Sayfa 1

Tritium Trust ile Nexus Proof-of-Stake
Colin Cantrell
Scott Simon
Ekim 12, 2018

Sayfa 2

1. Giriş
Nexus ağı, geçerli bloklar üretmek için üç kanal kullanarak çalışır
ve yeni NXS para birimi - iki Proof-of-Work kanalı ve bir Proof-
Bahis payı kanalı. Orijinal Proof-of-Stake kanalı, con-
tutarlı ve dürüst düşünceyi ölçmek için temel bir bileşen olarak güven duygusu
Nexus ağına bir düğüm tarafından haraç. Felsefesini takip etti
Zaman yatırımları için insanları ödüllendirmede “herkesin zamanı vardır”.
Tritium Trust, bir dizi sürümün ilkini temsil eder.
Nexus ağında Trityum protokolü. Bu sürümle birlikte
Nexus sürüm 0.2.5.0, güven ve Proof-of-Stake sistemleri revize edildi ve
geliştirilmiş. Bu değişiklikler sayesinde Nexus, gelecek için zemin hazırladı
Bir Güven ve İtibar sistemini içerecek şekilde TAO çerçevesinin sürümleri
üç boyutlu zincirin ayrılmaz bir parçası olan Güven Kilitleri gibi.[1]
Bu makale, özellikle Tritium Trust sürümündeki ayrıntıları tartışmaktadır.
Nexus Proof-of-Stake'in revize edilmiş uygulamasıyla ilgili olarak.
2 Terimlerin Tanımı
2.1 Genel Koşullar
adres - Genel tanımlayıcı görevi gören benzersiz bir karakter dizisi
size ödeme yapılmasını sağlamak. Bir adrese ödeme gönderildiğinde,
blockchain bu işlemi saklar. Ortaya çıkan denge düşünülebilir
bu adreste "saklandığı gibi".
bakiye - Sahip olduğunuz jeton miktarı. Toplamı temsil edebilir
tutar, tek bir cüzdandan erişilen miktar (cüzdan bakiyesi) veya
tek bir adres tarafından erişilen miktar (adres bakiyesi). Tüm bakiye
Tüm işlemleri kaydeden bir defter görevi gören blok zincirinde saklanır.
coin yaşı - Blockchain tek bir yerde bir bakiye depolamayabilir. O
genellikle birden çok konum arasında bölünür. Madeni para yaşı bir ortalamayı temsil eder
mevcut konumlarında ne kadar süreyle saklandığının ölçüsü.
1 bkz. "Nexus Üç Boyutlu Zinciri Basitleştirilmiş" gjsteele71 tarafından
https://steemit.com/bitcoin/@gjsteele71/the-nexus-three-dimensional-chain-simplified
1

---

3. Sayfa

coinbase işlemi - Proof-of-Work madencileri bu işlemi
her bloğu kazıyorlar. Ödül şeklinde yeni madeni paraları daraltır (oluşturur)
bloğu oluşturan madencinin adresine ödeme yaptı.
coinstake işlemi - Coinbase'in Proof-of-Stake karşılığı
işlem. Yeni bir Kanıt oluşturmanın ödülünü ödemek için yeni madeni paralar çıkarır.
of-Stake bloğu.
anahtar - Kriptografik algoritmalar genellikle bir çift oluşturan iki anahtar kullanır: a
elinde tutan kişi için gizli olan özel anahtar ve bunu yapabilecek bir genel anahtar
paylaşılmak. Kripto para birimleri için, anahtar terimi tipik olarak özel
anahtar. Bu, cüzdanınızda saklanan anahtardır. Dijital imzalar oluşturabilir
yalnızca paralarınıza erişmenize ve harcamanıza izin verir. Genel anahtar,
daha kısa ve daha kolay paylaşılan genel adresi türetmek
anahtar kendini.
node - Blockchain ağına bağlı ve çalışan bir bilgisayar

ağın blockchain yazılımı. Bu kripto para birimi düğümü bir kopyasını saklar
blok zincirinin kendisinin ve ağın doğrulanması ve aktarılması yoluyla desteklenmesi
hem bloklar hem de işlemler. Çoğu kripto para birimi düğümünde ayrıca bir
bilgisayar sahibinin sistemi kullanmasına izin veren cüzdan arayüzü.
Proof-of-Stake (PoS) - Bir para biriminin mülkiyetine dayalı bir madencilik şekli
öfke. Bu sahiplik, ilgi anlamında bir "hisseyi" temsil eder.
bir şey. PoS madencileri, nispeten basit bir şirketi çözerek paylarını kanıtlıyor.
gerçekleştirmek için sahiplik gerektiren varsayımsal sorun. Bunu yaparak
yeni bir blok oluşturmaya ve ödül kazanmaya uygun hale gelir. Bu süreç
genellikle "madeni paralarınızı stake etme" olarak anılır ve ortaya çıkan ödül,
"Stake etme ödülü".
Proof-of-Work (PoW) - Hesaplamaya dayalı bir madencilik türü
Çözmesi karmaşık ancak doğrulanması basit bir sorun. Bir so-
lution, sorunu çözmek için yapılan işin yapıldığını kanıtlayarak,
madenci yeni bir blok oluşturma ve ödül kazanma hakkını elde eder.
cüzdan - Özel anahtarlarınızı saklayan ve karşılık gelen bir yazılım programı
Blockchain üzerindeki bakiyenize erişim sağlayan adresler. Bir cüzdan

---

4. sayfa

aslında paralarınızı değil, yalnızca anahtarlarınızı saklıyor. Cüzdan bakiyesi temsilcisi
blok zincirinde depolanan değerin içindeki anahtarlar tarafından erişilebilen
Cüzdan.
2.2 Nexus Şartları
blok yaşı - Nexus Proof-of-Stake için bu,
bir cüzdan son PoS bloğunu başarıyla kazdığından ve
blok zinciri. Başka bir deyişle, oluşturulan en son PoS bloğu kaç yaşında?
o cüzdanla mı?
Genesis - Nexus Proof-of-Stake'in yeni bir
stake etmeye katılmak için cüzdan. Her cüzdan yalnızca bu işlemi gerçekleştirir
bir Zamanlar. Bir cüzdan ilk PoS bloğunu başarıyla kazdığında, Genesis
işlem cüzdanda, tüm PoS'lar için kullanılan bir güven anahtarı oluşturur.
ileriyi göster.
Genesis işlemi - PoS bloğunun coinstake işlemi bulundu
Başlangıç aşamasında bir cüzdan tarafından.
Güven işlemi - Bulunan herhangi bir PoS bloğunun eşleştirme işlemi
cüzdan Genesis aşamasını tamamladıktan sonra.
güven anahtarı - Genesis işlemi tarafından cüzdanınızda oluşturulan özel anahtar.
Bu anahtarla ilişkili genel NXS adresi, tüm stake etme işlemleri için kullanılır.
ödül ödemeleri. Stake etme süreci aynı zamanda mevcut cüzdan bakiyesini de hareket ettirir
ve bu adrese güven puanı kaydı ile birlikte kaydeder.
güven puanı - Ağın bir ağa atanan iç güven düzeyini yansıtır.
güven anahtarı, anahtar sahibinin çalıştırdığı eşdeğer sürenin bir ölçüsü olarak
Dürüst, güvenilir ve zamanında düğüm. Bu zaman ölçüsü
mutlak değil. Normal çalışma sırasında tahakkuk ettirilir, ancak tahakkuk eden tutar
dürüst, güvenilir veya zamanında olmadığında azaltılabilir.
TAO çerçevesi - Nexus Three'yi uygulamanın üç aşaması
sırasıyla Trityum, Amin ve Obsidian adlı boyutsal zincir. Her biri
genel mimarinin bir boyutunu uygulayan büyük bir güncellemeyi temsil eder.
tecture ve bir veya daha fazla sürümden oluşabilir.

5.Sayfa

Trityum - Nexus'u üç boyutlu uygulamanın ilk aşaması

zincir, Trityum White Paper'da tanımlandığı gibi2. Trityum'un kendisi com-
bir dizi yayınla ödüllendirildi: Tritium Trust, the Nexus Tritium Wallet ve
Trityum Çekirdeği. Tritium Trust, güven ve PoS sistemindeki değişiklikleri uygular.
Tritium Cüzdan tamamen güncellenmiş bir cüzdan deneyimi sağlar
ve mimarinin arayüz katmanını ve Tritium Core'u uygular
tam uygulama için gereken kalan önemli mimari güncellemeleri uygular
protokolün kabulü.

3 Proof-of-Stake

3.1 Proof-of-Stake nedir?

Proof-of-Stake kavramı ilk olarak 2012 yılında King & Nadal tarafından tanıtıldı.3
büyüyen sorununu ele alan bir madencilik biçimi geliştirmek için bir teklif olarak
Bitcoin Proof-of-Work madenciliğiyle ilgili enerji tüketimi. Geliştirdi
hibe aracı olarak bir para biriminin mülkiyet kanıtını kullanma fikri
blok zincirinde blok kazma yeteneği. Bu bloklar şunları içerir:
para sahibini benzer bir şekilde ödüllendiren işlemi yerine getirmek
Coinbase işlemlerinin Proof-of-Work madencilerini nasıl ödüllendirdiği.
Proof-of-Stake'in erken enkarnasyonları, madeni para çağı fikri etrafında inşa edildi. Üzerine
belirli bir madeni para çağına ulaştığında, para sahibi,
blok zincirine yeni bir blok yatırın.
Bu tasarım, enerji verimliliği konusunu zarif bir şekilde çözdü, ancak çekiciliğe sahipti.
geri döndüğümüzde, diğer madencilik türlerinin aksine, para birimi sahibinin
birşeyler yap. Cüzdanlarını çıkarabilir ve yalnızca etkinleştirebilirler.
katkıda bulunmadan ödül kazanmak için gereken yaş seviyesine ulaştıktan sonra
bir bütün olarak ağ.
Sonuç olarak, Proof-of-Stake aşamalı olarak iyileştirildi. Bir biçim olarak kaldı
enerji verimli madencilik, ancak para biriminin
sahipleri karşılığında sahip oldukları varlıkların büyüklüğü ile orantılı olarak ödül kazanabilirler

2 Nexus: Tritium Protokolü https://nexusearth.com/tritium-white-paper/
3 King, S .; Nadal, S. (12 Ağustos 2012). "PPCoin: Eşler arası kripto para birimi ile
Proof-of-stake "https://peercoin.net/assets/paper/peercoin-paper.pdf

---

Sayfa 6

bir düğümü her zaman (veya neredeyse her zaman) çalışır durumda tutmak için
blockchain ağının işleyişine ve güvenliğine atıfta bulunuyor.

3.2 Staking Kavramları

Zaman
Proof-of-Stake, başlangıçta madenciliğe girdi olarak zamanı tanıttı.
madeni para çağının kullanımı. Zamanı bu şekilde kullanmak, ham maddenin uygulanmasını engeller.
blokları daha hızlı çözmek için hesaplama gücü, böylece enerjiyi teşvik eder
verimlilik. Başarılı bir şekilde pay almak için önemli bir zaman yatırımı gerektiriyor
herhangi bir potansiyel saldırgana harici bir maliyet getirir. Bu, ağı iyileştirir
güvenlik.
Ağırlık
Farklı Proof-of-Stake sistemleri, ağırlık kavramı için farklı fikirler kullanır.
Temel olarak, bunların tümü, para biriminin kabiliyetinin
sahipler, bazılarının daha yüksek şansı olacak şekilde ağırlıklandırılmıştır.
diğerlerinden daha bloklar oluşturur. Madeni para yaşına dayalı sistemler genellikle ağırlıklıydı
sahip olunan madeni para sayısına göre, yani iki kişi aynı holdinge sahipse
dönem, ancak birinin sahip olacağından diğerinin iki katı madeni para vardı.
kazık blokları çıkarmak için iki kat daha fazla fırsat.
Darbe Oranı
Yıllık yüzde olarak ifade edilen bu oran, boyutu hesaplamak için kullanılır.
Bir PoS bloğundaki coinstake ödülünün, onu oluşturmak için harcanan zamandan itibaren
ve genel PoS dengesi.

PoS daha popüler hale geldikçe, para basma oranı daha yaygın olarak anılır hale geldi
faiz oranı olarak, çünkü benzer şekilde işliyor ve insanlar da
bu terimi anlamaya hazır. Ancak, bahis yapan herkes
madeni paralarının faiz getirmediğini anlayın. Madencilik yapıyorlar
blok zincirinin çalıştırılmasına ve güvenliğinin sağlanmasına yardımcı olma karşılığında ödülleri stake etme
ağ.
Dağıtım Sorunu
Saf PoS tabanlı bir para birimi, sizin gibi bir tavuk ve yumurta sorunundan muzdariptir.
Madeni paralar olmadan stake bloklarını çıkaramaz. Bu paralar önce olmalı
başka bir işlemle basılabilir. Bu nedenle, Proof'u kullanan çoğu para birimi
of-Stake ayrıca Proof-of-Work madenciliğine dayalı bir ilk dağıtım kullanır,

---

7. Sayfa

en azından geçici olarak.
Nexus, güvenliği artırmak için öncelikle 3 madencilik kanalı kullansa da, bu
tasarım aynı zamanda Proof-of-Work kanalları aracılığıyla ilk dağıtımı da destekler.
Tehlikede Olan Hiçbir Şey Problemi
Proof-of-Work madenciliği büyük miktarlarda enerji tüketimini gerektirir,
bu değerli bir kaynaktır. Diğer yandan temel bir Proof-of-Stake sistemi
el, yalnızca zaten ağda bulunan kaynakları kullanır ve kaybetmezsiniz
dürüst olmayan bir şekilde davranmak veya herhangi bir çataldaki tüm blokları imzalamak için herhangi bir şey
zincir, daha sonra tüm çatallar üzerinde inşa etmeye çalışıyor. Maliyet ya da "hiçbir şey yok
söz konusu ”. Bu, yine de yapılması gereken varsayımsal bir sorundur.
herhangi bir stake sistemi tarafından ele alınabilir.
Diğer avantajlara ek olarak, Nexus'ta birden çok kanalın kullanımı da reklam-
farklı kanallar birbirlerini dürüst tuttuğundan, bu sorunu giydirir. The
Nexus ağı, yanlış davranışa bir maliyet oluşturmak için güven kavramını da kullanır.
% 51 Saldırı
Diğer madencilik türlerinde olduğu gibi, Proof of Stake sistemleri potansiyel olarak
saldırgana ağın kontrolünü veren% 51'lik bir saldırıya maruz kalır. Un-
Ancak bu tür bir sistemde, bir saldırganın
ağdaki para biriminin en az% 51'i. Bu inanılmaz derecede eski hale geliyor
yapmak için sabırsızlanıyor ve bu nedenle, özellikle sınırlamalar eklediğinizde
frekansı engellemek ve bunu önemli bir zaman gereksinimi ile birleştirmek
stake ağırlığı oluşturmak.
Nexus içinde, yalnızca% 51'lik bir saldırının
Proof-of-Stake kanalı, ancak bir saldırganın da kontrolü ele geçirmesi gerekir.
her iki Proof-of-Work kanalının başarılı olması için.
Şişirme
Para basma oranının tanımlanması, herhangi bir stake sisteminin önemli bir yönüdür. Çok
düşük ve ödüller, düğümleri riske atmaya teşvik edecek kadar önemli değil. Çok
yüksek ve bunun sonucunda döviz arzının enflasyonu değerini aşındıracak,
özellikle zamanla birleştiğinde. Enflasyon hızla
aşırı yüksek ödüller vaat eden sistemler için nemesis.

---

8. Sayfa

Nexus'un ilk dağıtımı, 78 milyon NXS arz yaratacak ve
23 Eylül 2024 tarihinde. Daha sonra enflasyonist bir model izleyecek.
madencilik kaynaklı altın arzının yıllık enflasyonu. Altın değerini korudu

Yüzyıllardır, bu nedenle bu enflasyon seviyesinin ekonomik olarak sürdürülebilir olduğu kanıtlanmıştır.
Bu model altında, ilk dağıtım sona erdikten sonra her Çalışma Kanıtı kanal arzı yılda% 1 artıracak ve Proof-of-Stake kanalı maksimum% 3'e izin verecektir. Bu% 3 değeri ancak enlastik NXS tedariği maksimum Faiz Oranında stake edildi. Gerçekçi, Proof-of-Stake enflasyonu muhtemelen diğer iki darphaneyle uyumlu olacak kanallar.

4 Nexus Teminat Kanıtı

Tritium Trust sürümü, önceki Nexus Proof-of-Stake sistemine dayanmaktadır. tem. Önceki stake etme işleminde geliştirilen stake etme kavramlarının çoğunu kullanır sistemleri geliştirir, iyileştirir ve performansı daha da artıran yeni kavramlar ekler. Proof-of-Stake için formance ve güvenlik.

4.1 Yaratılış

Yeni bir cüzdanın Nexus ağında başarılı bir şekilde pay sahibi olabilmesi için önce bir güven anahtarı oluşturun. Bu anahtar, ilkini başarıyla madenciliği yaparak oluşturulmuştur Proof-of-Stake bloğu, Genesis olarak adlandırılan bir süreç.
Genesis için stake ederken, düğüm yavaşça Güven Ağırlığı oluşturacaktır (bkz. Bölüm 4.2). Zamanla, bu ilave ağırlık, madencilik yapma şansını artırır.
PoS bloğu ve bir Genesis işlemi oluşturma. Genesis öncesi değer Güven Ağırlığı yalnızca Genesis süreci için geçerlidir ve madeni para yaşına bağlıdır. Şekil 1'de gösterildiği gibi, maksimumun% 11'i düzeyinde kapanır .
Genesis işleminin bir parçası olarak, cüzdan ayrıca güven anahtarını oluşturur ve Tüm bakiyeyi stake etmek için o anahtarın adresine aktarır. Bunun etkisi yok cüzdan bakiyesinde, yeni adrese taşımanın yanı sıra.
Tritium Trust altında, her cüzdan Genesis'i yalnızca bir kez gerçekleştirecektir. Ondan sonra bir güven anahtarı oluştururursa, onu ömür boyu kullanmaya devam eder

---

Sayfa 9

Şekil 1: Trust Weight pre-Genesis

o cüzdanın.

4.2 Güven

Yeni bir güven anahtarı oluşturduktan sonra, ağ hemen o anahtarla ilişkili dahili güven puanı. Devam eden stake oluşacak düğüm başarılı bir şekilde madencilik yaptığında ek Güven işlemleri oluşturun Proof-of-Stake bloğu. Her ek işlem, cüzdan sahibini ödüllendirir düğümlerini çalıştırmaya devam etmek için.
Devam eden stake etme aynı zamanda güven puanını korur ve tahakkuk etmesini sağlar. ing. Güven anahtarı Bozulmaya maruz kalmadığı sürece (bkz. Bölüm 4.5) veya kötü davranıştan dolayı cezalandırılırsanız, güven puanı artmaya devam edecektir.
Dahili güven puanı Nexus Proof-of-Stake için önemlidir, çünkü ağın ilişkili güven anahtarına olan güven düzeyini gösterir. Devamı güven, ağ, stake etme için daha yüksek bir ağırlık ve daha yüksek bir ağırlık belirleyen Faiz Oranı (bkz. Bölüm 4.3). Verdiği ağırlık, Güven Ağırlığı. Güven Ağırlığı için daha yüksek bir değer, başarı şansını artırır

---

Sayfa 10

Şekil 2: Güven Ağırlığı

PoS bloklarını özenle araştırmak.
Şekil 2 , güven puanı ile Güven Ağırlığı arasındaki ilişkiyi göstermektedir. O Güven Ağırlığının, mümkün olan maksimum değerinin yüzdesi olarak nasıl ifade edildiğini gösterir. değer, tahakkuk eden güven puanı olarak büyür, günler olarak ifade edilir, artar.

Genesis işleminde olduğu gibi, Trust işlemleri de herhangi bir
yeni NXS, güven anahtarının stake etme adresine cüzdana gönderildi.
4.3 Faiz Oranı (Staking Ödüllerinin Darbe Oranı)
Proof-of Work madenciliğinin aksine, Nexus Proof-of-Stake'in bir re-
blok bulmak için koğuş. Bunun yerine, ödül boyutu güvenden hesaplanır
anahtarın cari Faiz Oranı (para basma oranı), bloğu bulmak için geçen süre,
ve cüzdan bakiyesi. Genesis aşaması,% 0,5'lik (yıllık) sabit bir oran kullanır.
Genesis'ten sonra ağ, Faiz Oranını mevcut seviyesinden belirler.
tahakkuk eden güven puanı ile ölçülen güven.
Bu yıllık faiz oranı, başlangıç değeri olan% 0,5'ten maks.

Sayfa 11

Şekil 3: Faiz Oranı
güven anahtarı bir yıllık toplam tutarına ulaştıktan sonra% 3.0 imum
güven puanı.
Şekil 3 , yıllık yüzde olarak ifade edilen Faiz Oranının nasıl büyüdüğünü göstermektedir
gün olarak ifade edilen tahakkuk eden güven puanı arttıkça artar. Faiz oranı
maksimum değer olan% 3'e ulaştığında kapanır.
4.4 Blok Ağırlığı
Blok Ağırlığı, ikinci bir ağırlık değerini temsil eder. Güven ile birleşir
Yeni bir PoS bloğu kazma şansını artırmak için ağırlık (bkz. Bölüm 4.2).
Blok Ağırlığı, cüzdanın en son madencilik yaptığından beri geçen süreden elde edilir.
PoS bloğu, blok yaşı ile ölçülmüştür. Son blok ne kadar eski olursa, o kadar fazla
ulaşılan maksimum değere kadar yeni bir tane bulmaya katkıda bulunur
üç gün sonra.
Genesis sırasında, cüzdan henüz herhangi bir Proof-of-Stake bloğu çıkarmadı.
Blok yaş değeri sıfır olarak kalır ve Blok Ağırlığı da öyle. Üzerine

---

Sayfa 12

İlk PoS bloğunu araştıran Nexus, bu bloğun yaşını ölçmeye başlar,
ve Blok Ağırlığı artmaya başlayacaktır.
Cüzdan ek bir PoS bloğu kazdığında, Nexus ölçmeye başlar-
öncekinin yerine yeni bloğun blok yaşını belirlemek. Bu var
Blok Ağırlığını sıfırlamanın etkisi ve yeni blok olarak yeniden büyümeye başlar
yaş artar.
Şekil 4 , Blok Ağırlığının maksimumun yüzdesi olarak nasıl ifade edildiğini göstermektedir.
değeri, blok yaşı arttıkça büyür.
Şekil 4: Blok Ağırlığı
3 gün (72 saat) sonra Blok Ağırlığı% 100'e ulaşırsa, güven anahtarı
Bozulmaya başlar (bkz. bölüm 4.5).
4.5 Bozunma
Tritium Trust, bir cüzdanın blokları çıkaramaması durumunda Decay sürecini tanıtıyor
zamanında. Zamanında kalmak için cüzdanın yeni bir PoS bloğu çıkarması gerekir
önceki blok yaşı üç güne ulaşmadan önce. Bu zaman sınırı

Sayfa 13

Blok Ağırlığı% 100'e ulaştığında ulaşılır.
Cüzdan, yeni bir PoS bloğu madenciliği yapmadan 3 günlük sınıra ulaşırsa,
güven anahtarının süresi dolmaz. Bunun yerine, o anahtarla ilişkili güven puanı
önceki Güven işleminin düzeyine sıfırlanacaktır. Herhangi bir güven puanı
o zamandan beri eklendi. Sonra o noktadan itibaren çürümeye başlar. Güven

Puan tahakkuk eden orana 3: 1 oranında azalır.
T s = T p - 3 · (bir b - 259200)
(1)
Burada T s = yeni güven puanı, T p = son işlemde önceki güven puanı, a b =
blok yaşı (son PoS blokundan bu yana geçen süre, saniye cinsinden) ve 259200 üç gündür
saniye cinsinden ifade edilir.
Normalde, Şekil 2'de gösterilen Güven Ağırlığı eğri boyunca ilerler
güven puanı arttıkça. Çürüme sırasında, etkili bir şekilde geriye doğru hareket eder.
aynı eğri. Aynı şey, Şekil 3'teki Faiz Oranı için de geçerli olacaktır .
Cüzdan herhangi bir zamanda yeni bir bahis bloğu çıkarırsa ve
bir Güven işlemi. Güven puanı bu noktadan itibaren yeniden tahakkuk etmeye başlar.
Tritium Trust'ta Decay'in yararı, güven anahtarlarının artık süresinin dolmamasıdır.
Sadece güven puanı ekler veya çıkarırlar. Çok yatırım yapanlar
güven inşa etme zamanı, bunun gibi rastgele bir olaydan sonra sona ermeyecektir.
elektrik kesintisi. Güven puanı bir şekilde azalabilir, ancak geri kazanılabilir.
Bununla birlikte güven puanı oluşturmak için gereken zaman yatırımı
güven puanı ekleme ve çıkarma becerisinin tanıtılması, ayrıca destek
Hatalı davranış veya sahtekarlık nedeniyle güven cezalarının liman idaresi ve
Güven ve İtibarın bir parçası olarak gelecekteki uygulama için temel oluşturur
Nexus TAO çerçevesinde sistem.
4.6 Nexus'ta Coin Age Kullanımı
Yeterince farklı Proof-of-Stake sistemleri madeni para çağını farklı şekillerde kullandı
bir kafa karışıklığı meselesi haline gelebileceğini. Bu belge zaten
Nexus'un kullandığı yerlerde bozuk para yaşını gösterir ve bunu bir
bölümü daha iyi açıklığa kavuşturacaktır.
12

Sayfa 14

Bir istisna dışında, Nexus yalnızca Genesis aşamasında jeton çağını kullanır.
Madeni para yaşı, yeni bir para yatırmadan önce beklemeniz gereken minimum süreyi belirler.
cüzdan. Ayrıca Güven Ağırlığını ve Gen-
esis işlemi.
Genesis ilk PoS bloğunu çıkardıktan sonra, Tritium Trust güven puanı kullanır ve
madeni para çağı yerine blok yaşı. Yalnızca yeni eklerseniz madeni para yaşını dikkate alır
Cüzdanınıza NXS. Bu durumda, tröstte saklanan önceki bakiye
anahtarın adresi blok yaşına göre bir ödül kazanır, ancak yeni NXS miktarı
yalnızca cüzdana ekledikten sonraki süre için bir ödül kazanır (madeni para yaşı).
Bir sonraki Güven işlemi, taşınırken de bunu hesaba katacaktır.
yeni tutarı güven anahtarının adresine yazın. Bundan sonra madeni para çağı yok
daha uzun düşünüldü.
Genesis'ten sonra, madeni para yaşının güven puanı, Güven Ağırlığı üzerinde hiçbir etkisi olmadığını
unutmayın.
Blok Ağırlığı veya Faiz Oranı.
5 Yeni Bir Cüzdan ile Stake Yapmaya Başlayın
5.1 Bir Güven Anahtarı Oluşturma
Güven, gerçek hayatta kolayca kazanılan bir şey değildir. Kolayca kurulmaz
Nexus Proof-of-Stake'de. Yeni bir güven anahtarı oluşturmak bir süreçtir. Bu
işlem, özellikle daha küçük bakiyeler için oldukça fazla zaman alabilir.
Genesis ilk PoS bloğunu başarıyla geliştirdikten ve güven oluşturduktan sonra
anahtar, o anahtarla ilişkili güven puanı birikmeye başlar ancak başlar
küçük. Bu, katkıda bulunmayan düşük bir Güven Ağırlığı değeriyle sonuçlanır
ek blokları çıkarmak için çok fazla ağırlık. Güven işlemleri seyrek kalır
quent.
Bu aşamada, içinde yeni bir PoS bloğu çıkarmaması normaldir.
üç günlük süre gereklidir. Anahtar yeni olduğu için Decay hemen azalır

güven puanı başlangıç değerine (önceki işlemin güven düzeyi) ne zaman
Blok Ağırlığı% 100'e ulaşır.
Bu noktadan itibaren, Blok Ağırlığı aramaya devam ederken% 100'de kalacaktır.
PoS bloğu için, ancak Güven Ağırlığı ve Faiz Oranı minimuma döner

---

Sayfa 15

başlangıç değerleri (sırasıyla% 1,11 ve% 0,5). Bu değerler değişmeyecek
ta ki bir hisseli blok çıkarana ve bir Güven işlemi oluşturana kadar. O zaman güven
puan yeniden büyümeye başlar.
Bu döngü, yeni bir güven anahtarı oluşturmadan önce birçok kez tekrarlanabilir.
Bozulmayı ve hatayı önlemek için yeterli sıklıkta yeterli Güven işlemi
güven puanını birleştirmek. Bu normal. Hepsi güven kazanmanın bir parçası.
5.2 Nexus Staking Gereksinimleri
Minimum Bakiye
Ne kadar NXS'ye sahip olursanız olun, bir düğümü çalıştırabilir ve maden ocağı ...
Nexus Proof-of-Stake kullanan muhafazalar. Minimum miktar gerekli değildir.
Başlangıçta hesaplanan stake ödülleri alacağınız garanti edilir.
% 0,5 Faiz Oranı.
Ancak, daha yüksek bir bakiyeniz varsa, PoS bloklarını bulacak ve
İşlemlere daha sık güven ve bu nedenle daha büyük bir olasılık var
artan güven puanının daha yüksek seviyelere çıkarılması. Bu aynı zamanda faiz oranını da artırır
Maksimum% 3'e kadar stake etme ödüllerinin hesaplanması.
Minimum Para Yaşı
Bir cüzdan Genesis'i deneyip ilk PoS bloğunu kazmadan önce, bir
minimum para yaşı 72 saattir. İlk NXS'sini yeni almış yeni bir cüzdan
Stake etmeye başlamak için bu kadar uzun süre beklemelisiniz. Herhangi bir ek gönderme veya alma
Bu süre zarfında NXS'nin% 50'si madeni para yaşını değiştirir ve bu da ne kadar uzun süre artabilir
beklemeli.
Donanım
En son Nexus cüzdanının desteklediği herhangi bir sistemde NXS yatırabilirsiniz
versiyon. Şu anda, Win-
dows, MacOS veya Linux. Cep telefonları veya Raspberry Pi gibi cihazlar
henüz desteklenmiyor. Stake etme işlemi, yüksek güçlü bir makine gerektirmez.
gerçi çene. Birçoğu eski dizüstü bilgisayarları veya Intel NUC gibi mini sistemleri kullanır
güç kullanımını en aza indirmek için.
Olgunluk
Proof-of-Stake bir madencilik türüdür ve Proof-of-Work'te olduğu gibi
stake etme işleminin olgunlaşması için minimum süre. Nexus için olgunluk

---

Sayfa 16

120 blok (yaklaşık 90 dakika) sürer. Bu süre zarfında cüzdan bakiyesi
"Staking" olarak görüntülenecek ve başka bir kullanım için mevcut olmayacaktır. Eğer gönderirsen
vade süresince cüzdana ek NXS, mevcut olacak
hemen.
Üç Gün Gereksinimi
Daha önce belirtildiği gibi, bir cüzdan yeni bir PoS bloğunu başarılı bir şekilde benimsemeli ve
Bir önceki işleminden itibaren üç gün içinde bir Güven işlemi oluşturmak. Değilse,
güven puanı Decay yaşayacaktır.
6 Teknik Detaylar
Bu bölüm, Tritium Trust'ın hesaplamak için kullandığı ayrıntılı formülleri belirtir.
önceki bölümlerde tartışılan değerler. Bunlar artık kullanılmayan cal-
orijinal olarak Nexus tanıtım belgesinde belgelenen düzenlemeler.[4]

6.1 Güven Ağırlığı
Daha önce tartışıldığı gibi, Tritium Trust iki farklı hesaplama kullanır.
Trust Weight, biri Genesis işlemi sırasında madeni para yaşına dayanır ve diğeri
Stake etme işleminin geri kalanı için mevcut güven puanına göre.
Güven Ağırlığının dahili değeri 1 ile 90 arasında değişir, ancak
monly, maksimum değerinin yüzdesi olarak ifade edilir.
Genesis Güven Ağırlığı
Tritium Trust bunu yalnızca ilk PoS bloğunu kazmaya çalışırken kullanır.
W t = Min (10.0,
9.0 · ln (2 · ac
7257600 +1)
ln (3)
+ 1.0)
(2)
A c mevcut madeni para çağı olduğu yerde.
4 Nexus: Eşler Arası Ağ https://nexusearth.com/nexus-white-paper/
15

Sayfa 17

Devam Eden Güven Ağırlığı
Genesis ilk PoS bloğunu çıkardıktan ve güven anahtarını oluşturduktan sonra, Tritium
Güven, bu yöntemi kullanarak Güven Ağırlığını hesaplar.
W t = Min (90.0,
44.0 · ln (2 · Ts
7257600 +1)
ln (3)
+ 1.0)
(3)
T s , geçerli güven puanıdır.
6.2 Faiz Oranı (Staking Ödüllerinin Darbe Oranı)
Genesis işlemine dahil edilen stake etme ödülü kullanılarak hesaplanır
% 0,5'lik başlangıç oranı. PoS blokları madenciliği için sonraki tüm ödüller
birikmiş güven puanından hesaplanan bir para basma oranı.
R m =
0.025 · ln (9 · Ts
31449600 +1)
ln (10)
+ 0,005
(4)
T s mevcut güven puanı ve R m sonuçta ortaya çıkan para basma oranıdır
(faiz oranı).
6.3 Staking Ödülleri
Genesis İşlemi
S r =
C w · 0,005 · a c
31449600
(5)
Burada C w cari cüzdan bakiyesi ve S r stake etme ödülüdür.
Güven İşlemi
Bir Güven işleminde alınan stake etme ödülünün iki olası komisyonu vardır.
ponents. İlk bölüm, güven anahtarında depolanan bakiye ödülüdür.
adres, blok yaşına göre (son stake işleminden itibaren geçen süre). The
ikinci kısım, cüzdana eklenen herhangi bir yeni NXS bakiyesini hesaba katar. Bu
NXS, yalnızca ekledikten sonra ödül kazanır.
S t =

C t · R m · a b
31449600
(6)
16

Sayfa 18

C t , güven anahtarının adresindeki denge olduğunda, a b blok yaşıdır ve S t
güven anahtarından elde edilen stake etme ödülüdür.
S n =
C n · R m · a c
31449600
(7)
C n , cüzdana eklenen herhangi bir yeni NXS olduğunda, a c bunun madeni para çağıdır
yeni denge ve S n ortaya çıkan stake etme ödülüdür. Yeni NXS o zaman
daha fazla istifleme için güven anahtarının adresine aktarılır.
Bir güven işlemi için toplam ödül S r = S t + S n
6.4 Blok Ağırlığı
Tritium Trust, Blok Ağırlığını yalnızca Genesis madenciliği yaptıktan sonra hesaplar
PoS bloğu. En son çıkarılan PoS bloğunun blok yaşını kullanır.
Blok Ağırlığının sayısal değeri 1'den 10'a kadar değişir, ancak com-
monly, maksimum değerinin yüzdesi olarak ifade edilir.
W b = Min (10.0,
9.0 · ln (
2 · ab
259200 +1)
ln (3)
+ 1.0)
(8)
6.5 Bahis Ağırlığı
Bahis Ağırlığı, birleşik ağırlık ef-
Güven Ağırlığı ve Blok Ağırlığının genel bir
blok. Gerekli Eşik (bkz.Bölüm 6.6), Güven Ağırlığını ve
Doğrudan Blok Ağırlığı, bu nedenle Stake Ağırlığının değeri bilgilendirme amaçlıdır.
sadece pozlar.
W s = W t + W b
(9)
Daha önce gösterildiği gibi, Güven Ağırlığı için dahili değerler 1-90 arasında değişir ve
1-10 arası Blok Ağırlığı. Bu nedenle, Bahis Ağırlığı 2-100 arasında değişecektir ve
doğrudan yüzde olarak ifade edilebilir.
17

Sayfa 19

6.6 Gerekli Eşik
R t =
(108 − W t −W b) · 1000
(C w + S r)
(10)
Enerji Verimliliği Eşiği değeri, enerji verimliliği için bu değerin üzerinde olmalıdır.
bahis bloğu oluşturmayı denemek için cüzdan.
6.7 Enerji Verimliliği Eşiği
E t =
100 t b
N kez
(11)

T b , blok zincirine son bloğun eklenmesinden bu yana geçen süredir.
saniye.
Tritium Trust stake etme süreci, deneme süreci boyunca yinelenecektir.
PoS zorluk gereksinimlerini karşılayan bir blok hash bulmak için
Her yinelemede bir kez N. Bu ne zaman Enerji için değer yaratırsa
Verimlilik Eşiğinin Gerekli Eşiğin altına düşmesi durur.
Son bloktan bu yana geçen süre arttıkça, Enerji Verimliliği de artacaktır.
Eşik ve tekrar yinelemeye başlayabilir. Daha Yüksek Güven Ağırlığı, Blok
Ağırlık ve cüzdan bakiyesi, Gerekli Eşiği azaltır, böylece
daha fazla sayıda yineleme için ve madencilik olasılığını artırmak için
blok.
Bu, bir PoS bloğu bulana kadar veya bilgisayardan yeni bir blok alana kadar devam eder.
ağ. Yeni bir blok alırsa, süreç sıfırlanır ve baştan başlar.
Bu sürece bakmanın bir başka yolu da Kanıtın anlaşılmasıdır.
bir madencilik şekli olarak of-Stake. Gerçekte, matematik, ağırlıklar ve eşikler
yalnızca Proof-of-Stake için etkili "hash rate" belirlemek için mevcuttur. İçinde
sonunda, bu hash oranı, ortalama olarak ne sıklıkla bir blok bulacağını belirler.
ve Proof-of-Work madenciliğinde olduğu gibi bir ödül kazanın.
Proof-of-Work kullanarak madencilik yapıyorsanız ve daha fazla sonuç elde etmek istiyorsanız, o zaman
daha fazla hash oranı eklersiniz. Proof-of-Stake ile de aynısını yaparsınız. En çok
Proof-of-Stake hashing özelliğini artırmanın etkili yolu,
cüzdan, güven oluşturmak da öyle.
18

Sayfa 20

Bu süreç boyunca, stake etme algoritması yoğun olmayan, verimli bir
cient süreç[5] cüzdanın güven anahtarının parametrelerine göre,
çok sayıda pahalı donanım ve enerji tüketimine duyulan ihtiyaç.
7 Özet
Nexus 0.2.5.0'ın etkinleştirilmesiyle, Tritium Trust sürümü revize edilir ve
NXS madenciliği için bir yöntem olarak Nexus Proof-of-Stake sistemini geliştirir. O
güven anahtarlarının süresinin dolmasını ortadan kaldırır ve her ikisi olarak güven puanını uygular
ağın güven düzeyinin bir ölçüsü ve belirleme için birincil girdi olarak
madencilik, stake etme parametrelerini güncelledi.
Güven puanı, bir
Zamanında bir şekilde ve Çürüme süreci boyunca azalır. Bu yatıyor
içinde Güven ve İtibarın daha da geliştirilmesi için temel
Genel TAO çerçevesinin bir parçası olarak Nexus mimarisi.
Teşekkürler
Dino Farinacci'ye düzenleme ve yapılandırma konusundaki yardımı için çok teşekkürler
bu belge. Teknik içerik yazma konusundaki deneyimi büyük ölçüde yardımcı oldu
nihai sonucu iyileştirin. Anastasiya Maslova ve Mike'a da teşekkürler
Casey önerileri ve girdileri için.
5 Mh / s değil, tipik olarak birkaç h / s değişken bir "hash rate" olan biri