Anreize in Mining-Pools

Ulrich Schmidt
Westfälische Wilhelms-Universität Münster
Institut für Wirtschaftsinformatik
Leonardo-Campus 3
48149 Münster
uli.schmidt@uni-muenster.de

ABSTRACT
Mining in der dezentralen digitalen P2P-Währung Bitcoin hat die Funktion des Bestätigens von Transaktionen, um Betrugsversuche aufzudecken. Mit dem Mining ist ein hoher Rechenaufwand verbunden, um einmal bestätigte Transaktionen nicht wieder als ungültig erklären zu können. Um diesem System einen Anreiz zu geben, gibt es für jeden gefundenen Block, der einzelne Transaktionen bündelt, einen Reward von momentan 25 Bitcoins. Damit werden durch das Mining zeitgleich neue Bitcoins erschaffen. Da es sich für Teilnehmer des Netzwerks kaum noch lohnt, alleine zu minen, haben sich sogenannte Mining-Pools entwickelt, in denen gemeinsam nach einem gültigen Block gesucht wird. Wenn dieser Block gefunden ist, muss der Reward unter den Beteiligten gerecht verteilt werden, je nachdem wie sehr sie an der Findung des passenden Hashes beteiligt waren. Dieser Prozess ist keineswegs trivial und es gibt zahlreiche Verteilungsmechanismen, die zum Teil anfällig für Missbrauch sind. Das gibt manchen Teilnehmern einen Anreiz, sich opportunistisch zu verhalten, um einen höheren Gewinn zu erzielen. In diesem Paper werden die gängigen Varianten der Verteilung auf die gerechte Verteilung untersucht und es kann gezeigt werden, dass insbesondere eine intuitive Methode nicht sehr sicher gegen solche Angriffe ist. Mit diesen Erkenntnissen können Mining-Pool Betreiber Methoden einsetzen, die für die Teilnehmer fair sind.

Keywords
Bitcoin, Mining-Pools, Verteilungsmechanismen, Anreize.

Münster Bitcoin Conference (MBC), 17-18 July ‘13, Münster, Germany

1. EINLEITUNG
Die dezentrale digitale P2P-Währung Bitcoin wurde ins Leben gerufen, um eine neue Alternative zum momentanen Bankensystem aufzubauen. Als Motivation lässt sich einerseits die Kostenreduktion durch den Wegfall einer zentralen Einheit ausmachen. Zum anderen müssen die Teilnehmer durch ein dezentrales System nicht mehr nur einer Institution vertrauen, sondern die Macht wird gleichmäßig über alle Teilnehmer verteilt. Der allgemeine Anreiz, sich bei Bitcoin zu beteiligen, ist demnach sowohl monetär als auch nicht-monetär, da einerseits Kosten durch den Wegfall der zentralen Instanz reduziert werden könnten und andererseits ein alternatives System für das derzeitige Bankensystem geschaffen werden kann.

Jeder Bitcoin-Teilnehmer kann seine Bitcoins (BTC) an andere verschicken, dieser Vorgang wird in einer Transaktion festgehalten. Um Betrug zu vermeiden, müssen diese Transaktionen auf ihre Richtigkeit überprüft werden. Dadurch, dass sich im Netzwerk keiner gegenseitig vertraut und es keine zentrale Kontrolle gibt, muss jede Überprüfung der Transaktionen dezentral geschehen. Dabei wird eine Anzahl an neuen Transaktionen in sogenannten Blocks zusammengefasst, die anschließend veröffentlicht werden. Um diesen als Mining bekannten Vorgang zu erschweren, muss ein mathematisches Problem in Form einer Suche nach einem passenden Hash gelöst werden, damit Blöcke nicht leicht wieder manipuliert werden können. Diese Suche kann je nach verfügbarer Rechenleistung im gesamten Netzwerk variabel angepasst werden. Anreize beim Bitcoin-Mining mitzumachen sind hauptsächlich monetär, da es für die erfolgreiche Suche eines Blocks ein Bonus (auch Reward) von momentan 25 Bitcoins gibt und außerdem die Transaktionsgebühren einbehalten werden dürfen.

In den Anfangszeiten des Bitcoin-Netzwerkes waren noch relativ wenige Computer im Netzwerk, sodass die gesamte Rechenleistung auch vergleichsweise gering war. Dadurch hatten einzelne Teilnehmer eine realistische Chance, durch das Minen einen Block zu finden und damit den Bonus zu verdienen. Im Laufe der Zeit wuchs das Bitcoin-Netzwerk stark an, sodass die Konkurrenz der Bitcoin-Miner schnell anstieg. Das hat zur Konsequenz, dass das alleinige Minen nur noch dann attraktiv ist, wenn entsprechend rechenintensive Hardware vorhanden ist, da ansonsten nur selten ein Block gefunden wird. Als Folge haben sich sogenannte Mining-Pools entwickelt, in denen gemeinsam nach einem passenden Hash für einen gültigen Block gesucht wird. Findet ein Teilnehmer schließlich einen Block, so wird der Bonus auf alle Teilnehmer aufgeteilt. Diese Aufteilung kann ein Anreiz für sich opportunistisch verhaltende Teilnehmer sein, das

System auszutricksen, um sich gegenüber den anderen ehrlichen Teilnehmern einen Vorteil zu verschaffen.

In dieser Arbeit werden zunächst in Kapitel 2 die Grundlagen des Bitcoin-Minings erläutert, um anschließend zu klären, ob ein opportunistisches Verhalten in Mining-Pools ein Anreiz darstellen kann. Dazu werden in Kapitel 3 die gängigen Verteilungsmechanismen vorgestellt und auf ihre gerechte Verteilung überprüft. Des Weiteren werden der Erfolg von den Mining-Pools im Zeitverlauf sowie die Popularität von den verschiedenen Verteilungsmechanismen dargestellt.

2. GRUNDLAGEN MINING

Bevor untersucht werden kann, wie gerecht die verschiedenen Mining-Pools ihren Reward für einen gefundenen Block an ihre beteiligten Nutzer verteilen, werden im Folgenden die Grundlagen des Minings und der Mining-Pools näher erläutert.

2.1 Bitcoin-Mining

Ziel des Bitcoin-Minings ist es, die Transaktionen zwischen den Benutzern auf ihre Richtigkeit zu überprüfen und Betrug zu erkennen. Dabei soll das sogenannte Double-Spending verhindert werden, indem geprüft wird, ob derselbe Bitcoin nur einmal ausgegeben wurde (Bitcoin Wiki 2013c). Als Faustregel hat sich etabliert, dass eine Transaktion erst dann als gültig angesehen wird, wenn sie von mindestens sechs weiteren Blöcken bestätigt wird (Bitcoin Wiki 2013b).

Die überprüften Transaktionen werden gebündelt in einen Block geschrieben und anschließend in der sogenannten Block-Chain miteinander so verbunden, sodass die Transaktionshistorie daraus abgelesen werden kann. Dazu verweist ein neuer Block immer auf genau einen vorherigen Block (Bitcoin Wiki 2012a).

Um den Nutzern des Bitcoin-Netzwerkes einen Anreiz zu geben, Blöcke zu generieren und damit Transaktionen zu verifizieren, sind zwei Möglichkeiten vorgesehen, die zeitgleich stattfinden. In der Anfangsphase, in der sich Bitcoin zurzeit noch befindet, gibt es für jeden gefundenen Block einen Reward von ursprünglich 50 BTC (momentan 25 BTC), dieser wird alle 210000 Blöcke halbiert. Das erfolgt in etwa alle 4 Jahre, da im Protokoll festgelegt ist, dass im Mittel alle 10 Minuten ein Block gefunden werden soll. Diese Phase dauert so lange, bis sich durch die Halbierung der Bonus praktisch null annähert. Die andere Möglichkeit, Bitcoins durch das Mining zu erhalten, besteht darin, an eine Transaktion eine Gebühr anzuhängen, die derjenige einbehalten darf, der den Block gefunden hat (Bitcoin Wiki 2013c; Nakamoto 2009, S. 4).

Um zu erreichen, dass im Mittel nur alle 10 Minuten ein Block gefunden wird, muss von den Minern ein kryptografisches Problem gelöst werden, das sich in seiner Schwierigkeit (sog. Difficulty) anpassen lässt. Wenn beispielsweise viel Rechenleistung im Netz verfügbar ist, wird ein Block schneller gefunden, sodass die Difficulty nach oben gesetzt wird (Nakamoto 2009, S. 3).

Als mathematisches Problem wird eine Hashberechnung durchgeführt, die die Eigenschaft besitzt, dass sie schwierig zu berechnen, aber leicht zu überprüfen ist. Dadurch kann ein gefundener Block sehr schnell von den anderen Teilnehmern verifiziert werden. Konkret besteht das Problem darin, einen SHA-256 Hash zu finden, der das sogenannte Target nicht überschreitet. Das Target ist eine Zahl, die abhängig von der momentanen Difficulty bestimmt wird (Nakamoto 2009, S.3).

Mit steigender Difficulty kann das Mining und damit die erfolgreiche Suche nach dem passenden Hash mit einem herkömmlichen PC mehrere Jahre in Anspruch nehmen. Die durchschnittliche Anzahl an gefundenen Blocks in einer gewissen Zeitspanne kann mit Hilfe folgender Formel berechnet werden (Rosenfeld 2011a, S. 1):

$$\text{Anzahl Blocks} = \frac{h \cdot t}{2^{32} \cdot D} \tag{1}$$

Dabei ist h die Hashrate, t die Zeit und D die aktuelle Difficulty. 2^{32} stellt die Anzahl der Veränderungsmöglichkeiten der Nonce dar, da sie aus einem 32Bit Integer besteht. Die Nonce ist ein einmalig generierter zufälliger Wert, der im Header jeden Blocks zu finden ist(Bitcoin Wiki 2012c).

Bei der momentanen Difficulty von 12.153.411,71 (Stand: 29.05.2013) und einer mittleren Hashrate von 100 Millionen Hashes pro Sekunde (Bitcoin Wiki 2013d) wird beim alleinigen Minen ca. alle 16,55 Jahre ein Block gefunden:

$$1\,[\text{Block}] = \frac{100\,[\frac{\text{MHash}}{\text{s}}] \cdot t}{2^{32} \cdot 12153411,71} \Leftrightarrow t = 16,55\,[\text{Jahre}] \tag{2}$$

Da durch das alleinige Minen viel Zeit bis zur ersten Auszahlung vergehen wird, gibt es die Möglichkeit, sich mit anderen Minern in sogenannten Mining-Pools zusammenzuschließen, worauf im Folgenden näher eingegangen wird.

2.2 Mining-Pools

Mining-Pools finden im Unterschied zum alleinigen Mining durch die größere Rechenkapazität aller Teilnehmer zusammen wesentlich häufiger einen Block und bekommen deshalb auch öfter den Bonus von momentan 25 BTC als alleinige Miner. Für den einzelnen Teilnehmer am Mining-Pool bedeutet das eine stetigere Ausschüttung von Bitcoins (Bitcoin Wiki 2013e). Im langfristigen Mittel ist allerdings die erwartete Auszahlung bei Teilnahme eines Mining-Pools genau gleich groß wie beim alleinigen Mining (Gebühren ausgenommen). Ein Vorteil für den Pool-Teilnehmer besteht darin, dass sich die Streuung der Auszahlungen deutlich reduziert, sodass die Gewinne besser geplant werden können (Rosenfeld 2011a, S. 2). Nachteilig wirken sich die erhobenen Gebühren zur Teilnahme an einem Mining-Pool aus.

Ein Mining-Pool wird auf einem Server betrieben, jeder der teilnehmen möchte, muss sich gegebenenfalls einmalig registrieren und kann sich dann am Server mit seinen Login-Daten anmelden. Es gibt auch komplett anonyme Zugänge, die lediglich die Bitcoin-Adresse als Login verlangen, z. B. der Mining-Pool 50BTC (https://50btc.com).

Jeder Teilnehmer bekommt vom Server das aktuelle Problem mitgeteilt und es wird versucht, einen passenden Hash zu finden. Das aktuelle Problem ist schematisch in Abbildung 1 dargestellt. Es besteht darin, für den Block einen passenden Hash zu finden, der eine bestimmte Grenze (sogenanntes Target) nicht überschreitet. Das Target ergibt sich aus der aktuellen Difficulty.

Der Block an sich besteht aus dem Hash des vorherigen Blocks und den Transaktionen, die in diesem Block überprüft wurden (X und Y in Abbildung 1). Lediglich die Nonce ist noch nicht vom Pool-Betreiber vorgegeben, sondern dieser wird von den Teilnehmern gesucht. Bei jeder Änderung der Nonce ändert sich auch der Hashwert, bis irgendwann ein passender Hash gefunden wurde. Dadurch dass der Pool-Betreiber das Problem bis auf die Nonce vorgibt, ist es für einen potenziellen Angreifer nicht möglich, sich den Reward selbst zuzuschreiben, da dieser bereits in den eingebauten Transaktionen vorhanden ist. Der Mining-Pool Betreiber würde einen solchen Betrugsversuch deshalb entdecken, da sich das Problem geändert hat.

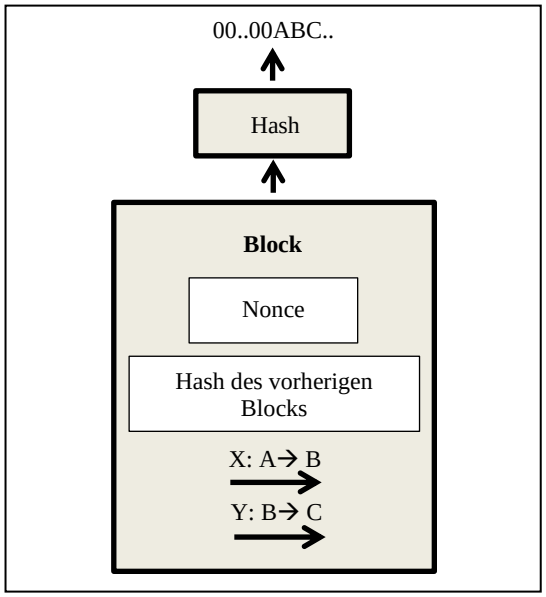

Abbildung 1. Schematische Darstellung der Hashsuche

Der Miner löst allerdings nicht direkt das Problem, sondern reicht als Lösung dem Server sogenannte *Shares* ein. Dieser beinhaltet einen Hash, der einen Block gefunden hätte, wenn die Difficulty deutlich kleiner als die momentan festgelegte gewesen wäre. Die Difficulty wird also künstlich nach unten gesetzt.

Die durchschnittliche Anzahl an gefundenen Shares in einer gewissen Zeitspanne kann der bereits bekannten Formel berechnet werden. Ein Share ist üblicherweise so definiert, als wäre es ein Block mit der Difficulty Eins (Rosenfeld 2011a, S. 1):

$$\text{Anzahl Shares} = \frac{h \cdot t}{2^{32} \cdot D} \tag{3}$$

Bei einer Hashrate von 100 Millionen Hashes pro wird somit ca. alle 43 Sekunden ein Share gefunden:

$$1\ [\text{Hash}] = \frac{100\ [\frac{\text{MHash}}{\text{s}}] \cdot t}{2^{32} \cdot 1} \Leftrightarrow t = 42{,}95\ [\text{s}]$$

Der Server wertet alle eingehenden Shares aus, bis einer zu dem wirklichen Problem mit der aktuellen Difficulty passt. Dann gilt der Block als gefunden und unter den mitwirkenden Teilnehmer wird anteilig der eingereichten Shares der aktuelle Reward abzüglich eventueller Gebühren verteilt. Diese Aufteilung ist keineswegs trivial, da sie möglichst fair ablaufen soll (Rosenfeld 2011a, S. 3). Dazu dienen verschiedene Ansätze, die im Kapitel 3 detailliert besprochen und auf eine gerechte Verteilung untersucht werden.

2.3 Bekannte Mining-Pools

In diesem Kapitel sollen die momentan bedeutendsten Mining-Pools dargestellt werden, um einen Überblick darüber zu bekommen, welche Auswahl an Pools es gibt und wie sich diese im Laufe der Zeit entwickelt haben.

Dabei wird die Bedeutung eines Mining-Pools anhand der Hashrate bestimmt, das heißt wie viele Hashes der Pool pro Sekunde berechnen kann. Die Hashrate wird in Bezug mit der Hashrate des gesamten Bitcoin-Netzwerkes gesetzt, um die relative Bedeutung der einzelnen Mining-Pools herauszufinden.

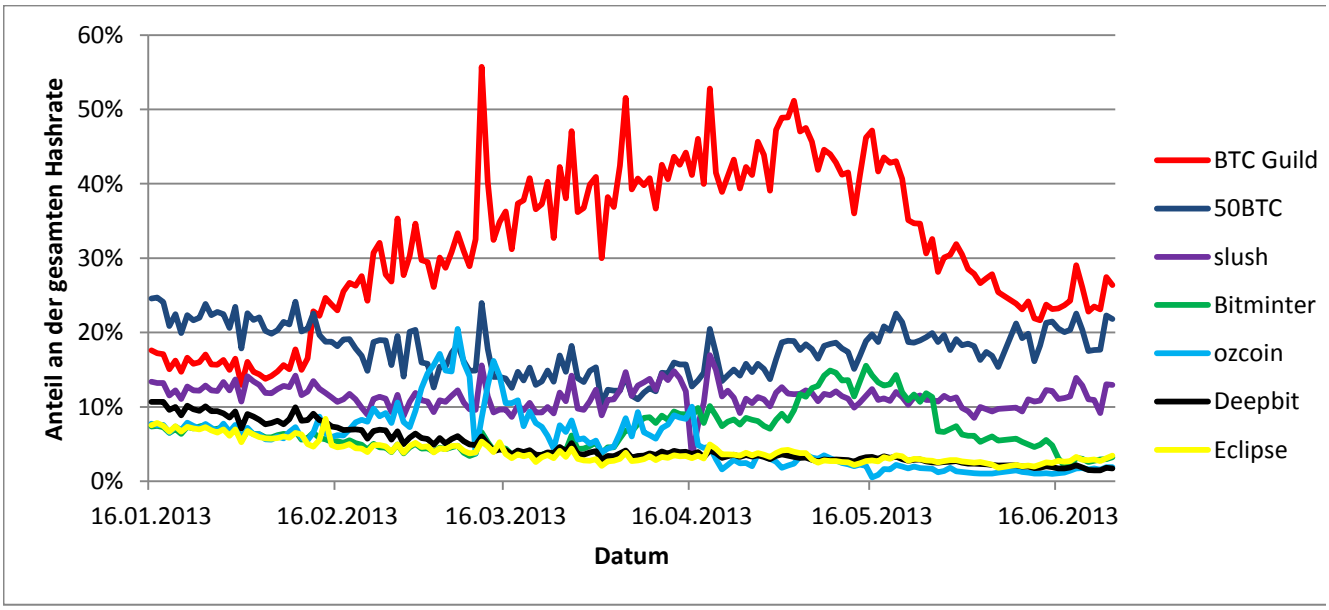

Abbildung 2. Übersicht über den Anteil der beliebtesten Mining-Pools am Gesamtnetzwerk

Die Daten der Hashrate stammen von der Internetseite bitcoinchain.com, die den Verlauf der sieben erfolgreichsten Mining-Pools seit Anfang 2013 auf Tagesbasis zusammenstellt. Da diese Seite nur die absoluten Hashraten angibt, werden diese mit den Daten über die Gesamthashrate der Internetseite blockchain.info zusammengesetzt und in relative Werte umgewandelt, um die Aussagekraft der Daten zu erhöhen. Für einige Tage lagen die Daten in einzelnen Pools nicht vor, sodass in diesem Fall die Hashraten aus der vorherigen und nachfolgenden Hashrate linear interpoliert wurden. Des Weiteren fehlen die Werte der Tage vom 07. und 08. Juni, die nicht veröffentlicht wurden. Die grafisch aufbereiteten Werte der relativen Hashrate der einzelnen Pools sind in Abbildung 2 dargestellt.

Auffällig ist, dass Anfang 2013 die Größe der Mining-Pools gemessen an der anteiligen Rechenkapazität relativ ausgeglichen war, wohingegen eine deutliche Steigerung des Mining-Pools BTC Guild zu erkennen ist. Am Ende des Zeitraumes (Juni 2013) gleicht sich die Anteile wieder langsam an. Im betrachteten Zeitraum hat der Mining-Pool BTC Guild mehrmals die Marke von 50 % erreicht hat. Diese absolute Mehrheit kann für das Netzwerk eine Bedrohung darstellen, welche im Folgenden näher betrachtet wird.

Da das gesamte Bitcoin-Netzwerk auf Dezentralität aufbaut und somit einzelne Teilnehmer mit viel Rechenleistung dieses Prinzip zunichtemachen könnten, stellt ein Mining-Pool mit über 50 % der gesamten Rechenleistung nach Bitcoin Wiki (Bitcoin Wiki 2013f) potenziell eine Gefahr dar. Der Pool kann theoretisch einzelne Transaktionen vor dem Einbau in die Blockchain verhindern. Das geschieht dadurch, dass der Angreifer mit mehr als 50% der Rechenleistung steuern kann, welche Transaktionen in einen Block aufgenommen werden, da er selbst die Transaktionen in den Block einbaut. Andere Miner, die andere Transaktionen in den Block eingebaut haben, werden durch die größere Rechenleistung verdrängt, da der Angreifer immer die längere Hauptkette in der Blockchain erzeugen kann. Als Folge können Transaktionen nicht bestätigt werden und andere Miner können davon abgehalten werden, gültige Blöcke zu finden, da alle Blöcke vom Angreifer gefunden werden.

Mit einer Rechenleistung von über 50 % kann der Angreifer nach Bitcoin Wiki (Bitcoin Wiki 2013f) allerdings nicht das Netzwerk für seine eigene Bereicherung nutzen, indem er zum Beispiel alle vergangenen Transaktionen zu sich umschreibt oder den Reward für einen neu gefundenen Block erhöht. Für die Manipulation der Transaktionen müsste der Angreifer zusätzlich alle privaten Schlüssel der Nutzer kennen, um die Transaktion signieren zu können. Darüber hinaus bedeutet eine Erhöhung des Rewards eine Protokolländerung, was nur durch absolute Mehrheit des gesamten Netzwerkes beschlossen werden kann. Absolute Mehrheit bedeutet in diesem Fall, dass mindestens die Hälfte aller Bitcoin-Teilnehmer und nicht nur die Hälfte der Rechenleistung diesem Vorschlag zustimmen muss. Diese eingeschränkte Macht soll potenzielle Angreifer abschrecken, dass sie den Versuch unternehmen, einen solchen Angriff überhaupt zu starten.

Die Pools 50BTC und slush haben ihren Anteil im Wesentlichen halten können, auch wenn es an einigen Tagen eine Schwankung von mehreren Prozentpunkte gab. An diesen Tagen sind aber haben sich die anderen Pools im gleichen Maße verändert, sodass von einer allgemeinen Fluktuation ausgegangen werden kann. Bitminter und ozcoin konnte im Mai 2013 seinen Anteil in etwa verdoppeln, haben allerdings seit Juni wieder nachgelassen und sind nun noch unter dem Niveau von Anfang des Jahres. Die Kurse schwankten zum Teil stark. Die Pools Deepbit und eclipse haben sich in dem Zeitraum nahezu nicht verändert, sondern sind ein paar Prozentpunkte zurückgegangen auf jeweils unter 5 %.

Um die Mining-Pools noch aus einer anderen Perspektive vergleichen zu können, werden die Gebühren für die Teilnahme in einem Mining-Pool miteinander verglichen. Typischerweise wird eine Gebühr verlangt, die einem bestimmten Prozentsatz vom momentanen Reward entspricht. Die folgende Tabelle 1 zeigt für die momentan (Stand: 11.05.2013) beliebtesten Mining-Pools die aktuellen Gebühren, die anhand der angegebenen Internetseiten bestimmt wurden.

Tabelle 1. Teilnahmegebühren bei ausgewählten Mining-Pools

Poolname	Internetadresse	Gebühr
50BTC	https://50btc.com/	3 % (PPS)
Bitminter	http://bitminter.com/	1 % (PPLNS)
BTC Guild	https://www.btcguild.com/	3 % (PPLNS), 7,5 % (PPS)
Deepbit	https://deepbit.net/	3 % (Prop.), 10 % (PPS)
Eclipse	https://eclipsemc.com	0 % (DGM), 5 % (PPS)
ozcoin	https://www.ozcoin.net/	1 % (DGM), 3 % (PPS)
slush	http://mining.bitcoin.cz/	2 % (Score)

Neben den Gebühren ist jeweils die Art der Verteilungsart des Rewards angegeben. Bei denjenigen Pools, die mehrere Verteilungsmechanismen anbieten, stehen alle Gebühren untereinander mit der dazugehörigen Verteilmethode.

Die unterschiedlichen Gebühren von 0% bis 10% lassen sich zum Teil durch die unterschiedliche Verteilungsmechanismen erklären, die sich auf das Risiko des Pools auswirken. Dazu werden im folgenden Kapitel die verschiedenen Methoden miteinander verglichen und jeweils auf ihre gerechte Verteilung untersucht.

3. VERTEILUNGSMECHANISMEN

Es gibt zahlreiche Verteilungsmechanismen, nach denen ein Mining-Pool den erhaltenen Bonus unter seinen Teilnehmern verteilen kann. Neben einfachen Verfahren, die zum Teil anfällig für Betrug sind, wurden Verfahren entwickelt, die möglichst gerecht den Beitrag zur Findung des Blocks von jedem einzelnen Teilnehmer widerspiegeln sollen. Im Folgenden werden diese Verteilungsverfahren vorgestellt und jeweils darauf geprüft, ob es für einzelne Teilnehmer einen Anreiz geben kann, sich unfair zu verhalten, um einen höheren Gewinn zu erzielen. Zuvor wird noch geklärt, was unter einer fairen Verteilung für Miner und Betreiber zu verstehen ist.

3.1 Faire Verteilung

Eine faire Verteilung zeichnet sich dadurch aus, dass sowohl die Miner als auch der Betreiber des Pools einen Vorteil durch das gemeinsame Minen erzielen. Auf der Seite der Betreiber heißt das, dass die erhobenen Gebühren nur so hoch sein sollten, dass sie die laufenden Kosten des Poolbetriebs (Server, Wartung, Kontaktmöglichkeiten) decken und nicht ausschließlich den Profit des Betreibers maximieren.

Für die Miner bedeutet eine faire Verteilung, dass sich niemand durch opportunistisches Verhalten einen Vorteil gegenüber anderen ehrlichen Minern verschaffen kann. Des Weiteren sind der Zeitpunkt des Minens und die Dauer der Teilnahme im Mittel nicht ausschlaggebend für die Auszahlung des Rewards. Der Erwartungswert der Auszahlung ist somit immer gleich.

3.2 Einfache Mechanismen

3.2.1 Proportionale Verteilung

Eine einfache und intuitive Variante der Verteilung ist nach Rosenfeld (Rosenfeld 2011a, S. 4) die sogenannte *Proportionale Verteilung*. Dabei wird nach jedem gefundenen Block vom Mining-Pool ausgezählt, wie viele Shares insgesamt eingereicht wurden. Der Reward wird dann gemessen an den eingereichten Shares an die Teilnehmer verteilt. Wenn beispielsweise ein Nutzer in einer Runde (Zeit zwischen zwei gefundenen Blöcken eines Mining-Pools) $n = 1000$ Shares eingereicht hat und alle eingereichten Shares sich auf $N = 1000000$ belaufen, erhält der Nutzer $\frac{n}{N} = \frac{1}{1000}$ des momentanen Rewards $B = 25$ BTC abzüglich der vom Mining-Pool einbehaltenen Gebühr.

Für eine feste Anzahl an Minern und eine feste Hashrate der einzelnen Teilnehmer ist bei dieser Verteilungsart die Auszahlung eines Miners proportional zu seiner Hashrate. Sobald Miner nicht die ganze Runde lang nach passenden Hashes suchen, sondern nach einer gewissen Zeit aufhören und alleine oder für einen anderen Pool weitersuchen, ist diese Proportionalität nicht mehr gegeben. Das Phänomen des Aufhörens oder Wechselns während einer Runde wird als Poolhopping bezeichnet, womit sich einzelne Teilnehmer einen Vorteil verschaffen können. Das kommt dadurch zustande, dass sie eine überproportionale Auszahlung auf Kosten der anderen Teilnehmer bekommen, die die ganze Runde lang für denselben Pool minen (Rosenfeld 2011a, S. 4). Dies wird im Folgenden näher erläutert.

Das Poolhopping ist nur deshalb für einen Teilnehmer attraktiv, da sich im Mittel durch das Wechseln eines Pools sein erwarteter Gewinn nicht schmälert, sondern exakt gleich bleibt (Raulo 2011, S. 2). Das Grundprinzip besteht darin, dass ein beigesteuerter Share in einer kurzen Runde mehr wert ist als in einer langen Runde, da der relative Anteil eines Shares größer ist und damit auch die Auszahlung. Das Ziel eines Poolhoppers besteht also darin, in einer kurzen Runde Shares beizutragen, in einer langen Runde sich einen anderen Pool zu suchen oder alleine zu minen (Rosenfeld 2011a, S. 4-5).

Um zu bestimmen, wann die beste Ausstiegszeit in Abhängigkeit der bereits beigesteuerten Shares ist, wird die erwartete Auszahlung für einen Share ausgewertet. Die nachfolgenden Rechnungen sind aus dem Paper von Rosenfeld (2011) entnommen und wurden mit eigenen Anmerkungen näher erläutert.

Die Wahrscheinlichkeit für die Gesamtanzahl N an Shares in einer Runde folgt einer geometrischen Verteilung mit Parameter p, da sie als Wiederholung eines unabhängigen Bernoulli-Experiments (Hash wird gefunden vs. Hash wird nicht gefunden) mit gleichbleibender Wahrscheinlichkeit interpretiert werden kann. Es gilt:

$$P(N) = p(1-p)^{N-1} \tag{4}$$

Wenn bereits I Shares eingereicht wurden, ist sicher, dass $N > I$ sodass die Anzahl an Wiederholungen des Bernoulli-Experiments um I reduziert werden kann. Mathematisch ausgedrückt bedeutet das für die Wahrscheinlichkeit:

$$P(N \mid N > I) = \begin{cases} 0 & \text{für } N \le 0 \\ p(1-p)^{N-I-1} & \text{für } N > 0 \end{cases} \tag{5}$$

Der Reward für einen Share ist der Anteil der selbst eingereichten Shares im Vergleich zu allen eingereichten Shares, er beträgt $w = \frac{B}{N}$. Demnach ist die erwartete Auszahlung für den Share die Summe aller Rewards jeweils multipliziert mit der Wahrscheinlichkeit diesen Reward mit diesem Share zu erhalten:

$$\mathrm{E}(w \mid N > I) = \sum_{N=I+1}^{\infty} \frac{p(1-p)^{N-I-1} \cdot B}{N} \tag{6}$$

Diese Formel kann mit Hilfe der Integralexponentialfunktion E_1 angenähert werden:

$$E_1(x) = \int_1^{\infty} \frac{\exp(-xt)}{t} dt \tag{7}$$

Um die Summenformel mit Hilfe von E_1 annähern zu können, werden die Variablen $x = pI$, $y = pN$ definiert, die die Anzahl der beigesteuerten Shares und die Gesamtanzahl der Shares bezogen auf die Difficulty ausdrücken:

$$\mathrm{E}(w \mid y > x) \approx \int_x^{\infty} \frac{p(1-p)^{\frac{y-x}{p}} \cdot B}{y} dy \approx \exp(x) \cdot E_1(x) \cdot pB \tag{8}$$

Die Teilfunktion $f(x) = \exp(x) \cdot E_1(x)$ kann als ein Faktor zur Gewichtung von der erwarteten Auszahlung pB interpretiert werden, der monoton fällt. Das bedeutet, dass je früher in einer Runde ein Share beigesteuert wird, desto höher ist seine erwartete Auszahlung.

Beim Wert von ca. 43,5 % liegt der Gewichtungsfaktor bei 1, was bedeutet, dass ein beigesteuerter Share zu diesem Zeitpunkt exakt so viel wert ist wie er auch beisteuert, der Verdienst ist in diesem Fall fair.

Für einen Miner, der abwägt, ob sich die weitere Teilnahme noch lohnt, bedeuten die 43,5 %, dass er bis zu diesem Zeitpunkt in einem Pool minen kann, um überproportional viel Anteil an den Shares zu erhalten. Danach kann er entweder zu einem Pool wechseln, dessen Anzahl an Shares diese Grenze noch nicht überschritten hat oder er wechselt auf das alleinige Minen.

Als Gegenmaßnahme kann es der Mining-Pool Betreiber dem Poolhopper schwerer machen, festzustellen, wann die Grenze von 43,5 % erreicht ist. Dazu können die Statistiken, die angeben, wann der letzte Block gefunden wurde und damit wie lange die aktuelle Runde bereits dauert, sowie die aktuelle Hashrate um ein paar Stunden verzögert aktualisiert werden, um den Angreifer keine Echtzeitdaten zu liefern. Dieser Ansatz behebt allerdings nicht das zugrundeliegende Problem, weswegen die proportionale

Verteilung in heutigen Mining-Pools fast nicht mehr zur Anwendung kommt (vgl. Kapitel 3.4 Beliebtheit der Methoden).

Diese Verteilungsmethode kann nicht als fair angesehen werden, da sie opportunistisches Verhalten zulässt und somit ehrliche Miner benachteiligen kann. Der Mining-Pool-Betreiber hat dagegen keine Einschränkung, da dieses Verhalten sich nicht auf die Gesamtauszahlung und die einbehaltenen Gebühren auswirkt.

3.2.2 Pay-Per-Share (PPS)

Ein anderer relativ einfacher Verteilungsmechanismus ist das sogenannte Pay-Per-Share-Verfahren. Dabei erhält jeder Teilnehmer unabhängig ob und wann ein Block gefunden wird, für jeden eingereichten Share eine bestimmte Auszahlung. Diese setzt sich aus dem erwarteten Gewinn abzüglich einer vom Mining-Pool einbehaltenen Gebühr zusammen (Rosenfeld 2011a, S. 6).

Dieses Verfahren hat für den Miner einige Vorteile, die für den Mining-Pool Betreiber ein höheres Risiko bedeuten, weswegen es als Nachteil für die Miner bei Mining-Pools mit PPS eine zusätzliche Gebühr gibt.

Teilnehmer des Pools können ihre erwartete Auszahlung recht genau bestimmen, da sie anhand ihrer Hashrate abschätzen können, wie viele Shares sie finden werden. Da dies deterministisch ist, ist die Streuung der Auszahlung für den Teilnehmer nahezu null, sodass Miner gut planen können. Des Weiteren ist die Gefahr der Unterbezahlung aufgrund von anderen Mining-Pool Teilnehmern durch Poolhopping nicht gegeben, da es bei diesem Verfahren nicht möglich ist. Das liegt daran, dass ein frühes Wechseln des Pools bevor ein Block gefunden wird, keine Auswirkungen auf den erwarteten Gewinn hat, da nur pro eingereichten Share bezahlt wird (Rosenfeld 2011a, S. 6).

Für den Betreiber des Mining-Pools besteht ein Risiko, in langen Runden mehr Geld an die Teilnehmer auszuzahlen, als es dem momentanen Reward für einen gefundenen Block entspricht. In diesem Fall macht der Betreiber einen Verlust, den er in kurzen Runden wieder ausgleichen kann, wenn die Auszahlungen an die Teilnehmer geringer als der erhaltene Reward sind (Rosenfeld 2011a, S. 6).

Um den Betrieb eines Mining-Pools mit dem Pay-Per-Share-Verfahren lukrativ und mit möglichst wenig Risiko auf beiden Seiten zu gewährleisten, behält der Betreiber üblicherweise eine zusätzliche Pay-Per-Share-Gebühr ein, die das Risiko abfedern soll. Diese ist bereits neben der normalen Mining-Pool Gebühr in der Auszahlung pro eingereichten Share beinhaltet (Rosenfeld 2011a, S. 6).

Der nachfolgende Boxplot in Abbildung 3 zeigt die Gebühren für das PPS-Verfahren für einige Mining-Pools. Dafür wurden die Daten von insgesamt elf Mining-Pools ausgewertet, die das Mining nach dem PPS-Verfahren anbieten. Daraus ist zu erkennen, dass im Mittel (als Mittelwert dient der Median) eine Gebühr von 5 % erhoben wird und nur ein geringer Teil nach oben und unten abweicht.

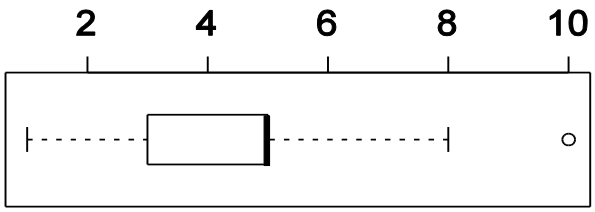

Abbildung 3. Boxplot der PPS-Gebühren in Mining-Pools

Für einen Miner bietet ein Mining-Pool, der nach PPS auszahlt, keinen Anreiz, sich opportunistisch zu verhalten, da es keine Möglichkeit gibt, sich einen Vorteil durch das Poolhopping zu verschaffen. Die erwarteten Auszahlungen sind ebenfalls gleich, allerdings sind die Gebühren zum Teil hoch. Das kommt daher, dass der Mining-Pool-Betreiber allein das Risiko trägt, wenn mehr ausgezahlt werden muss als durch den Reward und die Transaktionsgebühren eingenommen wurde. Die Methode ist demnach hauptsächlich für den Miner fair.

3.3 Fortgeschrittene Methoden

Aus den bereits vorgestellten Varianten der Verteilung wurden im Laufe der Zeit neue, fortgeschrittene Methoden entwickelt. Zum einen um das Problem des unfairen Minings mittels Poolhopping zu unterbinden, zum anderen entstanden Verteilungsmechanismen, mit denen es möglich ist, die Streuung der Auszahlungen für die Miner und den Mining-Pool Betreiber variabel anzupassen.

Im Folgenden werden die wichtigsten dieser neuen Methoden vorgestellt. Dabei wurden die am häufigsten verwendeten Methoden (vgl. 3.4 Beliebtheit der Methoden) näher betrachtet. Daneben gibt es noch spezielle Methoden, die eine der erläuterten Varianten leicht abwandeln, meistens mit dem Ziel, eine Schwäche einer vorherigen Methode zu verbessern. Diese werden allerdings kaum noch eingesetzt, sodass sie nicht näher besprochen werden, da sie kaum praktische Relevanz haben.

3.3.1 Slushs Score Methode

Um das Poolhopping zu verhindern und damit die Verteilung gerechter zu gestalten, hat der Mining-Pool *slush* eine Methode entwickelt, die das Poolhopping nicht mehr attraktiv machen soll. In dieser Methode wird für jeden eingereichten Share nicht wie bei der proportionalen Verteilung die Anzahl der eingereichten Shares um eins erhöht, sondern es wird für jeden Share ein sogenannter *Score* errechnet. Beim Fund des passenden Hashes, womit der Block gefunden wird, bestimmt die Summe aller Scores von einem Miner dessen Anteil der Auszahlung (Rosenfeld 2011a, S. 7).

Die Scores werden so bestimmt, dass am Anfang der Runde eingereichte Shares weniger wert sind als neuere Shares, was Poolhopper davon abhalten soll, zwischen Pools zu wechseln, da ihre eingereichten Shares beim Verlassen des Pools an Wert verlieren. Das hat zur Folge, dass das Poolhopping nicht mehr sehr attraktiv ist (slush 2011). Theoretisch wäre es für einen Miner attraktiver, sich nur am Ende einer Runde zu beteiligen, da er dann eine erhöhte Auszahlung erhält, allerdings ist im Vorhinein nicht bekannt, wann die Runde endet, da jeder

beigesteuerte Share die gleiche Wahrscheinlichkeit hat, die passende Lösung für das Problem zu sein.

Um den Score mathematisch zu berechnen, wird die Exponentialfunktion eingesetzt. Sie wächst monoton, sodass sie für diesen Einsatz gut genutzt werden kann. Der gesamte Score für einen Miner wird durch diese Formel bestimmt (slush 2011):

$$\text{Score} = \sum \exp\left(\frac{\text{Rundenzeit}}{C}\right) \tag{9}$$

Dabei gibt die Rundenzeit die Anzahl der Sekunden seit dem Start der aktuellen Runde an, die Konstante *C* legt fest, wie schnell der Score wachsen soll. Wenn *C* klein ist, haben die früh eingereichten Shares eine sehr geringe bis vernachlässigbare Auswirkung auf die Auszahlung, da die Funktion bei steigender Rundenzeit schnell wächst und die spät eingereichten Shares somit ein deutlich größeres Gewicht besitzen (Rosenfeld 2011a, S. 7). Aktuell ist der Mining-Pool von *slush* auf $C = 300$ eingestellt (slush 2011).

Für Miner, die nur eine geringe Hashrate haben oder sich nur gelegentlich am Mining beteiligen, verändert sich die erwartete Auszahlung durch das scorebasierte Verfahren nicht (slush 2011). Wenn nur relativ wenig Shares von einem Miner eingereicht werden, dann kann es passieren, dass diese am Anfang der Runde eingereicht werden, was zu einer geringeren Auszahlung führt. Es ist allerdings unwahrscheinlich, dass dies immer passiert, denn langfristig wird sich der Zeitpunkt, in dem ein Share eingereicht wurde, gleichmäßig zwischen Start und Ende der Runde verteilen, sodass die Auszahlung im Mittel gleich ist. Gleiches gilt auch für Miner, die sich nicht den ganzen Tag lang beteiligen, sondern nur gewisse Zeitabschnitte. Es kann passieren, dass der Miner mitten in einer Runde aufhört, sodass die zuletzt eingereichten Shares verhältnismäßig wenig Ertrag bringen. Da auch das Stoppen des Minens sich langfristig auf eine Runde gleichmäßig verteilen wird, können diese Nachteile ausgeglichen werden, sodass die mittlere Auszahlung gleich bleibt (slush 2011).

In der praktischen Implementierung kann die Formel zur Berechnung des Scores nicht direkt übernommen werden, da durch das exponentielle Wachstum der Score schnell an die Grenzen von üblichen Datentypen stößt, weil die Werte sehr groß werden können. Um dieses Problem zu beseitigen, werden im Mining-Pool *slush* jede Stunde die Scorewerte normalisiert, indem alle momentanen Scores durch einen bestimmten Wert dividiert werden. Das hat keinen Einfluss auf die Auszahlung, da alle Scores durch den gleichen Wert geteilt werden und somit alle wieder relativ gesehen auf demselben Stand sind (slush 2011).

Die vorgestellte Methode hat nach Rosenfeld (Rosenfeld 2011a, S. 7-8) einen Nachteil. Am Anfang einer Runde gibt es nur wenige Shares, die eingereicht werden. Wenn in dieser Zeit eine richtige Lösung gefunden wird, wird der Gewinn in Höhe des momentanen Rewards abzüglich der fixen Gebühr auf relativ wenige Nutzer aufgeteilt. Der erwartete Gewinn ist demnach höher als in langen Runden, sodass es für Miner attraktiver ist, nur in dieser Zeit zu minen. Dieser Effekt kann zwar nicht sehr effektiv vom Miner ausgenutzt werden, da er vor jeder Runde wissen müsste, wie lange sie dauert, sodass das Problem in der Praxis eine untergeordnete Rolle spielt. Um dieses eher theoretische Problem zu beseitigen, wurde u. a. die geometrische Methode entwickelt.

Für die Beurteilung der fairen Verteilung kann deshalb gesagt werden, dass diese Methode insgesamt für den Miner und den Betreiber fair ist, da die Möglichkeit, sich opportunistisch zu verhalten, begrenzt sind und es unwahrscheinlich ist, dass die Länge der Runden richtig geschätzt wird.

3.3.2 Geometrische Methode

Die geometrische Verteilung knüpft an der Idee von slushs scorebasierter Methode an und verbessert dessen Schwäche, dass es attraktiver ist, sich nur am Anfang jeder kurzen Runde zu beteiligen. Dazu gibt es neben der üblichen fixen Gebühr eine zusätzliche variable Gebühr, die einen Score für den Mining-Pool-Betreiber darstellt, der genauso schnell abfällt, wie der Score der Pool-Teilnehmer ansteigt. In kürzeren Runden ist diese variable Gebühr demnach hoch, da die Anzahl an eingereichten Shares klein ist. In langen Runden sinkt die Gebühr nahezu auf null ab. Mit diesem Prinzip ist der erwartete Gewinn eines Shares immer gleich, unabhängig davon, ob der Share am Anfang oder Ende einer Runde eingereicht wurde (Rosenfeld 2011a, S. 8). Auch bei dieser Methode ist es prinzipiell gewinnbringender für einen Miner, sich ausschließlich in kurzen Runden zu beteiligen, allerdings ist hier ebenfalls nicht bekannt, wann eine Runde endet, sodass dieses Problem vernachlässigt werden kann.

Um die geometrische Methode durchzuführen, werden folgende fünf Schritte durchgeführt (Rosenfeld 2011a, S. 8-9, 2011c):

1. Festlegung von Parametern f für die fixe Gebühr und Parameter c für die durchschnittliche variable Gebühr.
2. Zu Rundenbeginn wird der momentane Scorewert für den nächsten eingereichten Share initialisiert: $s = 1$. Für jeden Pool-Teilnehmer k wird der Score S_k initialisiert: $S_k = 0$.
3. Der Steigungsfaktor *r* für den Score gibt an, wie schnell der Score bei jedem eingereichtem Share wachsen soll. Er berechnet sich aus $r = 1 - p + \frac{p}{c}$, wobei p die Wahrscheinlichkeit angibt, dass ein Share die Lösung für einen Block darstellt, deshalb gilt: $p = \frac{1}{D}$, wobei *D* die aktuelle Difficulty ist. Wenn sich die Difficulty während einer Runde ändert, wird entsprechend *r* neu berechnet.
4. Wenn ein Pool-Teilnehmer einen Share einreicht, wird sein Score S_k um den momentanen Scorewert *s* multipliziert mit der erwarteten Auszahlung ($p \cdot B$, vgl. 3.2.1 Proportionale Verteilung) erhöht:

   $$S_k = S_k + s \cdot p \cdot B \tag{10}$$

   Anschließend wird der Scorewert *s* angepasst und um den Faktor *r* multipliziert: $s = s \cdot r$.
5. Wenn ein Share den Block löst, ist die Runde zu Ende. Anschließend wird jedem Teilnehmer folgender Gewinn ausgezahlt:

   $$\frac{(1-f)(r-1)S_k}{s \cdot p} \tag{11}$$

Der ausgezahlte Gewinn kann etwas umgeschrieben werden, damit deutlich wird, wie er sich zusammensetzt. Dafür wird angenommen, dass die Difficulty fest ist, was keine große Einschränkung ist, da sie nur alle 2016 Blocks neu festgelegt wird (Bitcoin Wiki 2012b). Der Reward *B* wird ebenfalls als konstant angenommen. Wenn *N* die Anzahl an insgesamt eingereichten Shares in einer Runde ist lässt sich der momentane Scorewert als

$s = r^N$ schreiben. Dann kann die Auszahlung der Mining-Pool-Teilnehmer umgeschrieben werden:

$$\frac{(1-f)(r-1)S_k}{s \cdot p} = \frac{S_k}{\frac{r^N \cdot p \cdot B}{r-1}}(1-f)B$$

$$= \frac{S_k}{\left(\sum_{i=-\infty}^{N} r^{i-1}\right) \cdot p \cdot B}(1-f)\mathrm{B} \quad (12)$$

Anhand der letzten Umformung kann man sehen, dass der Reward abzüglich der einbehaltenen fixen Gebühr auf die Teilnehmer verteilt wird, abhängig davon, wie groß der jeweilige Score ist. Dabei kann die Summe so aufgespalten werden, dass sie zum einen die variable Gebühr des Mining-Pool Betreibers darstellt und zum anderen den Anteil der Teilnehmer. Der Anteil vom Betreiber beträgt $(\sum_{i=-\infty}^{0} r^{i-1}) \cdot p \cdot B$, der Anteil der Teilnehmer beträgt entsprechend $(\sum_{i=1}^{N} r^{i-1}) \cdot p \cdot B$. Das bedeutet, dass bei Rundenstart dem Mining-Pool Betreiber unendlich viele Shares zugeschrieben werden, die im Laufe der Zeit an Bedeutung verlieren. Bei jeder Auszahlung für einen Teilnehmer wird der Anteil des Betreibers mit einberechnet, sodass je nach Rundenlänge mehr oder weniger von der variablen Gebühr zu zahlen ist. Wenn die Runde kurz dauert, ist der Score S_k noch relativ klein, sodass der Anteil des Mining-Pool Betreibers noch stark ins Gewicht fällt. Bei längeren Runden wird durch das exponentielle Wachstum des Scores dafür gesorgt, dass die variable Gebühr sehr gering wird, da der Anteil des Betreibers kaum noch eine Rolle spielt (Rosenfeld 2011a, S. 9).

In der praktischen Umsetzung dieses Verfahrens muss ebenfalls wie bei der Methode von *slush* darauf geachtet werden, dass die Scores beim Speichern nicht den Wertebereich des Datentyps überschreiten. Dazu schlägt Rosenfeld (Rosenfeld 2011a, S. 10) vor, entweder wie bei *slush* in gewissen Zeitabständen die Scores zu normalisieren oder alternativ eine logarithmische Skala zu verwenden. Dabei wird jeweils der logarithmierte Wert des momentanen Scorewertes sowie den Score für jeden Teilnehmer gespeichert, sodass die Wertebereiche nicht mehr überschritten werden sollten. Zusätzlich müssen noch die Berechnungen der einzelnen Werte auf die logarithmische Skala angepasst werden.

Dieses Verfahren ist ohne Einschränkung fair, da einerseits der Betreiber gegenüber zu hohen Auszahlungen durch die variable Gebühr gesichert ist. Andererseits gibt es für den Miner keinen Anreiz, sich opportunistisch zu verhalten.

3.3.3 Pay-per-last-N-Shares (PPLNS)

Beim Verteilungsmechanismus Pay-per-last-N-Shares (PPLNS) wird der Reward nicht wie bei den vorherigen Verfahren unter den Teilnehmern des Mining-Pools aus der aktuellen Runde verteilt, sondern der Gewinn wird unabhängig von den Runden an die Miner der zuletzt beigesteuerten Shares verteilt. Dadurch wird es für unfaire Miner nicht mehr lukrativ, nur am Anfang der Runde zu minen, da die Verteilung des Rewards unabhängig von begonnenen Runden funktioniert. Die Methode PPLNS kann trotz Einschränkungen nach Rosenfeld (Rosenfeld 2011a, S. 10) als fairer Verteilungsmechanismus angesehen werden.

Die Schwierigkeit bei diesem Verfahren ist es, eine passende Anzahl an Shares zu bestimmen, die in der Auszahlung berücksichtigt werden. Eine verbreitete Methode ist es, eine feste Anzahl an Shares festzulegen und bei einem gefundenen Block den Reward abzüglich einer fixen Gebühr gleichmäßig unter allen Shares aufzuteilen.

Bei dieser einfachen Variante von PPLNS kann ein Angreifer sich zunutze machen, dass es profitabler ist, wenn ein Abfall der Difficulty bevorsteht und nachteilig, wenn die Difficulty steigen wird. Das kommt daher, dass die erwartete Auszahlung bei PPLNS von der zukünftigen Difficulty abhängt, wohingegen die Beteiligung und der Einsatz des Miners von der momentanen Difficulty bestimmt werden. Ein Angreifer kann somit theoretisch einen gewissen Vorteil erlangen (Rosenfeld 2011d).

Eine naheliegende Verbesserung kann die Anzahl an relevanten Shares sein, die das Vielfache der momentanen Difficulty ist. Hierbei kommt es nach Rosenfeld (Rosenfeld 2011d) allerdings zu ähnlichen Problemen. Wenn beispielsweise die Anzahl der Shares gleich der Difficulty gesetzt wird, ist es lukrativer, unmittelbar vor einem Anstieg der Difficulty zu minen und Shares beizutragen. Der Grund liegt darin, dass sich durch die Erhöhung die Anzahl an für die Auszahlung relevanten Shares erhöht und damit der kurz vor Erhöhung der Difficulty eingereichte Share doppelt ausgezahlt wird. Der erwartete Gewinn für einen Share, der kurz vor einem Anstieg eingereicht wurde, ist somit höher als ein Share, der später eingereicht wurde. Das gleiche gilt für einen Share, der eingereicht wurde, bevor die Difficulty gesenkt wird, nur dass dann die erwartete Auszahlung kleiner ist.

Um die PPLNS-Methode sicher gegen Hopping-Angriffe zu machen, ist es nötig, zu jedem eingereichten Share die aktuelle Difficulty zu speichern, um diesen Angriff auszuschließen (Rosenfeld 2011a, S. 11-12). In der konkreten Umsetzung dieses Verfahrens sind allerdings noch weitere Schritte notwendig, die an dieser Stelle nicht weiter erläutert werden, da sie für das grundlegende Verständnis nicht weiter relevant sind.

Eine etwas abgewandelte Alternative zu PPLNS ist das sogenannte Pay-per-last-N-Shifts-Verfahren, was in der Praxis häufig Anwendung findet, da es für den Mining-Pool Betreiber ressourcenärmer ist, da nicht so viel gespeichert und verarbeitet werden muss wie beim klassischen Auszahlen per Share. Bei dieser Variante der Shifts wird anders als bei der Auszahlung nach Shares eine bestimmte Anzahl an Shares zu sogenannten *Shifts* zusammengefasst, wobei jeweils eine bestimmte Anzahl an vergangenen Shifts ausbezahlt wird. Der Mining-Pool BTC Guild definiert ein Shift beispielsweise als 25 Millionen Shares und zahlt die letzten 10 Shifts aus.

Für einen potenziellen Angreifer bietet weder das klassische PPLNS noch die abgewandelte Variante mit Shifts einen Anreiz, sich opportunistisch zu verhalten, um sich einen Vorteil gegenüber den ehrlichen Minern zu verschaffen, weil es keine effektive Strategie gibt, die erwartete Auszahlung für einen Share zu erhöhen. Für den Pool-Betreiber wird das Risiko, dass mehr ausgezahlt werden muss, als eingenommen wurde, durch die begrenzte Anzahl an auszahlungsrelevanten Shares bzw. Shifts minimiert, sodass dieses Verfahren als fair angesehen werden kann.

3.3.4 Double Geometric Method

Rosenfeld (2011b) schlägt im Bitcoin-Forum eine Kombination aus den beiden Methoden *Pay-per-last-N-Shares* und *geometrischer Methode* vor, die er Double Geometric Method nennt. Dabei sollen die Vorteile von beiden Verfahren kombiniert

werden, sodass im Ergebnis eine scorebasierte PPLNS-Variante entsteht.

Jedes gegen Poolhopping sichere Verfahren braucht eine gewisse Historie an eingereichten Shares bis der erwartete Gewinn gleich dem anteiligen Gewinn entspricht und das Verfahren somit fair ist. Sollte die Anzahl am Anfang einer Runde noch nicht ausreichen, können wie bei der geometrischen Methode diese notwendigen Shares mit einer variablen Gebühr simuliert werden.

Beim Pay-per-last-N-Shares wird dieses Ziel dadurch erreicht, dass die Historie sich aus zuletzt eingereichten Shares zusammensetzt, da bei diesem Verfahren die Rundengrenzen keine Rolle spielen.

Der Vorteil der Kombination beider Verfahren ist es, dass sich sowohl die poolbasierten Streuungen (Abweichungen in der Anzahl und Häufigkeit der eingereichten Shares) wie auch die sharebasierten Streuungen (Abweichungen von Zahlungen pro eingereichten Share) anpassen lassen. Bei den vorherigen Verfahren ließ sich jeweils nur eins davon anpassen.

Die genaue Vorgehensweise lautet:

1. Festlegung der Parameter f für die fixe Gebühr des Betreibers, der durchschnittlichen variablen Gebühr c sowie den Rundenüberschreitungsabfall o (sog. cross-round leakage), der angibt wie stark der Score nach jedem gefundenen Block abgesenkt werden soll.
2. Wenn der Pool zum ersten Mal gestartet wird, wird der momentane Scorewert initialisiert: $s = 1$. Für jeden Pool-Teilnehmer k wird der Score S_k initialisiert: $S_k = 0$.
3. Der Steigungsfaktor r wird bestimmt. Dabei ist p die Wahrscheinlichkeit, dass ein Share die Lösung für einen Block darstellt (vgl. 3.3.2 Geometrische Methode). Des Weiteren fließen die variable Gebühr c sowie der Rundenüberschreitungsabfall o mit ein:

$$r = 1 + \frac{p(1-p)(1-o)}{c} \tag{13}$$

   Sollte sich während der Laufzeit des Pools ein Parameter ändern, sollte r neu berechnet werden.
4. Wenn ein Teilnehmer einen Share beiträgt, wird sein Score entsprechend um den momentanen Scorewert abzüglich der Gebühren multipliziert mit der erwarteten Auszahlung ($p \cdot B$, vgl. 3.2.1 Proportionale Verteilung) erhöht:

$$S_k = S_k + (1-f)(1-c)s \cdot p \cdot B \tag{14}$$

   Anschließend wird der momentane Scorewert um den Faktor r erhöht: $s = sr$.
5. Falls der eingereichte Share ein gültiger Block sein sollte, wird nach dem 4. Schritt den Teilnehmern folgender Betrag ausgezahlt:

$$\frac{(1-o)S_k}{cs} \tag{15}$$

   Anschließend wird der Score der Nutzer um den Faktor o reduziert: $S_k = S_k \cdot o$.

Der Grundgedanke bei der Double Geometric Method ist es, dass ein Teil des Scores und damit auch ein Teil des Rewards nach jeder gefundenen Runde beibehalten bleibt. Bei PPLNS bleibt dieser Score unverändert, bei der geometrischen Methode werden nach jeder Runde die Scores zurück auf null gesetzt und damit dem Pool-Betreiber übertragen. Dadurch dass ein Teil der Scores bestehen bleiben, bleibt in langen Runden der Score nahezu unverändert, ähnlich wie bei PPLNS. In einigen aufeinanderfolgenden kurzen Runden wird dagegen der Score stark reduziert, sodass der Pool-Betreiber einen relativ hohen Anteil erhält. Die variable Gebühr ist in diesem Fall hoch. Dieser Anteil wird indirekt gespart und in den langen Runden wieder an die Nutzer ausgezahlt, wodurch sich die durchschnittliche variable Gebühr reduziert.

Wie auch bei den vorherigen scorebasierten Methoden schlägt Rosenfeld (2011a, S. 19) vor, bei der konkreten Implementierung dieser Methode mit einer logarithmischen Skala zu rechnen, da ansonsten die Werte vom Score schnell über den Wertebereich hinausgehen können.

Einem sich egoistisch verhaltenen Teilnehmer des Mining-Pools bietet diese Methode aus meiner Sicht und den zuvor dargelegten Gründen kein zuverlässiges Angriffsszenario, sodass hierbei kein Anreiz entsteht, sich unfair zu verhalten. Da der Pool-Betreiber die Streuung mittels den Parametern f, c und o regulieren kann, gilt dieses Verfahren als fair.

3.4 Beliebtheit der Methoden

Nachdem die wichtigsten Verteilungsmechanismen der Mining-Pools besprochen und ihre Stärken und Schwächen analysiert wurden, wird nun dargestellt, wie populär einzelne Verteilungsmethoden momentan sind.

Es wurden die aktuell aktiven Mining-Pools, die im Bitcoin-Wiki (Bitcoin Wiki 2013a) aufgelistet sind, ausgewertet. Dazu wurde die jeweilige Anzahl der eingesetzten Verteilungsmechanismen der Mining-Pools gezählt und anschließend in Relation mit der Gesamtanzahl gesetzt. Das Ergebnis ist Abbildung 4 dargestellt.

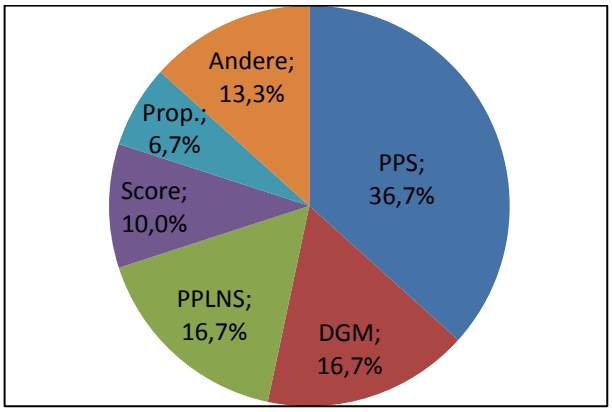

Abbildung 4. Beliebtheit der Verteilungsmechanismen

Auffällig ist, dass sich die einzelnen Methoden momentan in einer Art Wettbewerb stehen, da nicht erkennbar ist, dass sich eine Methode klar durchsetzen wird. Das Pay-per-Share-Verfahren ist in dieser Momentaufnahme am populärsten, es wird in 36,7 % der Mining-Pools eingesetzt. Das kann dadurch erklärt werden, dass es einerseits relativ einfach und intuitiv ist, andererseits sind für die Teilnehmer bei diesem Verfahren die Auszahlungen sehr gut planbar. Es ist ebenfalls denkbar, dass durch die faire Verteilung

auf der Teilnehmerseite dieses Verfahren gut dasteht. Die anderen eingesetzten Methoden werden alle in etwa gleich häufig eingesetzt, es ist kein klarer zweiter Favorit erkennbar.

Auffällig ist, dass das proportionale Verfahren noch eingesetzt wird. Es bietet einen Anreiz für opportunistisch verhaltende Teilnehmer, mehr Geld zu verdienen (vgl. Kapitel 3.2.1). Der Grund, dass diese Methode eingesetzt wird, kann einerseits sein, dass den Mining-Pool Betreibern die Möglichkeit des Betrugs bei der proportionalen Methode unbekannt ist. Andererseits kann es sein, dass das Risiko zwar bekannt ist, aber unterschätzt wird und die Methode deshalb trotzdem eingesetzt wird.

Im Mining-Pool *BitcoinPool.com* wird beispielsweise noch die proportionale Verteilung angewandt. Diesem Pool ist das Risiko des Poolhoppings offenbar bewusst. Es wird versucht abzuwenden, indem nach jeder langen Runde ein potenzieller Betrüger eine verringerte Auszahlung erhält (Geebus 2011). Hierbei kann es allerdings passieren, dass ehrliche Miner, die nur zufällig am Anfang der Runde ausgestiegen sind, dafür zu Unrecht bestraft werden. Diese Methode kann zwar den Anreiz für unfaire Teilnehmer einschränken, geht aber zulasten der ehrlichen Miner.

4. FAZIT / AUSBLICK

In dieser Arbeit wurde das Mining in das Bitcoin-Umfeld eingeordnet und als das Bestätigen von Transaktionen vorgestellt mit dem Anreiz, Geld zu verdienen. Der Bedarf an Mining-Pools wurde erläutert, da dadurch eine stetigere Auszahlung möglich ist. Als Folge sind faire Verteilungsmechanismen erforderlich, um den Bonus im Pool gerecht aufteilen zu können. Einzelne Miner oder der Betreiber sollen dadurch nicht benachteiligt werden. Es hat sich herausgestellt, dass insbesondere das proportionale Verfahren dieses Ziel nicht erfüllt. Es bietet einen Anreiz, sich opportunistisch zu verhalten und sich somit einen Vorteil gegenüber den ehrlichen Minern zu verschaffen. Weitere vorgestellte Verfahren sind weitestgehend sicher gegen ein solches Verhalten.

Die vorgestellten Verfahren stehen zurzeit im Wettbewerb miteinander, es kann nicht vorhergesagt werden, ob sich in Zukunft weitere Verfahren entwickelt werden oder ob sich ein Verteilungsmechanismus klar durchsetzt.

Die Popularität der wichtigsten Mining-Pools hat gezeigt, dass der Mining-Pool *BTC Guild* im Jahr 2013 mehrmals für kurze Zeit 50 % der Rechenleistung des gesamten Netzwerks besitzt, was eine potenzielle Bedrohung für das Netzwerk darstellt. Für folgende Arbeiten ist die weitere Entwicklung besonders zu beobachten, da eventuell ein Missbrauch dieser Rechenleistung möglich wäre.

Die Verteilung der beliebtesten Methoden der Verteilung des Rewards in Mining-Pools stellt nur eine Momentaufnahme dar, hier wäre es für weitergehende Analysen sinnvoll, den Zeitverlauf der Popularität zu untersuchen. Ein besonderes Augenmerk kann dabei auf die proportionale Verteilung gelegt werden, da dieses aufgrund der Betrugsanfälligkeit im Zeitverlauf abnehmen sollte.

5. REFERENCES

Bitcoin Wiki 2012a. “Block chain.” https://en.bitcoin.it/wiki/Block_chain. Abrufdatum: 10.05.2013.

Bitcoin Wiki 2013a. “Comparison of mining pools.” https://en.bitcoin.it/wiki/Comparison_of_mining_pools. Abrufdatum: 31.05.2013.

Bitcoin Wiki 2013b. “Confirmation.” https://en.bitcoin.it/wiki/Confirmation. Abrufdatum: 10.05.2013.

Bitcoin Wiki 2012b. “Difficulty.” https://en.bitcoin.it/wiki/Difficulty. Abrufdatum: 27.05.2013.

Bitcoin Wiki 2013c. “Mining.” https://en.bitcoin.it/wiki/Mining. Abrufdatum: 12.05.2013.

Bitcoin Wiki 2013d. “Mining hardware comparison.” https://en.bitcoin.it/wiki/Mining_hardware_comparison. Abrufdatum: 12.05.2013.

Bitcoin Wiki 2012c. “Nonce.” https://en.bitcoin.it/wiki/Nonce. Abrufdatum: 20.06.2013.

Bitcoin Wiki 2013e. “Pooled mining.” https://en.bitcoin.it/wiki/Pooled_mining. Abrufdatum: 10.05.2013.

Bitcoin Wiki 2013f. “Weaknesses.” https://en.bitcoin.it/wiki/Weaknesses. Abrufdatum: 12.05.2013.

Geebus 2011. “Anti-Pool Hopping Added.” http://bitcoinpool.com/forum/viewtopic.php?f=1&t=103. Abrufdatum: 31.05.2013.

Nakamoto, S. 2009. “Bitcoin : A Peer-to-Peer Electronic Cash System.”

Raulo 2011. “Optimal pool abuse strategy.” http://bitcoin.atspace.com/poolcheating.pdf.

Rosenfeld, M. 2011a. “Analysis of Bitcoin Pooled Mining Reward Systems.” https://bitcoil.co.il/pool_analysis.pdf.

Rosenfeld, M. 2011b. “Double geometric method: Hopping-proof, low-variance reward system.” https://bitcointalk.org/index.php?topic=39497.msg481864#msg481864. Abrufdatum: 28.05.2013.

Rosenfeld, M. 2011c. “Geometric method.” https://bitcointalk.org/index.php?topic=4787.msg69890#msg69890. Abrufdatum: 27.05.2013.

Rosenfeld, M. 2011d. “PPLNS.” https://bitcointalk.org/index.php?topic=39832.msg486012#msg486012. Abrufdatum: 27.05.2013.

slush 2011. “Slush’s Pool (mining.bitcoin.cz).” https://bitcointalk.org/index.php?topic=1976.msg50002#msg50002. Abrufdatum: 27.05.2013.