Sayfa 1

Sayfa 2

SORUMLULUK REDDİ

Buradaki hiçbir şey, herhangi bir jeton satma teklifi veya satın alma teklifi talebi oluşturmaz ve herhangi bir teklif, talep veya GoChain Token satışı olabilir. Dikkatlice okumalı ve tam olarak düşünmelisiniz
bu teknik incelemede yer alan bilgiler ve sonraki güncellemeler. Her potansiyel jeton
Katkıda bulunan kişinin bir işe alım kayıt sürecinden geçmesi gerekecektir. Bu, "Kendinizi Tanıyın Müşteri (KYC) kimlik doğrulaması ve adres belgelerinin kanıtı. Lütfen danıştığınızdan emin olun Token satışımıza katkıda bulunmadan önce uygun hukuk ve yatırım danışmanlarınızla. Bu beyaz kağıt, GoChain platformu için mevcut vizyonumuzu açıklıyor. Biz bunu gerçekleştirmeye çalışırken vizyon, lütfen bunun pek çok faktöre bağlı olduğunu ve oldukça fazla sayıda faktöre bağlı olduğunu kabul edin.
riskler. GoChain platformunun hiçbir zaman geniş çapta uygulanmaması veya benimsenmemesi tamamen mümkündür,
ya da vizyonumuzun sadece bir kısmının gerçekleşeceğini. Hiçbirini garanti etmiyoruz, temsil etmiyoruz veya garanti etmiyoruz
bu teknik incelemedeki ifadeler, çünkü mevcut inançlarımıza, beklentilerimize ve
Çeşitli beklenen ve / veya beklenmeyenler nedeniyle hakkında hiçbir güvence olamayacak varsayımlar meydana gelebilecek veya olmayabilecek olaylar. Lütfen başarıya ulaşmak için çok çalışmayı planladığımızı bilin.
vizyon ama bunların hiçbirinin gerçekleşeceğine güvenemezsin. Blockchain, kripto para birimleri ve diğer yönler
Teknolojimizin ve pazarlarımızın çoğu emekleme aşamasındadır ve birçok zorluğa, rekabete,
ve hızla değişen bir ortam. Büyüdükçe ve geliştikçe topluluğumuzu güncellemeye çalışacağız, ancak bunu yapma yükümlülüğünü üstlenmeyin.

---

3. Sayfa

1. Giriş

Kripto para birimi ve akıllı sözleşmeler dünya ekonomisini değiştiriyor. Bir para biriminden perspektif, daha önce dünyanın çoğunda imkansız olan şey - küresel olarak para transferi
anında - artık sadece mümkün değil, güvenli, hızlı, kolay ve neredeyse sürtünmesiz.
Akıllı sözleşmeler, iş yapma şeklini de hızla değiştiriyor. Bir **akıllı sözleşme** bir
Müzakereyi dijital olarak kolaylaştırmayı, doğrulamayı veya zorunlu kılmayı amaçlayan bilgisayar protokolü veya
bir sözleşmenin ifası. Akıllı sözleşmeler, güvenilir işlemlerin yapılmasına izin verir
üçüncü şahıslar olmadan. Bu işlemler izlenebilir ve geri alınamaz.
Kripto para biriminin ve akıllı sözleşmelerin blok zinciri aracılığıyla potansiyel kullanımları devrim niteliğindedir
ve akla gelebilecek hemen hemen her endüstri ve kurumu alt üst etme potansiyeline sahiptir. Ama orada
Bu vizyonu gerçeğe dönüştürmede sorun var. En büyük ve en acil sorunlar
Mevcut haliyle blockchain ölçeklenebilir değil, gerçek bir ademi merkeziyetçilikten yoksun ve saçma kullanıyor
Sürdürülebilir olmayan enerji miktarları. Bu sorunları anında çözmeyi planlıyoruz!

1.1. Yönetici Özeti

Bağımsız bir blok zinciri olan GoChain, yeni nesil bir akıllı sözleşme platformudur. Üzerine inşa edilmiştir
Ölçeklendirme problemini anında çözen gelişmiş bir Ethereum kod tabanı. Şu anda biz
devam eden saniyede 1300'den fazla işlemi gösteren çalışan bir TestNet'e sahip olmak
istikrar ve saniyede 2400 işlem kadar yüksek çalışıyor.
Ethereum'un kurucularından biri olan Vitalik Buterin, ölçeklenebilirliği bir trilema olarak etiketledi. sorunların aynı anda çözülmesi gerekir:

1. Ölçeklenebilirlik
2. Ademi merkeziyetçilik

---

4. sayfa

3. Güvenlik
Şu anda Ethereum saniyede yalnızca 13 işlemi işleyebiliyor ve bu nedenle ağları
kapasitede, yine de endüstri standardı. Denemek için boşluğa gelen başka oyuncular var.
Bu ölçeklenebilirlik sorununu çözmek için yeni blok zincirleri oluşturmak, ancak bu Ethereum
ölçeklemesini çözmeyecek
sorun. Daha sonra, bu yeni blok zinciri çözümlerinin çoğu 12-24 aydır. % 90'dan fazlası
akıllı sözleşmeler Ethereum tabanlıdır ve acil bir çözüme ihtiyaç duyarlar. Ve işte burada
GoChain devreye girer.
Sadece Ethereum ölçekleme problemini anında çözmeyeceğiz, şu anda herhangi biri
Ethereum kullanmak, herhangi bir kod yapmadan ağımıza sorunsuz bir şekilde aktarabilecektir.
alınacak değişiklikler:
1.
10 kat daha fazla ademi merkeziyetçilik
2.
Hızda 100 kat artış
3.
Enerji tüketiminde 1000 kat iyileştirme
Bunları tek tek ele alalım ve parçalayalım çünkü bu çok zor
Çözülmesi gereken sorun ve tartışmalı bir sorun. Kolay olsaydı bu beyazı okumazdın
kağıt. Ademi merkeziyetçilik ile başlayalım çünkü bu muhtemelen en tartışmalı olanlardan biri
konular bugün.
Gerçek anlamda ademi merkeziyetçi bir ağ vaadi ve şu anki gerçeklik, çarpıcı biçimde iki
Farklı şeyler. Bu yazının yazıldığı sırada, Çin'deki 4 şirket tüm şirketlerin% 70-80'ini oluşturuyor.
Ethereum dahil tüm büyük coin'ler / tokenlar için madencilik faaliyeti. Bu doğru olmaktan çok uzak
Yapabildiğiniz gibi ademi merkeziyetçilik, yine de safçılar hala onun faydalarını tartışmak
istiyorlar. Biz belli ki

5.Sayfa

katılmıyorum ve ayrıca en saf haliyle gerçek ademi merkeziyetçiliğin mümkün olmadığını kabul
ediyorum
bugün mümkün olduğunca yakınlaşmak için bazı fedakarlıklar yapmadan.
Öyleyse, sonraki en iyi çözüm nedir ve bu ademi merkeziyet sorununu nasıl çözeriz? bizim
çözüm, ortaya doğru bir adım atmaktır veya bu durumda merkezileşmeye doğru
Mümkün olan en merkezi olmayan çözümü oluşturmada ileriye doğru bir sıçrama. Bazen zorundasın
İleriye doğru bir sıçrama yapmak için bir veya iki adım geri atın.
Bunu, fikir birliği algoritmasını Proof of Work'ten (POW) Proof of
İtibar (POR). POR, yükseltilmiş, daha güçlü ve daha güvenli bir Yetki Kanıtı biçimidir
(POA). POA'da işlemler ve bloklar olarak bilinen onaylı hesaplar tarafından doğrulanır.
doğrulayıcılar. POA tipik olarak özel ağlarda ve son zamanlarda birkaç şirkette kullanılmıştır.
kimlikleri kamuya açıklanan doğrulayıcılar olarak kullanmak için benimseyenler
ve tehlikede.
Kimliklerini ele geçirme karşılığında ödüllendirilirler ve parasal olarak teşvik edilirler.
işlem işlemleri. Bireyin kimlikleri ifşa edildiğinde, bunun caydırıcı olması amaçlanmıştır.
itibarlarına zarar vereceği için kötü aktörler olmalarını engelliyorlar. Bunun olacağını sanmıyoruz
yeterince uzak çünkü ağın değeri arttıkça hile yapma teşviki daha da büyüyecek
ve daha büyük.
Bu nedenle, şirketleri doğrulayıcı olarak bireyler olarak kullanan POR'u bulduk. Bir
üne sahip bir şirket, bir bireyden çok daha fazla kaybedecek ve çok daha güçlü
risk çok daha büyük olduğu için kötü bir oyuncu olmaktan caydırıcı. Bir şirket hile yaparken yakalanır
sadece itibarını riske atmakla kalmıyor. Tüm piyasa değerini ve itibarını riske atacaktır.

şirketin görevlileri ve hissedarları. Kaybedecek her şeyden çok daha fazlası olurdu
bir birey.

Sayfa 6

Bunu bir adım öteye taşıyarak 50 farklı ülkede 50 şirketi doğrulayıcı olarak kullanmayı planlıyoruz.
ademi merkeziyetçiliği zorlamak. Doğrulayıcıları 50 farklı şirkete yayarak
söz konusu itibar neredeyse mükemmel bir ademi merkeziyetçilik yaratmalı ve ağı
ödün vermek çok zor. Dahası, düğümleri coğrafi olarak yayarak kimse
ABD veya Çin gibi hükümet girebilir ve ağı ele geçirebilir. Bu ikisi
% 51'lik saldırıları caydırmak gerekir.
Doğrulayıcılar nasıl seçilecek? Başlangıçta, GoChain doğrulayıcıları seçecek ve ardından
seçim süreci ağa devredilecektir. Ne tür şirketler olacaklar?
Think, Venture yanma oranına sahip girişimleri, VC ortakları, melek yatırımcıları ve yeni ürünü
destekledi
veya hizmet. Bu tür veya daha büyük şirketleri kullanarak büyük bir teşvik söz konusudur.
pazar kapasitesini ve profesyonel bütünlüğünü korumak için ağ bütünlüğü.
Sonra, saniyede 13 işlemden 1300+ tps'ye nasıl geçebiliriz? Bunu çözüyoruz
kısmen POR'a geçerek ve büyük miktarlarda veriyi izin verecek şekilde ele alarak
çok daha hızlı hızlar. Yine, bu çözülmesi kolay bir sorun değil. Veri depolama sorunu tek başına
Saniyede 1300 işlem, saatte 0,7 gigabayt veri üretir. bu not alınmalı
Plasma veya Raiden gibi herhangi bir zincir dışı çözüm, GoChain'in üstünde çalışarak
daha da hızlı.
Son olarak, POR'a geçerek enerji kullanımını önemli ölçüde azaltabileceğiz.
blokları işlemek için gerekli. Ağ etkisi 1000 ila 10.000x arasında bir yerde olacaktır.
enerji kullanımı açısından daha çevreci.
Iron.io'nun eski kurucusu Travis Reeder tarafından yönetilen birinci sınıf bir geliştirme ekibimiz
var. Ayrıca biz
Iron'ın eski Mühendislik Müdürü Romana Kononov'a sahip. Demir'deyken öncülük ettiler
Saniyede 1 milyondan fazla işleme kadar Sunucusuz Bulut Bilişim. Ayrıca ekibimizde Ben var

---

7. Sayfa

Johnson, Boltdb'nin yazarıdır. Bu nedenle, bunu çözmek için benzersiz niteliklere sahip olduğumuzu
düşünüyoruz
özel Ethereum ölçekleme sorunu.
İlerlerken, yeni nesil akıllı sözleşmeleri başlatmayı planlıyoruz. Akıllı düşünüyoruz
sözleşmeler, değiştirme, değiştirme, duraklatma ve / veya feshedilebilme özelliğine sahip "akıllı"
olmalıdır
zaman içinde koşullar ve / veya anlaşmalar değiştikçe. Tıpkı gerçek dünyadaki gibi.
MainNet'imiz Mayıs 2018'in sonunda başlayacak. Akıllı sözleşme güncellemeleri ve ardından
2018'in sonunda ağ hızı daha da artar. 2019'da ağımızı yükseltmeyi planlıyoruz.
Ethereum hızının 13.000 tps veya 1000 katından fazla.

1.2. Arka fon

1.2.1. Hız ve Hacim. Halka açık, merkezi olmayan kripto para birimleri yavaş işlemlerden muzdarip
ve düşük işlem hacmi. Bitcoin saniyede yalnızca 7 işlemi işleyebilir [1], Ethereum
yalnızca saniyede 13 işleyebilir [2]. Ek olarak, işlemleri doğrulama süresi aşağıdakiler arasında
değişebilir:
mevcut hacme bağlı olarak birkaç dakika ila birkaç saat [4]
Buna karşılık Visa, Inc. her gün ortalama 150 milyon işlem gerçekleştiriyor ve
saniyede 56.000'den fazla işlem [3]. Halka açık kripto para birimleri gerçek olamayacak kadar yavaş
4 büyüklük sırasına göre dünya işleme.

1.2.2. Enerji tüketimi. Blok madenciliği süreci muazzam miktarda enerji kullanıyor
Proof-of-Work (PoW) [12] adlı bir fikir birliği algoritması nedeniyle. PoW önemsiz olmayan
gerektirir

Madencilik düğümleri tarafından yapılan hesaplamalı çalışma, bu da kötü bir aktör için maliyeti engelleyici hale getirir.
kötü niyetli eylemler gerçekleştirmek. Bu hesaplama iş yükü enerji gerektirir.

---

8. Sayfa

Bugün itibariyle, 3,5 milyon ABD hanesi, elektrik santrallerini çalıştırmak için kullanılan enerjiyle güçlendirilebilir.
Bitcoin ağı, Ethereum ise 1 milyon hanenin [10], [11] eşdeğer gücünü kullanıyor.
Bu kabul edilemez ve sürdürülemez.
1.2.3. Ademi merkeziyetçilik. Ademi merkeziyet, kripto para birimlerinin merkezi bir kiracısıdır. Hayır sağlar
bir şirket veya hükümet onu kontrol edebilir. Bununla birlikte, pratikte çoğu madencilik, Elektriğin en ucuz olduğu Çin [26], [27]. Tüm blokların% 75'i büyük Çinliler tarafından çıkarılıyor Madencilik şirketleri. Bu Bitcoin, Bitcoin Cash, Ethereum ve en iyi kripto para birimleri için geçerlidir [5].
Şirkette gizli anlaşma veya hükümetin özelleştirilmesi durumunda,% 51 saldırılar [6] mümkün.
1.2.4. Katı Sözleşmeler. Ethereum, akıllı sözleşmeler adı verilen benzersiz bir özellik sunar. Bunlar akıllı
sözleşmeler, kullanıcıların tüm ilgili tarafların
mutlak kesinlikle bir dizi kurala bağlı. Bu o kadar başarılı oldu ki, neredeyse Geçen yılki her ICO, Ethereum'un akıllı sözleşme sistemiyle çalışıyor.
Ancak bu akıllı sözleşmeler hiç de akıllıca değil. Son derece katı sözleşmelerdir.
gerçek dünya sözleşmelerinde olduğu gibi değişikliklere uyum sağlayamıyor. Bir sözleşmeye dahil olan taraflar
Koşulları ayarlamak veya sözleşmedeki hataları düzeltmek için gerekirse sözleşmelerini yükseltme imkanına sahip değiller
kodu. Akıllı sözleşmelere [7] başarılı saldırılar düzenlenmiştir ve bilinen saldırılar [8], [9].
1.3 Önceki Çalışma
1.3.1. İş Kanıtı Algoritması . Proof-of-Work (PoW) [12], [13] bir fikir birliği algoritmasıdır. yaygın olarak kripto para birimlerinde kullanılır. PoW başlangıçta spam ile mücadele için bir araç olarak icat edildi
[15]; E-posta göndermeyi hesaplama açısından pahalı hale getirirseniz, spam göndermenin maliyeti olur
normal bir kullanıcının e-posta göndermesi için neredeyse ücretsizdir. Aynı kavram şudur:

Sayfa 9

Kripto para birimlerinde, onu yasaklayıcı şekilde pahalı hale getirerek kötü niyetli eylemleri önlemek için kullanılır.
blok zincirini değiştirin.
Kripto para ağlarında, "madenciler" PoW hesaplamasını bir
işlem kümesi artı önceki bloğun hash değeri, bir sonraki bloğu oluşturmak için blok zinciri. Blok, önceki bloğun karmasını içerdiğinden, tarihsel bir bloğun değiştirilmesi sonraki tüm blokların yeniden oluşturulmasını gerektirecektir. Tüm hash'lerin yeniden oluşturulması hesaplama açısından yoğun ve çok fazla enerji gerektiriyor - ve enerji bedava değil. Olur ayrıca zaman alıcı olabilir. İşi kanıtlama ve blok oluşturma sürecine "madencilik" denir. Madenciler, toplam arza eklenen yeni basılan madeni paralarla bu çalışma için ödüllendiriliyor. PoW, güvenli dağıtılmış defter sistemine doğru ilerlememize yardımcı olsa da, zayıf performans, ademi merkeziyetçilik eksikliği ve aşırı enerji tüketimi.
1.3.2. Proof-of-Stake Algoritması . Proof-of-Stake (PoS) [14] başka bir fikir birliği algoritmasıdır sözde rastgele doğrulayıcıları ağdaki paylarına göre seçen. Fikir şu ki
tedavülde en çok madeni paraya sahip olanlar en çok kaybedecek olanlara sahiptir, bu yüzden çalışmak üzere konumlandırılmışlardır.

ağın ilgisi. Bu yaklaşım, hesaplama karmalarının maliyetini ortadan kaldırır, ancak
üyelerinin menfaatlerinin ağa uygun olduğu konusunda varsayımlar yapar.
PoS ağındaki doğrulayıcılar, yalnızca cüzdanları tarafından tanımlanan anonim kullanıcılardır.
adres. Bu, biriktirebilecek kötü aktörler için PoW üzerinde ek bir hesap verebilirlik sağlamaz.
ağda önemli bir zenginlik. İkincisi, işlem ücretleri halihazırda sahip olanlara gidecek
ağdaki en fazla para ve büyük servet gereksinimleri, daha fakir madeni para sahiplerini hariç tutar
doğrulamadan. Son olarak, PoS enerji tüketimini azaltırken hedefi,
yüksek performans. Ethereum'un Casper uygulaması için ilk hedefler yalnızca 100 TPS'dir.
1.3.3. Yetki Kanıtı Algoritması. Proof-of-Authority [16] yeni bir fikir birliği algoritmasıdır
güvenilir bir küme bireyleri tüm işlem işlemlerini sağlar. Bu güven işleme izin verir

---

Sayfa 10

PoW hash hesaplamasını atlayarak önemli ölçüde iyileştirmek için işlem hızı. Birkaç
ağlar var, ancak şu anda yalnızca özel ağlara odaklanıyor veya
hedef olarak performans. Birçoğunun Ethereum ağıyla da uyumluluğu yoktur.
Bir kamu ağı, 12 kişinin kimliğini doğrulamak için ABD eyalet düzeyindeki Noter sistemine
güveniyor
ağda doğrulayıcı olarak hareket edecek kişiler [17]. Doğrulayıcı isteyen adaylar
durum fiziksel adres, banka hesabı, sosyal ağ ve cep telefonu kanıtı gönderin
gerçek dünyadaki kimliklerini doğrulayın. PoA madenciliğin hesaplama yükünü ortadan kaldırırken,
işlemlerin gerçekleştirilmesi için bireylere güvenmek, çeşitli nedenlerle büyük ölçekte bozuluyor.
Birincisi, ağın net değeri ile ağın piyasa değeri arasında bir eşitsizlik vardır.
ağ. PoS sisteminin çözmeye çalıştığı şey budur. Ortalama net değerin bir
Amerika Birleşik Devletleri'ndeki birey 68.828 $ [18], doğrulayıcıların toplam net değeri 825.936 $
'dır:

12 ∗ 68 ABD doları, 828 = 825, 936 ABD doları

Doğrulayıcıların sayısı bir derece artmış olsa bile, toplam net değeri
Doğrulayıcılar, Visa, Inc. tarafından her yıl gerçekleştirilen işlemlerde 6,8T $ 'ın çok küçük bir
kısmıdır [19].
Bu eşitsizlik, rüşvet için güçlü bir teşvik sağlar.
İkincisi, doğrulayıcılar fiziksel adreslerini herkese açık bir şekilde yayınlamalı ve bu da
gözdağı veya fiziksel tehditler. Terör örgütü veya haydut bir devlet,
bu doğrulayıcıların yarısını kontrol eden büyük ölçekli bir finansal sistem.
Son olarak, çoğu kişi, güvenli bir işlem yürütmek için gereken deneyim ve altyapıdan yoksundur
işleme sistemi. Bu, ağın kötü niyetli korsanlığa maruz kalma olasılığını önemli ölçüde artırır.

2. Uygulama

2.1. İtibar Kanıtı

Sayfa 11

GoChain, şirketin itibarına bağlı olan bir İtibar Kanıtı (PoR) fikir birliği modeli kullanır.
katılımcıları ağı güvende tutmak için. Bir katılımcının bir itibarı olmalıdır.
sistemi aldatırlarsa korkunç sonuçlarla karşılaşacakları kadar önemli
hem finansal şartlar hem de markalaşma. Çoğu işletme ciddi sonuçlarla karşılaşacaktır.
bir finans ağını dolandırırken yakalandı. Daha çok kaybedecek daha büyük şirketler seçilecek
daha az kaybedecek daha küçük şirketler üzerinden.
Bir şirket itibarını kanıtladığında, ağda yetkili olarak oylanabilirler.
düğüm ve bu noktada, bir Yetki Kanıtı ağı (PoA) gibi çalışır. Sadece
yetkili düğümler blokları imzalayabilir ve doğrulayabilir.
Ethereum'un ağı üzerine inşa ediyoruz çünkü bu sadece bir değer deposundan çok daha fazlası.
Bu nedenle bugün piyasadaki en iyi kripto para birimi ve blok zinciri olduğuna inanıyoruz ve
neden onu bir başlangıç noktası olarak kullanıyoruz. Tüm Ethereum cüzdanları ve geliştirme araçları
GoChain ile uyumludur.

2.2. Neden İtibar?

İtibar, bir işletme için çok önemlidir. Etik olmayan bir şekilde hareket eden bir işletme birçok kişiden zarar görür.
para cezaları, gelir kaybı, değerlemede düşüş, markalaşma ve halkla ilişkiler gibi seviyeler.
Güven, başarılı bir işin temel taşıdır ve bir marka güvenini kaybettiğinde
müşteriler, yıllarca onarım alabilir.
Volkswagen emisyon skandalı [20] mükemmel bir örnektir. Aldatmak için tek başlarına ameliyat ettiler
halk ve kendi müşterileri. Bir kez yakalandığında, mali ve halkla ilişkilerdi
hisse fiyatında% 30'luk bir düşüşe ve 25 milyar dolarlık cezaya neden olan felaket [21].

Sayfa 12

GoChain, şirketlerin birbirlerini kontrol altında tutmalarına ve ağı korumalarına izin vermek için bu modeli kullanıyor
güvenli. Volkswagen'in her birini doğrulamak ve doğrulamak için Ford, Toyota ve diğerleri ile çalıştığını hayal edin.
diğerlerinin emisyon testleri. Volkswagen'in onların yanına gitmesi pek olası değil.
hileli emisyon testleri. Eğer denemiş olsalardı, o zaman hızla oylanacaklardı.
konsorsiyum ve ağın bir parçası olma haklarını kaybederler.
PoR, daha geniş iş dünyası için güvenilmeyen ağlara göre daha çekicidir.
PoW veya PoS. Risk açısından olumsuz şirketler, bilinen markalara aynı şekilde güvenebileceklerdir.
Visa, Inc. veya JPMorgan Chase & Co. gibi şirketlere güvenin PoR'da herkes tam olarak kimin verileriyle güveniyorlar.

2.3. İtibar Ölçümü

İtibarın kesin olarak ölçülmesi imkansızdır, ancak birkaç önemli ölçütü tartıyoruz.
bizim kararımız:
1) Piyasa Değeri
2) Halka Açık
3) Marka Önemi
Büyük bir piyasa değerine sahip şirketlerin, küçük sermayeli şirketlerden daha fazla kaybedecekleri var. Bunu kullanıyoruz
Üye şirketlerin değerinin olması gerektiği için şirketleri değerlendirirken metrik
hile yapmayı caydırmak için işlem ağının değeriyle eşitlik.
Daha sonra, bir şirketin halka açık mı yoksa özel olarak mı tutulduğuna bakacağız. İtibarın etkisi halka açık şirketler, özel şirketlere göre daha doğrudan ve anında. Etik olmayan
Ağ ile ilgili karar, bir kamu şirketinin hisse senedi fiyatını dakikalar içinde etkileyebilir.

Sayfa 13

Son olarak, işleri için güçlü kamu markalarına ihtiyaç duyan şirketleri tercih ediyoruz.
Örneğin, Coca-Cola veya Apple gibi bir şirketin itibarını kaybetmesi daha etkili olacaktır.
bir kömür madenciliği şirketine göre.

2.4. Yetkili İmzalayanlar

Yetkili imzalayanlar, bloklar oluşturan, bunları imzalayan ve bunları şu adrese dağıtan güvenilir düğümlerdir.
diğer düğümler. Bir Proof-of-Work (PoW) sistemindeki madencilere benzer şekilde bloklar oluşturmaları ve
madencilik maliyeti olmadan imzalayın.
Blok zincirinde yetkili imzalayanların bir listesi tutulacaktır. Yalnızca yetkili düğümler şunları yapabilir:
işaret blokları ve tüm bloklar, imzalayanın yetkili durumda olup olmadığı kontrol edilerek bunun doğru olduğu doğrulanır.
liste. İmzalama algoritması, temelde PoW ile aynı imza algoritmasıdır, ancak
farklı üstbilgi kümesi. PoW'ye özgü başlıklar kaldırılacak ve ek başlıklar eklenecektir.
oylamayı etkinleştirin.
N yetkili imzalayan verildiğinde, bir imzalayan yalnızca her (N / 2) + 1'de bir blok imzalayabilir. Bu,

birisinin kötü niyetli bir saldırı gerçekleştirmek için imzalayanların% 50'den fazlasını kontrol etmesi gerekir [6].
2.4.1. Teşvikler / Ödüller . Yetkili imzalayanlar, GoChain Coins (GOC) ile ödüllendirilecektir.
blok imzalandı. Başlangıçta bu oran, 50.000.000 yeni token olan toplam tokenlerin% 5'i olacaktır.
ilk yıl. Bu oran zamanla azalacaktır. Blok başına miktar, kesinleşmiş olana bağlı olacaktır.
blok süreleri. Örneğin, blok süreleri 10 saniyeyse, düğüm bir ödülle ödüllendirilecektir.
ilk yılda imzalanmış blok başına ortalama 15,9 token.
Ayrıca, bloğu imzalayan yetkili düğümün küçük işlem ücretleri de olacaktır.
içeren işlemleri saklayacaktır.

Sayfa 14

Şekil 1. Toplam GOC (milyarlarca)
Mutabakat protokolü, bir kişinin atanmış imzalayanını teşvik ederek adalet ve canlılık sağlar.
imzalamayı gerçekleştirmek için engelleme, ancak aynı zamanda atanan imzalayan varsa diğer blokların imzalamasına
kullanım dışı. Bir blok için atanan imzalayan, sırayla yapılan bir arama ile belirlenir.
yetkili imzalayan listesi. Atanan imzalayan yanıt vermezse, diğer imzalayanlar şurada oturum açabilir:
daha düşük bir blok zorluk seviyesi. Algoritma 1'e bakınız.
Algoritma 1: Blokların İmzalanması
2.5. Oylama
GoChain, iki aşamalı bir oylama süreci uyguladı. İlk sunum için GoChain
Vakıf, ilk 50 imzalayanı yetkilendirme listesine ekleyecektir. Bunlar orijinal
50 imzalayan, birden çok sektörden şirket olacak ve birden çok ülkeye yayılmış olacak.
Bu, zorla ademi merkeziyetçiliğin sağlanmasına ve herhangi bir tek hükümetin müdahalesini önlemeye yardımcı olacaktır.
50 yetkili imzalayan belirlendikten sonra, oylama kontrolü şu adrese devredilecektir:
imzalayanlar kendilerini yönetecek. Bu oylama süreci Algoritma 2'de gösterilmektedir. PoA
uygulama, oylama bilgilerini düğümler arasında geçirmek için birkaç blok başlığını yeniden tasarlar.
2.6. İmzalayan Doğrulaması

Sayfa 15

Yetkili imzalayan düğümlerini işleten şirketler, bir doğrulama sürecinden geçecektir.
kimliklerinin doğru olduğundan emin olun. Bu doğrulama adımları, aşağıdakiler kullanılarak otomatik hale getirilecektir:
blok zincirinde akıllı sözleşmeler.
PoA uygulaması, üzerine inşa edebileceğimiz bir noktada imzalayan ve oylama durumu sağlar
son kullanıcılara tam şeffaflık sağlar. Smart içinde depolanan doğrulama verileriyle birleştirildi
sözleşmeler, kullanıcılar herhangi bir noktada hangi şirketlerin hangi düğümleri çalıştırdığını yapabilir.
2.6.1. Şirket Doğrulaması . İlk doğrulama adımı, şirketlerin
Dun & Bradstreet D- UNS numarası. Bu tanımlayıcı, seçmenlerin bir D&B raporu almasına izin verir.
resmi iletişim bilgilerini görüntülemek için şirket. Bu bilgiler kurmak için kullanılacaktır
iletişim. Şekil 2'ye bakın
Algoritma 2: İmzalayan eklemek / kaldırmak için oy verin
2.6.2. DNS Doğrulaması. İkincil bir doğrulama adımı, şirketlerin bir TXT girişi eklemesini gerektirir
DNS kayıtlarına rastgele bir belirteçle. Bu, alan adını doğrularken yaygın bir uygulamadır
mülkiyet [28]. GoChain, istek sahipleri için token üreten ve doğrulayan bir DApp barındıracak
DNS kayıtları. Yetkili imzalama düğümleri, doğrulamayı görüntülemek için bu DApp'ı
kullanabilir. Şekil 3'e bakın

Sayfa 16

Şekil 3. DNS Doğrulama Sırası
2.7. Kontrol noktaları

Kontrol noktası, belirli bir noktadaki tüm blok zincirinin mevcut durumunun imzalı bir anlık görüntüsüdür.
blok numarası. Sıfır olmayan tüm hesap bakiyelerini ve akıllı sözleşme durumlarını içerecektir. Birkez kontrol noktası oluşturulur, önceki tüm bloklar ve veriler kaldırılabilir.
Yeni bir düğüm başlatıldığında, son kontrol noktasını indirecek ve ardından almaya devam edecektir. o noktadan itibaren bloklar ve durum. Bu, senkronize olmak için günler olmasa da saatler kazandıracak. Bu şu anlama gelir
bir düğüm dakikalar içinde kurulup çalışmaya başlayabilir.
GoChain, herhangi bir geçmiş bloğu almak için herkese açık, salt okunur bir API sağlayacaktır. herkes verilere anahtarlarla bakabilir. Bu açık kaynak olacaktır, böylece herkes bunu tam olarak tutmak için çalıştırabilir.
Tarih. Daha fazla doğrulama ve hesap verebilirlik için teşvik ediyoruz. Bu daha kolay hale getirecek blok kaşifleri gibi üçüncü taraf hizmetleri oluşturun.

2.8. Performans ve Optimizasyonlar

2.8.1. İşlemlerin Hızı ve Hacmi. Güvenilir düğümler kullanılarak işlemler doğrulanabilir
çok hızlı bir şekilde ve ağın işleyebileceği işlem hacmi,
büyüklük. Google gibi her gün kullandığımız ve yüksek hacimli işleyebilen sistemlere benzer arama veya Visa ödemelerinde, bu sistemler yalnızca
sunucular ve üzerinde çalıştıkları ağ.
Blok boyutu ve gaz limitleri gibi diğer faktörler, hesaplama nedeniyle yapay olarak düşüktür. PoW tarafından gereken güç. Mutabakat düğümlerine güvenerek,
ağ, Ethereum'un şu anda kaldırabileceğinden 100 kat daha fazla. Güvenilir fikir birliği dışarıda kullanılır

---

Sayfa 17

etcd gibi sistemlerde saniyede 141.578 işleme ulaşabilen kripto para birimleri
Mütevazı donanım [?] Kullanan 3 düğümlü küme. Verimi iyileştirmek, büyüme oranı kadar kritik öneme sahiptir
Ethereum, sürdürülemez bir orana hızla yükseliyor. Ethereum şu anda 13 tx / saniyede çalışıyor; mainnet lansmanında 1.300 tx / saniye hedefliyoruz.
İnce ayar yapabileceğimiz iki ana parametre blok boyutu (gaz limiti) ve blok süreleridir. Nedeniyle (PoW'daki madencilerin sayısına kıyasla) nispeten küçük bir imzalayan grubumuz olduğu gerçeği yetenekleri sayesinde, blok boyutunu büyük ölçüde artırabilir ve blok sürelerini kısaltabiliriz. Bu tek başına saniyedeki işlem sayısını büyük ölçüde artırır. Yukarıda belirtildiği gibi, nedeniniz PoW'da blok boyutunu artıramazsa, hash algoritmasını çok zorlaştırır ve
pahalı. GoChain'in bu sınırlaması yoktur.
2.8.2. Enerji tüketimi. Güvenilir bir yetkili düğümler ağı kullanmak, orada olduğu anlamına gelir madencilik olmayacak. Madencilik olmaması, bilgisayarlar arasında blokları kazanmak için savaş olmayacağı anlamına gelir
ve bu nedenle boşa harcanan enerji yok. Düğümler, bu enerjinin yalnızca küçük bir kısmını gerektirir. işlemleri işleyin, akıllı sözleşmeler çalıştırın ve blokları doğrulayın.
Bu yazı yazıldığı sırada Ethereum'un tahmini enerji tüketimi 14 TWh ve artıyor [32].
Sunucu başına 450 W güç kullanımı varsayıldığında [31], 50 düğümlü kümemiz yalnızca 197,1 MWh veya
Ethereum ağının enerjisinin% 0,001'i.

Sayfa 18

2.8.3. Ağ oluşturma. İmzalayanlar birbirleriyle doğrudan iletişim kuracak. Bu şu anlama gelir: imzalamayı yeni bitiren düğüm, yeni imzalanmış bloğu yetkili
bir çoğaltma düğümüne göndermeden önce imzalayanlar listesi. Bu, yetkili imzalayanların için blok zinciri ve API sorgularını boşaltırken ihtiyaç duydukları bilgileri olabildiğince hızlı ağın geri kalanını ayrılmış çoğaltma düğümlerine.
Kopyalama katmanı, imzalayan olmayan düğümlerin (diğer herkes) blok talep etmesi ve sorgulaması için mevcuttur

salt okunur bir API kullanan durum. Çoğaltma katmanı salt okunur olduğundan, yatay olarak küresel ölçekte bir kullanıcı grubunun ihtiyaçlarını karşılamak için ölçeklendirin. Şekil 6, bu 3 kademenin bir örneğini göstermektedir
ağ stratejisi.

Sayfa 19

2.8.4. Depolama. Tüm blok zincirini depolamak için depolama gereksinimleri oldukça büyüktür. Ethereum boyutu yüzlerce gigabayttır ve hızla büyüyor. Saatler veya günler sürebilir
yeni bir düğüme senkronize etmek, bunu sadece yapmak isteyen ortalama bir kullanıcı için kullanışsız hale getirir.
bir işlem gönderin. Hızlı ve hafif gibi boyutu küçültmek için çalıştırabileceğiniz daha yeni modlar var modu, boyutu büyük ölçüde küçültür ve bu doğru yönde atılmış iyi bir adımdır.
GoChain 100 kat daha fazla işlem hacmi işleyeceğinden, depolama alanı çok daha büyük hale geliyor. potansiyel olarak 100x daha büyük. Bu yazı itibariyle, Ethereum işlemleri ortalama 174 bayt ve Günde 120.4MB blok verisi üreten günde 700.000 işlem gerçekleşir [29] veya
Yılda 43,9 GB. Verimi 2 büyüklük sırası artırmak, 4,4 TB blok oluşturacaktır
yıllık veri. Bunu Ethereum ağındaki 23.000 düğümün tamamına yaymak [30],
101 petabayt gerektirir.

Sayfa 20

Veri kümesinde çalışan düğüm kümesini sınırlayarak ağ trafiğini ve depolamayı azaltıyoruz Gereksinimler. Kontrol işaretleme, düğümlerin toplamın yalnızca küçük bir kısmını depolamasına izin verir
Mevcut işlem için gerekli olan blok zinciri. Mevcut bulut fiyatlandırması, başına 0,022 ABD doları GB / ay [33], blok zinciri geçmişinin bir kopyasını depolamayı yılda yalnızca 1,161.60 USD yapar. veriyi engelle.
2.8.5. Gelecek. Yukarıda açıklanan ilk hedeflerimizin ötesinde,
daha kolay ve daha az hataya açık hale getirmek için akıllı sözleşme sistemi. Yazılım neredeyse her zaman şunları içerir:
yayınlandığı sırada bilinmeyen hatalar ve geliştiricilerin bu hataları düzeltmenin bir yolunu bulması gerekir.
Ethereum, sözleşmelerinizi yükseltmenize izin vermez ve bu, 100'lerce milyon dolar ile sonuçlanır. çalınan değer [7]. Akıllı sözleşmeler yazmayı daha kolay ve daha kolay hale getirmeyi amaçlıyoruz çok büyük miktarlarda hırsızlığı önlemek için onları daha güvenli hale getirmenin yanı sıra
olay. Akıllı sözleşmelerin değiştirilebilecekleri gerçek dünyaya daha çok benzemesi gerekir, duraklatıldı ve / veya sonlandırıldı.
Ayrıca sözleşmelerin nasıl ve ne zaman olabileceğini tanımlamak için sözleşmelere standartlaştırılmış kural setleri ekliyoruz.
değiştirilmiş. Bunun daha geniş işletmeler tarafından akıllı sözleşmelerin benimsenmesine yardımcı olacağını umuyoruz.
tanıdık sözleşme koşullarını kullanarak topluluk. Örneğin, bir kooperatif organizasyonu bir
üye sayısı bir sözleşmeyi değiştirirken diğer kuruluşlar tüm katılımcıları gerekli kılabilir
bir değişikliği kabul etmek için bir sözleşmede. GoChain, varsayılan sözleşmelerin değişmez olmaya devam edecek
Ethereum ile uyumluluk için varsayılan olarak. GoChain ayrıca ek güvenlik özellikleri de ekleyecek Saldırı riskini en aza indirmek için sözleşmelere erişimi korumak için beyaz listeler gibi.
3. Yol Haritası

Sayfa 21

Sayfa 22

4. Tokenomik

Sayfa 23

- Sert Kapak 26,500 ETH
- % 10 çekirdek ekibe gidiyor
- Danışmanlara% 6
- % 10 Vakıf ve ikramiyeler
- % 4 pazarlama ve yasal
- % 10 GoChain Fonu - ekosistem projelerini finanse etmek için VC kolu
- 1 yıllık bir kilitlenme ile% 10 Yedek
- % 50 jeton satışı
- Danışmanlar için 6 aylık kilit
- Takım kilidi 6 ay, 12 ay, 18 ay, 24 ayda% 25

Toplam Token Arzı
1.000.000.000 GOC
Token Satışı Yumuşak Kapak
2.500 ETH

Sayfa 24

Token Satışı Hard Cap
26.500 ETH
Yaklaşık. Yetkili düğümler için yılda 50.000.000 yeni token oluşturulacak. Bu azalacak
mesai.

5. Takım

Jason Dekker - CEO
Jason, 250 milyon doları aşan bir bütçeyi yöneten eski bir serbest yatırım fonu yöneticisi olan bir seri girişimci,
melek yatırımcı, yönetim kurulu üyesi ve halka açık bir şirkete çıkışı olan danışman. O geniş
Finans, biyoteknoloji, teknoloji ve yiyecek ve içecek endüstrilerinde C düzeyinde deneyim.
Travis Reeder - Baş Yazılım Mimarı
Travis, yüksek verimli, yüksek ölçekli uygulamalar geliştirmede 20 yılı aşkın deneyime sahiptir ve
bulut hizmetleri. Başarılı teknoloji şirketleri kurdu ve
Silikon Vadisi'ndeki en iyi risk sermayesi şirketlerinden bazılarının finansmanı. Ölçeklendirme problemlerini çözmüş ve
kariyeri boyunca ölçeklenebilir hizmetler sunarken, şimdi bu bilgiyi uyguluyor ve
blockchain deneyimi. Travis, Bilgisayar Bilimleri alanında lisans derecesine sahiptir.
Ben Johnson - Kıdemli Yazılım Mühendisi
Ben Johnson, veritabanları yazma konusunda uzmanlaşmış açık kaynaklı bir yazılım geliştiricisidir ve
dağıtılmış sistemler. Çok popüler bir süreç içi, işlemsel, anahtar / değer olan BoltDB'yi yarattı
CoreOS etcd ve Hashicorp Consul dahil birçok proje tarafından kullanılan mağaza.
Guilherme Rezende - Kıdemli Yazılım Mühendisi

Sayfa 25

Guilherme, hem bulut teknolojisinde hem de açık alanda kapsamlı yazılım geliştirme deneyimine sahiptir.

kaynak. Aynı zamanda bir blockchain geliştiricisi ve konuşmacısıdır. Guilherme lisans derecesine sahiptir
Bilgisayar Bilimi.
Jordan Krage - Kıdemli Yazılım Mühendisi
Jordan Krage, büyük veri ve dağıtılmış sistemler konusunda deneyime sahip bir yazılım mühendisidir. O
Go (golang) bağımlılık yönetimi aracı dep. geliştiricilerinden biri. Ürdün bir
Bilgisayar Bilimleri alanında yüksek lisans derecesi.
Roman Kononov
Kıdemli Yazılım Mühendisi
Roman, yazılım ve lider mühendislik ekipleri geliştirme konusunda 12 yıllık deneyime sahiptir. O da siber güvenlik konusunda kapsamlı bilgi ve deneyime sahiptir ve şirketlerin korunmasına yardımcı olur
kendilerini tehditlerden. Roman, Bilgisayar Bilimleri alanında yüksek lisans derecesine sahiptir.

6. Danışmanlar

Matthew Skinner
EtherSportz şirketinde Founder
Shihab Ali
HODL Gang şirketinde Chief Strategy Officer
Chad Arimura

Sayfa 26

Oracle'da VP Cloud
Jameson Stafford
Catalytic, Inc. şirketinde VP Corporate Development
Morgan Mackles
X.ai şirketinde VP Sales
Alex Barrett
Likemoji şirketinde Founder and CEO
Justin Mares
Kettle & Fire şirketinde Founder
Traction Yazarı

Referanslar

[1] Bitcoin Ölçeklenebilirlik Sorunu, https://en.wikipedia.org/wiki/Bitcoin ölçeklenebilirlik sorunu
[2] Blockchain Ölçeklenmiyor, https://hackernoon.com/2cb43946551a
[3] VisaNet dakikada 100.000 işlem gerçekleştiriyor,
https://mybroadband.co.za/news/security/190348.html
[4] Ortalama Blockchain Onay Süresi, https://blockchain.info/charts/avg-confirmation-
saat, https://etherscan.io/chart/pendingtx

Sayfa 27

[5] Bitcoin Merkezi Olmayan Aramayı Durdurun, https://medium.com/@homakov/cb703d69dc27
[6]% 51 Saldırı, https://www.investopedia.com/terms/1/51-attack.asp
[7] DAO Saldırıya Uğradı: Kod Sorunu 60 Milyon Dolarlık Eter Hırsızlığına Yol Açıyor,
https://www.coindesk.com/
dao-attacked-code-issue-lead-60-milyon-eter-hırsızlığı /
[8] Ethereum akıllı sözleşmelerine yönelik saldırı araştırması, https://eprint.iacr.org/2016/1007.pdf
[9] Bilinen Saldırılar, https://consensys.github.io/smart-contract-best-practices/known saldırılar
[10] Bitcoin Enerji Tüketimi, https://digiconomist.net/bitcoin-energy-consumption
[11] Ethereum Enerji Tüketimi, https://digiconomist.net/ethereum-energy-consumption
[12] Proof-of-Work, https://en.wikipedia.org/wiki/Proof-of-work-system
[13] Proof-of-Work, https://en.bitcoin.it/wiki/Proof-of-work
[14] Proof-of-Stake, https://en.wikipedia.org/wiki/Proof-of-stake
[15] İşleme yoluyla Fiyatlandırma, http://www.wisdom.weizmann.ac.il/~naor/ PAPERS / pvp.ps

[16] Yetki Kanıtı, https://en.wikipedia.org/wiki/Proof-of-authority
[17] POA Ağ Yönetişimine Genel Bakış,
https://github.com/poanetwork/wiki/wiki/Governance-Overview
[18] Amerikalıların ortalama net değeri, http://www.businessinsider.com/heres-the-average-net-değeri-amerikalılar-her yaşta-2017-6

Sayfa 28

[19] Visa, Inc., https://en.wikipedia.org/wiki/Visa Inc.
[20] VW, 'Dieselgate' İçin 25 Milyar Dolar Ödedi ve Kolay Çıktı
http://fortune.com/2018/02/06/volkswagen-vw-emissions-scandal-penalties/
[21] VW Skandalı: Volkswagen'in Hisse Senedini Nasıl Etkiledi ?,
https://www.investopedia.com/news/ vw-scandal-how-has-it-etkiledi-volkswagens-stock-vlkay /
[22] Blok Boyutu ve Saniyedeki İşlemler, https://www.bitcoinplus.org/blog/block-size-and-işlemler-saniye
[23] Ethereum Blok Boyutu, https://www.reddit.com/r/ethereum/comments/4a3kqo/what-is-ethereums-blok boyutu /
[24] Lütfen gaz limitini artırabilir miyiz ?,
https://www.reddit.com/r/ethereum/comments/7hmlm4/can-we-please-increase-the-gas-limit /
[25] Blok Boyutu Sınırı Tartışması, https://en.bitcoin.it/wiki/Block boyut sınırı-tartışma # Blok boyutunu artırmaya karşı argümanlar
[26] Çin'de Elektrik Sektörü, https://en.wikipedia.org/wiki/Elektrik sektörü-Çin
[27] Çin Neden Diğer Ülkelerden Daha Fazla Bitcoin Madenciliği Yapıyor?
http://www.businessinsider.com/ why-china-mayines-more-bitcoin-than-any-other-country-2017-12
[28] Şifreleyelim, Nasıl Çalışır, https://letsencrypt.org/how-it-works/ [29] Ethereum İşlem Geçmiş Tablosu, https://bitinfocharts.com/comparison/ethereum-transaction.html

---

Sayfa 29

[30] Ethereum Mainnet Node Explorer, https://www.ethernodes.org/network/1
[31] Google Çevre Dostu Bilgi İşlem, https://static.googleusercontent.com/media/www.google.com/en//green/pdfs/google-green-computing.pdf
[32] Ethereum Enerji Tüketim Endeksi, https://digiconomist.net/ethereum-energy-tüketim
[33] AWS S3 Fiyatlandırması, https://aws.amazon.com/s3/pricing