeForce RTX 2070 SUPER [3] and BTG -
   ZHash (GMiner) remains the most profitable.
5 20:19:36 Profit switching test ended, no algorithm was
   changed
```

Listing 6.6: BetterHash AutoSwitching Log (Auszug)

7 Auswertung & Analyse

Das Kapitel 7 beschäftigt sich mit der Auswertung und Analyse der Daten. Insgesamt wurden 34 Test-Szenarien zu je 24 h durchgeführt und dabei entsprechende Daten gesammelt. Allerdings ohne Berücksichtigung der beiden Auto-Switching Szenarien, die im Kapitel davor behandelt werden. Die Daten der verbleibenden 32 Test-Szenarien werden in einer komprimierten Form nachfolgend zusammenfassend aufbereitet und dargestellt.

7.1 Allgemeine Analyse

Bei Betrachtung der Daten fällt auf, dass im Zwischenfazit bereits die richtigen Schlüsse gezogen werden konnten. Während im Windows-Umfeld noch Szenarien mit Verlusten in der Bilanz auftreten, sind alle im Anschluss durchgeführten Test-Szenarien gewinnbringend. Werden die Windows-Tests auf die ausgewählten Top-Szenarien reduziert, so lässt sich ein Vergleich zwischen den eingesetzten Betriebssystemen durchführen.

Rein spekulativ werden die besten Ergebnisse mit Linux oder mit Hive-OS erwartet, da beide Systeme CLI basierend sind und so gut wie keine Grafikleistung aufgrund der GUI reserviert wird. Außerdem sind Linux Systeme wie Ubuntu Server deutlich geringer im Umfang als Windows. Gleiches gilt für Hive-OS, welches ebenfalls auf Ubuntu basiert. Das Ergebnis kann diese Spekulation allerdings nur bedingt bestätigen. Es werden in den Test-Szenarien unter Linux und unter Hive-OS die höchsten Hashraten erreicht. Allerdings zeigen die Messungen einen höheren Leistungsbedarf als mit dem Vergleichssystem Windows.

Um die Werte miteinander vergleichen zu können, ist es sinnvoll, diese ins Verhältnis zu setzen. Die Maßeinheit Hashrate/Watt (MH/s/W) liefert einen Wert, der die Effizienz der eingesetzten Hardware beschreibt. Der Faktor richtet sich nach der Hardware und nicht nach der Software und bleibt stabil. Das ergibt in den Top-Szenarien (ausgenommen Übertaktungs-Szenarien) mit der allein eingesetzten ZOTAC GAMING GeForce RTX 2070 SUPER AMP einen Effizienz-Wert von 0,21 MH/s/W. Dagegen wird beim Einsatz

der Asus Radeon RX 580 8 GB Strix gemeinsam mit der ZOTAC GAMING GeForce RTX 2070 SUPER AMP einen Effizienz-Wert von 0,18 MH/s/W. Mit allen drei Grafikkarten zusammen wird ein Effizienz-Wert von 0,17 MH/s/W erreicht. Dabei spielt es keine Rolle, welches Betriebssystem oder Miner zum Einsatz kommt, der Wert ist eine Kennzahl der Hardware. Dieser Effizienzwert ist von Kryptowährung zu Kryptowährung jedoch unterschiedlich und kann durch Übertaktungsmaßnahmen beeinflusst werden.

Allerdings lässt sich damit alleine noch keine konkrete Aussage über die Rentabilität einer Grafikkarte in Bezug auf Kryptomining treffen. Bei Ethereum skaliert der Gewinn durch eine höhere Hashrate weniger als die Abnahme der Leistung, dies zeigen die Tests deutlich. Zum Beispiel wird im Szenario 20 (vgl. Kapitel 6.7.6) eine Hashrate von 90,11 MH/s erreicht bei einer GPU-Leistung von 530 W und Systemlast von 575 W. Dies ergibt einen Tagesgewinn von 0,55 €. Im Szenario 14 (vgl. Kapitel 6.6.14) wird eine Hashrate von 89,48 MH/s erreicht, allerdings mit 520 W GPU-Leistung und 564 W Systemleistung. Dadurch ergibt sich ein Tagesgewinn von 0,57 €, obwohl beide Szenarien einen Effizienzwert von 0,17 MH/s/W aufweisen.

Eine weitere Auffälligkeit der Daten ergibt sich aus den eingesetzten Minern, PhoenixMiner und lolMiner. Es können über alle Systeme hinweg höhere Gewinne mit dem PhonixMiner erzielt werden. Je mehr Grafikkarten zum Einsatz kommen, desto größer ist der Gewinnsprung. Bei einer Karte ist eine Gewinnsteigerung bis zu 11%, bei zwei Karten bis zu 18% und bei drei Karten sogar bis zu 50% zu beobachten gegenüber dem lolMiner. Da dieser Effekt kein Einzelfall, sondern in jedem einzelnen Test zu beobachten ist, ist davon auszugehen, dass der PhoenixMiner Algorithmus in der Momentaufnahme der effektivere der beiden ist. Allerdings gibt es keine Langzeitstudien, die beschreiben, welcher der beiden Miner die Hardware wie stark belastet und letztlich, wie sich dies auf deren Lebenszeit auswirkt.

Eine Betrachtung der Top-Szenarien über alle Systeme hinweg ergibt, dass Windows im Schnitt die höchsten Gewinne erzielt, obwohl Windows nicht die höchsten Hashraten erreicht. Der lolMiner läuft auf Windows besser als auf Vergleichssystemen, sodass der Unterschied zwischen den Minern nur bis zu 10% beträgt.

7.2 Windows Ergebnisse

Die Tabelle 7.1 zeigt die erhobenen Daten der 14 durchgeführten Test-Szenarien unter Windows 10 Pro. Getestet werden alle Kombinationen aus drei Grafikkarten. Eine Menge aus drei Elementen (Grafikkarten) lässt sich in acht Teilmengen unterteilen, darunter ist allerdings auch die leere Menge. Dies ergibt ein Test-Szenario ohne Grafikkarten und macht keinen Sinn, daher bleiben nur noch sieben Szenarien offen. Bei zwei verschiedenen Minern macht das zusammen 14 Szenarien. Insgesamt wurden dafür 111 kWh Strom verbraucht, die Kosten in Höhe von 28,80 € verursacht haben. Das Ethereumsschürfen ergab einen Ertrag von 0.000733 BTC. Mit dem in Kapitel 6.5 festgeschriebenen Umrechnungsfaktor ergibt das eine Summe von 32,26 € und einen Gesamtgewinn von 3,46 €.

Szenario	Miner	Ethereum [BTC]	Hashrate [MH/s]	GPU-Power [W]	Effizienz [MH/s/W]	Total-Power [W]	Revenue [€]	Loss [€]	Profit [€]
1	L	0,000028	26,65	177	0,15	200	1,23	1,25	0,02
2	L	0,000024	22,91	156	0,15	197	1,06	1,23	0,17
3	L	0,000038	36,87	172	0,21	206	1,67	1,28	0,39
4	L	0,000052	49,99	337	0,15	370	2,29	2,31	0,02
5	L	0,000066	63,51	350	0,18	379	2,90	2,37	0,53
6	L	0,000063	60,22	330	0,18	375	2,77	2,34	0,43
7	L	0,000090	86,85	512	0,17	553	3,96	3,45	0,51
8	P	0,000029	27,70	185	0,15	205	1,28	1,28	0,00
9	P	0,000026	24,62	164	0,15	208	1,14	1,30	0,16
10	P	0,000039	37,17	175	0,21	207	1,72	1,29	0,43
11	P	0,000054	52,40	349	0,15	386	2,38	2,41	0,03
12	P	0,000067	64,87	357	0,18	385	2,95	2,40	0,55
13	P	0,000064	61,83	340	0,18	380	2,82	2,37	0,45
14	P	0,000093	89,48	520	0,17	564	4,09	3,52	0,57

Tabelle 7.1: Ergebnisse Windows Test-Szenarien

Dieselbe Rechnung auf die drei Top-Szenarien angewandt und beschränkt, ergeben sich Stromkosten von 14,31 € und ein Ertrag von 17,29 €. Das ergibt einen Gewinn von 2,98 €. Somit ist Windows im Vergleich zu Linux mit 2,77 € und HiveOS mit 2,55 € bei Betrachtung der Top-Szenarien das rentabelste System. Szenario 2 (vgl. Kapitel 6.6.2) mit der Power Color RX 580 Grafikkarte, der Leistungsschwächsten der drei Grafikkarten und dem lolMiner schneidet am unprofitabelsten mit 0,17 € Verlust über 24 Stunden ab. Dagegen erweist sich Szenario 14 (vgl. Kapitel 6.6.14) mit allen drei Grafikkarten in Verbindung mit dem PhoenixMiner mit 0,57 € Gewinn als profitabelstes Szenario unter Windows.

7.3 Linux-Ergebnisse

Nach den durchgeführten Tests mit dem Betriebssystem Windows 10 Pro wurden unter dem Betriebssystem Linux Ubuntu 20.04 LTS nur noch die drei Top-Szenarien getestet, die im Kapitel 6.6.15 bestimmt wurden. Das Schürfen übernehmen dabei der loMiner sowie der PhoenixMiner. So entstehen sechs Test-Szenarien unter Linux Ubuntu 20.04 LTS. Für diese Tests verbraucht das Mininig-Rig 56,11 kWh Strom zum Preis von 14,61 €. Beim Schürfen werden 17,38 € erwirtschaftet und damit ein Gewinn von 2,77 € erzielt. Die Tabelle 7.2 zeigt die durchgeführten Test-Szenarien 15 bis 20 im Detail.

Szenario	Miner	Ethereum [BTC]	Hashrate [MH/s]	GPU-Power [W]	Effizienz [MH/s/W]	Total-Power [W]	Revenue [€]	Loss [€]	Profit [€]
15	L	0,000038	36,93	174	0,21	206	1,67	1,28	0,39
16	L	0,000066	63,65	361	0,18	388	2,90	2,42	0,48
17	L	0,000090	87,07	527	0,17	577	3,96	3,60	0,36
18	P	0,000039	37,15	175	0,21	207	1,72	1,29	0,43
19	P	0,000068	65,19	362	0,18	389	2,99	2,43	0,56
20	P	0,000094	90,11	530	0,17	575	4,14	3,59	0,55

Tabelle 7.2: Ergebnisse Linux Test-Szenarien

Szenario 17 (vgl. Kapitel 6.7.3) unter Einsatz von allen drei Grafikkarten und dem lolMiner hat dabei am schlechtesten, aber mit Gewinn von 0,36 € am Tag, abgeschlossen. Entgegen der Erwartung hat nicht das gleich besetzte Szenario 20 (vgl. Kapitel 6.7.6) mit dem PhoenixMiner die höchste Ausbeute erzielt, sondern Szenario 19 (vgl. Kapitel 6.7.5). Dabei werden ZOTAC GAMING GeForce RTX 2070 SUPER AMP und Asus Radeon RX 580 8 GB Strix im Mining-Rig mit dem PhoenixMiner betrieben. Der Gewinn in dieser Kombination beläuft sich auf 0,56 € innerhalb von 24 Stunden. Gesamt betrachtet liegt das Linuxsystem damit eine Platzierung hinter Windows. Das Linux Ubuntu 20.04 LTS erreicht zusammen mit dem Mining-Betriebssystem HiveOS allerdings die höchsten Hashraten. Bei Nutzung aller drei Karten sowie dem PhoenixMiner wurde ein Wert von 90,11 Mh/s erreicht.

7.4 Hive-OS-Ergebnisse

Das Mining-Betriebssystem HiveOS hat für den Betrieb der Top-Szenarien mit 57,00 kWh den meisten Strom verbraucht. Auch wenn der Unterschied gering ausfällt, beträgt der Stromverbrauch bei Windows 55,06 kWh und bei Linux 56,21 kWh. So belaufen sich die Stromkosten auf 14,83 €. Insgesamt wurde so ein Kryptowert von 17,38 € mit HiveOS und ein Gewinn von 2,55 € erwirtschaftet. Die Tabelle 7.3 zeigt die durchgeföhrten Szenarien 21 bis 26 mit HiveOS.

Szenario	Miner	Eternum [BTC]	Hashrate [MH/s]	GPU-Power [W]	Effizienz [MH/s/W]	Total-Power [W]	Revenue [€]	Loss [€]	Profit [€]
21	L	0,000038	36,93	174	0,21	208	1,67	1,30	0,37
22	L	0,000066	63,67	363	0,18	395	2,90	2,46	0,44
23	L	0,000090	87,10	527	0,17	583	3,96	3,64	0,32
24	P	0,000039	37,15	175	0,21	209	1,72	1,31	0,41
25	P	0,000068	65,19	364	0,18	396	2,99	2,47	0,52
26	P	0,000094	90,11	530	0,17	584	4,14	3,65	0,49

Tabelle 7.3: Ergebnisse Hive-OS Test-Szenarien

Ähnlich wie unter Linux Ubuntu 20.04 LTS erzielt Szenario 23 (vgl. Kapitel 6.8.3) das schlechteste Ergebnis. Mit dem lolMiner kommen in diesem Szenario alle drei Grafikkarten zum Einsatz. Das Szenario 25 (vgl. Kapitel 6.8.5) ist deckungsgleich mit Szenario 19 (vgl. Kapitel 6.7.5) nur auf dem Betriebssystem HiveOS. Dabei werden ZOTAC GAMING GeForce RTX 2070 SUPER AMP und Asus Radeon RX 580 8 GB Strix im Mining-Rig mit dem PhoenixMiner betrieben. Diese Kombination bildet auch unter HiveOS das stärkste Szenario. Auch mit HiveOS kann eine Hashrate von 90,11MH/s erreicht werden.

7.5 Overclocking-Ergebnisse

Bei Betrachtung der Top-Szenarien mit Übertaktung fällt die deutlich höhere Effizienz der einzelnen Grafikkarten auf. Diese ergibt sich aus der durch das Übertakten gesteigerten Hashrate und der geringeren Leistungsaufnahme. Der höchste und damit beste Effizienzwert wird mit der ZOTAC GAMING RTX 2070 Super AMP Extreme und den Übertaktungsparametern aus Kapitel 6.9 erreicht. Ohne Übertaktung besitzt sie eine Effizienz von 0,21 MH/s/W, mit Übertaktung eine von 0,34 MH/s/W. Dies entspricht einer Steigerung von circa 61%. Bei der Kombination von zwei Grafikkarten, der ZOTAC GAMING RTX 2070 Super AMP Extreme und der Asus Radeon RX580 8 GB Strix, ergibt sich ohne Übertaktung eine Effizienz von 0,18 MH/s/W und mit einer Effizienz von 0,27 MH/s/W. Somit beträgt die Effizienzsteigerung 50%. Die Kombination aus der ZOTAC GAMING RTX 2070 Super AMP Extreme, der Power Color Radeon RX580 8 GB und der Asus Radeon RX580 8 GB Strix Grafikkarte besitzt ohne Übertaktung eine Effizienz von 0,17 MH/s/W. Mithilfe der Übertaktung aller drei Grafikkarten lässt sich diese auf 0,24 MH/s/W erhöhen. Daraus ergibt sich eine Steigerung um 41%. Dies zeigt, dass insgesamt bei verschiedenen Kombinationen von Grafikkarten in jedem Fall die Effizienz durch Übertaktung gesteigert werden kann, selbst wenn eine schwächere Grafikkarte Teil des Verbunds ist. Offensichtlich erreicht die ZOTAC GAMING RTX 2070 Super AMP Extreme Grafikkarte durch Übertaktung die größte Effizienzsteigerung, jedoch lässt sich dies nicht direkt auf den Profit im Mining-Prozess übertragen. Wie bereits erwähnt, schneidet das Windows Betriebssystem in Kombination mit dem PhoenixMiner am besten ab. Deswegen wurden alle Übertaktungsszenarien auch auf Windows durchgeführt. Das beste Ergebnis hinsichtlich des Profits wird hierbei in Szenario 32 (vgl. Kapitel 6.9.7) erzielt. Obwohl beide RX 580 Grafikkarten prozentual gesehen nicht an die Effizienzsteigerung von circa 61% der ZOTAC Grafikkarte herankommen, schneidet dieses Szenario dennoch mit einer Hashrate von 103,11 MH/s, einer Leistungsaufnahme

von insgesamt 473 Watt und einem Profit von 1,76 € am besten ab. Dem gegenüber steht das schlechteste Übertaktungsszenario, Szenario 27 (vgl. Kapitel 6.9.2). Zwar erreicht die ZOTAC Grafikkarte aus Sicht der Effizienz den höchsten absoluten Wert und die höchste Steigerung, jedoch schneidet sie aus Profit Sicht alleine am schlechtesten ab. Dies ist unter anderem mit der Systemlast zu erklären. Bei einer einzelnen Grafikkarte im Rig sorgt dies für eine höhere Gewichtung der Systemlast. Wenn beispielsweise alle drei Grafikkarten im Verbund betrieben werden, ist der Einfluss der Systemlast auf den Profit deutlich geringer. Die ZOTAC Grafikkarte erreicht bei einer Leistungsaufnahme von 160 Watt eine Hashrate von 42,63 MH/s und damit ein Profit von 0,94 €. Dies soll zeigen, dass die Kombination verschiedener Grafikkarten, auch mit teilweise schwächeren, in Bezug auf Hashrate und geringerer Leistungssteigerung durch Übertakten dennoch wirtschaftlich sinnvoll sein kann. Tabelle 7.4 zeigt die Ergebnisse der Overclocking Szenarien.

Szenario	Miner	Ethereum [BTC]	Hashrate [MH/s]	GPU-Power [W]	Effizienz [MH/s/W]	Total-Power [W]	Revenue [€]	Loss [€]	Profit [€]
27	L	0,000044	42,63	124	0,34	160	1,94	1,00	0,94
28	L	0,000077	73,70	278	0,27	312	3,39	1,95	1,44
29	L	0,000105	101,08	421	0,24	470	4,62	2,93	1,69
30	P	0,000045	42,98	125	0,34	160	1,98	1,00	0,98
31	P	0,000078	74,60	279	0,27	315	3,43	1,97	1,46
32	P	0,000107	103,11	422	0,24	473	4,71	2,95	1,76

Tabelle 7.4: Ergebnisse Overclocking Test-Szenarien

8 Fazit

In diesem Kapitel werden die zuvor analysierten Daten anhand von festgelegten Kriterien zusammenfassend bewertet. Auf Basis dieser Bewertung wird eine abschließende Empfehlung gegeben.

8.1 Bewertung

Im Folgenden werden Kriterien definiert, welche im Anschluss auf die im Rahmen dieser Arbeit durchgeführten Test-Szenarien angewendet werden.

8.1.1 Kriterien

Die einzelnen Kriterien werden für die Anwendung auf die Szenarien wie folgt aufgebaut: Im ersten Schritt wird der minimale und der maximale Wert des Kriteriums aus den Daten bestimmt. Daraus wird ein Intervall gebildet, welches den gesamten Bereich abbildet. Dieses Intervall wird in sieben gleich große Intervalle aufgeteilt. Diesen neu gebildeten Intervallen werden Zahlenwerte von ”-3” bis ”+3” zugeordnet. Zusätzlich findet noch eine Gewichtung der einzelnen Kriterien in Bezug zum Gesamtergebnis statt. Die folgende Auflistung ist absteigend nach der Gewichtung sortiert:

- Profit
- Stromverbrauch
- Hashrate / Effizienz
- Hardware-Kosten / Break-even-Point
- Mining-Software

Die Tabelle mit den Gewichtungswerten kann dem Anhang A.1 entnommen werden. Zur Nachvollziehbarkeit der Einordnung der Szenarien in die Intervalle sind die Schwellenwerte im Anhang A.3 aufgeführt.

Hardware-Kosten

Hardware-Kosten sind in Bezug auf Wirtschaftlichkeit und den Break-even-Point ein wichtiges Kriterium. Daher werden die Szenarien hinsichtlich ihrer Hardware-Kosten bewertet. Dafür werden die gesamten Kosten der Hardware bewertet. Die Hardware-Kosten sollten möglichst gering sein, daraus ergibt sich bei hohen Hardware-Kosten ein negativer Bewertungswert und bei niedrigen Kosten entsprechend ein hoher Bewertungswert.

Stromverbrauch

Das Kriterium Stromverbrauch ist ein großer Kostenfaktor während des Mining-Betriebs. Betrachtet wird der gesamte Stromverbrauch, da sich dieser bei unterschiedlichen Betriebssystemen und in Abhängigkeit der eingesetzten Mining-Software unterscheidet. Ziel ist es, einen möglichst geringen Stromverbrauch zu erzielen. Je niedriger der Stromverbrauch, desto positiver wird dies bewertet.

Hashrate

Die Hashrate ist die Leistungskennzahl eines Mining-Rigs in Abhängigkeit eines Algorithmus und wird daher ebenfalls als Kriterium betrachtet. Da im Rahmen dieser Arbeit ausschließlich ETH-Mining evaluiert wird, beziehen sich alle Hashrate Angaben auf den Ethereum Algorithmus Ethash. Bei Szenarien mit mehreren Grafikkarten wird die gesamte Hashrate dieser Kombination angenommen. Je höher die Hashrate, desto positiver ist dies zu bewerten.

Effizienz

Mithilfe des Effizienzwertes lässt sich der Wirkungsgrad des Rigs ermitteln, d.h. wie gut elektrische Leistung durch die Hardware des Rigs in Hashes des entsprechenden Algorithmus umgewandelt wird. Hierbei gilt wie bei der Hashrate, dass beim Einsatz von

mehreren Grafikkarten der Effizienzwert der entsprechenden Kombination angenommen wird. Je größer der Effizienzwert Wert, desto positiver ist dies zu bewerten.

Break-even-Point

Der Break-even-Point spielt bei der Kalkulation für ein Mining-Rig eine entscheidende Rolle. Er gibt an, ab wann mit dem Rig Gewinn erzielt wird, nachdem bereits alle entstandenen Kosten durch das Rig erwirtschaftet wurden. Hierbei werden die gesamten Kosten, d.h. Rig inklusive Grafikkarten der jeweiligen Szenarien angenommen. Je niedriger der Break-even-Point, desto positiver ist dies zu bewerten.

Profit

Durch den Profit lässt sich eine Aussage über die Wirtschaftlichkeit des Rigs treffen. Dabei sollte dieser stets größer 0 sein. Ist das der Fall, wird dies positiv bewertet. Es gilt, je größer der Wert, desto positiver ist dies zu bewerten.

Mining-Software

Ein weiteres Kriterium bildet die eingesetzte Mining-Software. Dabei wird jedoch ausschließlich entweder mit ”-3” oder mit ”+3” bewertet. Positiv wird bewertet, wenn durch die Mining-Software bei gleicher oder fast identischer Leistung eine höhere Hashrate erreicht wird. Dagegen negativ bewertet, wenn bei gleicher oder ähnlicher Leistung eine geringere Hashrate erreicht wird.

8.1.2 Ergebnis

Allgemeine Bewertung

Die Bewertungsmatrix im Anhang A.1 weist zwei Gruppen auf. Alle Szenarien, die unter Windows mit Übertaktung durchgeführt werden, schneiden deutlich besser ab, als die restlichen. Das Bewertungsintervall beginnt bei dem schlechtesten Wert von -1,96 und geht bis hin zum besten Wert von 1,47. Alle Übertaktungs-Szenarien liegen nach Bewertung weit im positiven Bereich mit Werten von 0,89 bis 1,47. Dagegen weisen alle anderen

Szenarien Werte von -1,96 bis -0,01 auf. Weitere Details zu den Top-Szenarien werden im nächsten Punkt 8.1.2 genannt. Bei einer Betrachtung ohne Übertaktungs-Szenarien schneidet Szenario 10 (vgl. Kapitel 6.6.10) mit einem Bewertungswert von -0,01 am besten ab. In diesem Aufbau läuft das Mining-Rig alleinig mit der ZOTAC GAMING GeForce RTX 2070 SUPER AMP Grafikkarte. Diese erwirtschaftet mit einer GPU-Leistung von etwa 175 W und einer Systemleistung von 205 W einen Betrag von 1,72 € am Tag. Das ergibt einen Gewinn von 0,43 € täglich. Der eingesetzte Miner spielt dabei ebenso eine Rolle. Im vergleichbaren Szenario 3 (vgl. Kapitel 6.6.3) schneidet die gleiche Grafikkarte mit einem Wert von -0,07 geringfügig schlechter ab, da der lolMiner zum Einsatz kommt. Die Karte einzeln zu betreiben macht nur bedingt Sinn, da die Systemleistung im Verhältnis zu einer Karte einen höheren Einfluss hat. Trotz dieses Umstandes wird ein besseres Ergebnis als in allen Szenarien erreicht, bei denen drei Grafikkarten zum Einsatz kommen. Nahezu alle Szenarien sind profitabel ausgefallen und der Profit wird mit einem hohen Gewicht belegt, dennoch eignen sich nur die Top-Szenarien mit Werten von oder oberhalb von 0,89 wirklich dazu, in einem Mining-Rig betrieben zu werden, da nur dort ansatzweise davon ausgegangen werden kann, den Break-even-Point zu erreichen und das in die Hardware investierte Geld wieder zu erwirtschaften.

Top-Szenarien

Die Szenarien 6.9.2 und 6.9.5 sind mithilfe der durchgeführten Bewertung als Top-Szenarien zu identifizieren. Wenngleich sie aus reiner Profit Sicht nicht die Top-Szenarien sind. Die Gründe hierfür liegen im niedrigeren Break-even-Point als auch an der guten Effizienz und dem geringen Stromverbrauch. Unter dem Kriterium Profit schneiden sie jedoch schlechter ab als beispielsweise Szenario 6.9.7. Ebenfalls hervorragend schneidet das Szenario 6.9.6 ab, jedoch in Bezug auf Szenario 6.9.5 schlechter aufgrund des höheren Stromverbrauchs. Die Ergebnisse zeigen, dass es zwei verschiedene Definitionen von Top-Szenarien gibt. Zum einen lässt sich Top-Szenario auf den Profit bezogen definieren. Dies würde bedeuten, dass das beste Szenario das Szenario ist, mit dem höchsten Profit. Zum anderen lässt sich jedoch ein Top-Szenario anhand von mehreren Kriterien, wie in diesem Kapitel ausgeführt, definieren.

Schwache-Szenarien

Es ist widersprüchlich, dass die profitabelsten Szenarien die schletesten Bewertungen bekommen. Auch wenn der Profit hoch gewichtet ist, bilden die restlichen Faktoren die Überhand. So erhalten alle Szenarien, die mit allen drei Grafikkarten durchgeführt werden, Bewertungswerte von -1,54 bis -1,96. Das Gleiche zeichnet sich auch unter den Übertaktungs-Szenarien ab. Wie kann das sein? Es wird eine leistungsstarke mit zwei mittel starken Karten betrieben, sodass die Leistung pro Karte unterhalb der leistungsstarken fällt. Das bedeutet eine schlechte Skalierung des Mining-Rigs mit mehreren Karten gleicher Art. Ebenso wird durch die Kombination unterschiedlicher Karten die Effizienz der ZOTAC GAMING GeForce RTX 2070 SUPER AMP gemindert und fällt folglich im Verbund von 0,21 auf 0,17 ab. Eine schlechtere Effizienz bedeutet auch mehr benötigte Leistung pro Hash, sodass der Stromverbrauch durchgängig mit -3 bewertet wird. Das Szenario 17 (vgl. Kapitel 6.7.3) und das Szenario 23 (vgl. Kapitel 6.8.3) schneiden am schletesten ab. Hier spielt die ineffizientere Mining-Software lolMiner eine weitere Rolle. Während der lolMiner unter Windows auch schwächere Ergebnisse liefert, so geht unter dem Linux-basiiernden Betriebssystem die Schere deutlich weiter auseinander. Am Ende ist der Bewertungswert eine gute Kennzahl für das Szenario, das am besten nach oben skalierbar ist. Gleichzeitig zeigt dieser Wert auch, welche Szenarien dafür nicht geeignet sind.

Bilanz

Über alle 34 Test-Szenarien inklusive den beiden Auto-Switching Szenarien hinweg ist ein Stromverbrauch von 307,49 kWh angefallen. Dieser wird verrechnet mit dem festgeschriebenen Strompreis pro Kilowattstunde von 0,26 €. Für die Unterhaltung des Mining-Rigs ergeben sich daraus Gesamtstromkosten in Höhe von 76,47 €. Insgesamt wurden Kryptowährungen, vorwiegend ETH, die dem Wert von 0,002106 BTC entsprechen geschürft. Das entspricht einem Betrag von 92,67 € mit dem festgeschriebenen Umrechnungsfaktor. Somit wurden in der Theorie 16,20 € Gewinn erwirtschaftet. Da im Laufe der Studienarbeit, der BTC- sowie der ETH-Kurs stetig am Fallen war, konnte in der Praxis kein Gewinn erzielt werden, was allerdings auch nicht Ziel dieser Arbeit ist.

8.2 Empfehlung

Aus den im Rahmen dieser Arbeit erlangten Erkenntnissen lässt sich eine Empfehlung für die Konzeptionierung eines neuen oder zusätzlichen Mining-Rigs aussprechen. Grundsätzlich haben die durchgeführten Szenarien gezeigt, dass die ZOTAC GAMING GeForce RTX 2070 SUPER AMP alleine aus Profit Sicht am besten abschneidet. Werden dabei das Windows Betriebssystem sowie die Mining-Software Phoenix Miner eingesetzt, verbessert sich der Profit nochmals. Dies kombiniert mit den vorgestellten Übertaktungsparametern stellt das beste Szenario der gesamten Arbeit dar. Zusätzlich ist anzumerken, dass die ZOTAC GAMING GeForce RTX 2070 SUPER AMP nicht wie andere Grafikkarten von Nvidia softwaretechnisch für Mining gesperrt ist. Ein weiterer wichtiger Faktor ist die Effizienzklasse des Netzteils sowie dessen Auslastung. Hier wird empfohlen, ein hoch zertifiziertes Netzteil zu nutzen, mindestens Gold, wobei mit Platinum oder Titanium eine noch höhere Effizienz erzielt werden kann. Die Auslastung des Netzteils sollte unter Last bei circa 50% bis max 80% liegen. Darüber oder darunter sinkt die Effizienz. Von Miningprogrammen wie NiceHash und deren AutoSwitching Funktion ist abzuraten, da diese in den durchgeführten Tests schlechter abschnitten als direktes Pool-Mining. Letztlich sind diese Programme für Einsteiger gedacht, deren Ziel es ist, unkompliziert Mining zu betreiben. Als Alternative zur ZOTAC GAMING GeForce RTX 2070 SUPER AMP Grafikkarte eignet sich eine beliebige Grafikkarte mit ähnlichem Effizienzwert und gleichen oder geringeren Anschaffungskosten.

9 Ausblick

9.1 Ethereum 2.0

Für das Jahr 2022 war und ist das große Update im Ethereum-Netzwerk angekündigt. Die "neue" Kryptowährung Ethereum 2.0 (ETH2) und die damit verbundene Umstellung des Konsensverfahrens Proof of Work (PoW) auf Proof of Stake (PoS) soll auf den Markt kommen. Das Wort neu ist dabei relativ zu betrachten, da ETH selbst kein Konkurrent zu ETH2 sein soll. Auch wird ETH mit der Einführung von ETH2 nicht wertlos sein. Geplant ist ein flüssiger Übergang von der einen Währung auf die neue, vergleichbar dem Übergang der Deutschen Mark auf den Euro. Auf dem Zeitplan war dieses Vorhaben bis Juni 2022 eingeplant. Dafür ist eine Verschmelzung der Beacon-Cain und dem Ethereum-Mainnet notwendig. Mit der Bacon-Chain wird PoS in das Ethereum-Ökosystem eingeführt. Sie übernimmt die Koordination und Verknüpfung des Netzwerks der Shards und Staker. Aber sie ist nicht mit dem Ethereum-Mainnet von heute vergleichbar, da sie keine Konten oder Smart Contracts verarbeitet. [80] [81]

Im ersten Schritt sollen Beacon-Chain und das Ethereum-Mainnet getrennt voneinander existieren, allerdings funktional miteinander verbunden sein. Der Plan ist, das Mainnet mit dem PoS-System zu "verschmelzen", das von der Beacon-Chain kontrolliert und koordiniert wird. Nach der erfolgreichen Verschmelzung sollen dann im zweiten Schritt die sogenannten Shard-Chains etabliert werden. Die Intension dahinter ist, die Kapazität des Netzwerks zu erhöhen und zugleich die Transaktionsgeschwindigkeit zu verbessern. Für die Umsetzung soll das Netzwerk auf 64 Blockchains erweitert werden. Für diesen Schritt ist eine funktionsfähige Beacon-Chain die Grundlage. Allerdings haben sich die Betreiber für die Verschmelzung mehr Zeit eingeräumt, um eben jene neue Beacon-Chain gründlich zu prüfen. Demnach ist frühestens im dritten Quartal 2022 mit ETH2 zu rechnen. [82]

9.2 Energiekosten in Zukunft

Deutschland ist Weltmeister beim Strompreis. In keinem anderen Land der Welt kostet der Strom so viel wie in Deutschland. Der Durchschnittsstrompreis betrug vor der Kriegserklärung von Russland an die Ukraine 0,32 € pro kWh. Durch dieses Ereignis, mit globalen Folgen in Bezug auf Energieengpässe und Inflation, gibt es lokale Strompreise von über 0,40 € pro kWh. Die globale Klimakrise, das Atomreaktorunglück nach einem Tsunami in Fukushima 2011 und der damit verbundene Atomausstieg der Regierung machen uns Deutsche zum Rekordhalter in Sachen Energiekosten. Abbildung 9.1 verdeutlicht die Zusammensetzung der aktuellen Stromkosten in einem Kreisdiagramm [9].

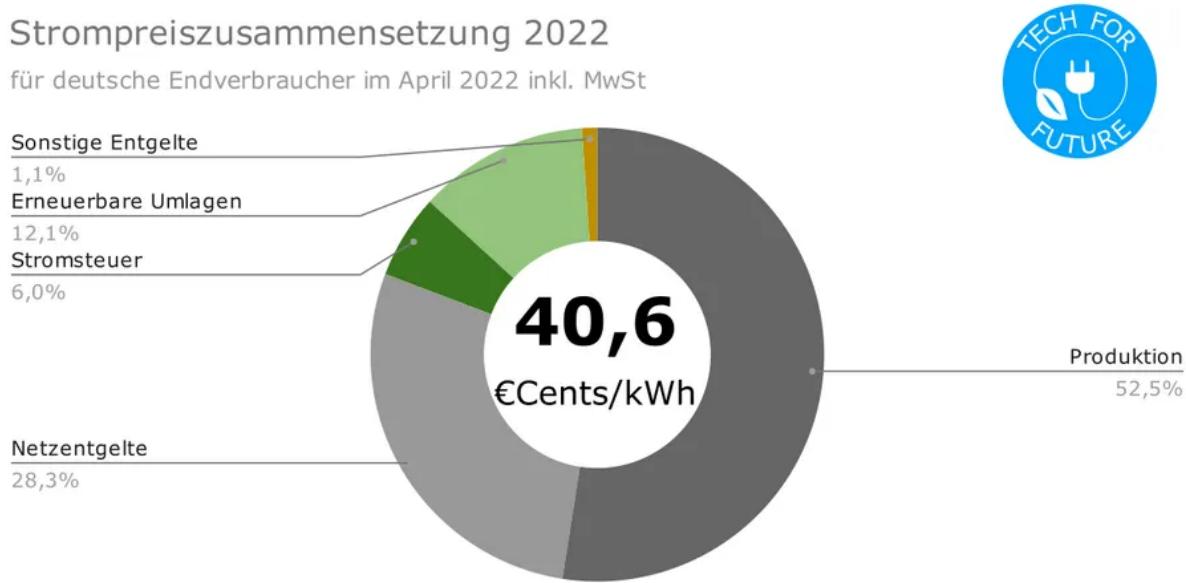


Abbildung 9.1: Zusammensetzung der Stromkosten im April 2022 in Deutschland [9]

Die Stromkosten im April 2022 in Deutschland setzen sich wie folgt zusammen:

- 21,3 €Cents/kWh Produktion & Bereitstellung
- 11,5 €Cents/kWh Netzentgelt, Konzessionsabgabe & StromNEV-Umlage
- 4,9 €Cents/kWh EEG-Umlage & Offshore-Haftungsumlage
- 2,4 €Cents/kWh Energiesteuer auf Strom
- 0,4 €Cents/kWh KWK-Aufschlag & Umlage für abschaltbare Lasten

Im Folgenden zeigt Abbildung 9.2 die Strompreisentwicklung seit dem Jahr 2000.

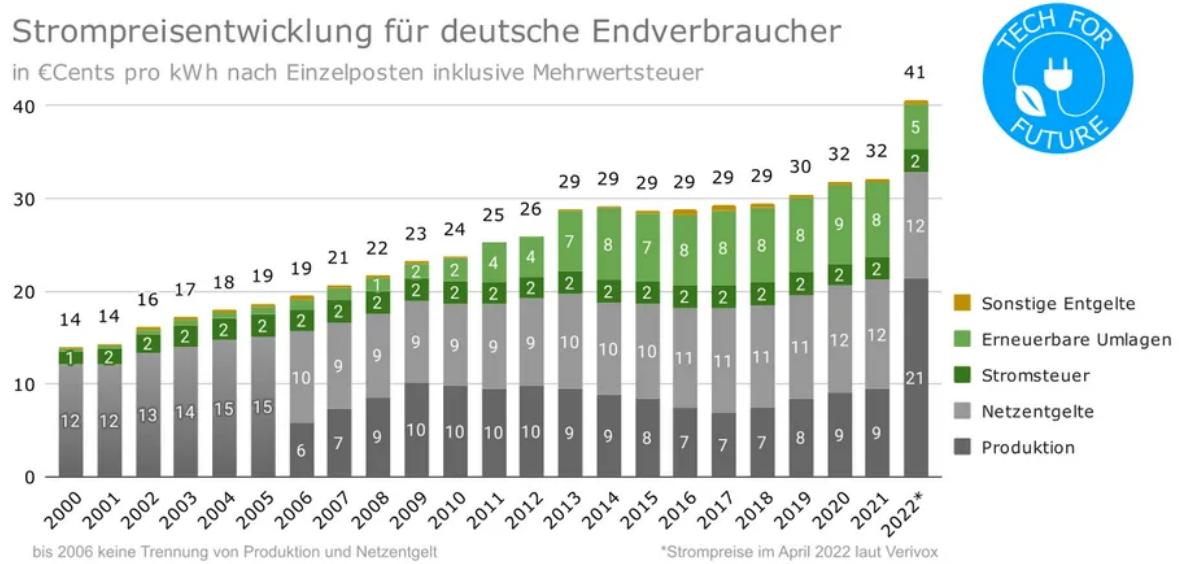


Abbildung 9.2: Strompreisentwicklung von 2000 bis 2022 [9]

Der Strompreis hat sich seit 2000 mit 13,9 €Cents/kWh bis heute verdreifacht. Im Schnitt steigt er pro Jahr um 6%. Der Sprung von 2021 auf 2022 ist mit 28 Prozent dagegen gewaltig. Die oben genannten Gründe ergeben dieses Resultat. Die genaue Preisentwicklung in naher Zukunft kann aufgrund der aktuellen Weltgeschehnisse keiner vorhersagen. Statistisch gesehen wird auch in Zukunft der Strompreis pro Jahr sechs Prozent oder mehr zunehmen in Deutschland. Nur eine komplett anders geführte Politik oder eine bahnbrechende technische Innovation zur Stromerzeugung wie die "Kernspaltung 2.0" oder Kernfusion kann die Stromkosten senken. Mit diesen Aussichten ist und bleibt Kryptomining in Deutschland eher ein Hobby als ein lukrativer Trend. Zum Vergleich dazu verdeutlicht eine Auflistung die Strompreise aus den Top-Kryptomining-Ländern vor Kriegsbeginn [9].

- 22,6 €Cents/kWh Irland
 - 12,3 €Cents/kWh USA
 - 9,3 €Cents/kWh Kanada
 - 5,0 €Cents/kWh Russland
 - 4,8 €Cents/kWh Malaysia
 - 3,4 €Cents/kWh Kasachstan

Die aufgeführten Stromkosten zielen auf Privatpersonen und deren privaten Nutzung ab. Wer ein Gewerbe betreibt, kann und darf Industriestrom beziehen. Industriestrom ist in der Regel günstiger. Der Killowattstundenpreis für Industriestrom ist abhängig von Region und Bezugsgröße. In Sachen Industriestrompreis ist Deutschland im weltweiten Vergleich ebenfalls Weltmeister und verdeutlicht Abbildung 9.3. [10]

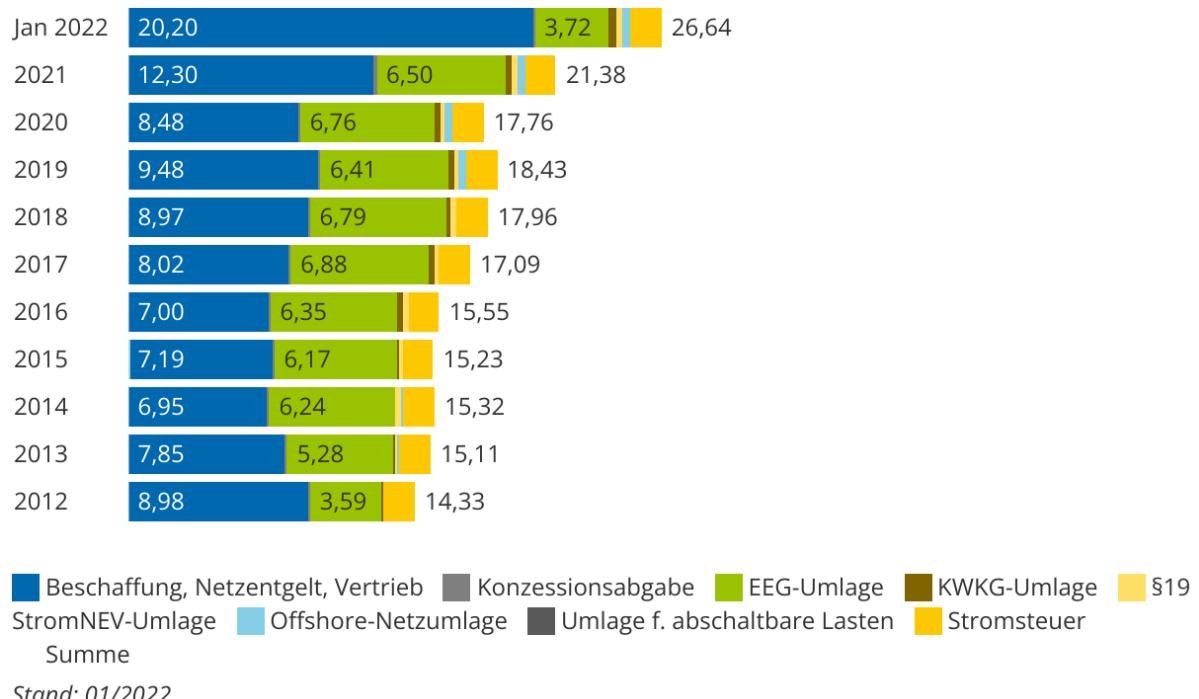


Abbildung 9.3: Industriestrompreis Deutschland im Januar 2022 [10]

9.3 Mining in der Zukunft

Das Mining der Zukunft wird sich wandeln müssen. Die virtuellen Güter bzw. Kryptowährungen beanspruchen Unmengen von Energien, ein Wert aus dem Jahr 2021 summiert über 120 Terawattstunden pro Jahr. Das übersteigt den Wert, den die Niederlande im Jahr verbraucht. Den größten Anteil davon trägt China dazu bei. Zum Vergleich verbraucht Deutschland jährlich rund 525 Terawattstunden. In Sachen Klimaschutz ist Kryptomining für viele Experten deswegen unbegreiflich und eher ein Gegenspieler. Allerdings steckt hinter den Kryptowährungen die Idee, das Finanzsystem fairer und transparenter zu machen. Neue Technologien stehen anfangs immer in der Kritik und solange der Leitsatz gilt - Geld regiert die Welt - steht der Klimaschutz zumindest hinten an, bis er zur

realen, spürbaren Bedrohung wird. Der CO₂-Fußabdruck von Kryptomining ist nicht unerheblich, deswegen fordern Experten eine Regulierung von Kryptomining. So ist allerdings abzusehen, dass sich Kryptowährungen, die energieeffizienter sind, auf Dauer durchsetzen werden. Bis es so weit ist, werden die Krypto-Miner sich immer mehr auf Billigstrom-Länder fokussieren und versuchen, so viel Geld wie möglich damit zu verdienen. Dieses Vorgehen nimmt teilweise mafiose Zustände an, sodass das Kryptomining eine große Mitschuld am weltweiten Halbleiter-Chip-Mangel und besonders am Grafikkarten-Mangel hat. Der Kryptomarkt wird weiter wachsen und möglicherweise ist es denkbar, dass sich irgendwann eine Kryptowährung durchsetzt, mit der wir all unsere Finanzen von morgen regeln [83] [84].

Evaluation eines Crypto Mining Systems**Dominik Klein & Robin Weisenburger**

A Anhang

A.1 Anhang Bewertungsmatrix

Kriterium		Szenario	Gewichtung	Windows 10 Pro													
				1	2	3	4	5	6	7	8	9	10	11	12	13	14
Hardware-Kosten	0,10	0,10	3	3	2	2	-1	-1	-3	3	3	2	2	-1	-1	-3	
Stromverbrauch	0,20	0,20	3	3	3	0	0	0	-3	3	3	3	0	0	0	0	-3
Hashrate	0,15	0,15	-3	-3	-2	-1	0	0	2	-3	-3	-2	-1	0	0	0	2
Effizienz	0,15	0,15	-3	-3	-1	-3	-2	-2	-3	-3	-3	-1	-3	-2	-2	-2	-3
Break-Even-Point	0,10	0,10	-3	-3	-1	-3	-2	-2	-3	-3	-3	-1	-3	-2	-2	-2	-3
Miner	0,01	0,01	-3	-3	-3	-3	-3	-3	-3	3	3	3	3	3	3	3	3
Profit	0,29	0,29	-3	-3	-1	-3	-1	-1	-1	-3	-3	-1	-3	-1	-1	-1	-1
Gesamt	1,00	1,00	-1,20	-1,20	-0,07	-1,60	-0,92	-0,92	-1,67	-1,14	-1,14	-0,01	-1,54	-0,86	-0,86	-1,61	

Kriterium		Szenario	Gewichtung	Ubuntu Linux				HiveOS				Windows 10 Pro OC								
				15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Hardware-Kosten	0,10	0,10	1	-1	-3	1	-1	-3	1	-1	-3	1	-1	-3	1	-1	-3	1	-1	-3
Stromverbrauch	0,20	0,20	3	0	-3	3	0	-3	3	0	-3	3	0	-3	3	1	-2	3	1	-2
Hashrate	0,15	0,15	-2	0	2	-2	0	2	-2	0	2	-2	0	2	-2	1	3	-2	1	3
Effizienz	0,15	0,15	-1	-2	-3	-1	-2	-3	-1	-2	-3	-1	-2	-3	3	1	0	3	1	0
Break-Even-Point	0,10	0,10	-1	-2	-3	-1	-2	-3	-1	-2	-3	-1	-2	-3	3	3	3	3	3	3
Miner	0,01	0,01	-3	-3	-3	3	3	3	3	3	3	3	3	3	-3	-3	3	3	3	3
Profit	0,29	0,29	-1	-1	-2	-1	-1	-2	-1	-2	-1	-1	-2	-1	-1	1	2	3	1	2
Gesamt	1,00	1,00	-0,17	-0,92	-1,96	-0,11	-0,86	-1,61	-0,46	-0,92	-1,96	-0,11	-0,86	-1,61	-1,41	1,25	0,89	1,47	1,31	0,95

A.2 Anhang Break-even-Point Matrix

Betriebs- system	Szenarios	Profit/Tag	GPU-Kosten	Gesamt-Kosten	BEP-GPU		BEP- System		Effizienz	Effizienz pro Euro (GPU)	Hashrate	Hashrate pro Euro (GPU)
					Tag	Jahre	Tag	Jahre				
Windows	1	-0,02 €	300,00 €	2.261,86 €	-	-	-	-	0,15	0,000050	26,65	0,089
	2	-0,17 €	254,11 €	2.215,97 €	-	-	-	-	0,15	0,000059	22,91	0,090
	3	0,39 €	583,99 €	2.545,85 €	1497	4,1	6528	17,9	0,21	0,000036	36,87	0,063
	4	-0,02 €	554,11 €	2.515,97 €	-	-	-	-	0,15	0,000027	49,99	0,090
	5	0,53 €	883,99 €	2.845,85 €	1668	4,6	5370	14,7	0,18	0,000020	63,51	0,072
	6	0,43 €	838,10 €	2.799,96 €	1949	5,3	6512	17,8	0,18	0,000021	60,22	0,072
	7	0,51 €	1.138,10 €	3.099,96 €	2232	6,1	6078	16,7	0,17	0,000015	86,85	0,076
	8	0,00 €	300,00 €	2.261,86 €	-	-	-	-	0,15	0,000050	27,70	0,092
	9	-0,16 €	254,11 €	2.215,97 €	-	-	-	-	0,15	0,000059	24,62	0,097
	10	0,43 €	583,99 €	2.545,85 €	1358	3,7	5921	16,2	0,21	0,000036	37,17	0,064
	11	-0,03 €	554,11 €	2.515,97 €	-	-	-	-	0,15	0,000027	52,40	0,095
	12	0,55 €	883,99 €	2.845,85 €	1607	4,4	5174	14,2	0,18	0,000020	64,87	0,073
	13	0,45 €	838,10 €	2.799,96 €	1862	5,1	6222	17,0	0,18	0,000021	61,83	0,074
	14	0,57 €	1.138,10 €	3.099,96 €	1997	5,5	5439	14,9	0,17	0,000015	89,48	0,079
Linux	15	0,39 €	583,99 €	2.545,85 €	1497	4,1	6528	17,9	0,21	0,000036	36,93	0,063
	16	0,48 €	883,99 €	2.845,85 €	1842	5,0	5929	16,2	0,18	0,000020	63,65	0,072
	17	0,36 €	1.138,10 €	3.099,96 €	3161	8,7	8611	23,6	0,17	0,000015	87,07	0,077
	18	0,43 €	583,99 €	2.545,85 €	1358	3,7	5921	16,2	0,21	0,000036	37,15	0,064
	19	0,56 €	883,99 €	2.845,85 €	1579	4,3	5082	13,9	0,18	0,000020	65,19	0,074
	20	0,55 €	1.138,10 €	3.099,96 €	2069	5,7	5636	15,4	0,17	0,000015	90,11	0,079
HiveOS	21	0,37 €	583,99 €	2.545,85 €	1578	4,3	6881	18,9	0,21	0,000036	36,93	0,063
	22	0,44 €	883,99 €	2.845,85 €	2009	5,5	6468	17,7	0,18	0,000020	63,67	0,072
	23	0,32 €	1.138,10 €	3.099,96 €	3557	9,7	9687	26,5	0,17	0,000015	87,10	0,077
	24	0,41 €	583,99 €	2.545,85 €	1424	3,9	6209	17,0	0,21	0,000036	37,15	0,064
	25	0,52 €	883,99 €	2.845,85 €	1700	4,7	5473	15,0	0,18	0,000020	65,19	0,074
	26	0,49 €	1.138,10 €	3.099,96 €	2323	6,4	6326	17,3	0,17	0,000015	90,11	0,079
Windows OC	27	0,94 €	583,99 €	2.545,85 €	621	1,7	2708	7,4	0,34	0,000058	42,63	0,073
	28	1,44 €	883,99 €	2.845,85 €	614	1,7	1976	5,4	0,27	0,000031	73,70	0,083
	29	1,69 €	1.138,10 €	3.099,96 €	673	1,8	1834	5,0	0,24	0,000021	101,08	0,089
	30	0,98 €	583,99 €	2.545,85 €	596	1,6	2598	7,1	0,34	0,000058	42,98	0,074
	31	1,46 €	883,99 €	2.845,85 €	605	1,7	1949	5,3	0,27	0,000031	74,60	0,084
	32	1,76 €	1.138,10 €	3.099,96 €	647	1,8	1761	4,8	0,24	0,000021	103,11	0,091

A.3 Anhang Bewertungsschwellenwerte

Einstufung ab	Stromverbrauch Gesamt [kWh]	Hashrate [MH/s]	Effizienz [MH/s/W]	Profit / Tag [€]	Break-Even- Point [Jahre]	Gesamt-Kosten [€]	Miner
3	160,00	91,65	0,31	1,48	4,83	2215,97	Phoenix Miner
2	220,57	80,20	0,29	1,21	7,93	2342,25	
1	281,14	68,74	0,26	0,93	11,03	2468,54	
0	341,71	57,28	0,23	0,66	14,13	2594,82	
-1	402,29	45,82	0,20	0,38	17,24	2721,11	
-2	462,86	34,37	0,18	0,11	20,34	2847,39	
-3	523,43	22,91	0,15	-0,17	23,44	2973,68	Iol Miner

Literaturverzeichnis

- [1] *Bitcoin Backups.* <https://shiftcrypto.ch/blog/so-funktionieren-bitcoin-backups-5-haufige-fehler-und-wie-du-diese-vermeidest/>, o. J. [Online], Zugriff am 11.01.2022.
- [2] *Wie funktioniert eine Blockchain?* <https://www.bitpanda.com/academy/de/lektionen/wie-funktioniert-eine-blockchain/>, o. J. [Online], Zugriff am 10.01.2022.
- [3] Shubhani Aggarwal. *The Blockchain technology for secure and smart applications across industry verticals.* Advances in Computers ; Volume 121. Academic Press, Cambridge, Massachusetts, 2021.
- [4] *Etherscan Blockchain Explorer.* <https://etherscan.io/address/0x0a161c1d37545e77b193681686808e0026b6ebbb>. [Online], Zugriff am 11.05.2022.
- [5] Michaela [VerfasserIn] Hönig. *ICO und Kryptowährungen : neue digitale Formen der Kapitalbeschaffung,* [2020].
- [6] Mark Mantel. *Kryptowährung Ethereum: ETH2 ist tot, lang lebe ETH Consensus Layer.* <https://www.heise.de/news/Kryptowaehrung-Ethereum-ETH2-ist-tot-lang-lebe-ETH-Consensus-Layer-6339598.html>, 2022. [Online], Zugriff am 26.01.2022.
- [7] *Ring Signatures And Anonymisation.* <https://medium.com/a-security-site-when-bob-met-alice/ring-signatures-and-anonymisation-c9640f08a193>. [Online], Zugriff am 01.02.2022.
- [8] *Wie man Ethereum abbaut.* <https://ichi.pro/de/wie-man-ethereum-abbaut-update-auf-meinem-1-000-ethereum-mining-rig-build-231082374192670>. [Online], Zugriff am 18.03.2022.

- [9] Florian Blümm. *Strompreisentwicklung Deutschland 2022: Warum steigen die Stromkosten?* <https://www.tech-for-future.de/strompreisentwicklung/>, April 2022. [Online], Zugriff am 12.05.2022.
- [10] *Strompreise für Unternehmen: Was die aktuelle Strompreisentwicklung mit sich bringt.* <https://www.eha.net/blog/details/strompreise-unternehmen.html>, April 2022. [Online], Zugriff am 12.05.2022.
- [11] *Top 100 Kryptowährungen nach Börsenwert.* <https://coinmarketcap.com/de/>. [Online], Zugriff am 11.05.2022.
- [12] *Kryptowährung im Aufwind.* <https://de.statista.com/infografik/1939/marktkapitalisierung-von-kryptowaehrungen/>, August 2021. [Online], Zugriff am 13.01.2022.
- [13] Rabe. *Entwicklung des Bitcoin-Kurses von Januar 2017 bis Januar 2022.* <https://de.statista.com/statistik/daten/studie/781906/umfrage/kursentwicklung-des-bitcoin-gegenueber-dem-euro/>, 2022. [Online], Zugriff am 13.01.2022.
- [14] Mark Mantel. *Teure Grafikkarten: Nvidia-CEO erwartet Lieferengpässe bis Ende 2022.* <https://www.heise.de/news/Teure-Grafikkarten-Nvidia-CEO-erwartet-Lieferengpaesse-bis-Ende-2022-6170174.html>, 2021. [Online], Zugriff am 13.01.2022.
- [15] Bundesamt für Sicherheit in der Informationstechnik. *Blockchain macht Daten praktisch unveränderbar.* https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html, o. J. [Online], Zugriff am 12.01.2022.
- [16] Julian Hosp. *Kryptowährungen: Bitcoin, Ethereum, Blockchain.* FinanzBuch Verlag, 2018.
- [17] Bundesanstalt für Finanzdienstleistungsaufsicht. *Virtuelle Währungen.* https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html, 2020. [Online], Zugriff am 10.01.2022.
- [18] Bundesministerium der Finanzen. *Umsatzsteuerliche Behandlung von Bitcoin und anderen sog. virtuellen Währungen.* <https://www.bundesfinanzministerium.de>

- de/Content/DE/Downloads/BMF_Schreiben/Steuerarten/Umsatzsteuer/Umsatzsteuer-Anwendungserlass/2018-02-27-umsatzsteuerliche-behandlung-von-bitcoin-und-anderen-sog-virtuellen-waehrungen.html, 2018. [Online], Zugriff am 13.01.2022.
- [19] *Bitcoin Wallet - Private keys und Seeds*. <https://bitcoin-uni.de/wallet-seed-privatekey.html>, o. J. [Online], Zugriff am 11.01.2022.
- [20] *Bitcoin Seed Phrase*. https://en.bitcoin.it/wiki/Seed_phrase, o. J. [Online], Zugriff am 11.01.2022.
- [21] *Bitcoin Wallet: Was ist sicher?* <https://www.gdata.de/ratgeber/bitcoin-wallet-schutz>, o. J. [Online], Zugriff am 11.01.2022.
- [22] Andreas M. [VerfasserIn] Antonopoulos. *Bitcoin und Blockchain - Grundlagen und Programmierung : die Blockchain verstehen, Anwendungen entwickeln*. O'Reilly, Heidelberg, 2. Auflage, 2018.
- [23] *What are the different types of cryptocurrency wallets?* https://www.europeanbusinessreview.com/what-are-the-different-types-of-cryptocurrency-wallets/?__cf_chl_f_tk=zImu9siATH4AB3XsLkEx_DsAWvP.kLpVfnvY7jtntS4-1642337946-0-gaNycGzNCH0, 2021. [Online], Zugriff am 13.01.2022.
- [24] *Watch-Only Wallet*. <https://river.com/learn/terms/w/watch-only-bitcoin-wallet/>. [Online], Zugriff am 16.01.2022.
- [25] *Storing Bitcoins*. https://en.bitcoin.it/wiki/Storing_bitcoins, o. J. [Online], Zugriff am 11.01.2022.
- [26] *Cold storage*. https://en.bitcoin.it/wiki/Cold_storage. [Online], Zugriff am 13.01.2022.
- [27] *The different types of crypto wallets, explained*. <https://azbigmedia.com/business/the-different-types-of-crypto-wallets-explained/>. [Online], Zugriff am 16.01.2022.
- [28] *What Is a Multisig Wallet?* <https://academy.binance.com/en/articles/what-is-a-multisig-wallet>, 2020. [Online], Zugriff am 16.01.2022.

- [29] *How do hardware wallets work?* <https://zipmex.com/learn/how-do-hardware-wallets-work/>, 2020. [Online], Zugriff am 16.01.2022.
- [30] Jörg Platzer. *Bitcoin - kurz und gut*. O'Reilly, 2014.
- [31] *Bitcoin Core Download*. <https://bitcoin.org/de/download>, o.J. [Online], Zugriff am 11.01.2022.
- [32] Jake Frankenfield. *Cryptocurrency Difficulty*. <https://www.investopedia.com/terms/d/difficulty-cryptocurrencies.asp>, June 2021. [Online], Zugriff am 10.04.2022.
- [33] finanzen.net. *Bitcoin - Euro Kurs*. <https://www.finanzen.net/devisen/bitcoin-euro-kurs>, 2022. [Online], Zugriff am 16.01.2022.
- [34] *Proof of Stake*. <https://www.btc-echo.de/academy/bibliothek/proof-of-stake/>. [Online], Zugriff am 16.01.2022.
- [35] Keira Wright. *Unwahrscheinlich ist noch untertrieben: Zweiter Miner löst alleine Block*. <https://de.cointelegraph.com/news/1-in-a-billion-second-tiny-miner-solves-a-block>, 2022. [Online], Zugriff am 17.01.2022.
- [36] *Definition Proof of Activity (PoA)*. <https://www.blockchain-insider.de/was-ist-proof-of-activity-poa-a-954104/>, o.J. [Online], Zugriff am 23.01.2022.
- [37] Iddo Bentov, Charles Lee, Alex Mizrahi, und Meni Rosenfeld. *Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]* y. *ACM SIGMETRICS Performance Evaluation Review*, 42(3):34–37, 2014. [Online], Zugriff am 23.01.2022.
- [38] *What Is Proof-of-Activity (PoA)?* <https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp>, o.J. [Online], Zugriff am 23.01.2022.
- [39] *Definition Proof of Capacity (PoC)*. <https://www.blockchain-insider.de/was-ist-proof-of-capacity-poc-a-954183/>, o.J. [Online], Zugriff am 23.01.2022.
- [40] Changqiang Zhang, Cangshuai Wu, und Xinyi Wang. *Overview of Blockchain consensus mechanism*. In *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, pages 7–12, 2020.
- [41] *Proof of Capacity (Cryptocurrency)*. <https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp>, o.J. [Online], Zugriff am 23.01.2022.

- [42] *Bitcoin Kurs.* <https://www.blockchaincenter.net/bitcoin/bitcoin-kurs/>. [Online], Zugriff am 23.01.2022.
- [43] *51% Attacke.* <https://wwwbtc-echo.de/academy/bibliothek/51-attacke/>. [Online], Zugriff am 23.01.2022.
- [44] *Was ist ein 51% Angriff und wie wird er verhindert?* <https://wwwbtc-echo.de/academy/bibliothek/51-attacke/>. [Online], Zugriff am 23.01.2022.
- [45] *Schützen Sie Ihre Privatsphäre.* <https://bitcoin.org/de/schuetzen-sie-ihre-privatsphaere>. [Online], Zugriff am 23.01.2022.
- [46] Prof. Dr. Michaela Hönig. *Studie zu Kryptowährungen und der Blockchain-Technologie.* https://www.frankfurt-university.de/fileadmin/standard/Hochschule/Fachbereich_3/Kontakt/Professor_inn_en/Hoenig/20180502_Bitcoin_Studie_fra_uas_Hoenig_V1.0.pdf, May 2018. [Online], Zugriff am 01.02.2022.
- [47] *Bitcoin & Blockchain - Grundlagen und Programmierung : Die Blockchain verstehen, Anwendungen entwickeln*, 2018.
- [48] *Ethereum.* <https://wwwbtc-echo.de/academy/bibliothek/ethereum-2/>, o. J. [Online], Zugriff am 25.01.2022.
- [49] *Today's Cryptocurrency Prices by Market Cap.* <https://coinmarketcap.com/>, January 2022. [Online], Zugriff am 25.01.2022.
- [50] *What is the Ethash mining algorithm?* <https://academy.bit2me.com/en/what-is-the-algorithm-of-ethash-mining/>, o. J. [Online], Zugriff am 26.01.2022.
- [51] *Tether (USDT).* <https://wwwbtc-echo.de/academy/bibliothek/tether-usdt/>, o. J. [Online], Zugriff am 01.02.2022.
- [52] Jannis Grunewald. *Chia Coin.* <https://coincierge.de/2021/chia-coin-xch-kurs-prognose-80-rueckgang-jetzt-einsteigen-oder-nie/>, 2021. [Online], Zugriff am 16.02.2022.
- [53] Chia. *Chia Whitepaper.* <https://www.chia.net/assets/Chia-Business-Whitepaper-2021-02-09-v1.0.pdf>, 2021. [Online], Zugriff am 16.02.2022.

- [54] Jarred Walton. *How to Farm Chia Coin, Now With Pooling.* <https://www.tomshardware.com/how-to/how-to-farm-chia-coin-the-new-storage-based-cryptocurrency>, 2021. [Online], Zugriff am 17.02.2022.
- [55] *Über Monero.* <https://www.getmonero.org/de/resources/about/index.html>. [Online], Zugriff am 01.02.2022.
- [56] *What Is Monero (XMR)? - An In-Depth Guide to the Privacy Coin.* <https://coincentral.com/what-is-monero/>, 2019. [Online], Zugriff am 01.02.2022.
- [57] *ASIC-Miner, die Spezialisten des Minings.* <https://www.blocktrainer.de/blocktrainer-1x1/was-sind-asic-miner/>, o.J. [Online], Zugriff am 16.02.2022.
- [58] SSD-Tester. *Welche SSD nimmt man zum Chia Plotten (wegen TBW)?* https://ssd-tester.de/text_gute_ssd_fuers_chia_plotten.php. [Online], Zugriff am 17.03.2022.
- [59] GIGA. *Chia Coin (XCH): Plotting, Farming, SSD-Wahl und meine bisherigen Erfahrungen.* https://ssd-tester.de/text_gute_ssd_fuers_chia_plotten.php. [Online], Zugriff am 17.03.2022.
- [60] Was ist CUDA? <https://www.bigdata-insider.de/was-ist-cuda-a-851005/>, 2019. [Online], Zugriff am 17.03.2022.
- [61] Dipl. Math. F. Braun. *OpenCL - Open Computing Language.* https://homepages.uni-regensburg.de/~brf09510/EDV/kurs_info/brf09510/hpc/opencl/opencl.html, 2019. [Online], Zugriff am 19.03.2022.
- [62] What is OpenCL? <https://streamhpc.com/knowledge/what-is/opencl/>. [Online], Zugriff am 19.03.2022.
- [63] Was ist ein Mining-Pool? Solo- vs. Pool-Mining. <https://bitcoin-live.de/was-ist-ein-mining-pool-solo-vs-pool-mining/>, September 2018. [Online], Zugriff am 23.03.2022.
- [64] Stratum Protocol. <https://reference.cash/mining/stratum-protocol>. [Online], Zugriff am 10.04.2022.
- [65] Mining Protocol Stratum. <https://braiins.com/stratum-v1/docs>. [Online], Zugriff am 10.04.2022.

- [66] *Technische Daten - Corsair RM850.* [http://www.netzteil-test.de/80-plus-netzteile-was-ist-das-und-lohnt-sich-das/](https://www.corsair.com/de/de/Kategorien/Produkte/Netzger\protect\unhbox\voidb@x\bgroup\U@D1ex{\setbox\z@\hbox{\char127}\dimen@-.45ex\advance\dimen@\ht\z@\}\accent127\fontdimen5\font\U@Da\egroupte/Hochleistungs-Netzger\protect\unhbox\voidb@x\bgroup\U@D1ex{\setbox\z@\hbox{\char127}\dimen@-.45ex\advance\dimen@\ht\z@\}\accent127\fontdimen5\font\U@Da\egroupte/RM-Series-80-PLUS-Gold-Power-Supplies/p/CP-9020196-EU#tab-tech-specs. [Online], Zugriff am 19.03.2022.</p><p>[67] <i>Was ist 80 PLUS und lohnt sich das?</i> <a href=). [Online], Zugriff am 19.03.2022.
- [68] *Intel Core i7-4770K Prozessor Spezifikationen.* <https://www.intel.de/content/www/de/de/products/sku/75123/intel-core-i74770k-processor-8m-cache-up-to-3-90-ghz/specifications.html>. [Online], Zugriff am 19.03.2022.
- [69] *ROG-STRIX-RX580-O8G-GAMING Technische Daten.* <https://rog.asus.com/de/graphics-cards/graphics-cards/rog-strix/rog-strix-rx580-o8g-gaming-model/spec>. [Online], Zugriff am 19.03.2022.
- [70] *8GB PowerColor Radeon RX 580 Technische Daten.* https://www.mindfactory.de/product_info.php/8GB-PowerColor-Radeon-RX-580-Red-Dragon-Aktiv-PCIe-3-0-x16--Retail-_1167666.html. [Online], Zugriff am 19.03.2022.
- [71] *ZOTAC GAMING GeForce RTX 2070 SUPER AMP Extreme Technische Daten.* https://www.zotac.com/at/product/graphics_card/zotac-gaming-geforce-rtx-2070-super-amp-extreme#spec. [Online], Zugriff am 19.03.2022.
- [72] *NiceHash Plugins.* <https://github.com/nicehash/NiceHashMiner/blob/master/doc/Plugins/Plugins.md>. [Online], Zugriff am 23.03.2022.
- [73] *Algorithms supported by Awesome Miner.* <https://www.awesomeminer.com/algorithm-list>. [Online], Zugriff am 23.03.2022.
- [74] *BetterHash.* <https://www.betterhash.net/>. [Online], Zugriff am 23.03.2022.
- [75] Ulrich Wöhe. *Einführung in die Allgemeine Betriebswirtschaftslehre*. Verlag Vahlen, München, 22. Auflage, 2005.

- [76] Statistisches Bundesamt. *Erdgas- und Stromdurchschnittspreise*. https://www.destatis.de/DE/Themen/Wirtschaft/Preise/Erdgas-Strom-DurchschnittsPreise/_inhalt.html. [Online], Zugriff am 19.03.2022.
- [77] Kann ich an meine eigene Bitcoin-Geldbörse bezahlt werden? <https://www.nicehash.com/support/mining-help/earnings-and-payments/can-i-get-paid-to-an-external-wallet-address>. [Online], Zugriff am 19.03.2022.
- [78] *TPLink Energy Monitor GitHub Projekt*. <https://github.com/jamesbarnett91/tplink-energy-monitor>, 2019. [Online], Zugriff am 11.05.2022.
- [79] *AMD GPU Power Profiles*. <https://wiki.archlinux.org/title/AMDGPU>. [Online], Zugriff am 11.05.2022.
- [80] Ethereum 2.0: Zusammenführung der beiden Chains lässt weiter auf sich warten. <https://t3n.de/news/ethereum-20-zusammenfuehrung-1466172/>, April 2022. [Online], Zugriff am 11.05.2022.
- [81] ETH 2.0: Das große Ethereum-Upgrade kommt später. <https://www.computerbild.de/artikel/cb-News-Finanzen-ETH-2.0-Ethereum-Upgrade-kommt-spaeter-32490585.html>, April 2022. [Online], Zugriff am 12.05.2022.
- [82] Die Beacon Chain. <https://ethereum.org/de/upgrades/beacon-chain/>. [Online], Zugriff am 12.05.2022.
- [83] Ruby Layram. Ist die Zukunft von Bitcoin das Mining zu Hause? <https://cryptomonday.de/news/2021/09/27/ist-die-zukunft-von-bitcoin-das-mining-zu-hause/>, May 2022. [Online], Zugriff am 12.05.2022.
- [84] Thomas Spinnler. *Stromfresser Bitcoin*. <https://www.tagesschau.de/wirtschaft/technologie/stromfresser-bitcoin-mining-101.html>, February 2021. [Online], Zugriff am 12.05.2022.