PPCoin: Peer-to-Peer Kryptowährung mit Proof-of-Stake

Sunny King, Scott Nadal
(sunnyking9999@gmail.com, scott.nadal@gmail.com)

19. August 2012

Auszug

Peercoin ist eine Peer-to-Peer Kryptowährung, welche auf dem Design von Satoshi Nakamotos Bitcoin basiert. Proof-of-Stake ersetzt Proof-of-Work um den Großteil der Netzwerksicherheit zu gewährleisten. In diesem Hybriddesign wird Proof-of-Work nur für das anfängliche Erzeugen der Währung genutzt. Auf lange Sicht wird es aber an Wichtigkeit verlieren. Das Sicherheitsniveau des Netzwerkes ist dabei unabhängig von der Leistungsaufnahme. Dadurch wird eine energieeffiziente und preisgünstige Peer-to-Peer Kryptowährung bereitgestellt. Proof-of-Stake basiert auf dem Coin-Alter und wird von jedem Knoten erzeugt. Dies geschieht über ein Hashing-Schema, welches beeinflusst und ähnlich zu Bitcoins ist (mit limitiertem Hash-Suchbereich). Die Blockkette und die Transaktionen sind darüber hinaus über einen zentral verteilten Checkpunktmechanismus geschützt.

Einleitung

Seit der Erschaffung von Bitcoin (Nakamoto 2008), ist Proof-of-Work immer das vorherrschende Design von Peer-to-Peer Kryptowährungen gewesen. Das Konzept von Proof-of-Work bildet das Rückgrat bei dem Erzeugungs- und Sicherheitsmodell von Nakamotos Design.

Im Oktober 2011 haben wir erkannt, dass das Konzept des *Coin-Alters* ein alternatives Design zu Bitcoins Proof-of-Work, bekannt als *Proof-of-Stake*, ermöglicht. Wir haben seitdem ein Design formuliert, in dem Proof-of-Stake das Sicherheitsmodell einer Peer-to-Peer Kryptowährung bildet und einen Teil des Erzeugungsprozesses darstellt. Proof-of-Work wird dabei den initialen Teil des Erzeugungsprozesses ermöglichen, dann aber langsam an Bedeutung verlieren. Dieses Design versucht die Durchführbarkeit von zukünftigem Peer-to-Peer Kryptowährungen, die nicht vom Energieverbrauch abhängen, zu demonstrieren. Wir haben dieses Projekt *ppcoin* genannt.

Coin Alter

Das Konzept des Coin-Alters war Nakamoto mindestens seit 2010 bekannt. Es kommt auch im Bitcoin zum Einsatz, dient aber beispielsweise nur dazu die einzelnen Transaktionen zu priorisieren. Es spielt aber keine wichtige Rolle im Bitcoin Sicherheitsmodell. Eine einfache Definition des Coin-Alters ist die Dauer über die sich Währungseinheiten im eigenen Besitz befinden. Ein einfaches Beispiel soll dies

verdeutlichen: Wenn Bob 10 Coins von Alice erhält und diese für 90 Tage hält, dann fallen für Bob 900 Coin-Tage an.

Wenn Bob jetzt diese 10 Coins, die er von Alice erhalten hatte, ausgibt, so *konsumiert* (oder *zerstört*) Bob alle Coin-Tage die er mit diesen Coins erhalten hatte.

Um die Berechnung des Coin-Alters zu ermöglichen, haben wir ein Zeitstempelfeld für jede Transaktion eingeführt. Block und Transaktionszeitstempel Protokolle wurden gestärkt um die Berechnung des Coin-Alters zu sichern.

Proof-of-Stake

Proof-of-Work hat dazu beigetragen Nakamotos großen Durchbruch zu verwirklichen. Jedoch bedeutet es für diese Kryptowährungen auch vom ständigen Energieverbrauch des Proof-of-Work abzuhängen. Dies führt dann zu signifikanten Unkosten, welche für den Betrieb der Netzwerke notwendig werden. Diese Netzwerke werden von den Nutzern aufgrund einer Kombination von Inflation und Transaktionsgebühren getragen. Sobald die Erzeugungsrate im Bitcoinnetzwerk abnimmt, könnte es eventuell notwendig werden den Druck auf höhere Transaktionsgebühren zu erhöhen, um weiterhin ein angestrebtes Sicherheitsniveau zu halten. Man fragt sich natürlich ob dieser Energieverbrauch nötig ist um eine dezentrale Kryptowährung zu haben. Folglich ist es ein wichtiger Meilenstein, theoretisch und technisch, zu demonstrieren, dass die Sicherheit einer Peer-to-Peer Kryptowährung nicht vom Energieverbrauch abhängen muss.

Das als Proof-of-Stake bezeichnete Konzept wurde in Bitcoinkreisen seit Anfang 2011 diskutiert. Grob gesagt steht Proof-of-Stake für den Besitznachweis an Währungseinheiten. Das Coin-Alter, das innerhalb einer Transktion konsumiert wird, kann als eine Form des Proof-of-Stake bezeichnet werden. Wir haben unabhängig dazu im Oktober 2011 das Konzept des Proof-of-Stake und des Coin-Alters entwickelt. Dabei haben wir erkannt, dass Proof-of-Stake tatsächlich die meisten Proof-of-Work Funktionen ersetzen kann. Erreicht wurde es mit vorsichtigen Designänderungen an dem Währungs-Erzeugungsprozess und Sicherheitsmodell des Bitcoin. Dies ist möglich, da Proof-of-Stake, ähnlich zum Proof-of-Work, nicht leicht gefälscht werden kann. Natürlich ist die Fälschungssicherheit eine der kritischsten Anforderung an ein Geldsystem. Philosophisch gesprochen: Geld war bereits in der Vergangenheit eine Form von Arbeitsbeweis und sollte daher in der Lage sein einen weiteren „Proof-of-Work“ durch sich selbst zu ersetzen.

Block Erstellung durch Proof-of-Stake

In unserem Hybriddesign werden die Blöcke in zwei unterschiedliche Typen separiert: Proof-of-Work und Proof-of-Stake Blöcke.

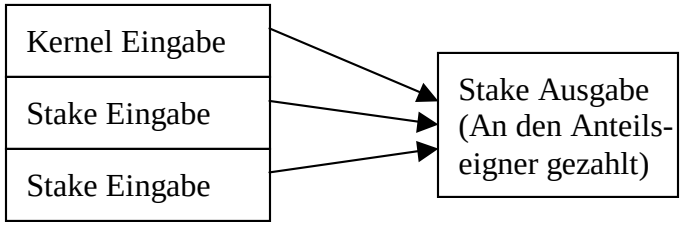

Abb.: Struktur einer Proof-of-Stake (coinstake) Transaktion

In dem neuen Proof-of-Stake Blocktyp gib es eine spezielle Transaktion welche *coinstake* genannt wird (benannt nach der speziellen Bitcointransaktion *coinbase*). In einer coinstake-Transaktion entlohnt sich der Finder des Blockes selbst. Dabei wird das Coin-Alter konsumiert, aber auch das Recht erlangt einen Block für das Netzwerk zu erstellen und einen monetären Proof-of-Stake Anteil zu erzeugen. Die erste Eingabe im coinstake wird *kernel* genannt und ist nötig für die definierten Hashziele im Protokoll. Durch diese Hashziele wird die Erzeugung von Proof-of-Stake Blöcken ein stochastischer Prozess. Ganz ähnlich zu den Proof-of-Work Blöcken. Jedoch gibt es einen wichtigen Unterschied. Die Hashingoperation wird über einen begrenzten Suchbereich ausgeführt (genauer gesagt gibt es einen Hash für jede nicht ausgegebene Einheit pro Sekunde). Im Gengensatz dazu steht ein unbegrenzter Proof-of-Work Suchbereich. Somit ist kein signifikanter Verbrauch an Energie beteiligt.

Das Hashziel, welches ein Stake-kernel erreichen muss ist eine bestimmte Menge an Coin-Alter (Coin-Tage) welches im kernel verbracht wird. Im Gegensatz dazu steht Bitcoins Proof-of-Work Ziel, welches ein fixes Ziel darstellt, das über alle Knoten angewendet wird. Daher wird es mit steigendem Coin-Alter leichter das Hashziel zu erreichen, welches im kernel konsumiert wird. Ein Beispiel: Wenn Bob Einheiten mit einem zusammengesetzten Coin-Alter von 100 Coin-Jahren hat und einen kernel alle 2 Tage erzeugt, dann kann Alice mit ihren 200 Coin-Jahren einen kernel in einem Tag erzeugen.

In unserem Design wird das Proof-of-Work und Proof-of-Stake Ziel kontinuierlich neu justiert um plötzliche Sprünge der Blockerzeugungsrate des Netzwerks zu verhindern. Dies steht im Gegensatz zu Bitcoins, bei denen alle zwei Wochen eine Neujustierung stattfindet.

Coin-Erzeugung basierend auf Proof-of-Stake

Ein neuer Erzeugungsprozess für Coins wurde mit der Einführung von Proof-of-Stake Blöcken im Zusatz zu Bitcoins Proof-of-Work geschaffen. Ein Proof-of-Stake Block erzeugt Coins basierend auf dem konsumierten Coin-Alter innerhalb der coinstake Transaktion. Eine Coin-Erzeugungsrate von einem Cent pro konsumiertem Coin-Jahr führt zu einer leichten zukünftigen Inflationsrate.

Obwohl wir Proof-of-Work als Teil des Erzeugungsprozesses behalten haben, um den initialen Erzeugungsprozess zu ermöglichen, ist es denkbar, dass in einem reinen Proof-of-Stake Sytem die initiale Erzeugung von Coins bereits im Genesisblock geschehen kann. Dies könnte in einem Prozess ähnlich wie bei einem Börsengang geschehen, indem ein initiales öffentliches Angebot gemacht wird (IPO).

Hauptketten Protokoll

Das Protokoll um zu ermitteln, welche konkurrierenden Blockketten (block chains) sich durchsetzen, wurde auf einen Prozess basierend auf dem Coin-Alter geändert. Dabei trägt jede Transaktion in dem Block zu dem insgesamt konsumiertem Coin-Alter des Blockes bei. Die Blockkette mit dem höchsten Coin-Alter setzt sich als Hauptkette durch.

Dies steht im Kontrast zu dem Bitcoin Proof-of-Work Hauptketten Protokoll, bei dem die insgesamt geleistete Arbeit genutzt wird um die Hauptkette zu bestimmen.

Dieses Design mindert einige Bedenken bzgl. des 51% Ansatzes von Bitcoin, bei dem das System nur als sicher gelten kann, solange die guten Knoten 51% der Netzwerk Hashingleistung aufbringen. Zunächst einmal sind die Kosten, um einen signifikanten Besitz zu kontrollieren, deutlich höher als eine signifikante Menge an Hashingpower zu kontrollieren. Dies hebt die Kosten solcher Attacken für entsprechend mächtige Gruppen. Zudem wird das Coin-Alter in einer solchen Attacke konsumiert, was es deutlich schwieriger für den Angreifer gestaltet es fortlaufend zu verhindern, dass neue Transaktionen in die Hauptkette einfließen.

Checkpunkte: Schutz der Historie

Einer der Nachteile beim Ermitteln der Hauptkette durch konsumieren des gesamten Coin-Alters ist, dass es die Kosten einer Attacke über die gesamte Historie der Blockkette reduziert. Wenn auch Bitcoin einen relativ starken Schutz über die Block Historie hat, so hat Nakamoto dennoch 2010 Checkpunkte, als eine Mechanismus um die Blockkette zu härten, eingeführt. Dies verhindert alle Änderungen an der Blockkette vor diesem Checkpunkt.

Eine andere Sorge ist es, dass die Kosten für die doppelte Ausgabe von Coins ebenfalls gesenkt werden würden. Der Angreifer muss nur ein bestimmtes Coin-Alter aufbringen um eine Reorganisation der Blockkette zu erzwingen. Um den Handel in einem solchen System praktikabel zu machen haben wir uns entschieden eine weitere Form von Checkpunkten einzuführen. Diese werden zentral über das Netzwerk verteilt. Dies geschieht in viel kürzeren Intervallen als nur ein paar Mal täglich um sicher zu stellen, dass die Blockkette regelmäßig eingefroren und Transaktionen abgeschlossen werden. Dieser neue Typ von Checkpunkten wird genauso verteilt, wie das Alarmsystem von Bitcoin.

Laurie (2011) hat argumentiert, dass Bitcoin das s.g. „verteilte Konsens“ (distributed concensus) Problem noch nicht vollständig gelöst hat, da die Funktionen für die Erstellung von Checkpunkten nicht verteilt werden. Wir versuchten ein praktisches verteiltes Checkpunktprotokoll zu schreiben, aber fanden es schwierig eine Absicherung gegen einen „network split“ zu finden. Auch wenn der aktuell verwendete Mechanismus zum Verteilen der Checkpunkte eine Form von Zentralisierung darstellt, so denken wir dennoch, dass es akzeptabel ist, bis eine verteilte Lösung bereit steht.

Es folgt ein weiterer technischer Grund, weshalb zentral verteilte Checkpunkte genutzt werden. Zum Schutz gegenüber Denail of Service Attacken muss der coinstake kernel validiert werden, bevor ein Proof-of-Stake Block akzeptiert und in die lokale Datenbank (block tree) jedes Knoten aufgenommen werden kann. Aufgrund des Bitcoinknoten Datenmodells (speziell der Transaktionsindex) ist eine Frist innerhalb der Erstellung von Checkpunkten nötig. Damit soll sichergestellt werden, dass alle Knoten in der Lage sind einen coinstake kernel zu verifizieren, bevor dieser in die lokale Datenbank geschrieben wird. Aufgrund der oben genannten praktischen Überlegungen haben wir entschieden das Datenmodell der Knoten nicht zu verändern, sondern stattdessen zentrale Checkpunkte zu nutzen. Unsere Lösung ist es, die Berechnung des Coin-Alters zu verändern, um ein minimales Alter zu verlangen, wie etwa einen Monat. Jedes Coin-Alter unterhalb ist gleich null. Die zentralen Checkpunkte werden dann genutzt um sicherzustellen, dass alle Knoten mit den Transaktionen älter als einen Monat übereinstimmen. Dies erlaubt dann die Überprüfung von coinstake kerneln, da ein kernel ein ungleich Null Coin-Alter aufweisen muss. Daher muss für diesen kernel ein mehr als einen Monat alter Ertrag verwendet werden.

Blocksignaturen und das Duplicate Stake Protokoll

Jeder gefundene Block muss vom Besitzer signiert werden um zu verhindern, dass er kopiert und von Angreifern genutzt wird.

Ein “duplicate-stake” Protokoll wurde zum Schutz gegen solche Attacken entworfen. Andernfalls könnte ein Angreifer aus einem gefunden Proof-of-Stake Block eine Vielzahl an Blocken generieren und damit eine Denail of Service Attacke ausführen. Jeder Knoten sammelt alle kernel/Zeitstempel Paare von allen coinstake Transaktionen die er gesehen hat. Sobald ein Block ein kernel/Zeitstempel Duplikat eines vorhergehenden Blocks aufweist, so ignorieren wir diesen Block bis ein nachfolgender Block als verweist (orphan) gilt.

Energieeffizienz

Wenn die Proof-of-Work Rate gegen Null geht, dann wird es immer weniger Anreize dafür geben weitere Proof-of-Work Blöcke zu erzeugen. In diesem Scenario wird der

Energieverbrauch auf einen sehr niedrigen Wert fallen, da desinteressierte Miner die Suche nach solchen Blöcken beenden werden. Das Bitcoinnetzwerk wird mit diesem Problem konfrontiert werden, wodurch das Transaktionsvolumen oder die Transaktionsgebühr steigen müssen um den benötigten hohen Energieverbrauch weiter wirtschaftlich erhalten zu können. In unserem Design ist es möglich das Netzwerk mit Proof-of-Stake zu schützen, selbst wenn der Proof-of-Work Energieverbrauch null erreicht. Wir nennen eine Kryptowährung *long-term energy-efficient* (langzeit Energieeffizient), wenn es möglich ist, dass der Proof-of-Work Energieverbrauch null erreichen darf.

Weitere Überlegungen

Wir haben die Proof-of-Work Erzeugungsrate so modifiziert, dass es nicht von der Blockanzahl (Zeit) abhängt, sondern von der Schwierigkeit (Difficulty). Sobald die Erzeugungsschwierigkeit steigt, wird sich die Proof-of-Work Erzeugungsrate senken. Wir haben uns somit für eine geglättete Erzeugungskurve gegenüber der Stufenkurve des Bitcoin entschieden um den Markt nicht plötzlich künstlich zu Schocken. Genauer gesagt wurde eine kontinuierliche Kurve gewählt, bei der die Erzeugungsrate sich halbiert, sobald die Erzeugungsschwierigkeit um den Faktor 16 steigt.

Über einen längeren Zeitraum wird die Proof-of-Work Erzeugungskurve nicht stark vom inflationären Verhalten des Bitcoin abweichen (Moores Law). Wir denken es ist klug, ungeachtet der starken Kritik einiger Ökonomen an Bitcoin, der traditionellen Beobachtung zu folgen, dass ein Markt eine leichte Inflation gegenüber einer hohen Inflation vorzieht.

Babaioff et al. (2011) hat den Effekt von Transaktionsgebühren studiert und argumentiert, dass diese Transaktionsgebühr einen Anreiz für die Miner darstellt nicht miteinander zu kooperieren. In unserem System wird dieser Anreiz verschärft, daher geben wir die Transaktionsgebühr nicht an den Blockfinder weiter. Wir haben uns dazu entschieden die Transaktionsgebühr stattdessen zu vernichten. Das stoppt den Anreiz die von anderen gefundenen Blöcke zu ignorieren. Ebenso dient es auch als deflationäre Kraft, um der inflationären Kraft des Proof-of-Stake entgegenzuwirken.

Wir haben uns auch dafür entschieden feste Transaktionsgebühren auf Protokollebene zu erzwingen, um damit Transaktionsspam (block bloating) zu verhindern.

Während unserer Forschung haben wir auch eine dritte Möglichkeit neben Proof-of-Work und Proof-of-Stake entdeckt. Wir haben es *Proof-of-Excellence* genannt. In diesem System wird regelmäßig ein Turnier veranstaltet um Coins zu erzeugen. Die Erzeugungsrate basiert dann auf der Leistung der Turnierteilnehmer. Diese Erzeugungsrate stellt also eine Nachbildung der Preise eines echten Turniers dar. Allerdings tendiert auch dieses System dazu Energie zu verbrauchen, sobald eine

künstliche Intelligenz die Beteiligten übertrifft. Wir finden dieses Konzept dennoch interessant, selbst in solchen Situationen, da es eine Form des „intelligenten“ Energieverbrauchs darstellt.

Abschluss

Nach Prüfung des Designs für den Markt erwarten wir, dass das Proof-of-Stake Design eine potentiell wettbewerbsfähigere Form der Peer-to-Peer Kryptowährungen im Gegensatz zum Proof-of-Work Design wird. Dies ist durch die Unabhängigkeit zum Energieverbrauch, niedrige Inflation und niedrige Transaktionsgebühren, bei vergleichbaren Sicherheitsniveau, möglich.

Danksagung

Vielen Dank an Richard Smith für die Hilfe beim Testen und die verschiedenen Netzwerk- / Entwicklungszweigarbeiten.

Wir bedanken uns bei Satoshi Nakamoto und den Bitcoin Entwicklern deren brilliante Pionierarbeit uns den Verstand erweitert und ein Projekt wie dieses erst ermöglicht hat.

Referenzen

Babaioff M. et al. (2011): On Bitcoin and red balloons.

Laurie B. (2011): Decentralised currencies are probably impossible (but let’s at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)