TECHNICAL NOTES

Seesaw Reward Balance System

Whitepaper
aka the
'Purplepaper'

Revision 0.8a March 23 2017 Pivx.org

Der Zweck dieser technischen Dokumentation ist es, die Eigenschaften und Konzepte der Kryptowährung PIVX (Private Instant Verified Transaction) zu beschreiben. Dieses Dokument erklärt umfassend die technischen Details des “Seesaw Reward Balance Systems” (Vergütungsbalancierung) und der damit einhergehenden Vorteile.

www.pivx.org
media@pivx.org

EINFÜHRUNG

Die Mehrheit der Kryptowährungen, die Masternodes nutzen, teilen die Block-Vergütung zu gleichen Teilen zwischen den Verteilungsmechanismen “Mining” einerseits und “Masternodes” andererseits auf. Die beabsichtigte Fairness eines solchen Vergütungssystems kann durch eine steigende Anzahl von Masternodes untergraben werden, wenn diese von großen Investoren betrieben werden und es somit potenziell zu einer Zentralisierung des Budget-Systems kommen kann - ähnlich einem Großaktionär in einer Aktiengesellschaft. Der originäre Nutzen, welcher sich aus dem Konzept von Masternodes ergibt, kann somit dazu führen, dass weniger Nutzer Proof-Of-Stake-Mining (PoS) betreiben, womit die Sicherheit des PoS-Netzwerkes gesenkt wird.

Masternodes stellen wertvolle Services bereit und sollten daher für diese Dienstleistungen vergütet werden. Unser Ziel ist es, diese Dienste nicht in höherem Maße zu entlohnen, als die Services wert sind. Unserer Meinung nach nutzt eine höhere Vergütung von Masternodes disproportional den Betreibern dieser, und nicht anderen Nutzern des Systems; dies führt ultimativ zu einer größeren Zentralisierung.

Das in diesem Dokument dargestellte Feature wurde mit dem Ziel entwickelt und implementiert, das oben beschriebene Problem zu beseitigen und somit die Sicherheit des PoS-Netzwerkes zu gewährleisten. Dies wird dadurch erreicht, indem wir die Nutzer zum “Staken” (engl. “der Einsatz”) motivieren, was in der Folge zu mehr Liquidität bei Exchanges und zu einer besseren Kontrolle des Wachstums und der Knoten im Masternode-Netzwerk führt.

PIVX

Private Instant Verified Transaction, kurz PIVX, ist eine auf die Privatsphäre der Nutzer fokussierte und dezentrale Open-Source-Kryptowährung. PIVX startete am ersten Februar 2016 unter dem Namen Darknet (DNET) und wurde später als PIVX neu positioniert. Die initiale Phase der Proof-Of-Work-Verteilung (PoW) endete im August 2016, als DNET in den derzeitigen Proof-Of-Stake-Status (PoS) überführt wurde.

PIVX läuft auf einem speziellen, auf Konsens basierten Proof-Of-Stake-Algorithmus und basiert auf der Bitcoin Core 0.10.x Code-Base. Es wird ein Netzwerk von Masternodes [2] eingesetzt, um einen dezentralen Selbstverwaltungsmechanismus und eine erhöhte Privatsphäre bei den Transaktionen zu gewährleisten.

Das Hauptziel von PIVX ist es, vertrauliche Transaktionen in Fast-Echtzeit zu ermöglichen und ein Selbstverwaltungssystem zu etablieren, welches den Aufbau eines nachhaltigen Netzwerks unterstützt - zum Vorteil aller Nutzer. Wir sind hierbei auf gutem Wege, einige Features sind noch in der Entwicklung und werden daher erst in naher Zukunft erscheinen.

PIVX Weiterführung

PIVX bietet ein transparentes Maßnahmensystem, ein technisches Entwicklungsumfeld sowie ein hochgradig zugängliches Entwicklungsteam. Das Team nutzt eine Vielzahl an Social Network-Kanälen, inklusive Social Media. Das Entwicklungsteam heißt jede und jeden herzlich willkommen, unabhängig von deren technischer Expertise. Wir ermutigen Menschen, Dinge einfach zu tun, anstatt das persönliche Engagement durch hierarchische Strukturen und das Einholen von Genehmigungen in seine Schranken zu weisen.

Für mehr Details zu PIVX, siehe pivx.org.

PROOF OF STAKE 2.0

Um Konsens zu erreichen, benötigt Proof-Of-Stake 2.0 (PoS) Netzwerkknoten, welche durch die Wallet-Software Coins in der Blockchain nachweisen und Transaktionen verifizieren. Die teilnehmenden Knoten erhalten innerhalb einer festgelegten Zeitspanne, proportional zum jeweiligen Stake-Anteil, eine Anzahl an Blöcken; diese werden vergütet.

Das bedeutet, dass das Netzwerk durch viele teilnehmende Knoten (bei ähnlicher Verteilung der Coins) sehr sicher wird. Dadurch wird es schwieriger, die Mehrheit an Coins innerhalb des Netzwerkes zu besitzen.

MASTERNODES

Masternodes sind Netzwerkknoten, welche mit derselben Blockchain verbunden sind, dieselbe Wallet-Software ausführen und dabei zusätzliche Services im Netzwerk anbieten. Diese Services beinhalten Coin-Mixing (um eine erhöhte Vertraulichkeit bei Transaktionen zu gewährleisten), Transaktionen in Echtzeit, sowie das dezentrale Selbstverwaltungssystem, welches ein dezentrales Budget-System mit einem unveränderlichen Vorschlags- und Abstimmungssystem beinhaltet.

Für diese Services erhalten die Betreiber von Masternodes eine Vergütung pro Block. Diese Vergütung, abzüglich der Kosten für den Betrieb der Knoten, kann für die Betreiber von Masternodes ein passives Einkommen darstellen.

HAUPT-FEATURE

Um im Netzwerk ein ausgewogenes Verhältnis an Staking- und Master-Knoten zu erreichen, hat das PIVX-Team ein System zur variablen Vergütung entwickelt. Dieses sogenannte “Seesaw Reward Balance System” reguliert dynamisch die Block-Vergütung zwischen Masternodes und Staking-Nodes.

Jede PoS-Block-Vergütung von PIVX ist wie folgt aufgeteilt: 10% sind für das Budget-System und 90% sind gemeinsam für Masternodes und Stake-Mining vorgesehen. Letzteres wird durch das Seesaw Reward Balance System wiederum zwischen Master- und Staking-Nodes aufgeteilt.

Die Logik ist im Grunde einfach: Je mehr Masternodes teilnehmen, umso kleiner ist der Vergütungsanteil eines jeden PoS-Blocks für Masternodes und umso höher ist der Anteil für Staking-Nodes. Umgekehrt, wenn die Anzahl der Masternodes fällt, steigt der Vergütungsanteil für Masternodes und fällt entsprechend für Staking-Nodes.

Die PoS-Block-Vergütung startet mit einem Verhältnis von neun zu eins zugunsten von Masternodes; vorausgesetzt der in Masternodes gehaltene Anteil an Coins ist niedriger als 1% des gesamten Angebots an Coins. Wenn der Anteil an in Masternodes gehaltenen Coins jedoch 41,5% des gesamten Angebots an PIVX Coins überschreitet, verlagert sich die Block-Vergütung und mehr als 50% der Block-Vergütung gehen an Staking-Nodes.

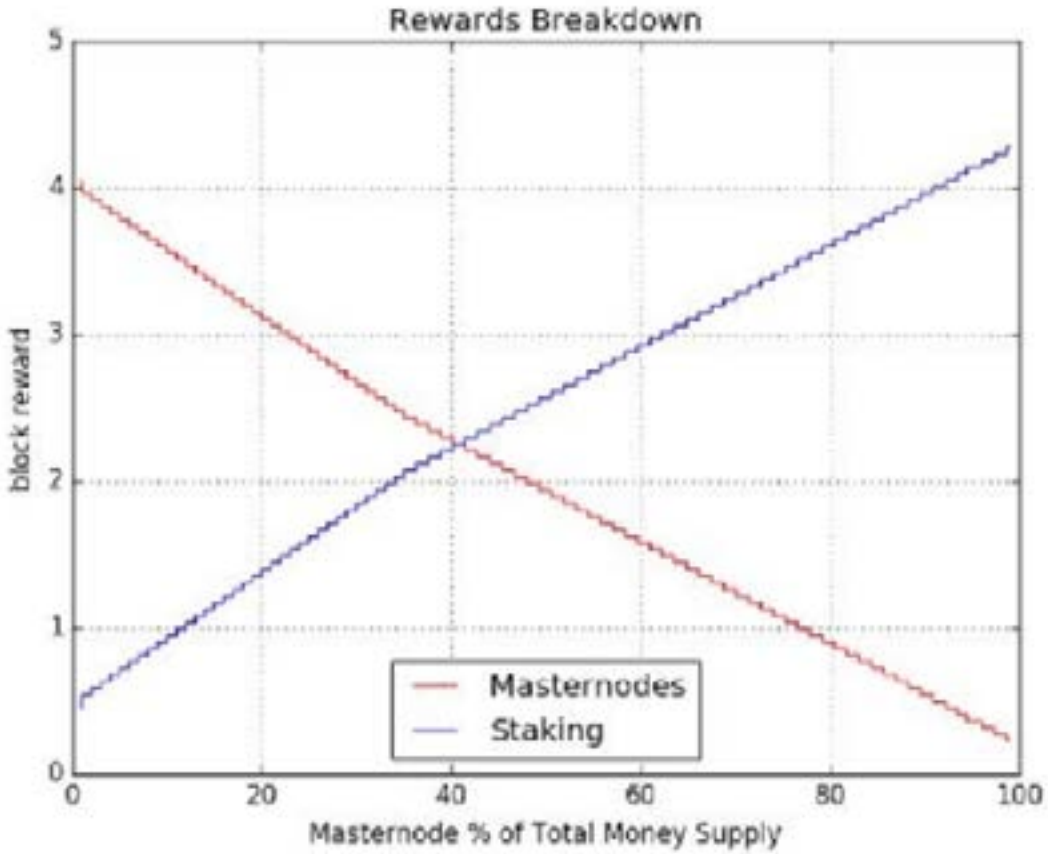
Dieser Effekt macht es weniger attraktiv, zunehmend mehr Masternodes zu betreiben, weil damit die Profitabilität potentiell signifikant niedriger als beim Staking ausfällt, welches zudem geringere Betriebskosten aufweist.

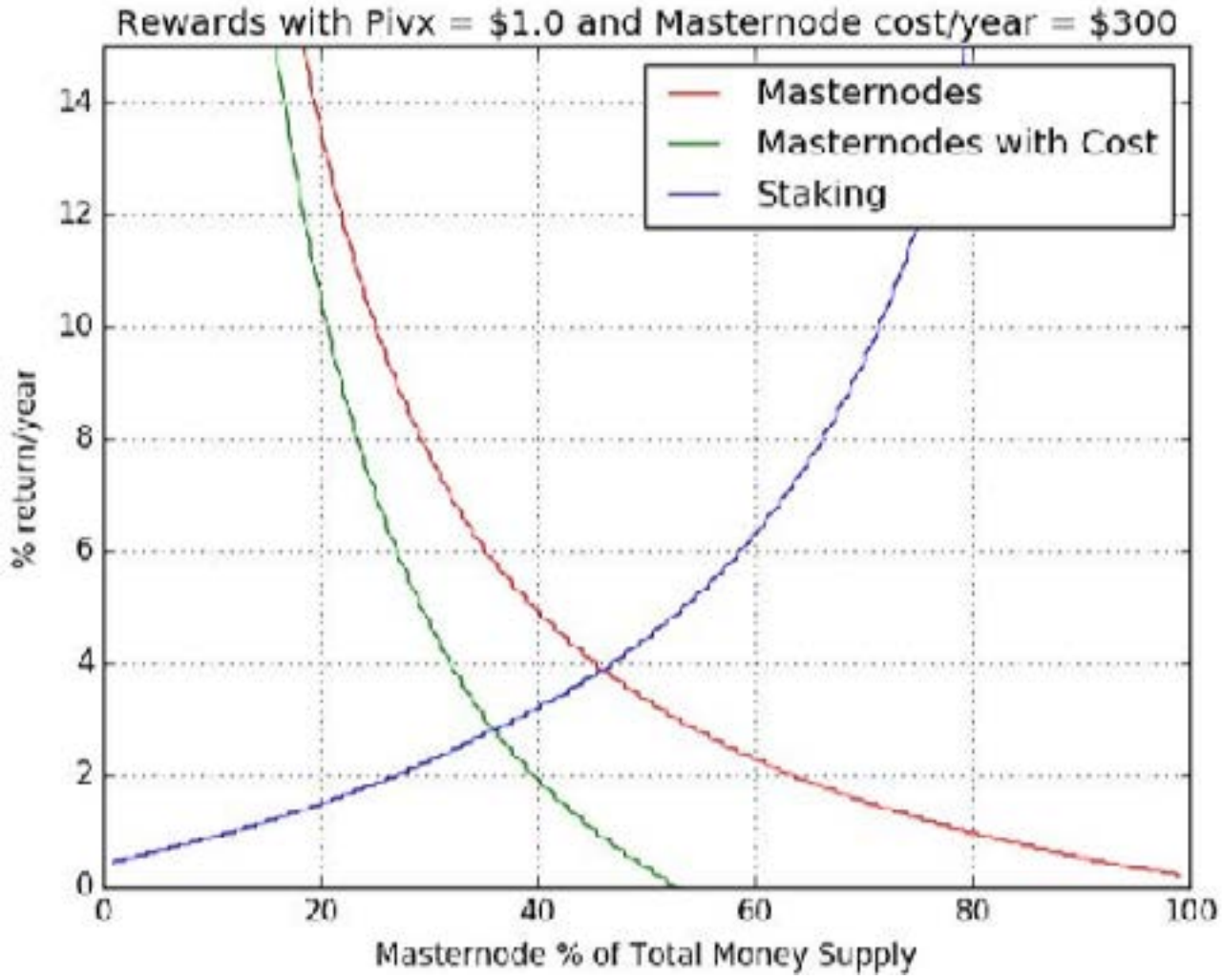
Durch diese Logik kann sich einerseits ein starkes Netzwerk an profitablen Masternodes bilden, während andererseits ungefähr 60% der gesamten zur Verfügung stehenden Coins für Staking-Aktivitäten bereitstehen und somit das Netzwerk sicher machen und entsprechende Liquidität zur Verfügung steht.

Ein weiterer beabsichtigter Effekt und ein Ziel der Vergütungsbalancierung ist, dass es profitabler ist Masternodes zu betreiben, anstatt dieselbe Menge an Coins zu “staken” (vorausgesetzt ist der Normalzustand, der unterhalb des Gleichgewichts-Schwellenwert liegt). Der Grund dafür liegt darin, dass es riskanter sowie kosten- und zeitintensiver ist, eine Masternode zu betreiben als lediglich zu staken.

WIPPEN-EFFEKT

Die folgende Grafik zeigt die Block-Vergütung (Y-Achse) für Masternodes (rot) und Staking-Nodes (blau) im Verhältnis zum prozentualen Anteil des Gesamtangebots an Coins, welche in Masternodes gebunden sind (X-Achse) [ab Block 648.000, Mitte Mai 2017], wobei jede Block-Vergütung 5 PIV fix beträgt. Die danach folgende Grafik zeigt die theoretische jährliche Rendite ab Block 648.000 wobei jeder Block fix 5 PIV und das Intervall 60 Sekunden beträgt (1.440 Blöcke pro Tag).





Die rote Linie repräsentiert die Rendite von Masternodes im Falle von keinen Betriebskosten, und die grüne Linie zeigt die Renditen-Kurve pro Masternode in einem hypothetischen Szenario, in dem die Betriebskosten pro Masternode und Jahr 300 USD und der Preis pro PIV ein USD betragen.
The BLUE line represents the % return per year calculation of staking nodes

BESCHREIBUNG DER CODE-LOGIK

Die Logik soll so einfach wie möglich und gleichzeitig effektiv sein. Damit wird Stabilität sichergestellt, das Ergebnis transparent nachvollziehbar gemacht und die zugrunde liegende Logik kann - sollte die Notwendigkeit auftreten - einfacher optimiert werden.

```
if (mNodeCoins <= (nMoneySupply * .01) && mNodeCoins > 0) {
   ret = blockValue * .90;
}
```

BlockValue ist die Gesamtzahl an Coins pro Block. Dieser Wert wird mit dem variablen Verhältnis multipliziert, welches durch den Prozentsatz von Masternode-Coins (mNodeCoins) in Relation zur Gesamtanzahl an Coins (nMoneySupply) ermittelt wird. Der resultierende Wert ret ist die Anzahl an Coins, welche für die Vergütung der Masternodes zur Verfügung gestellt wird.

Das obige Beispiel zeigt die ursprüngliche Logik, um die höchste Masternode-Vergütung zu bestimmen. Wenn mNodeCoins kleiner oder gleich 1% der Gesamtanzahl an Coins (nMoneySupply) und zudem größer als 0 ist, dann ist die Blockvergütung für Masternodes 90% des PoS-Blocks (ret = blockValue * 0,90).

Mit jeder Erhöhung in festen Prozentschritten fährt die Logik fort bis mNodeCoins kleiner oder gleich 99% der Gesamtmenge an Coins ist:

```
else if (mNodeCoins <= (nMoneySupply * .99)
        && mNodeCoins > (nMoneySupply *.987)) {
   ret = blockValue * .05;
}
```

Jeder mNodeCoins-Wert über 99% der Gesamtmenge an Coins resultiert in einem fixen Wert von 1% von blockValue. Die Erwartung ist, dass es nie zu diesem Punkt kommt, die Logik adressiert somit jedoch alle möglichen Ergebnisse.

```
else {
   ret   = blockValue *          .01;
}
```

Der Algorithmus des Seesaw Reward Balance Systems startete ursprünglich mit nur 16 Prozentschritten und wurde seitdem verbessert: Die aktuelle Implementierung des variablen Wippen-Mechanismus besteht aus 105 Prozentschritten wodurch eine präzisere Abstufung gewährleistet werden kann.

ZUSAMMENFASSUNG

Das von PIVX eingesetzte Seesaw Rewards Balance System bietet gegenüber den Vergütungsmethoden von anderen, auf Masternodes basierenden Proof-Of-Stake-Kryptowährungen eine Vielzahl an Vorteilen:

1. Das System kann indirekt die Gesamtzahl von Masternodes im Netzwerk beeinflussen, indem sich die Vergütung in Relation zum Staking verändert.
2. Es fördert das Staking durch erhöhte Auszahlungen, wenn die Anzahl der Masternodes hoch ist. Somit wird ein hohes Maß an Netzwerk-Sicherheit gewährleistet.
3. Die Profitabilität der Masternodes ist höher als bei Staking; vorausgesetzt die Anzahl an Masternodes bleibt unter dem Gleichgewichtsbereich (ca. 40% des Angebots an Coins).
4. Es ermöglicht allen Besitzern von Coins, eine Vergütung zu erhalten, nicht nur den Betreibern von Masternodes. Dies führt zu einem ausgeglichenen und weniger zentralisierten System.

AUSBLICK

Das Seesaw Reward Balance System ist relativ neu (lediglich fünf Monate alt als dieses Dokument geschrieben wurde). Daher kann es sein, dass durch ein weiteres Wachstum des Netzwerkes weitere Feineinstellungen nötig sein können und sich bessere Grenzwerte als effektiver herausstellen.

In den ersten fünf Monaten von PoS mit über 1.400 Masternodes, welche über 30% der Gesamtzahl an Coins repräsentieren, hat der Algorithmus jedoch bewiesen, dass er wie vorgesehen und reibungslos funktioniert.

QUELLCODES

GITHUB
https://github.com/PIVX-Project/PIVX/blob/v2.1.6/src/main.cpp#L1786

LINKS
BTC Bekanntmachung:
https://bitcointalk.org/index.php?topic=1262920.0

Offizielle Website https://pivx.org
Masternode Payment Information http://178.254.23.111/~pub/DN/DN_masternode_payments_stats.html

EINZELNACHWEISE

[1] PoS 2.0 Whitepaper http://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper-cn.pdf

[2] DASH Masternodes https://dashpay.atlassian.net/wiki/display/DOC/Masternode

AUTOR

Geschrieben von: jakiman
Editiert von: werwortmann, spock
'PurplePaper' Formatiert von: @money-alchemist
Übersetzt von: jan

www.pivx.org