Woodcoin:
Eine elektronische Peer-to-Peer-Währung, erschaffen für Stabilität und Langlebigkeit
v1.0

Funkenstein der Zwerg

31. Oktober 2014

Ins Deutsche übersetzt von Kilian Kunst

Übersicht:

Wir beschreiben hier die Überlegungen zum Design von Woodcoin, sowie dessen Implementierung, mit Fokus auf den Eigenschaften, welche Woodcoin von anderen Kryptowährungen abgrenzen. Ähnlich wie Bitcoin ist Woodcoin eine Kryptowährung. Jedoch ist Bitcoin so entworfen, dass es einer nicht erneuerbaren Ressource gleicht: Gold. Woodcoin hingegen gleicht eher einer nachhaltigen Ressource. Insbesondere verhindert Woodcoin zeitliche Asymmetrien welche bei Bitcoin durch seinen Schöpfungsmechanismus auftreten. Dadurch wird ein Anreiz zur Partizipation, geschaffen, sowie die Langlebigkeit von Woodcoin gewährleistet. Unsere Lösung basiert auf einem logarithmischen Wachstum der Geldmenge. Zusätzlich skizzieren wir die Gestaltungsüberlegungen hinter den beiden anderen Änderungen des Kernprotokolls: Mining mit der Skein-Hash-Funktion, sowie die Absicherung von digitalem Besitz mithilfe der X9_prime256v1 Kurve durch ECDSA.

Einführung:

Vor sechs Jahren befreite der große Zauberer, Satoshi Nakamoto, Mittelerde von den Fängen der Fälscher, indem er den Proof-of-Work Algorithmus in der ersten Implementierung einer öffentlichen Kryptowährung publizierte: Bitcoin [Nakamoto, 2008]. Unser jetziges Werk, Woodcoin, ist eine experimentelle Kryptowährung, die von der Bauweise her Bitcoin sehr ähnelt und seine Codebasis mit Bitcoin, sowie zwei seiner Nachfolger teilt: Litecoin und Quark. Das Ziel von Woodcoin ist es, eine sehr langfristige Währung zu schaffen, die auch in sehr ferner Zukunft praktikabel und stabil ist.

Schöpfungsmechanismus:

Ausschlaggebend für die finanzielle Anwendbarkeit und Stabilität einer Kryptowährung ist der Belohnungsplan, auch Schöpfungsmechanismus genannt. Man könnte es auch den Inflationsplan der Geldmenge nennen. Bei öffentlichen Kryptowährungen ist dieser Plan nicht privat oder diskret, sondern im Voraus geplant, verifizierbar und wird von allen Teilnehmern reguliert. Satoshi hat ein Modell ausgewählt, welches simpel gesagt das Abbauen einer nichterneuerbaren Ressource simuliert. Ein konstanter Betrag werde dabei nach jedem Block geschöpft und nach einem fixen Betrag an Blöcken (210,000 Blöcke oder nach nahezu vier Jahren bei dem klassischen Bitcoin) werde dieser Betrag um die Hälfte reduziert. Dies kann man als geometrische Reihe beschreiben:

$$R_n = \frac{k}{2^n} \qquad (1)$$

Hier ist R_n die Belohnung zu einem Zeitpunkt n mit k als initialer Konstante (k=50 bei dem klassischen Bitcoin).

Dies ist in der Mathematik üblicherweise auch als geometrische Reihe bekannt, deren Summe rapide mit einem Ansteigen von n konvergiert. Das Ergebnis ist, dass nach den ersten vier Jahren die Hälfte aller jemals zu schöpfenden Bitcoin abgebaut sind. Außerdem wird in relativ naher Zukunft die Belohnung pro Block gegen Null tendieren und der weitere Abbau von Bitcoin wird

allein durch den Anreiz von Transaktionskosten geschaffen werden. Es ist unklar, wie Bitcoin und andere Kryptowährungen sich in so einem Stadium verhalten. Das Problem ist, dass die Kosten für eine Double-Spend-Transaktion innerhalb eines Blocks proportional zu der Belohnung für das Abbauen von Bitcoins stehen.

Es sind eben diese Eigenschaften, die wir durch unseren logarithmischen Schöpfungsmechanismus im Rahmen von Woodcoin verbessern wollen. Anstelle einer geometrischen Reihe verwenden wir bei Woodcoin eine Harmonische, in welcher die Belohnung wie folgt ausgegeben wird:

$$R_n = \frac{k}{n} \tag{2}$$

In diesem Fall gibt es einen unmittelbaren Unterschied, der sich darin äußert, dass die Summe der Reihen nicht konvergiert. Theoretisch resultiert das in einer unendlichen Geldmenge. Dadurch, dass unser Belohnungslimit jedoch durch die kleinstmögliche Einheit, nämlich 1 Satoshi (10^{-8} LOG), begrenzt wird, wird es auch ein endgültiges Limit der Geldmenge geben.

Nichtsdestotrotz wächst die harmonische Reihe unglaublich langsam. Der Zeitpunkt der letzten Belohnung wird erreicht sein, wenn $R_n = 10^{-8}$ ist. Für Woodcoin haben wir $k = 1000000$ gesetzt, sodass wir den letzten LOG-Satoshi im Block $n = 10^{14}$ erreichen werden, nach dem Julianischen Kalendar etwa im Jahr 380 Millionen.
Das Maximum der Geldmenge wird in dem Jahr bei etwa 27,625,814 LOG liegen.

Während Bitcoin die Hälfte seiner BTC bereits in vier Jahren geschöpft hat, erwarten wir, dass die Hälfte aller LOG nach dem Julianischen Kalendar um das Jahr 2305 geschöpft sein werden.

Die gesamte LOG Geldmenge an einer Blockgröße n ist durch die Addition aller Belohnungen der vorigen Blöcke festgelegt:

$$S_n = \sum_{100}^{n} \frac{k}{n} \approx k \cdot \log(n + \gamma) - F \tag{3}$$

Wobei die Annäherung dem großen Zauberer Euler zu verdanken ist. Hier ist γ die Euler-Mascheroni-Konstante bei ~0.577, und *log* ist der natürliche Logarithmus. *F* repräsentiert die Größe des Waldes, welcher aus diesen initialen Blöcken hergestellt worden ist, für die das Holz nicht zu der Menge hinzugezählt wird:

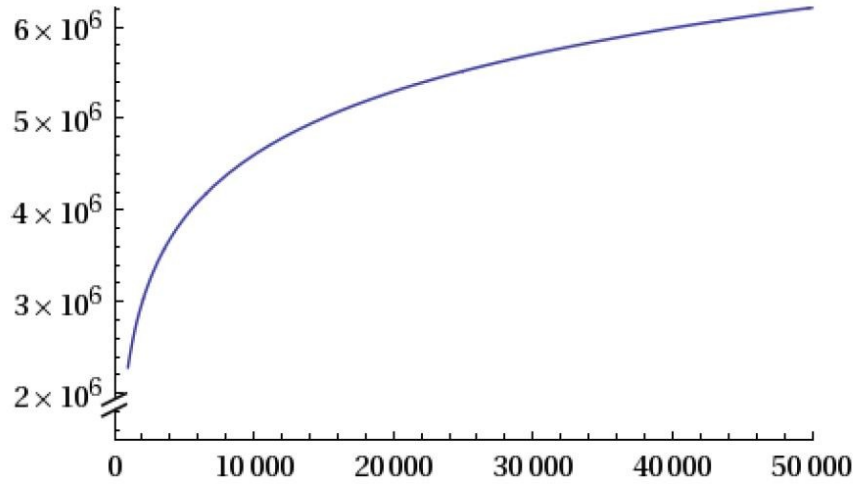
$$F = \sum_{0}^{100} \frac{k}{n} = 5{,}187{,}377 \tag{4}$$

Der Wald wird eingeführt, um extrem hohen Belohnungen für die frühen Blöcke vorzubeugen und um einen rationalen Nutzen einer erneuerbaren Ressource zu modellieren.

Einige Kryptowährungen haben entschieden, ab einem gewissen Punkt eine fixierte, konstante Belohnung einzuführen (z.B. Dogecoin). Dies bedeutet eine letztendlich lineare Inflation und Abwertung bereits existierender Coins, weshalb wir uns entschieden, diesen Ansatz zu verwerfen. Andere Coins haben eine Belohnung eingeführt, die sich proportional zu einer externen Auswirkung verhält, wie z.B. der Hashrate (z.B. Peercoin). Wir lehnen auch diesen Ansatz ab, da dieser Unsicherheit in Bezug auf die Berechnungen der Geldmenge und dem Potenzial für zukünftig

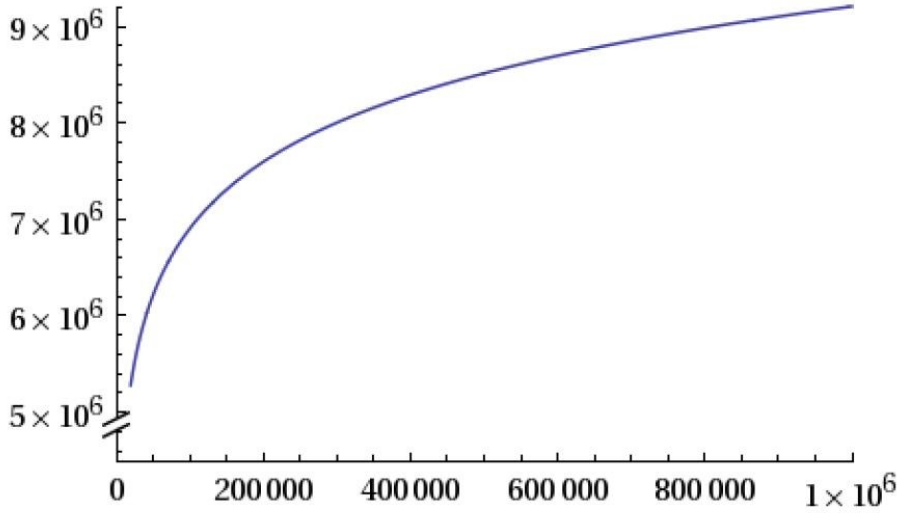
lineare Inflation birgt. Diese Ansätze versuchen zu der Langlebigkeit der Coins beizutragen, indem sie einen Anreiz schaffen, den Coin abzubauen, jedoch zu einem Nachteil. Mit Woodcoins Ansatz hingegen sichern wir die Langlebigkeit des Holzabbau-Anreizes, ohne die negativen Effekte von unbegrenzter oder unsicherer Inflation.

Die seichte Schöpfungskurve von Woodcoin is wohl am besten visualisierbar, indem man die gesamte Geldmenge der Blockzahl gegenüberstellt, wie zu sehen in Darstellung 1 und 2.



Darstellung 1: Woodcoins gesamte Geldmenge für die Blöcke 0 bis 50000.

Wie man beim Vergleich der Darstellungen Eins und Zwei sehen kann, ist eine wichtige Eigenschaft der logarithmischen Funktion die Selbstähnlichkeit. Bei jedem Block sinkt die Belohnung und ein Holzfäller wird einen Vorteil gegenüber jedem zukünftigen Holzfäller haben. Der Anreiz Holz zu hacken, ist in jedem gegenwärtigen Moment vorhanden und wird nicht künstlich verringert.



Darstellung 2: Gesamtmenge von Woodcoin für die Blöcke 0 bis 1 Million.

Proof-of-Work Algorithmus:

Bei der Auswahl einer Hash-Funktion über die Proof-of-Work stattfindet und Blöcke erstellt werden, welche die Transaktionen verifizieren, gibt es viel Diversität in der Welt der

Kryptowährungen. Viele Coins wählen Funktionen, die versuchen normale CPU-Leistung zum Abbau zu verwenden, ohne einen Anreiz für Spezialhardware zu schaffen. Wenn diese Coins erfolgreich sind und an Wert gewinnen, werden sie in diesem Unterfangen scheitern, da alle Algorithmen mit der richtigen Hardware schneller ausgeführt werden können. Für unsere Wahl einer Hash-Funktion versuchen wir nicht, ASIC oder GPU Holzhacken zu vermeiden. Vielmehr wählen wir eine Hash-Funktion, die wir als die Sicherste ansehen und dessen Implementierungen wir verstehen. Die Beschreibung und Promotion der Skein-Funktion sprengt den Rahmen dieser Arbeit und ist am besten deren Erschaffern überlassen [Ferguson et al., 2008]. Nichtsdestotrotz heben wir zwei Fakten der Skein-Hash-Funktion hier hervor:

1) Sie wurde zu Teilen von Bruce Schneier erschaffen
2) Sie wurde nicht von der NSA als offizielle SHA3-Hash-Funktion ausgewählt

Wahl der elliptischen Kurve für ECDSA:

Die wahrscheinlich wichtigste Technologie, welche Kryptowährungen möglich macht, ist ein Digital Signature Algorithmus, welcher Teilnehmern ermöglicht, den Besitz eines Coins zu belegen und ihn somit auszugeben. Diese Technologie wurde das erste mal 1976 von den großen Zauberern Whitfield Diffie und Martin Hellman bekannt gemacht. Eine Angemessene Diskussion der Geschichte würde den Rahmen dieser Arbeit sprengen, aber es sollte bemerkt werden, dass ihr Werk aus dem Jahr 1976 bereits den Aufstieg von digitalen Handelsgütern vorhersagte. Wie die meisten Kryptowährungen haben auch wir uns dazu entschieden, einen anderen Algorithmus als denjenigen zu verwenden, welcher in der Arbeit von 1976 beschrieben worden ist, um digitale Unterschriften zu erstellen: Wir nutzen den Elliptic Curve Digital Signature Algorithm (ECDSA). Um dieses System zu verwenden, benötigt es die Wahl einer bestimmten elliptischen Kurve. Auch wenn wir über keine praktische Schwäche irgendeiner bekannten Kurvenwahl Bescheid wissen, nutzen wir die Gelegenheit um weitere kryptographische Vielfalt zu schaffen und wählen eine andere Kurve als die meisten anderen Kryptowährungen, welche eine Kurve wählen, die als secp256k1 bekannt ist. Die Kurve, die wir nutzen, ist bekannt als ANSI X9.62 Prime 256v1 und wurde als empfohlene Kurve für finanzielle Institutionen vor der Jahrhundertwende bekannt [ANSI, 1999].

Fazit:

Beim Lesen der vorigen technischen Diskussion über die Eigenschaften von Woodcoin, wurde ein wichtiges Element vergessen. Wir haben den Wald vor lauter Bäumen nicht gesehen. Holzhacken soll ein unterhaltsamer, neuer Weg sein, um an Kryptowährungen heranzugehen und uns ermutigen, die Minen für einen Augenblick zu verlassen und die Schönheit des Holzes zu bewundern. Holzhacken ist erheiternd, und während wir holzhacken können wir daran denken, dass diese Ressource, aufgrund unserer sorgsamen und nachhaltigen Planung, auch in ferner Zukunft noch vorhanden sein wird. Wir erinnern uns darüber hinaus auch an die Wichtigkeit, den Wald, ein vielfältiges Ökosystem, zu erhalten, Rücksicht auf die Intelligenz der Bäume und das Geschenk von frischer kühler Luft zu nehmen und das Ökosystem des Waldes zu respektieren. Während Kryptowährungen auf dem Vormarsch sind und nichterneuerbare Energiequellen weiter dezimiert werden, ist zu erwarten, dass der duale Nutzen des Holzhackens und Hauswärmens weit verbreitet sein wird. Holz ist auch in anderen Bereichen eine wichtige Ressource und wir hoffen, LOG zu entwickeln um es für eine Vielfalt von Anwendungen anderer Kryptowährungen einzusetzen, sobald atomische Cross-Chain-Transaktionen implementiert sind.

„Blockchains sind Datenbanken, die wie ein Baumstamm strukturiert sind.“ – Funkenstein der Zwerg

Referenzen:

1) “Bitcoin: A peer to peer electronic currency”, Satoshi Nakamoto, 31. Oktober, 2008

2) “The Skein Hash Function Family”, Niels Furguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker, 15. November, 2008

3) ANSI X9.62, “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 1999