**Sayfa 1**

**Dağıtık Defterler Ağı**

Jae Kwon jae@tendermint.com
Ethan Buchman ethan@tendermint.com

Tartışmalar için topluluk sohbetimize katılın !

*NOT: Bunu GitHub'da okuyabiliyorsanız, o zaman hala aktif*
*bu belgeyi geliştirmek. Lütfen güncellemeleri düzenli olarak kontrol edin!*

Açık kaynak ekosisteminin birleşik başarısı,
merkezi olmayan le-paylaşım ve halka açık kripto para birimleri
merkezi olmayan internet protokollerinin
sosyo-ekonomik altyapıyı kökten iyileştirmek için kullanılabilir.
Bitcoin [1] (a
cryptocurrency), Zerocash [2] (gizlilik için bir kripto para birimi ) ve
Ethereum [3] gibi genelleştirilmiş akıllı sözleşme platformları ,
Etherium Virtual için sayısız dağıtılmış uygulama
Augur (bir tahmin pazarı) ve TheDAO gibi makine (EVM)
[4] (bir yatırım kulübü).
Ancak bugüne kadar, bu blok zincirlerinde bir dizi sorun yaşandı.
brüt enerji verimsizliği, zayıf veya
sınırlı performans ve olgunlaşmamış yönetişim mekanizmaları.
Bitcoin'in işlem hacmini ölçeklendirmek için teklifler, örneğin
Segregated-Witness [5] ve BitcoinNG [6] , dikey ölçeklendirmedir
tek bir fiziksel kapasite ile sınırlı kalan çözümler
tam denetlenebilirlik özelliğini sağlamak için makine.
Lightning Network [7] , Bitcoin işlemlerinin ölçeklenmesine yardımcı olabilir

---

**Sayfa 2**

bazı işlemleri defterden tamamen çıkararak hacim,
ve mikro ödemeler ve gizliliği korumak için çok uygundur
ödeme rayları, ancak daha genelleştirilmiş olanlar için uygun olmayabilir
ölçeklendirme ihtiyaçları.
İdeal bir çözüm, birden fazla paralel blok zincirinin
güvenlik özelliklerini korurken birlikte çalışın. Bu var
iş kanıtı ile imkansız değilse de zor olduğu kanıtlanmıştır. Birleştirilmiş
Örneğin madencilik, yapılan işin bir ebeveyni güvence altına almasına izin verir.
zincir bir alt zincirde yeniden kullanılacak, ancak işlemler yine de
sırayla, her bir düğüm ve birleştirilmiş mayınlı blok zinciri tarafından doğrulanır
hashing gücünün çoğunluğunun üzerinde olması durumunda saldırıya karşı savunmasızdır.
ebeveyn, çocuğu aktif olarak birleştirme madenciliği yapmaz. Akademik bir inceleme
ve alternatif blockchain ağ mimarileri sağlanır
ek bağlam ve diğer tekliflerin özetlerini sunuyoruz
ve İlgili Çalışmadaki dezavantajları .
Burada yeni bir blockchain ağ mimarisi olan Cosmos'u sunuyoruz
tüm bu sorunlara hitap eden. Cosmos, birçokları barındıran bir ağdır
bölge adı verilen bağımsız blok zincirleri. Bölgeler tarafından desteklenmektedir
Yüksek performans sağlayan Tendermint Core [8] ,
Tutarlı, güvenli PBFT benzeri konsensüs motoru, nerede sıkı fork-
hesap verilebilirlik garantileri kötü niyetli kişilerin davranışlarını kontrol altına alır
aktörler. Tendermint Core'un BFT fikir birliği algoritması çok uygundur
halka açık kanıtı blok zincirlerini ölçeklendirmek için.
Cosmos üzerindeki ilk bölge Cosmos Hub olarak adlandırılır. Kozmos
Hub, çok varlıklı bir hisse kanıtı kripto para birimidir.
ağın uyum sağlamasına ve
Yükselt. Ek olarak, Cosmos Hub aşağıdakilerle genişletilebilir:

diğer bölgelerin bağlanması.
Cosmos ağının hub ve bölgeleri ile iletişim
blok zincirler arası iletişim (IBC) protokolü aracılığıyla birbirlerine,
blok zincirleri için bir tür sanal UDP veya TCP. Jetonlar olabilir
güvenli ve hızlı bir şekilde bir bölgeden diğerine aktarılır

---

**3. Sayfa**

bölgeler arasında döviz likiditesine gerek kalmadan. Yerine,
tüm bölgeler arası belirteç transferleri, Cosmos Hub'dan geçer.
her bölge tarafından tutulan toplam token miktarını takip eder.
hub, her bir bölgeyi diğer bölgelerin arızasından izole eder. Çünkü
Cosmos Hub'a herkes yeni bir bölge bağlayabilir, bölgeler izin verir
yeni blok zinciri yenilikleriyle gelecekteki uyumluluk için.
Bu bölümde Tendermint konsensüs protokolünü açıklıyoruz
ve onunla uygulamalar oluşturmak için kullanılan arayüz. Daha fazlası için
ayrıntılar için eke bakın .
Klasik Bizans hataya dayanıklı (BFT) algoritmalarında, her düğüm
aynı ağırlığa sahiptir. Tendermint'te düğümlerin negatif olmayan
*oylama gücü* miktarı ve olumlu oyu olan düğümler
güce *doğrulayıcılar* denir . Doğrulayıcılar katılır
kriptografik imzalar yayınlayarak fikir birliği protokolü veya
*oylar* , bir sonraki blok üzerinde anlaşmaya varır.
Doğrulayıcıların oylama yetkileri oluşum aşamasında belirlenir veya
bağlı olarak, blok zinciri tarafından belirleyici olarak değişti.
uygulama. Örneğin, bir kanıt kanıtı uygulamasında, örneğin
Cosmos Hub, oylama gücü tarafından belirlenebilir
teminat olarak bağlanan stake jetonlarının miktarı.
*NOT: ⅔ ve ⅓ gibi kesirler toplam oylamanın kesirlerini ifade eder*
*güç, hiçbir zaman doğrulayıcıların toplam sayısı, tüm doğrulayıcılar olmadıkça*
*eşit ağırlığa sahip. > ⅔ "⅔'den fazla" anlamına gelir, ≥⅓ "en azından*
*⅓ ".*
Tendermint, kısmen senkronize bir BFT konsensüs protokolüdür
DLS konsensüs algoritmasından türetilmiştir [20] . Tendermint

---

**4. sayfa**

basitliği, performansı ve çatal hesap verebilirliği ile dikkat çekiyor .
Protokol, sabit olarak bilinen bir dizi doğrulayıcı gerektirir; burada her biri
doğrulayıcı, açık anahtarıyla tanımlanır. Doğrulayıcılar şunları dener:
bir bloğun bir liste olduğu her seferinde bir blok üzerinde fikir birliğine varmak
işlemlerin. Bir blokta fikir birliği için oylama,
mermi. Her turda bir yuvarlak lider veya teklif veren vardır.
bir blok önerir. Doğrulayıcılar daha sonra aşamalı olarak oylama
önerilen bloğu kabul etmek veya bir sonraki tura geçmek için.
tur için teklif veren, sipariş edilenler arasından belirleyici olarak seçilir
oylama güçleriyle orantılı olarak onaylayıcıların listesi.
Protokolün tüm ayrıntıları burada açıklanmaktadır .
Tendermint'in güvenliği, optimum Bizans
Üstün çoğunluk (> ⅔) oylama ve kilitleme yoluyla hata toleransı
mekanizma. Birlikte şunları sağlarlar:
≥⅓ Oy verme yetkisi, ihlallere neden olmak için Bizans olmalıdır.
ikiden fazla değerin taahhüt edildiği yerlerde güvenlik.
herhangi bir doğrulayıcı grubu güvenliği ihlal etmeyi başarırsa, hatta
bunu yapmaya teşebbüs ederse, protokol tarafından tanımlanabilirler. Bu
hem çakışan bloklar hem de yayın için oylamayı içerir

haksız oylar.
Güçlü garantilerine rağmen, Tendermint olağanüstü
verim. 7'ye dağıtılmış 64 düğümün karşılaştırmalı değerlendirmelerinde
emtia bulut örneklerinde 5 kıtada veri merkezleri,
Tendermint fikir birliği, her biri için binlerce işlemi işleyebilir.
ikincisi, bir ile iki saniye arasında tamamlama gecikmeleriyle.
Özellikle, binin üzerinde işlem performansı
İkincisi, zorlu olumsuz koşullarda bile korunur.
Doğrulayıcıların kötü niyetle oluşturulmuş oyları çökertmesi veya yayınlaması. Görmek
ayrıntılar için aşağıdaki şekil.

---

**5.Sayfa**

Tendermint'in fikir birliği algoritmasının önemli bir faydası basitleştirilmiştir
hafif istemci güvenliği, onu mobil cihazlar için ideal bir aday yapar ve
nesnelerin interneti kullanım durumları. Bir Bitcoin light istemcisinin senkronize olması gerekirken
blok başlık zincirleri ve en çok kanıtı olanı bulun.
çalışın, Tendermint light istemcilerinin yalnızca değişikliklere ayak uydurması gerekir
doğrulayıcı kümesine girin ve ardından> ⅔ ÖnKomutları doğrulayın
en son durumu belirlemek için en son blok.
Özlü hafif istemci provaları, bloklar arası zincirlemeyi de etkinleştirir
iletişim .
Tendermint, belirli bazı sorunları önlemek için koruyucu önlemlere sahiptir.
uzun menzilli tehlikede olmayan çift harcamalar gibi kayda değer saldırılar
ve sansür . Bunlar ekte daha ayrıntılı olarak tartışılmaktadır .

---

**Sayfa 6**

Tendermint fikir birliği algoritması bir
Tendermint Core adlı program. Tendermint Core bir
uygulamadan bağımsız "fikir birliği motoru", herhangi bir
dağıtılmış olarak çoğaltılmış bir belirleyici kara kutu uygulaması
blok zinciri. Tendermint Core, blok zinciri uygulamalarına bağlanır
Uygulama Blok Zinciri Arayüzü (ABCI) aracılığıyla [17] . Böylelikle ABCI
blok zinciri uygulamalarının herhangi bir
dil, sadece fikir birliğinin sağladığı programlama dili değil
motor yazılmıştır. Ek olarak, ABCI,
mevcut herhangi bir blok zinciri yığınının fikir birliği katmanını değiştirin.
Tanınmış kripto para birimi Bitcoin ile bir benzetme yapıyoruz.
Bitcoin, her düğümün koruduğu bir kripto para birimi blok zinciridir
tamamen denetlenmiş bir Harcanmamış İşlem Çıktısı (UTXO) veritabanı. Eğer
ABCI'nin üstüne Bitcoin benzeri bir sistem oluşturmak istendi,
Tendermint Core şunlardan sorumlu olacaktır:
Düğümler arasında blokları ve işlemleri paylaşma
Kanonik / değişmez bir işlem sırası oluşturmak (
blok zinciri)
Bu arada, ABCI uygulaması aşağıdakilerden sorumlu olacaktır:
UTXO veritabanının bakımı
İşlemlerin kriptografik imzalarının doğrulanması
İşlemlerin var olmayan fonları harcamasını önleme
İstemcilerin UTXO veritabanını sorgulamasına izin verme
Tendermint, blok zinciri tasarımını şu şekilde ayrıştırabilir:
başvuru süreci arasında çok basit bir API sunmak ve
fikir birliği süreci.

---

**7. Sayfa**

Cosmos, bağımsız paralel blok zincirlerinden oluşan bir ağdır.
her biri klasik BFT fikir birliği algoritmalarıyla desteklenmektedir.
Tendermint 1 .
Bu ağdaki ilk blok zinciri Cosmos Hub olacaktır.
Cosmos Hub, diğer birçok blok zincirine (veya *bölgelere* ) bir
yeni blok zincirler arası iletişim protokolü. Cosmos Merkezi
çok sayıda simge türünü izler ve toplamın kaydını tutar
her bağlı bölgedeki token sayısı. Jetonlar olabilir
güvenli ve hızlı bir şekilde bir bölgeden diğerine aktarılır
bölgeler arasında sıvı değişimine gerek kalmadan, çünkü hepsi
bölgeler arası madeni para transferleri Cosmos Hub üzerinden gerçekleştirilir.
Bu mimari, blockchain alanının yarattığı birçok sorunu çözer.
uygulama birlikte çalışabilirliği, ölçeklenebilirlik ve
sorunsuz yükseltilebilirlik. Örneğin, Bitcoind'den türetilen bölgeler,
Go-Ethereum, CryptoNote, ZCash veya herhangi bir blockchain sistemi,
Cosmos Hub'a takılabilir. Bu bölgeler Cosmos'un
küresel işlem talebini karşılamak için tam anlamıyla ölçeklendirin. Bölgeler ayrıca
dağıtılmış bir değişim için harika bir t, şu şekilde desteklenecektir:
iyi.
Cosmos, yalnızca dağıtılmış tek bir defter değildir ve Cosmos
Merkez, duvarlarla çevrili bir bahçe veya evreninin merkezi değildir. Biz
Açık bir dağıtılmış defterler ağı için bir protokol tasarlama
gelecekteki finansal sistemler için yeni bir temel oluşturabilecek,
kriptografi ilkelerine dayalı, sağlam ekonomi, fikir birliği
teori, şeffaflık ve hesap verebilirlik.
Cosmos Hub, Cosmos'taki ilk halka açık blok zinciridir
Tendermint'in BFT fikir birliği algoritması tarafından desteklenen ağ.
Tendermint açık kaynak projesi, 2014'te doğdu.
Bitcoin'in kanıtı hız, ölçeklenebilirlik ve çevre sorunları
iş birliği algoritması. Kanıtlanmış olarak kullanarak ve geliştirerek

---

**8. Sayfa**

1988'de MIT'de geliştirilen BFT algoritmaları [20] , Tendermint
ekibi kavramsal olarak bir risk kanıtı gösteren ilk kişi oldu
tehlikede olmayan problemi ele alan kripto para birimi
birinci nesil teminatlı kripto para birimlerinden muzdarip
NXT ve BitShares1.0 olarak.
Bugün, pratik olarak tüm Bitcoin mobil cüzdanları, güvenilir sunucuları kullanarak
onlara işlem doğrulaması sağlayın. Bunun nedeni kanıt-
iş, bir
işlemin geri çevrilemez şekilde gerçekleştirildiği kabul edilebilir. Çift-
gibi hizmetlerde harcama saldırıları zaten gösterildi
CoinBase.
Diğer blok zinciri konsensüs sistemlerinden farklı olarak, Tendermint teklifleri
anında ve kanıtlanabilir şekilde güvenli mobil müşteri ödeme doğrulaması.
Tendermint asla çatallanmayacak şekilde tasarlandığından, mobil
cüzdanlar anında işlem onayı alabilir, bu da
güvenilir ve pratik ödemeler akıllı telefonlarda bir gerçeklik. Bu
Nesnelerin İnterneti uygulamaları için önemli uzantıları vardır.
iyi.
Cosmos'taki doğrulayıcılar, Bitcoin madencileri ile benzer bir role sahiptir, ancak
bunun yerine oy vermek için kriptografik imzalar kullanın. Doğrulayıcılar
taahhütten sorumlu olan güvenli, özel makineler
bloklar. Doğrulayıcı olmayan kişiler stake jetonlarını devredebilir (
"Atomlar") blok ücretlerinin ve atomun bir kısmını kazanmak için herhangi bir doğrulayıcıya

ödüller, ancak eğer cezalandırılma (kesilme) riskiyle karşı karşıya kalırlar.
temsilci doğrulayıcı saldırıya uğrar veya protokolü ihlal eder. Kanıtlanmış
Tendermint BFT konsensüsünün güvenlik garantileri ve teminat
paydaşların mevduatı - onaylayıcılar ve delege ediciler -
Düğümler ve hafif istemciler için kanıtlanabilir, tutarlı güvenlik.
Dağıtılmış halka açık defterlerin bir anayasası ve
yönetişim sistemi. Bitcoin, Bitcoin Vakfı'na dayanır ve

---

**Sayfa 9**

yükseltmeleri koordine etmek için madencilik, ancak bu yavaş bir süreçtir.
Ethereum, ele almak için zor çatallanmanın ardından ETH ve ETC'ye ayrıldı
TheDAO hack, büyük ölçüde önceden bir sosyal sözleşme olmadığı için
ne de bu tür kararları alma mekanizması.
Cosmos Hub'daki doğrulayıcılar ve temsilciler oy verebilir
sistemin önceden ayarlanmış parametrelerini değiştirebilen öneriler
otomatik olarak (blok gaz limiti gibi), yükseltmeleri koordine et,
ve insan tarafından okunabilir anayasa değişiklikleri için oylama
Cosmos Hub politikalarını yöneten. Anayasa
gibi konularda paydaşlar arasında uyumu sağlar
hırsızlık ve hatalar (TheDAO olayı gibi), daha hızlı ve
daha temiz çözünürlük.
Her bölgenin kendi anayasası ve yönetimi de olabilir
mekanizma da. Örneğin, Cosmos Hub bir
Merkezde değişmezliği zorlayan anayasa (geri alma yok,
Cosmos Hub düğümü uygulamasındaki hatalar için tasarruf edin),
her bölge geri alma ile ilgili kendi politikalarını belirleyebilir.
Farklı politika bölgeleri arasında birlikte çalışabilirliği etkinleştirerek,
Cosmos ağı, kullanıcılarına nihai özgürlük ve potansiyel
izinsiz deney.
Burada yeni bir ademi merkeziyetçilik ve ölçeklenebilirlik modelini açıklıyoruz.
Cosmos, birçok blok zincirinden oluşan bir ağdır.
Tendermint. Mevcut teklifler bir "tek
toplam küresel işlem siparişi ile blockchain ", Cosmos
birçok blok zincirinin birbiriyle aynı anda çalışmasına izin verir
birlikte çalışabilirliği korurken.
Cosmos Hub temelde birçok bağımsız
"bölgeler" olarak adlandırılan blok zincirleri (bazen "parça" olarak da anılır.
"parçalama" olarak bilinen veritabanı ölçekleme tekniğine referans).

---

**Sayfa 10**

Üzerinde yayınlanan bölgelerden gelen son blok işlemlerinin sürekli akışı
Hub, Hub'ın her bölgenin durumuna ayak uydurmasını sağlar.
Aynı şekilde, her bölge Hub'ın durumuna ayak uydurur (ancak
dolaylı yoldan hariç olmak üzere birbirinize ayak uydurmayın
Hub). Bilgi paketleri daha sonra birinden iletilir
Merkle-proofs yayınlayarak başka bir bölgeye
bilgi gönderildi ve alındı. Bu mekanizmaya
inter-blockchain iletişimi veya kısaca IBC.
Bölgelerden herhangi biri, döngüsel olmayan bir grafik oluşturmak için merkez olabilir,
ancak açıklık adına sadece basit olanı tanımlayacağız
tek bir merkezin olduğu ve çok sayıda hub olmayan konfigürasyon
bölgeler.
Cosmos Hub, çoklu varlık barındıran bir blok zinciridir
Jetonların bireysel kullanıcılar tarafından tutulabileceği dağıtılmış defter veya

bölgelerin kendileri tarafından. Bu jetonlar bir bölgeden taşınabilir
"bozuk para paketi" adı verilen özel bir IBC paketinde diğerine. Merkez
toplamın küresel değişmezliğini korumaktan sorumlu
bölgelerdeki her bir jetonun miktarı. IBC para paketi
işlemler gönderen, merkez ve alıcı tarafından yapılmalıdır
blok zincirleri.

---

**Sayfa 11**

Cosmos Hub, bütün için merkezi defter görevi gördüğünden
sistem, Hub'ın güvenliği son derece önemlidir. Süre
her bölge, aşağıdaki şekilde güvence altına alınan bir Tendermint blok zinciri olabilir.
4 kadar az (veya BFT fikir birliğine gerek yoksa daha da az), Hub
küresel olarak merkezi olmayan bir doğrulayıcı seti tarafından güvence altına alınmalıdır.
en şiddetli saldırı senaryolarına dayanabilir, örneğin
kıtasal ağ bölümü veya ulus devlet destekli bir saldırı.
Cosmos bölgesi, IBC'yi değiştiren bağımsız bir blok zinciridir
Hub ile mesajlar. Merkezin bakış açısından, bir bölge bir
çok varlıklı dinamik üyeli çoklu imzalı hesap
IBC paketlerini kullanarak token gönderip alabilir. Gibi
kripto para birimi hesabı, bir bölge şundan daha fazla token transfer edemez:
vardır, ancak bunlara sahip olanlardan jeton alabilir. Bir bölge
bir veya daha fazla jeton türünün "kaynağı" olarak belirlenebilir,
O jeton arzını içten içe tüketme gücü veriyor.
Cosmos Hub atomları, bir bölgenin doğrulayıcıları tarafından istiflenebilir
Hub'a bağlı. Bu bölgelere çift harcama saldırıları sırasında
Tendermint'in çatalı ile atomların kesilmesine neden olur.
hesap verebilirlik, oylama gücünün> ⅔'ünün olduğu bir bölge
Bizans geçersiz bir devlet işleyebilir. Cosmos Hub,
diğer bölgelerde taahhüt edilen işlemleri doğrulayın veya yürütün, bu nedenle
kullanıcıların güvendikleri bölgelere token gönderme sorumluluğu.
Gelecekte, Cosmos Hub'ın yönetim sistemi Hub'ı geçebilir
bölge arızalarını hesaba katan iyileştirme önerileri. İçin
Örneğin, bazı (veya tüm) bölgelerden giden jeton transferleri
Bölgelerin acil devre kesilmesine izin vermek için kısılma
(belirteç transferlerinin geçici olarak durdurulması) bir saldırı tespit edildiğinde.
Şimdi Merkezin ve bölgelerin her biriyle nasıl iletişim kurduğuna bakıyoruz.
diğer. Örneğin, üç blok zinciri varsa, "Bölge1", "Bölge2",

---

**Sayfa 12**

ve "Hub" ve "Bölge1" in hedefli bir paket oluşturmasını diliyoruz.
"Zone2" için "Hub" üzerinden geçiyor. Bir paketi birinden taşımak için
blok zincirini diğerine aktarırsanız, alıcı zincirde bir kanıt yayınlanır.
Kanıt, gönderen zincirin bir paket için bir paket yayınladığını belirtir.
iddia edilen hedef. Alıcı zincirin bu kanıtı kontrol etmesi için,
gönderenin blok başlıklarına ayak uydurabilmelidir. Bu
mekanizma, yan zincirler tarafından kullanılana benzer.
Birbirinden haberdar olmak için etkileşim halindeki iki zincir
varoluş kanıtı datagramlarının çift yönlü akışı
(işlemler).
IBC protokolü doğal olarak iki tür kullanılarak tanımlanabilir
işlemler: bir **IBCBlockCommitTx** işlemi,
Blockchain, en son blok hash'ini herhangi bir gözlemciye kanıtlamak için,
ve bir blok zincirine izin veren bir **IBCPacketTx** işlemi
herhangi bir gözlemciye verilen paketin gerçekten yayınlandığını kanıtlayın

gönderenin başvurusu ile, Merkle-kanıtı aracılığıyla en son
blok karması.
IBC mekaniğini iki ayrı işleme ayırarak,
alıcı zincirinin yerel ücret piyasası mekanizmasının
hangi paketlerin işleneceğini (yani onaylanacağını) belirlerken
nasıl olduğu konusunda gönderen zincir üzerinde tam bir özgürlüğe izin verilmesi
birçok giden pakete izin verilir.
Yukarıdaki örnekte, "Zone1" blok karmasını güncellemek için
"Hub" (veya "Zone2" üzerindeki "Hub"), bir **IBCBlockCommitTx**

---

**Sayfa 13**

işlemin blok karması ile "Hub" a kaydedilmesi gerekir
"Zone1" (veya "Hub" blok karması ile "Zone2" üzerinde).
*Daha fazla bilgi için IBCBlockCommitTx ve IBCPacketTx'e bakın*
*iki IBC işlem türünde.*
Bitcoin'in dağıtılmış olarak daha güvenli olması gibi,
toplu çoğaltılmış defter, borsaları daha az savunmasız hale getirebiliriz
blockchain üzerinde çalıştırarak harici ve dahili hackler. Biz
bunu dağıtılmış bir değişim olarak adlandırın.
Kripto para topluluğunun merkezi olmayan dediği şey
bugünkü değişim, "atomik haç" denen bir şeye dayanmaktadır.
zincir ”(AXC) işlemleri. Bir AXC işlemi ile, iki kullanıcı
iki farklı zincir, iki transfer işlemi yapabilir.
her iki defterde birlikte taahhüt edilmiş veya hiç olmamıştır (ör.
atomik olarak). Örneğin, iki kullanıcı ether (veya
AXC işlemlerini kullanarak iki farklı defterdeki herhangi iki token),
Bitcoin ve Ethereum birbirine bağlı olmasa bile
diğer. AXC işlemlerinde bir borsa çalıştırmanın faydası,
ne kullanıcıların birbirlerine ne de takas eşleştirmeye güvenmesi gerekmiyor
hizmet. Olumsuz yanı, her iki tarafın da çevrimiçi olması gerektiğidir.
ticaret gerçekleşecek.
Başka bir merkezi olmayan değişim türü, toplu olarak çoğaltılmış
kendi blok zincirinde çalışan dağıtılmış değişim. Üzerindeki kullanıcılar
bu tür bir değişim bir limit emri gönderebilir ve
bilgisayar kapanır ve ticaret kullanıcı olmadan yürütülebilir.
internet üzerinden. Blockchain, ticareti adına eşleştirir ve tamamlar
tüccarın.

---

**Sayfa 14**

Merkezi bir değişim, derin bir limit emir defteri oluşturabilir
sipariş verir ve böylece daha fazla tüccar çeker. Likidite daha fazlasını yaratır
borsa dünyasında likidite ve dolayısıyla güçlü bir ağ var
değişimde etki (veya en azından bir kazanan-en çok etkiyi alır)
iş. Bugün kripto para borsalarının mevcut lideri
24 saatlik hacmi 20 milyon dolar olan Poloniex ve ikinci sırada
24 saatlik hacmi 5 milyon dolar olan bit nex. Böyle güçlü bir ağ verildiğinde
etkileri nedeniyle, AXC tabanlı merkezi olmayan borsaların
merkezi borsalarda hacim kazanın. Merkezi olmayan bir
merkezi bir borsa ile rekabet edebilmek için
limitli emirlere sahip derin emir defterlerini desteklemek. Sadece dağıtılmış
bir blok zincirinde değişim bunu sağlayabilir.
Tendermint, daha hızlı işlem için ek faydalar sağlar
taahhüt eder. Hızlı kaliteden ödün vermeden öncelik vererek
tutarlılık, Cosmos'taki bölgeler işlemleri hızlı bir şekilde

hem döviz sipariş işlemleri hem de IBC token transferleri
ve diğer bölgelerden.
Bugün kripto para birimi borsalarının durumu göz önüne alındığında, harika
Cosmos uygulaması, dağıtılmış değişimdir (aka
Cosmos DEX). İşlem çıktı kapasitesi ve
taahhüt gecikmesi, merkezileştirilmiş olanlarla karşılaştırılabilir
değişimler. Yatırımcılar, gerçekleştirilebilecek limit emirleri gönderebilirler
her iki tarafın da çevrimiçi olması gerekmeden. Ve Tendermint ile
Cosmos merkezi ve IBC'de, yatırımcılar fonları içeri ve dışarı taşıyabilir
diğer bölgelere ve diğer bölgelerden hızlı değişim.
Ayrıcalıklı bir bölge, bir köprülü belirtecin kaynağı olarak hareket edebilir.
başka bir kripto para birimi. Bir köprü ilişkiye benzer
bir Cosmos hub ve bölgesi arasında; her ikisi de yetişmeli
tokenlerin sahip olduğu kanıtları doğrulamak için diğerinin en son blokları
birinden diğerine taşındı. Cosmos'ta bir "köprü bölgesi"
ağ, Hub'a ve diğerlerine ayak uydurur

---

**Sayfa 15**

kripto para. Köprü bölgesi üzerinden yönlendirme,
Merkezin diğerlerine karşı basit ve agnostik kalma mantığı
Bitcoin'in çalışma kanıtı gibi blok zinciri fikir birliği stratejileri
madencilik.
Her köprü bölgesi doğrulayıcı, Tendermint destekli bir
özel bir ABCI köprü uygulamasına sahip blok zinciri, ancak aynı zamanda
"kaynak" blok zinciri.
Başlangıçta yeni bloklar çıkarıldığında, köprü bölgesi
Doğrulayıcılar, imzalayarak taahhüt edilen bloklar üzerinde anlaşmaya varacaklar
ve menşe blok zincirine ilişkin kendi yerel görüşlerini paylaşmak
İpucu. Bir köprü bölgesi menşe üzerinden ödeme aldığında (ve
davada yeterli onay görüldüğüne karar verildi
Ethereum veya Bitcoin gibi bir PoW zincirinin), karşılık gelen
hesap bu bakiye ile köprü bölgesinde oluşturulur.
Ethereum durumunda, köprü bölgesi aynı şeyi paylaşabilir
Doğrulayıcı-set, Cosmos Hub olarak. Ethereum tarafında (
menşe), bir köprü sözleşmesi, eter sahiplerinin eter göndermesine izin verir
köprü sözleşmesi üzerine göndererek köprü bölgesine
Ethereum. Eter, köprü sözleşmesi tarafından alındıktan sonra,
uygun bir IBC paketi olmadıkça eter geri çekilemez.
köprü-bölgesinden köprü sözleşmesi tarafından alındı.
köprü sözleşmesi, köprü bölgesinin doğrulayıcı kümesini izler.
Cosmos Hub'ın doğrulayıcı kümesiyle aynı olabilir.
Bitcoin durumunda, kavram bunun yerine benzerdir.
tek bir köprü sözleşmesi, her UTXO, bir
eşik çoklu imzalı P2SH pubscript. Sınırlamalar nedeniyle
P2SH sistemi, imzalayanlar Cosmos ile özdeş olamaz
Merkez doğrulayıcı seti.

---

**Sayfa 16**

Köprü bölgesindeki eter ("köprülü eter") şu adrese aktarılabilir:
ve Merkezden ve daha sonra bir işlemle yok edilir.
Ethereum'da belirli bir para çekme adresine gönderir. IBC
işlemin köprü bölgesinde gerçekleştiğini kanıtlayan paket
etere izin vermek için Ethereum köprü sözleşmesine gönderilebilir
geri çekilmek.

Bitcoin söz konusu olduğunda, kısıtlı komut dosyası sistemi bunu
IBC para transfer mekanizmasını yansıtmak zordur. Her UTXO
kendi bağımsız yayınına sahiptir, bu nedenle her UTXO,
kümesinde bir değişiklik olduğunda yeni bir UTXO'ya taşınmıştır.
Bitcoin emanet imzalayanlar. Çözümlerden biri sıkıştırmak ve
Toplam sayıyı korumak için gerektiği şekilde UTXO-set'i açın
UTXO'lar azaldı.
Böyle bir köprüleme sözleşmesinin riski, haydut bir doğrulayıcı kümesidir. ≥⅓
Bizans oylama gücü, eteri geri çekerek çatallaşmaya neden olabilir
Ethereum üzerindeki köprü sözleşmesinden
köprü bölgesinde eter. Daha da kötüsü,> ⅔ Bizans oylama gücü,
onu köprü sözleşmesine gönderenlerden doğrudan eteri çalmak
köprü bölgesinin orijinal köprüleme mantığından saparak.
Köprü olacak şekilde tasarlanarak bu sorunları çözmek mümkündür.
tamamen sorumlu. Örneğin, tüm IBC paketleri, merkezden ve
menşe, içerisindeki köprü bölgesi tarafından onaylanmasını gerektirebilir.
öyle bir şekilde köprü bölgesinin tüm durum geçişleri
ya merkez ya da başlangıç noktası tarafından etkili bir şekilde sorgulanmış ve doğrulanmıştır.
köprü sözleşmesi. Merkez ve çıkış, köprüye izin vermelidir.
teminat göndermek için bölge doğrulayıcıları ve
köprü sözleşmesi ertelenmelidir (ve teminat bağları çözülmelidir)
yeterince uzun bir süre) tarafından yapılabilecek herhangi bir zorluğa izin vermek için
bağımsız denetçiler. Spesifikasyonun tasarımını bırakıyoruz ve
Bu sistemin uygulanması, geleceğin Cosmos'u olarak açık

---

**Sayfa 17**

iyileştirme önerisi, Cosmos Hub'ın
yönetişim sistemi.
Ölçeklendirme problemini çözmek Ethereum için açık bir sorundur.
Şu anda Ethereum düğümleri her bir işlemi işliyor ve
ayrıca tüm durumları depolar. bağlantı .
Tendermint, blokları Ethereum'dan çok daha hızlı işleyebildiğinden
iş kanıtı, Tendermint fikir birliği ile desteklenen EVM bölgeleri ve
köprülü eter üzerinde çalışmak, daha yüksek performans sağlayabilir.
Ethereum blok zincirleri. Ek olarak, Cosmos Hub ve
IBC paket mekaniği, keyfi sözleşme mantığına izin vermiyor
yürütme, token hareketlerini koordine etmek için kullanılabilir
farklı bölgelerde çalışan Ethereum sözleşmeleri arasında,
token merkezli Ethereum ölçeklendirmesi için bir temel sağlar
parçalama.
Cosmos bölgeleri, aşağıdaki adreste tanımlanan rastgele uygulama mantığını çalıştırır.
bölgenin yaşamının başlangıcı ve potansiyel olarak güncellenebilir
zaman içinde yönetişim tarafından. Böyle bir esneklik, Cosmos bölgelerinin
Ethereum gibi diğer kripto para birimlerine köprü görevi görür veya
Bitcoin ve bu blok zincirlerinin türevlerine de izin veriyor,
aynı kod tabanını kullanan ancak farklı bir doğrulayıcı setiyle ve
ilk dağıtım. Bu, birçok mevcut kripto para birimine izin verir
Ethereum, Zerocash, Bitcoin gibi çerçeveler,
CryptoNote ve benzeri, Tendermint Core ile kullanılacak olan
ortak bir ağda daha yüksek performanslı bir fikir birliği motoru,
birlikte çalışabilirlik için muazzam bir fırsat yaratıyor
platformlar. Ayrıca, çok varlıklı bir blok zinciri olarak, tek bir
işlem birden fazla girdi ve çıktı içerebilir, burada her biri
girdi herhangi bir simge türü olabilir ve Cosmos'un doğrudan
merkezi olmayan değişim için bir platform, ancak siparişler varsayılıyor

**Sayfa 18**

diğer platformlar aracılığıyla eşleştirilecek. Alternatif olarak, bir bölge hizmet verebilir
dağıtılmış, hataya dayanıklı bir değişim olarak (sipariş defterleriyle),
mevcut merkezi sistem üzerinde katı bir gelişme olabilir
zamanla saldırıya uğrama eğiliminde olan kripto para birimi borsaları.
Bölgeler aynı zamanda kurumun blockchain destekli versiyonları olarak da kullanılabilir
ve belirli bir hizmetin parçalarının
geleneksel olarak bir kuruluş veya kuruluşlar grubu tarafından yönetilir
bunun yerine belirli bir bölgede bir ABCI uygulaması olarak çalıştırılır.
halkın güvenliğini ve birlikte çalışabilirliğini devralmasına izin verir
Altta yatan kontrolden ödün vermeden Cosmos ağı
hizmet. Böylece, Cosmos her iki dünyanın en iyisini sunabilir:
blockchain teknolojisini kullanmak isteyen ancak kimler
kontrolü tamamen dağıtılmış bir üçüncüye bırakma konusunda temkinli
Parti.
Bazıları, tutarlılık lehinde büyük bir problem olduğunu iddia ediyor
Tendermint gibi fikir birliği algoritmaları, herhangi bir ağın
> ⅔ ile tek bir bölüm olmamasına neden olan bölüm
oylama gücü (örneğin in ine gitmesi) fikir birliğini tamamen durduracaktır.
Cosmos mimarisi, bu sorunu azaltmaya yardımcı olabilir.
oylama gücünün bulunduğu bölgesel özerk bölgelere sahip küresel bir merkez
her bölge için ortak bir coğrafi bölgeye göre dağıtılır
bölge. Örneğin, ortak bir paradigma bireysel olabilir
şehirler veya bölgeler, paylaşırken kendi bölgelerini işletmek için
ortak merkez (örneğin, Cosmos Merkezi), belediye faaliyetlerinin
geçici bir ağ nedeniyle hub'ın durması durumunda devam eder
bölüm. Bunun gerçek jeolojik, politik ve
sağlam tasarımda dikkate alınması gereken ağ-topolojik özellikler
federe hataya dayanıklı sistemler.

**Sayfa 19**

NameCoin,
Bitcoin blok zincirini uyarlayarak isim çözümleme problemi.
Ne yazık ki bu yaklaşımla ilgili birkaç sorun var.
Namecoin ile, doğrulayabilir, örneğin, *@satoshi* oldu
geçmişte bir noktada belirli bir ortak anahtara kaydedilmiş,
ancak o zamandan beri genel anahtarın
son günden beri tüm blokları indirmedikçe yakın zamanda güncellenmiştir
bu adın güncellenmesi. Bu, Bitcoin'in kısıtlılığından kaynaklanmaktadır.
UTXO işlemi Merkle -izasyon modeli, burada yalnızca
işlemler (ancak değişebilen uygulama durumu değil) Merkle uyumludur
blok karması içine. Bu, varoluşu kanıtlamamıza izin verir, ancak olmayanı değil
bir ad için daha sonra yapılan güncellemelerin varlığı. Böylece bilemeyiz
tam olarak güvenmeden bir ismin en son değerinden emin olun
düğüm veya indirerek bant genişliğinde önemli maliyetler doğuyor
tüm blok zinciri.
NameCoin'de Merkle uyumlu bir arama ağacı uygulanmış olsa bile,
iş kanıtı bağımlılığı, hafif müşteri doğrulamasını sağlar
sorunlu. Light istemcilerinin tam bir kopyasını indirmesi gerekir.
tüm blok zincirindeki tüm bloklar için başlıklar (veya en azından tüm
bir adın son güncellemesinden itibaren başlıklar). Bu şu anlama gelir:
bant genişliği gereksinimleri, zaman miktarına göre doğrusal olarak ölçeklenir
[21] . Ek olarak, bir iş kanıtı blok zincirinde isim değişiklikleri

ek iş kanıtı onay bloklarının beklenmesini gerektirir,
Bitcoin'de bir saat kadar sürebilir.
Tendermint ile tek ihtiyacımız olan en son blok karması
onaylayıcılar yeter sayısı (oylama gücüyle) ve bir Merkle tarafından imzalandı
isimle ilişkili mevcut değerin kanıtı. Bu onu yapar
kısa, öz, hızlı ve güvenli bir hafif istemciye sahip olmak mümkün
isim değerlerinin doğrulanması.
Cosmos'ta bu kavramı alıp daha da genişletebiliriz. Her biri
Cosmos'taki ad kayıt bölgesi ilişkili bir üst
".com" veya ".org" gibi düzey alan (TLD) adı ve her ad-

---

**Sayfa 20**

kayıt bölgesi kendi yönetimine ve tesciline sahip olabilir
kurallar.
Cosmos Hub çok varlıklı dağıtılmış bir defter iken,
*atom* adı verilen özel bir yerel belirteç . Atomlar tek bahis
Cosmos Hub simgesi. Atomlar, sahibin aşağıdakileri yapması için bir lisanstır:
oylama, doğrulama veya diğer onaylayıcılara yetki verme. Ethereum'unki gibi
eter, atomlar ayrıca işlem ücretlerini ödemek için kullanılabilir.
istenmeyen postaları azaltmak. Ek olarak tasyoner atomlar ve blok işlemi
ücretler onaylayıcılara ve delege edenlere ödüllendirilir
doğrulayıcılar.
**BurnAtomTx** işlemin herhangi kurtarmak için kullanılabilir
rezerv havuzundan orantılı miktarda token.
Genesis'teki atom tokenleri ve doğrulayıcıların ilk dağıtımı
Cosmos Fundraiser bağışçılarına (% 75), baş bağışçılara gidecek
(% 5), Cosmos Network Foundation (% 10) ve ALL IN BITS, Inc
(% 10). Oluşumundan itibaren, toplam atom miktarının 1 / 3'ü
her yıl gümrüklü onaylayıcılara ve delegatörlere ödüllendirilecektir.
Bkz Cosmos Planı Ek ayrıntılar için.
Bitcoin veya diğer iş kanıtı blok zincirlerinin aksine, bir Tendermint
blok zinciri, artan
iletişim karmaşıklığı. Neyse ki, yeterince destekleyebiliriz
Küresel olarak dağıtılmış sağlam bir blok zinciri oluşturmak için doğrulayıcılar
çok hızlı işlem onay süreleriyle ve bant genişliği olarak,

---

**Sayfa 21**

depolama ve paralel hesaplama kapasitesi arttıkça,
gelecekte daha fazla doğrulayıcıyı desteklemek.
Başlangıç gününde, maksimum doğrulayıcı sayısı şu şekilde ayarlanacaktır:
100 olup bu sayı 10 yıl boyunca% 13 oranında artacak ve
300 doğrulayıcıya yerleşir.
Halihazırda onaylayıcı olmayan atom sahipleri,
bir **BondTx** işleminin imzalanması ve gönderilmesi . Miktarı
teminat olarak verilen atomlar sıfırdan farklı olmalıdır. Herkes olabilir
geçerli boyutun olmadığı durumlar haricinde herhangi bir zamanda bir doğrulayıcı
doğrulayıcı grubu, maksimum doğrulayıcı sayısından daha büyük
izin verilir. Bu durumda, işlem yalnızca tutarının
atomlar tarafından tutulan etkili atomların miktarından daha büyüktür.
etkili atomların delege edilmiş atomları içerdiği en küçük doğrulayıcı.
Yeni bir doğrulayıcı, mevcut bir doğrulayıcıyı bu şekilde değiştirdiğinde,
mevcut doğrulayıcı devre dışı kalır ve tüm atomlar ve
delege edilmiş atomlar bağsız duruma girer.
Doğrulayıcılara herhangi bir ceza uygulanmalıdır.

yaptırımdan kasıtlı veya kasıtsız sapma
protokol. Aşağıdaki gibi bazı kanıtlar hemen kabul edilebilir
aynı yükseklikte ve yuvarlakta çift imza veya ihlal
Yıl 0: 100
1. Yıl: 113
2. Yıl: 127
3. Yıl: 144
4. Yıl: 163
Yıl 5: 184
Yıl 6: 208
7. Yıl: 235
Yıl 8: 265
Yıl 9: 300
Yıl 10: 300
...

---

**Sayfa 22**

"Prevote-the-lock" (Tendermint konsensüs protokolünün bir kuralı).
Bu tür kanıtlar, doğrulayıcının itibarını kaybetmesine neden olacaktır
ve bağlı atomlarının yanı sıra, içindeki tokenlerin orantılı payı
Rezerv havuzu - topluca "hissesi" olarak adlandırılır - kesilir.
Bazen, bölgesel nedenlerden dolayı doğrulayıcılar da kullanılamayacaktır.
ağ kesintileri, elektrik kesintisi veya diğer nedenler. Eğer, herhangi bir zamanda
geçmiş **ValidatorTimeoutWindow** bloklarındaki nokta , bir doğrulayıcının
commit oyu blok zincirine şu değerden daha fazla dahil değildir:
**ValidatorTimeoutMaxAbsent** zamanlar, bu doğrulayıcı olacak
etkin değil ve **ValidatorTimeoutPenalty** (VARSAYILAN% 1)
kazık.
Bazı "kötü niyetli" davranışlar açıkça farkedilebilir
blok zincirine ilişkin kanıt. Bu durumlarda, doğrulayıcılar şunları yapabilir:
bu kötü niyetli kişilerin zaman aşımını zorlamak için bant dışı koordine
Doğrulayıcılar, eğer bir süper çoğunluk fikir birliği varsa.
Cosmos Hub'ın bir ≥⅓ koalisyonu nedeniyle durduğu durumlarda
oy verme yetkisi yok denecek kadar az veya bir koalisyonun bulunduğu durumlarda
oylama gücü sansürü kötü niyetli davranış kanıtı
blok zincirine girerken, hub hard fork ile kurtarılmalıdır
reorg-öneri. ("Çatallar ve Sansür Saldırıları" na bağlantı).
Cosmos Hub doğrulayıcıları herhangi bir simge türünü veya kombinasyonunu kabul edebilir
bir işlemin işlenmesi için ücret olarak türler. Her doğrulayıcı şunları yapabilir:
sübjektif olarak istediği döviz kurunu belirleyin ve
**BlockGasLimit** olduğu sürece istediği işlem ne olursa olsun
aşılmadı. Aşağıda belirtilen vergiler hariç toplanan ücretler,
bağlı paydaşlara orantılı olarak yeniden dağıtılır
bağlı atomları, her **DoğrulayıcıÖdeme Süresi** (VARSAYILAN 1
saat).

---

**Sayfa 23**

Toplanan işlem ücretlerinden **Rezerv Vergisi** (VARSAYILAN% 2)
rezerv havuzunu artırmak için rezerv havuzuna doğru gidin ve
Cosmos ağının güvenliğini ve değerini artırın. Bunlar
Fonlar da kararlara uygun olarak dağıtılabilir
yönetişim sistemi tarafından yapılmıştır.
Oylama yetkilerini diğer doğrulayıcılara devreten atom sahipleri
Yetki verilen doğrulayıcıya bir komisyon ödeyin. Komisyon şunları yapabilir:

her doğrulayıcı tarafından ayarlanmalıdır.
Cosmos Hub'ın güvenliği, cihazın güvenliğinin bir işlevidir.
temelde yatan onaylayıcılar ve delegatörler tarafından yetkilendirme seçimi.
Bulunanların keşfedilmesini ve erken bildirilmesini teşvik etmek için
açıklar, Cosmos Hub bilgisayar korsanlarını yayınlamaya teşvik ediyor
**ReportHackTx** işlemi aracılığıyla "Bu,
doğrulayıcı saldırıya uğradı. Lütfen bu adrese ödül gönderin ". Üzerine
böyle bir istismar, onaylayıcı ve temsilciler etkisiz hale gelecektir,
**HackPunishmentRatio** (varsayılan% 5) herkesin atomunun alacağı
eğik **çizgi** ve herkesin atomlarının **HackRewardRatio** (varsayılan% 5)
bilgisayar korsanının ödül adresine ödüllendirilecek. Doğrulayıcı
yedek anahtarlarını kullanarak kalan atomları kurtarmalıdır.
Bu özelliğin kötüye kullanılmasını önlemek için transfer
yatırım yapılmamış atomlar, kazanılmış ve kazanılmamış atomların kısmı
**ReportHackTx'ten** önceki ve sonraki doğrulayıcılar ve temsilciler ,
aynı kalacak ve hacker ödülü bazılarını içerecek
yatırım yapılmamış atomlar, varsa.
Cosmos Hub, dağıtılmış bir kuruluş tarafından işletilmektedir.
iyi tanımlanmış bir yönetişim mekanizması gerektirir.
değişken gibi blok zincirindeki çeşitli değişiklikleri koordine edin

---

**Sayfa 24**

sistemin parametrelerinin yanı sıra yazılım yükseltmeleri ve
Anayasa değişikliği.
Tüm onaylayıcılar, tüm tekliflerin oylanmasından sorumludur. Başarısız
bir teklif üzerinde zamanında oylama doğrulayıcı ile sonuçlanacaktır
adı verilen bir süre için otomatik olarak devre dışı bırakılıyor
**DevamsızlıkPenaltı Süresi** (VARSAYILAN 1 hafta).
Yetkilendirenler, yetki verilenlerin oylarını otomatik olarak devralır.
doğrulayıcı. Bu oy manuel olarak geçersiz kılınabilir. Bağlanmamış atomlar
oy yok.
Her teklif, **MinimumProposalDepozito** depozitosu gerektirir
jetonlar, bir veya daha fazla jetonun bir kombinasyonu olabilir
atomlar dahil. Seçmenler her öneri için oy kullanabilirler.
depozito. Seçmenlerin yarısından fazlası seçim yaparsa
depozito (örneğin, teklif spam olduğu için), para yatırma
Yanan atomlar hariç rezerv havuzu.
Her öneri için seçmenler aşağıdaki seçeneklerle oy kullanabilir:
Evet
YeaWithForce
Hayır
NayWithForce
Çekimser
Yea veya YeaWithForce oylarının (veya Nay veya
NayWithForce oyları), teklifin aşağıdaki şekilde karara bağlanması için gereklidir.
geçti (veya başarısız olduğuna karar verildi), ancak 1/3 + çoğunluğu veto edebilir
"zorla" oylama ile karar. Katı çoğunluk veto edildiğinde,
Herkes **VetoPenaltyFeeBlocks'u** kaybederek cezalandırılır
(VARSAYILAN 1 günlük blok değeri) değerinde ücretler (vergiler hariç)
etkilenmeyecek) ve çoğunluğu veto eden taraf

---

**Sayfa 25**

Karar ayrıca **VetoPenaltyAtoms'u** kaybederek cezalandırılacaktır.
(VARSAYILAN% 0.1) atomlarının.

Burada tanımlanan parametrelerden herhangi biri ile değiştirilebilir.
bir **ParameterChangeProposal** öğesinin geçirilmesi .
Atomlar atlanabilir ve havuz fonları ile harcanabilir.
Bir **Ödül Teklifinin geçmesi** .
Protokolü yükseltme teklifi gibi diğer tüm teklifler,
genel **TextProposal** aracılığıyla koordine **edilecektir** .
Planı görün .
Blockchain konsensüsünde birçok yenilik oldu ve
son birkaç yılda ölçeklenebilirlik. Bu bölüm kısa bir bilgi sağlar
seçilmiş birkaç önemli konunun araştırılması.
Kötü niyetli katılımcıların varlığında fikir birliği bir sorundur
Leslie Lamport'un
"Bizans hatası" ifadesi, keyfi süreç davranışına atıfta bulunur.
bir "çarpışma hatası" nın aksine amaçlanan davranıştan saparsa,
burada bir süreç basitçe çöker. Erken çözümler keşfedildi
üst sınırın olduğu zaman uyumlu ağlar için

---

**Sayfa 26**

mesaj gecikmesi, pratik kullanım oldukça sınırlıydı
uçak kontrolörleri gibi kontrollü ortamlar ve
veri merkezleri atomik saatler aracılığıyla senkronize edilir. Kadar değildi
Uygulama Bizans Hata Toleransı (PBFT), geç 90s [11] idi
etkili, kısmen eşzamanlı bir fikir birliği olarak sunuldu
Algoritma davranan işlemlerin ⅓'üne kadar tolere edebilir
keyfi olarak. PBFT, standart algoritma haline geldi ve birçok
en son IBM tarafından oluşturulmuş olanı da dahil olmak üzere varyasyonlar
Hyperledger'a katkıları.
Tendermint mutabakatının PBFT üzerindeki ana faydası şudur:
Tendermint geliştirilmiş ve basitleştirilmiş bir alt yapıya sahiptir,
bunlardan bazıları blok zinciri paradigmasını benimsemenin bir sonucudur.
Tendermint blokları sırayla işlemelidir, bu da
PBFT'lerle ilişkili karmaşıklık ve iletişim ek yükü
görünüm değişiklikleri. Cosmos'ta ve birçok kripto para biriminde
Blok imkan vermek için ihtiyaç $K + i\ i> = 1$ işlemek için, blok $N$
kendisi henüz taahhüt etmedi. Bant genişliği, *N'yi* engellemenin nedeni ise
bir Cosmos bölgesinde taahhütte bulunmadıysa, kullanmanın faydası olmaz
$N + i$ blokları için bant genişliği paylaşım oyları . Bir ağ bölümü veya
ine düğümlerinin sayısı, blok *N'nin* taahhüt etmemesinin sebebidir , o zaman
$N +$ *ben* zaten taahhüt etmeyeceğim.
Ek olarak, işlemlerin bloklar halinde gruplandırılması,
uygulama durumunun düzenli Merkle hashing'i yerine
PBFT'nin kontrol noktası şemasında olduğu gibi periyodik sindirimler. Bu izin verir
hafif müşteriler için daha hızlı ve daha hızlı kanıtlanabilir işlem taahhütleri için
blok zincirleri arası iletişim.
Tendermint Core ayrıca birçok optimizasyon ve özellik içerir
PBFT'de belirtilenin ötesine geçen. Örneğin,
Doğrulayıcılar tarafından önerilen bloklar parçalara ayrılmıştır,
ve yayını iyileştirecek şekilde dedikodu yaptılar
performans ( ilham için bkz. LibSwift [19] ). Ayrıca Tendermint
Core, noktadan noktaya herhangi bir varsayımda bulunmaz

---

**Sayfa 27**

bağlantı ve P2P ağı olduğu sürece çalışır
zayıf bağlı.

İlk dağıtım kanıtı (PoS) olmasa da, BitShares1.0 [12]
PoS'nin araştırılmasına ve benimsenmesine önemli ölçüde katkıda bulundu
blok zincirleri, özellikle "delege edilmiş" PoS olarak bilinenler. İçinde
BitShares, pay sahipleri sipariş vermekten sorumlu "tanıkları" seçer
ve işlemleri yapmak ve "delegeler",
yazılım güncellemelerini ve parametre değişikliklerini koordine etmek.
BitShares2.0, yüksek performans (100k tx / s, 1sn
gecikme) ideal koşullarda, her bloğun tek bir
imzalayan ve işlemin uygunluğu,
blok aralığı. Kanonik bir spesifikasyon hala geliştirme aşamasındadır.
Paydaşlar, kötü davranan tanıkları bir
günlük bazda, ancak tanıkların önemli bir teminatı veya
Tendermint PoS benzeri delegatörler kesildi
başarılı bir çift harcama saldırısı durumu.
Ripple'ın öncülüğünü yaptığı bir yaklaşımı temel alan Stellar [13] ,
Federe Bizans Anlaşması modeli, burada süreçler
fikir birliğine katılmak, bir xed oluşturmaz ve küresel olarak
bilinen küme. Aksine, her işlem düğümü bir veya daha fazla
Her biri bir dizi güvenilir süreç oluşturan "yetersayı dilimleri". Bir
Stellar'daki "çekirdek", aşağıdakileri içeren bir düğüm kümesi olarak tanımlanır:
kümedeki her düğüm için en az bir çekirdek dilimi, öyle ki
anlaşmaya varılabilir.
Stellar mekanizmasının güvenliği varsayıma dayanır
*herhangi* iki yeter sayının kesişiminin boş olmadığını, oysa
Bir düğümün kullanılabilirliği, çekirdek dilimlerinin en az birini gerektirir.
tamamen doğru düğümlerden oluşur ve aralarında bir değiş tokuş yaratır.
Dengelenmesi zor olabilecek büyük veya küçük çekirdek dilimlerinin kullanılması
güven konusunda önemli varsayımlar empoze etmeden. Sonuçta,

---

**Sayfa 28**

düğümler bir şekilde oraya gitmek için yeterli çekirdek dilimlerini seçmelidir.
yeterli hata toleransı (veya herhangi bir "bozulmamış düğüm") olması
makalenin sonuçlarının çoğu) ve tek
böyle bir konfigürasyonun hiyerarşik olmasını sağlamak için sağlanan strateji
ve top- tarafından kullanılan Sınır Ağ Geçidi Protokolüne (BGP) benzer
küresel yönlendirme tabloları oluşturmak için internette katmanlı ISS'ler ve
TLS sertifikalarını yönetmek için tarayıcılar tarafından kullanılan; ikisi de ünlü
güvensizlikleri için.
Tendermint temelli ispatın Stellar gazetesindeki eleştiri
riskli sistemler, açıklanan jeton stratejisi ile hafifletilir
burada, *atom* adı verilen yeni bir jeton türü verilir.
Gelecekteki ücret ve ödüllere ilişkin talepleri temsil eder.
Tendermint temelli Proof of Stake'in avantajı görecelidir.
basitlik, yine de yeterli ve kanıtlanabilir güvenlik sağlar
garantiler.
BitcoinNG, Bitcoin'e izin verecek önerilen bir iyileştirmedir.
blok boyutunu artırmak gibi dikey ölçeklenebilirlik biçimleri için,
tipik olarak ilişkili olumsuz ekonomik sonuçlar olmadan
orantısız büyük etki gibi böyle bir değişiklikle
küçük madencilerde. Bu iyileştirme,
işlem yayınından lider seçimi: liderler ilk sırada
"mikro bloklarda" çalışma kanıtı tarafından seçilir ve daha sonra
yeni bir mikro bloğa kadar yapılacak yayın işlemleri
bulunan. Bu, gerekli bant genişliği gereksinimlerini azaltır.
PoW yarışını kazanmak, küçük madencilerin daha adil bir şekilde rekabet etmesine izin vermek,

ve işlemlerin daha düzenli olarak yapılmasına izin vermek
mikro blok bulmak için son madenci.
Casper [16] , aşağıdakiler için önerilen bir kanıt kanıtı fikir birliği algoritmasıdır.
Ethereum. Başlıca çalışma modu "bahisle oybirliği" dir. Tarafından
Doğrulayıcıların, inandıklarına inandıkları blok üzerine yinelemeli olarak bahse girmelerine izin vermek

---

**Sayfa 29**

diğer bahislere bağlı olarak blok zincirine bağlanmak
Şimdiye kadar gördükleri gerçeğe eninde sonunda ulaşılabilir. bağlantı .
Bu, Casper ekibi tarafından aktif bir araştırma alanıdır.
en büyük zorluk, bir bahis mekanizması oluşturmaktır.
evrimsel olarak istikrarlı bir strateji olduğu kanıtlanmıştır. Ana faydası
Tendermint ile karşılaştırıldığında Casper, "kullanılabilirlik" sunabilir
aşırı tutarlılık ”- fikir birliği için> ⅔ yeter çoğunluk gerektirmez
oylama gücü - belki de taahhüt hızı pahasına veya
uygulama karmaşıklığı.
Interledger Protokolü [14] kesinlikle bir ölçeklenebilirlik çözümü değildir. O
farklı defter arasında geçici bir birlikte çalışma sağlar
gevşek bağlı ikili ilişki ağı aracılığıyla sistemler.
Lightning Network gibi, ILP'nin amacı da
ödemeler, ancak özellikle farklı ülkelerdeki ödemelere odaklanır.
defter türleri ve atomik işlem mekanizmasını genişletir.
yalnızca karma kilitleri değil, aynı zamanda noter yeter sayısını da içerir (
Atomik Taşıma Protokolü). İkinci mekanizma
Defterler arası işlemlerde atomikliği zorlamak,
Tendermint'in hafif istemci SPV mekanizması, bu nedenle
ILP ile Cosmos / IBC arasındaki ayrım garantilidir ve
aşağıda verilmiştir.
1. ILP'deki bir bağlayıcının noterleri üyeliği desteklemez
değişir ve aralarında esnek ağırlıklandırma yapılmasına izin vermez.
noterler. Öte yandan, IBC özellikle aşağıdakiler için tasarlanmıştır:
doğrulayıcıların farklı ağırlıklara sahip olabileceği blok zincirleri ve
üyelik süreci boyunca nerede değişebilir?
blok zinciri.
2. Yıldırım Ağında olduğu gibi, ILP'de ödeme alıcısı
gönderene bir onay göndermek için çevrimiçi olmalıdır. İçinde

---

**Sayfa 30**

alıcının doğrulayıcı seti olan IBC üzerinden token transferi
Doğrulama sağlamaktan blok zinciri sorumludur,
alıcı kullanıcı.
3. En çarpıcı fark, ILP'nin konektörlerinin
ödemelerle ilgili sorumlu veya yetkili devleti sürdürmek,
Cosmos'ta ise, bir merkezin doğrulayıcıları,
IBC belirteç transferlerinin durumu ve ayrıca
her bölge tarafından tutulan token miktarı (ancak miktarı değil
bir bölgedeki her hesap tarafından tutulan jetonlar). Bu
asimetrik güvenliğe izin veren temel yenilik
jetonların bölgeden bölgeye aktarılması; ILP'lerin analogu
Cosmos'taki bağlayıcı kalıcı ve maksimum düzeyde güvenli
blockchain defteri, Cosmos Hub.
4. ILP'deki defterler arası ödemelerin bir
asimetrik transfer olmadığı için değişim emir defteri

bir defterden diğerine bozuk paralar, yalnızca değerin aktarımı veya
piyasa eşdeğerleri.
Yan zincirler [15] , Bitcoin'i ölçeklendirmek için önerilen bir mekanizmadır
ağa "iki yönlü sabitlenmiş" alternatif blok zincirleri üzerinden ağ
Bitcoin blok zinciri. (İki yönlü pimleme eşdeğerdir
köprüleme. Cosmos'ta piyasadan ayırt etmek için "köprü" diyoruz.
pimleme). Yan zincirler, bitcoinlerin
Bitcoin blok zincirinden yan zincire ve geriye doğru ve izin verin
yan zincirdeki yeni özelliklerde deneme. Olduğu gibi
Cosmos Hub, yan zincir ve Bitcoin,
madeni paraların ne zaman olması gerektiğini belirlemek için SPV kanıtlarını kullanarak
yan zincire ve geriye aktarılır. Tabii ki Bitcoin'den beri
iş kanıtı kullanır, Bitcoin merkezli yan zincirler zarar görür
iş kanıtı olarak birçok sorun ve riskten
fikir birliği mekanizması. Dahası, bu bir Bitcoin maksimalistidir
çeşitli belirteçleri yerel olarak desteklemeyen çözüm ve

---

**Sayfa 31**

Cosmos'un yaptığı gibi bölgeler arası ağ topolojisi. Bu, çekirdek dedi
iki yönlü mandalın mekanizması prensipte bununla aynıdır
Cosmos ağı tarafından kullanılmaktadır.
Ethereum şu anda bir dizi farklı strateji araştırıyor
Ethereum blok zincirinin durumunu ele almak için
ölçeklenebilirlik ihtiyaçları. Bu çabaların amacı,
Mevcut Ethereum Sanal Makinesi tarafından sunulan soyutlama katmanı
paylaşılan durum uzayında. Çoklu araştırma çabaları
şu anda yapım aşamasında. [18] [22]
Cosmos ve Ethereum 2.0 Mauve [22] farklı tasarım hedeflerine sahiptir.
Cosmos, özellikle belirteçlerle ilgilidir. Mauve, ölçeklendirmeyle ilgilidir
genel hesaplama.
Cosmos, EVM'ye bağlı değildir, bu nedenle farklı VM'ler bile
birlikte çalışın.
Cosmos, bölge oluşturucunun, bölgeyi kimin doğrulayacağını belirlemesine izin verir.
bölge.
Herkes Cosmos'ta yeni bir bölge başlatabilir (yönetim
aksi karar verir).
Hub, bölge hatalarını izole eder, böylece küresel belirteç değişmezleri
korunmuş.
Lightning Network, önerilen bir belirteç aktarım ağıdır
Bitcoin blok zincirinin üzerindeki bir katmanda (ve diğer halka açık
blok zincirleri), birçok büyüklükte iyileştirme sağlar
işlemlerin çoğunu taşıyarak işlem hacminde
mutabakat defterinin dışında sözde “ödeme kanallarına”.

---

**Sayfa 32**

Bu, zincir üzerindeki kripto para birimi komut dosyalarıyla mümkün kılınmıştır.
tarafların ikili devlet sözleşmelerine girmesini sağlamak
durum, dijital imzalar ve sözleşmeler paylaşılarak güncellenebilir
blok zincirinde doğal olarak kanıt yayınlayarak kapatılabilir, bir
mekanizma öncelikle zincirler arası atomik takaslarla popüler hale getirildi. Tarafından
birçok tarafla ödeme kanallarının açılması, katılımcıların
Lightning Network,
başkalarının ödemeleri, tamamen bağlantılı bir ödeme kanalına yol açar
ödeme kanallarına bağlanan sermaye pahasına ağ.

Lightning Network, aynı zamanda kolayca genişleyebilir.
*değer* transferine izin vermek için birden fazla bağımsız blok zinciri
bir döviz piyasası aracılığıyla, asimetrik olarak kullanılamaz
Transfer *belirteçleri* birinden diğerine blockchain. Ana fayda
burada açıklanan Cosmos ağından
jeton transferleri. Bununla birlikte, ödeme kanalları bekliyoruz ve
Lightning Network, yaygın olarak benimsenecek
maliyet tasarrufu ve gizlilik nedenleriyle belirteç aktarım mekanizması.
Ayrılmış Tanık, bir Bitcoin iyileştirme önerisi bağlantısıdır .
blok başına işlem hacmini 2X veya 3X artırmayı hedefler,
Aynı anda yeni düğümler için blok senkronizasyonunu daha hızlı hale getirir.
Bu çözümün parlaklığı, içinde nasıl çalıştığıdır.
Bitcoin'in mevcut protokolünün sınırlamaları ve soft-fork'a izin veriyor
yükseltme (yani, yazılımın daha eski sürümlerine sahip istemciler
yükseltmeden sonra çalışmaya devam edin). Tendermint, yeni olmak
protokol, tasarım kısıtlaması yoktur, bu nedenle farklı bir ölçeklendirmeye sahiptir
öncelikler. Öncelikle, Tendermint bir BFT round-robin algoritması kullanır
madencilik yerine kriptografik imzalara dayanır.
birden fazla paralel üzerinden yatay ölçeklemeye önemsiz bir şekilde izin verir
blokzincirleri, normal, daha sık blok işlemleri izin verirken
dikey ölçekleme de.

---

**Sayfa 33**

İyi tasarlanmış bir fikir birliği protokolü, bazı
tolerans kapasitesinin aşılması durumunda garanti
ve fikir birliği başarısız olur. Bu özellikle ekonomik
Bizans davranışının önemli finansal
ödül. Bu türden en önemli garanti bir çeşit *çataldır.*
*hesap verebilirlik* , uzlaşmaya neden olan süreçlerin
başarısız (yani, protokol istemcilerinin farklı değerleri kabul etmesine neden oldu - a
çatal) kurallarına göre tanımlanabilir ve cezalandırılabilir
protokol veya muhtemelen yasal sistem. Hukuk sistemi ne zaman
güvenilmez veya aşırı pahalı, doğrulayıcılar olabilir
katılmak için depozito yatırmak zorunda olanlar ve
kötü niyetli davranışlar söz konusu olduğunda depozitolar iptal edilebilir veya kesilebilir.
tespit edildi [10] .
Bunun çatallanmanın düzenli bir olay olduğu Bitcoin'den farklı olduğunu unutmayın.
ağ eşzamansızlığı ve nding'in olasılıklı doğası nedeniyle
kısmi hash çarpışmaları. Çoğu durumda kötü amaçlı bir çatal,
Eşzamansızlık nedeniyle bir çataldan ayırt edilemez, Bitcoin yapamaz
Örtülü olanlar dışında, güvenilir bir şekilde çatal hesap verebilirliği uygulamak
madenciler tarafından öksüz kalmış bir bloğun madenciliği için ödenen fırsat maliyeti.
Oylama aşamalarına *PreVote* ve *PreCommit diyoruz* . Bir oy olabilir
belirli bir blok veya *Nil için* . Bir koleksiyon> ⅔ PreVotes diyoruz
aynı turdaki tek bir blok için bir *Polka* ve bir> of koleksiyonu için
Bir *Commit* turunda tek bir blok için PreCommits . Eğer> ⅔
Nil için PreCommit aynı turda, bir sonraki tura geçiyorlar
yuvarlak.
Protokoldeki katı determinizmin zayıf bir
hatalı liderler tespit edilmeli ve

---

**Sayfa 34**

atlandı. Bu nedenle, doğrulayıcılar bir süre bekler,
*Zaman Aşımı* , *Sıfırdan* Önce *Oylamadan* önce önerin ve

Zaman Aşımı Teklifi her turda artar. İlerleme
bir raundun geri kalanı tamamen eşzamansızdır, bu süreçte yalnızca
bir doğrulayıcı ağın ⅔ 'sinden duyduğunda yapılır. Uygulamada,
Son derece güçlü bir düşmanın gerçekten de son derece güçlü bir rakibin
zayıf eşzamanlı varsayım (fikir birliğinin başarısız olmasına neden olur.
bir blok yaparsanız) ve bunu yapmak daha da fazla yapılabilir
Her birinde rasgele TimeoutPropose değerleri kullanarak zor kült
doğrulayıcı.
Ek bir dizi kısıtlama veya Kilitleme Kuralları,
ağ sonunda her yükseklikte sadece bir blok işleyecektir. Hiç
birden fazla bloğun işlenmesine neden olmak için kötü niyetli girişim
belirli bir yükseklikte tanımlanabilir. İlk olarak, bir blok için bir Ön Komite
bu blok için bir Polka şeklinde gerekçeyle gelmelidir.
Doğrulayıcı, R_1 turunda bir blok önceden *vermişse* ,
o blokta *kilitli* olduklarını söylüyorlar ve Polka,
R_2 turundaki yeni Ön Komite, *R_polka* turunda *gelmelidir*
burada *R_1 <R_polka <= R_2* . İkincisi, doğrulayıcılar önermek zorundadır
ve / veya kilitlendikleri bloğu Ön Oylayın. Birlikte bunlar
koşullar, bir doğrulayıcının,
gerekçe olarak yeterli kanıt ve sahip olan doğrulayıcılar
Halihazırda PreCommit, PreCommit için kanıtlara katkıda bulunamaz
başka bir şey. Bu, hem güvenliği hem de canlılığı sağlar.
fikir birliği algoritması.
Protokolün tüm ayrıntıları burada açıklanmaktadır .
Tendermint'te tüm blok başlıklarını senkronize etme ihtiyacı ortadan kalkar.
Alternatif bir zincirin (çatal) varlığı olarak PoS,
bonolu hisseler kesilebilir. Tabii ki, eğik çizgi gerektirdiğinden
O *birisi* bir çatal payı kanıt, hafif istemciler saklamalısınız
gördüğü herhangi bir blok karma işlemi. Ek olarak, hafif istemciler

---

**Sayfa 35**

Doğrulayıcı kümesindeki değişikliklerle periyodik olarak senkronize kalabilir
uzun menzilli saldırılardan kaçınmak için (ancak diğer çözümler
mümkün).
Ethereum'a benzer bir ruhta, Tendermint, uygulamaların
her bloğa genel bir Merkle kök karması yerleştirerek
hesap bakiyeleri, değer gibi şeyler için doğrulanabilir durum sorguları
bir sözleşmede depolanmış veya harcanmamış bir işlemin varlığı
uygulamanın doğasına bağlı olarak çıktı.
Yeterince esnek bir yayın ağları koleksiyonu varsayarsak
ve statik bir doğrulayıcı setinde, blok zincirindeki herhangi bir çatal,
tespit edildi ve suçlu doğrulayıcıların mevduatları kesildi. Bu
İlk olarak 2014'ün başlarında Vitalik Buterin tarafından önerilen yenilik,
diğer kanıtın tehlikede olmayan sorunu
kripto para birimleri ( İlgili Çalışmaya bakınız ). Ancak, doğrulayıcı belirlediğinden
orijinali uzun bir süre boyunca değiştirebilmeli
Doğrulayıcıların tümü bağsız hale gelebilir ve bu nedenle
oluşum bloğundan yeni bir zincir oluşturun,
artık kilitli depozitoları yok. Bu saldırı geldi
Kısa Menzilli Saldırının aksine, Uzun Menzilli Saldırı (LRA) olarak bilinir.
Menzil Saldırısı, halihazırda bağlı olan doğrulayıcıların
çatal ve bu nedenle cezalandırılır (çataldan sorumlu bir BFT varsayılarak)
Tendermint konsensüsü gibi algoritma). Uzun Menzilli Saldırılar
genellikle risk kanıtı için kritik bir darbe olduğu düşünülür.
Neyse ki, LRA aşağıdaki gibi hafifletilebilir. Birincisi, bir

validator'un tahvilini çözmesi (böylece teminat mevduatını geri alma)
ve artık fikir birliğine katılmak için ücret kazanmıyorsa),
depozito bir süre için aktarılamaz hale getirilmelidir
"bağsızlık dönemi" olarak bilinir ve şu sırayla olabilir:
haftalar veya aylar. İkincisi, hafif bir müşterinin güvende olması için,
ağa bağlandığında, yeni bir blok karmasını doğrulaması gerekir
güvenilir bir kaynağa veya tercihen birden çok kaynağa karşı. Bu

---

**Sayfa 36**

durum bazen “zayıf öznellik” olarak anılır. En sonunda,
Güvende kalması için, şu adreste ayarlanan en son doğrulayıcı ile senkronize edilmesi gerekir:
en az bağlama süresinin uzunluğu kadar sık. Bu
hafif istemcinin doğrulayıcıdaki değişiklikleri bilmesini sağlar
bir doğrulayıcının sermayesi serbest bırakılmadan önce belirlenir ve bu nedenle artık
tehlikede, bu da müşteriyi kandırmasına izin verir
bir anda yeni bloklar oluşturarak uzun menzilli bir saldırı
bağlandığı yerin yüksekliği (yeterince kontrol sahibi olduğu varsayılarak
erken özel anahtarların çoğu).
Bu şekilde LRA'nın üstesinden gelmenin bir revizyon gerektirdiğini unutmayın.
çalışma kanıtının orijinal güvenlik modeli. PoW'da
hafif bir istemcinin şu anki yüksekliğe senkronize edebileceği varsayılmıştır.
güvenilir oluşum bloğu herhangi bir zamanda sadece ispatı işleyerek
her blok başlığında çalışma. Bununla birlikte, LRA'nın üstesinden gelmek için
hafif bir müşterinin biraz düzenli olarak çevrimiçi olmasını
Doğrulayıcı kümesindeki değişiklikleri izleyin ve ilk kez
çevrimiçi olduklarında, kimlik doğrulaması için özellikle dikkatli olmaları gerekir
güvenilir kaynaklara karşı ağdan duyduklarını. Nın-nin
Tabii ki, bu ikinci gereksinim Bitcoin ile benzerdir, burada
protokol ve yazılım da güvenilir bir
kaynak.
LRA'yı önlemek için yukarıdaki yöntem doğrulayıcılar için çok uygundur
ve Tendermint destekli bir blok zincirinin tam düğümleri, çünkü bunlar
düğümlerin ağa bağlı kalması amaçlanmıştır.
yöntem aynı zamanda beklenen hafif istemciler için de uygundur.
ağ ile sık sık senkronize edin. Ancak, hafif müşteriler için
İnternete veya
blockchain ağı, üstesinden gelmek için başka bir çözüm kullanılabilir
LRA. Doğrulayıcı olmayan jeton sahipleri, jetonlarını şu şekilde yayınlayabilir:
Bağlantısızlık süresi çok uzun olan teminat (örneğin, çok daha uzun
doğrulayıcılar için bağlayıcı olmayan dönemden daha fazla) ve hafif müşterilere hizmet
akımın geçerliliğini kanıtlamak için ikincil bir yöntemle ve
geçmiş blok karmaları. Bu belirteçler,
blockchain'in mutabakatının güvenliği, yine de

---

**Sayfa 37**

hafif müşteriler için güçlü garantiler sağlar. Tarihsel blok karması ise
Ethereum'da sorgulama desteklendi, herkes kendi
özel olarak tasarlanmış bir akıllı sözleşmede belirteçler ve
ödeme için tasdik hizmetleri, ışık için etkili bir pazar yaratma-
istemci LRA güvenliği.
Bir blok taahhüdün tanımına bağlı olarak, herhangi bir ≥⅓ koalisyonu
Oylama gücü, blok zincirini ine ya da ine ederek durdurabilir
oylarını yayınlıyor. Böyle bir koalisyon aynı zamanda
bunları içeren blokları reddederek belirli işlemler

önemli bir oranla sonuçlansa da
oranı yavaşlatacak olan reddedilecek blok tekliflerinin oranı
Blok zincirinin blok taahhütleri, faydasını ve değerini azaltarak.
Kötü niyetli koalisyon, oyları yavaş yavaş da yayınlayabilir, bu nedenle
blockchain blok taahhütlerini neredeyse durma noktasına getirmek veya
bu saldırıların herhangi bir kombinasyonu. Son olarak,
çift imzalayarak veya kilitlemeyi ihlal ederek blok zincirden çatala
kurallar.
Küresel olarak aktif bir düşman da dahil olsaydı, bölünebilirdi
ağ, yanlış görünebilecek şekilde
yavaşlamadan doğrulayıcıların bir alt kümesi sorumluydu. Bu değil
sadece Tendermint'in bir sınırlaması, daha ziyade hepsinin bir sınırlaması
ağı potansiyel olarak bir tarafından kontrol edilen fikir birliği protokolleri
aktif düşman.
Bu tür saldırılar için, doğrulayıcıların bir alt kümesi,
bir yeniden düzenleme teklifini imzalamak için dış yollarla koordine edin.
bir çatalı (ve bunun herhangi bir kanıtını) ve ilk alt kümesini seçer
onaylayıcıları imzaları ile. Böyle bir yeniden düzenlemeyi imzalayan onaylayıcılar
teklif, diğer tüm çatallarda teminatlarından vazgeçer. Müşteriler
yeniden düzenleme teklifindeki imzaları doğrulayın, herhangi bir kanıtı doğrulayın,
ve bir yargıda bulunun veya son kullanıcıyı bir karar için yönlendirin. İçin
Örneğin, bir telefon cüzdanı uygulaması kullanıcıya bir güvenlik

---

**Sayfa 38**

uyarı, bir buzdolabı herhangi bir yeniden düzenleme teklifini kabul edebilir
oylama gücü tarafından orijinal doğrulayıcıların + power ile imzalanmıştır.
Senkronize olmayan Bizans hataya dayanıklı algoritma gelemez
oylama gücünün ≥⅓'ü dürüst olmadığında, ancak bir çatal olduğunda fikir birliğine varmak
oylama gücünün ≥⅓'ünün tarafından zaten sahtekâr olduğunu varsayar
gerekçesiz çift imza veya kilit değiştirme. Yani imzalamak
yeniden düzenleme önerisi, yapılamayacak bir koordinasyon problemidir
senkronize olmayan herhangi bir protokol tarafından çözüldü (yani otomatik olarak ve
güvenilirliği hakkında varsayımlar yapmadan
temel ağ). Şimdilik, yeniden düzenleme sorununu bırakıyoruz.
sosyal mutabakat yoluyla insan koordinasyonuna teklif koordinasyonu
İnternet medyasında. Doğrulayıcılar, aşağıdakilerden emin olmak için özen göstermelidir:
bir yeniden düzenleme imzalamadan önce kalan ağ bölümü yok
iki çelişkili yeniden yapılanmanın olduğu durumlardan kaçınmak için öneri
teklifler imzalanır.
Harici koordinasyon ortamının ve protokolün
sağlam, çatalların sansürden daha az endişe verici olduğu sonucu çıkar
saldırılar.
Çatallar ve sansüre ek olarak, ≥⅓ Bizans
oylama gücü,> ⅔ oylama gücünden oluşan bir koalisyon taahhüt edebilir
keyfi, geçersiz durum. Bu, herhangi bir (BFT) özelliğidir.
fikir birliği sistemi. Çatal oluşturan çift imzalamanın aksine
kolayca doğrulanabilir kanıtlarla, bir taahhüdün tespit edilmesi
geçersiz durum, tüm blokları doğrulamak için doğrulanmayan eşler gerektirir,
bu, eyaletin yerel bir kopyasını tuttuklarını ve
her işlem, durum kökünü bağımsız olarak hesaplamak için
kendilerini. Bir kez tespit edildiğinde, böyle bir başarısızlığı halletmenin tek yolu
sosyal fikir birliği yoluyladır. Örneğin, Bitcoin'in
Yazılım hataları nedeniyle çatallama olsun, başarısız oldu (Mart ayında olduğu gibi)
2013), veya Bizans'ın davranışları nedeniyle geçersiz devlet işlemek
madenciler (Temmuz 2015'te olduğu gibi), iyi bağlantılara sahip topluluk

işletmeler, geliştiriciler, madenciler ve diğer kuruluşlar
manuel eylemlerin ne olduğu konusunda sosyal bir fikir birliği oluşturdu

---

**Sayfa 39**

katılımcılar tarafından ağı iyileştirmek için gereklidir. Ayrıca, o zamandan beri
Bir Tendermint blok zincirinin doğrulayıcılarının
tanımlanabilir, geçersiz bir durumun taahhüdü bile olabilir
İstenirse, kanun veya bazı harici içtihatlarla cezalandırılabilir.
ABCI, şuradan teslim alınan 3 birincil mesaj türünden oluşur:
uygulamanın çekirdeği. Uygulama şu şekilde yanıt verir:
karşılık gelen yanıt mesajları.
**AppendTx** mesajı uygulamanın çalışma atı. Her biri
blok zincirindeki işlem bu mesajla birlikte teslim edilir.
uygulamanın, alınan her işlemi doğrulaması gerekir.
Mevcut duruma karşı AppendTx mesajı, uygulama protokolü,
ve işlemin kriptografik kimlik bilgileri. Doğrulanmış
işlemin daha sonra uygulama durumunu güncellemesi gerekir - tarafından
bir anahtar değer deposuna bir değer bağlama veya UTXO'yu güncelleyerek
veri tabanı.
**CheckTx** mesajı AppendTx benzer, ancak yalnızca içindir
işlemleri doğrulama. Tendermint Core'un mempool ilk kontrolleri
CheckTx ile bir işlemin geçerliliği ve yalnızca geçerli geçişler
emsallerine yapılan işlemler. Uygulamalar artışı kontrol edebilir
işlemde nonce ve CheckTx sırasında bir hata döndürürse
nonce eskidir.
**Teslim** mesajı bir şifreleme hesaplamak için kullanılır
mevcut başvuru durumuna bağlılık,
sonraki blok başlığı. Bunun bazı kullanışlı özellikleri var.
Bu durumu güncellemedeki tutarsızlıklar artık şu şekilde görünecektir:
bütün bir programlama sınıfını yakalayan blockchain çatalları
hatalar. Bu aynı zamanda güvenli hafif yapının geliştirilmesini de basitleştirir.
müşteriler, Merkle hash provaları ile kontrol edilerek doğrulanabildiğinden
blok karması ve blok karması bir yeter sayı ile imzalanır
doğrulayıcılar (oylama gücüne göre).

---

**Sayfa 40**

Ek ABCI mesajları, uygulamanın aşağıdakileri takip etmesine izin verir:
ve doğrulayıcı setini değiştirin ve uygulamanın
yükseklik ve commit oyları gibi blok bilgileri.
ABCI istekleri / yanıtları basit Protobuf mesajlarıdır. Kontrol
dışarı şema le .
**Bağımsız değişkenler** :
**Veri ([] bayt)** : İstek işlem baytları
**İade** :
**Kod (uint32)** : Yanıt kodu
**Veri ([] bayt)** : Varsa sonuç baytları
**Günlük (dize)** : Hata ayıklama veya hata mesajı
**Kullanım** :
Bir işlem ekleyin ve çalıştırın. İşlem geçerliyse,
CodeType.OK döndürür
**Bağımsız değişkenler** :
**Veri ([] bayt)** : İstek işlem baytları
**İade** :
**Kod (uint32)** : Yanıt kodu

**Veri ([] bayt)** : Varsa sonuç baytları
**Günlük (dize)** : Hata ayıklama veya hata mesajı
**Kullanım** :
Bir işlemi onaylayın. Bu mesaj,
durum. İşlemler önce CheckTx ile çalıştırılır.
mempool katmanındaki eşlere yayın. Yapabilirsin
CheckTx yarı durumludur ve durumu **Commit** veya
**Bağımlı** işlem dizilerine izin vermek için **BeginBlock**
aynı blokta.

---

**Sayfa 41**

**İade** :
**Veri ([] bayt)** : Merkle kök karması
**Günlük (dize)** : Hata ayıklama veya hata mesajı
**Kullanım** :
Uygulama durumunun Merkle kök karmasını döndürür.
**Bağımsız değişkenler** :
**Veri ([] bayt)** : Sorgu isteği baytları
**İade** :
**Kod (uint32)** : Yanıt kodu
**Veri ([] bayt)** : Sorgu yanıt baytları
**Günlük (dize)** : Hata ayıklama veya hata mesajı
**Kullanım** :
Yanıt kuyruğunu temizleyin. Uygulayan uygulamalar
**types.Application'ın** bu mesajı uygulamasına gerek yoktur -
proje tarafından ele alındı.
**İade** :
**Veri ([] bayt)** : Bilgi baytları
**Kullanım** :
Uygulama durumu hakkında bilgi verir. Uygulama
özel c.
**Bağımsız değişkenler** :
**Anahtar (dize)** : Ayarlama anahtarı

---

**Sayfa 42**

**Değer (dize)** : Anahtar için ayarlanacak değer
**İade** :
**Günlük (dize)** : Hata ayıklama veya hata mesajı
**Kullanım** :
Uygulama seçeneklerini ayarlayın. Örneğin Anahtar = "mod", Değer = "mempool" için
bir mempool bağlantısı veya Anahtar = "mod", Değer = "fikir birliği" için
bir fikir birliği bağlantısı. Diğer seçenekler uygulamaya özeldir.
**Bağımsız değişkenler** :
**Doğrulayıcılar ([] Doğrulayıcı)** : İlk oluşum doğrulayıcıları
**Kullanım** :
Bir zamanlar doğuştan çağrıldı
**Bağımsız değişkenler** :
**Yükseklik (uint64)** : **Başlayan** blok yüksekliği
**Kullanım** :
Yeni bir bloğun başlangıcını işaret eder. Herhangi birinden önce aradı
AppendTxs.
**Bağımsız değişkenler** :
**Yükseklik (uint64)** : **Biten** blok yüksekliği
**İade** :

**Doğrulayıcılar ([] Doğrulayıcı)** : Doğrulayıcılar yenileriyle değiştirildi
oylama yetkileri (kaldırmak için 0)
**Kullanım** :
Bir bloğun sonunu işaret eder. Sonuçta her bir Commit'ten önce çağrılır
işlemler
Daha fazla ayrıntı için ABCI deposuna bakın.

---

**Sayfa 43**

Bir gönderenin bunu istemesinin birkaç nedeni vardır.
bir paketin alıcı zincir tarafından teslim edildiğinin kabulü.
Örneğin, gönderen sayfanın durumunu bilmiyor olabilir.
hatalı olması bekleniyorsa hedef zinciri. Veya gönderen
pakete bir zaman aşımı uygulamak istiyorum ( **MaxHeight ile**
paket alanı), herhangi bir hedef zincir bir reddinden muzdarip olabilir.
gelen sayısında ani bir artışla hizmet dışı saldırı
paketler.
Bu durumlarda, gönderen teslimat onayını isteyebilir
ilk paket durumunu **AckPending** olarak **ayarlayarak** . O zaman
dahil ederek teslimatı onaylamak için zincirin sorumluluğunu alan
Merkle hash uygulamasında **IBCPacket** kısaltılmış .
İlk olarak, bir **IBCBlockCommit** ve **IBCPacketTx** "Hub" da yayınlanır
Bu , " **Bölge1** " üzerinde bir **IBCPacket'in** varlığını kanıtlar . Şunu söyle
**IBCPacketTx** aşağıdaki değere sahiptir:
**FromChainID** : " **Bölge1** "
**FromBlockHeight** : 100 (söyle)
**Paket** : bir **IBCPacket** :

---

**Sayfa 44**

**Header** : bir **IBCPacketHeader** :
**SrcChainID** : " **Bölge1** "
**DstChainID** : "Bölge2"
**Sayı** : 200 (söyle)
**Durum** : **Kabul Ediliyor**
**Tür** : "madeni para"
**MaxHeight** : 350 ("Hub" şu anda 300 yüksekliğinde olduğunu söyleyin)
**Yük** : <"Madeni para" yükünün baytları>
Ardından, bir **IBCBlockCommit** ve **IBCPacketTx** "Zone2" de yayınlanır
Bu , "Merkez" üzerinde bir **IBCPacket'in** varlığını kanıtlar . Şunu söyle
**IBCPacketTx** aşağıdaki değere sahiptir:
**FromChainID** : "Merkez"
**FromBlockHeight** : 300
**Paket** : bir **IBCPacket** :
**Header** : bir **IBCPacketHeader** :
**SrcChainID** : " **Bölge1** "
**DstChainID** : "Bölge2"
**Numarası** : 200
**Durum** : **Kabul Ediliyor**
**Tür** : "madeni para"
**MaxHeight** : 350
**Yük** : <"Madeni para" yükünün aynı baytları>
Ardından, "Bölge2", uygulama karmasında kısaltılmış bir paket içermelidir
**AckSent'in** yeni durumunu gösterir . Bir **IBCBlockCommit** ve
**IBCPacketTx** , varlığını kanıtlayan "Hub" a geri gönderilir
"Zone2" üzerinde kısaltılmış bir **IBCPacket** . Söyle **IBCPacketTx**

aşağıdaki değere sahiptir:
**FromChainID** : "Bölge2"

---

**Sayfa 45**

**FromBlockHeight** : 400 (söyle)
**Paket** : bir **IBCPacket** :
**Header** : bir **IBCPacketHeader** :
**SrcChainID** : " **Bölge1** "
**DstChainID** : "Bölge2"
**Numarası** : 200
**Durum** : **AckSent**
**Tür** : "madeni para"
**MaxHeight** : 350
**PayloadHash** : <Aynı "bozuk para" yükünün karma baytları>
Son olarak, "Hub" paketin durumunu şuradan güncellemelidir:
**AckPending** için **AckReceived** . Bu yeni onaylanmış statünün kanıtı
"Bölge2" ye geri dönmelidir. **IBCPacketTx'in** aşağıdakilere sahip olduğunu **söyleyin**
değer:
**FromChainID** : "Merkez"
**FromBlockHeight** : 301
**Paket** : bir **IBCPacket** :
**Header** : bir **IBCPacketHeader** :
**SrcChainID** : " **Bölge1** "
**DstChainID** : "Bölge2"
**Numarası** : 200
**Durum** : **Kabul Edildi**
**Tür** : "madeni para"
**MaxHeight** : 350
**PayloadHash** : <Aynı "bozuk para" yükünün karma baytları>
Bu arada, "Bölge 1" iyimser bir şekilde teslimatın başarılı olduğunu varsayabilir
aksi kanıtlanmadıkça bir "bozuk para" paketinin
"Hub". Yukarıdaki örnekte, "Hub" bir **AckSent almamışsa**

---

**Sayfa 46**

350 bloğuna göre "Bölge2" den durumu, durumu ayarlayabilirdi
otomatik olarak **Zaman Aşımına** . Bir zaman aşımının bu kanıtı alabilir
"Bölge1" de geri gönderilir ve herhangi bir jeton iade edilebilir.
Bölgede desteklenen iki tür Merkle ağacı vardır.
Tendermint / Cosmos ekosistemi: Basit Ağaç ve IAVL +
Ağaç.
Basit Ağaç, statik bir öğe listesi için bir Merkle ağacıdır. Eğer
madde sayısı ikinin üssü değil, bazı yapraklarda olacak
farklı seviyeler. Basit Ağaç, ağacın her iki tarafını da
aynı yükseklik, ancak sol bir tane daha büyük olabilir. Bu Merkle ağacı
bir bloğun işlemlerini Merkle-ize ve üst düzey
uygulama durumu kökünün öğeleri.

---

**Sayfa 47**

IAVL + veri yapısının amacı, kalıcılık sağlamaktır.
uygulama durumundaki anahtar / değer çiftleri için depolama alanı
deterministik Merkle kök karması verimli bir şekilde hesaplanabilir.
ağaç, AVL algoritmasının bir varyantı kullanılarak dengelenir ve tümü
işlemler O (log (n)).
Bir AVL ağacında, herhangi bir düğümün iki alt ağacının yükseklikleri

en fazla bir farklılık gösterir. Bu koşul bir
güncelleme, ağaç O (log (n)) yeni düğümler oluşturarak yeniden dengelenir.
yaşlı ağacın değişmemiş düğümlerini göster. Orijinal AVL'de
algoritması, iç düğümler de anahtar-değer çiftlerini tutabilir. AVL +
algoritması (artıya dikkat edin) AVL algoritmasını tüm
anahtarları depolamak için yalnızca dal düğümlerini kullanırken yaprak düğümlerdeki değerler.
Bu, merkle hash izini korurken algoritmayı basitleştirir
kısa.
AVL + Ağacı, Ethereum'un Patricia denemelerine benzer . Var
değiş tokuş. Anahtarların yerleştirilmeden önce hashing uygulanmasına gerek yoktur.
IAVL + ağaçları, böylece bu, anahtarda daha hızlı sıralı yineleme sağlar
t bazı uygulamalardan yararlanabilecek alan. Mantık daha basittir
yalnızca iki tür düğüm gerektiren uygulama - iç düğümler ve
yaprak düğümleri. Merkle kanıtı ortalama olarak daha kısadır,

```
*
/ \
/ \
/
\
/
\
*
*
/ \
/ \
/ \
/ \
/ \
/ \
* * * h6
/ \ / \ / \
h0 h1 h2 h3 h4 h5
```

7 öğeli bir SimpleTree

---

**Sayfa 48**

dengeli ikili ağaç. Öte yandan, bir Merkle kökü
IAVL + ağacı, güncellemelerin sırasına bağlıdır.
Aşağıdakiler gibi ek verimli Merkle ağaçlarını destekleyeceğiz.
İkili değişken olduğunda Ethereum'un Patricia Trie'si
mevcut.
Kanonik uygulamada işlemler,
ABCI arayüzü aracılığıyla Cosmos hub uygulaması.
Cosmos Hub bir dizi birincil işlemi kabul eder
**SendTx** , **BondTx** , **UnbondTx** , **ReportHackTx** dahil **türler** ,
**SlashTx** , **BurnAtomTx** , **ProposalCreateTx** ve **ProposalVoteTx** ,
oldukça açıklayıcı olan ve bir
bu yazının gelecekteki revizyonu. Burada iki birincil
IBC için işlem türleri: **IBCBlockCommitTx** ve **IBCPacketTx** .
Bir **IBCBlockCommitTx** işlemi şunlardan oluşur:
**ChainID (string)** : **Blok** zincirinin kimliği
**BlockHash ([] bayt)** : Blok hash baytları, Merkle kökü
uygulama karmasını içeren
**BlockPartsHeader (PartSetHeader)** : Blok parça seti başlığı
bayt, yalnızca oylama imzalarını doğrulamak için gerekli
**BlockHeight (int)** : **İşlemenin** yüksekliği

**BlockRound (int)** : **İşlemin** turu
**Taahhüt ([] Oy)** :> ⅔ **Tendermint Precommit** oyu
bir blok kaydetme içerir
**DoğrulayıcılarHash ([] bayt)** : Yeninin Merkle-ağaç kök karması
doğrulayıcı seti

---

**Sayfa 49**

**DoğrulayıcılarHashProof (SimpleProof)** : A SimpleTree Merkle-
**ValidatorsHash'i BlockHash'e** karşı kanıtlamak için kanıt
**AppHash ([] bayt)** : Bir IAVLTree Merkle-ağaç kök karması
uygulama durumu
**AppHashProof (SimpleProof)** : Bir SimpleTree Merkle geçirmez
kanıtlayan **AppHash** karşı **BlockHash**
Bir **IBCPacket** şunlardan oluşur:
**Header (IBCPacketHeader)** : Paket başlığı
**Yük ([] bayt)** : Paket yükünün baytları. *İsteğe bağlı*
**PayloadHash ([] bayt)** : Paketin baytları için hash.
*İsteğe bağlı*
Ya bir **yükü** veya **PayloadHash** mevcut olması gerekir. Karma
Bir ait **IBCPacket** iki öğe, basit bir Merkle kökü **Başlık**
ve **Yük** . Tam **yüksüz** bir **IBCPacket'e**
*kısaltılmış paket* .
Bir **IBCPacketHeader** şunlardan oluşur:
**SrcChainID (string)** : Kaynak blok zinciri kimliği
**DstChainID (string)** : Hedef blok zinciri kimliği
**Sayı (int)** : Tüm paketler için benzersiz bir sayı
**Durum (enum)** : **AckPending** , **AckSent olabilir** ,
**AckReceived** , **NoAck** veya **Timeout**
**Tür (dize)** : Türler uygulamaya bağlıdır. Evren
"bozuk para" paket tipini rezerve eder
**MaxHeight (int)** : Durum **NoAckWanted** veya **AckReceived değilse**
bu yüksekliğe kadar durum **Zaman Aşımı** olur . *İsteğe bağlı*
Bir **IBCPacketTx** işlemi şunlardan oluşur:

---

**Sayfa 50**

**FromChainID (string)** : **Blockchain** kimliği olan
bu paketi sağlamak; mutlaka kaynak değil
**FromBlockHeight (int)** :
Aşağıdaki paket, blok karmasına dahil edilir (Merkle uyumlu)
kaynak zinciri
**Paket (IBCPacket)** : Durumu bir olabilen bir veri paketi
arasında **AckPending** , **AckSent** , **AckReceived** , **Noack** veya **Zaman Aşımı**
**PacketProof (IAVLProof)** : Kanıtlamak için bir IAVLTree Merkle geçirmez
paketin karması , kaynak zincirinin **AppHash'ına** karşı
verilen yükseklik
"Bölge1" den "Bölge2" ye bir paket gönderme sırası
"Hub" aracılığıyla {Şekil X} 'de gösterilmektedir. İlk olarak, bir **IBCPacketTx**
"Hub" a paketin uygulama durumuna dahil olduğunu kanıtlar
"1. Bölge". Ardından, başka bir **IBCPacketTx** , "Zone2" ye
paket, "Hub" ın uygulama durumuna dahildir. Bu sırada
prosedür, **IBCPacket** elds aynıdır: **SrcChainID** olan
her zaman "Bölge1" ve **DstChainID** her zaman "Bölge2" dir.
**PacketProof** gibi doğru Merkle geçirmez yolunu olmalıdır
aşağıdaki gibidir:

"Bölge1", "Hub" aracılığıyla "Bölge2" ye bir paket göndermek istediğinde,
**IBCPacket** veri paketi Merkle- olup özdeş
"Zone1", "Hub" veya "Zone2" olarak belirlenmiştir. Değişebilir tek alan
Teslimatı izleme **durumu** .
Kavramsallaştırmadaki yardımları için arkadaşlarımıza ve meslektaşlarımıza teşekkür ederiz,
Tendermint ile çalışmamızı incelemek ve destek sağlamak
ve Cosmos.
IBC / <SrcChainID> / <DstChainID> / <Number>

---

**Sayfa 51**

SkuChain'den Zaki Manian , biçimlendirme ve
ifadeler, özellikle ABCI bölümü altında
Althea'dan Jehan Tremback ve yardım için Dustin Byington
ilk yinelemeler
Andrew Miller ve Bal Badger uzlaşma konusunda geri bildirim
Fikir birliği ve ifadeler hakkında geri bildirim için Greg Slepak
Ayrıca Bill Gleim ve Seunghwan Han'a çeşitli
katkılar.
**Katkılarınız için adınız ve kuruluşunuz burada**
1 Bitcoin: https://bitcoin.org/bitcoin.pdf
2 ZeroCash: http://zerocash-project.org/paper
3 Ethereum: https://github.com/ethereum/wiki/wiki/White-
Kağıt
4 TheDAO:
https://download.slock.it/public/DAO/WhitePaper.pdf
5 Ayrı Tanık:
https://github.com/bitcoin/bips/blob/master/bip-
0141.mediawiki
6 BitcoinNG: https://arxiv.org/pdf/1510.02037v2.pdf
7 Yıldırım Ağı: https://lightning.network/lightning-
network-paper-DRAFT-0.5.pdf
8 Tendermint:
https://github.com/tendermint/tendermint/wiki
9 FLP İmkansızlığı:
https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf
10 Slasher: https://blog.ethereum.org/2014/01/15/slasher-a-
cezalandırıcı-teminat-kanıtı-algoritması /
11 PBFT: http://pmg.csail.mit.edu/papers/osdi99.pdf
12 BitShares: https://bitshares.org/technology/delegated-
kanıtı-fikir birliği /

---

**Sayfa 52**

13 Yıldız: https://www.stellar.org/papers/stellar-consensus-
protocol.pdf
14 Interledger: https://interledger.org/rfcs/0001-interledger-
mimari/
15 Yan Zincirler: https://blockstream.com/sidechains.pdf
16 Casper:
https://blog.ethereum.org/2015/08/01/introducing-casper-
arkadaş canlısı hayalet /
17 ABCI: https://github.com/tendermint/abci
18 Ethereum Parçalama:
https://github.com/ethereum/EIPs/issues/53
19 LibSwift:

http://www.ds.ewi.tudelft.nl/ leadmin / pds / paper / Performa
nceAnalysisOfLibswift.pdf
20 DLS:
http://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf
21 İnce İstemci Güvenliği:
https://en.bitcoin.it/wiki/Thin_Client_Security
22 Ethereum 2.0 Leylak Kağıdı:
http://vitalik.ca/ les / mauve_paper.html
https://www.docdroid.net/ec7xGzs/314477721-ethereum-
özel için platform inceleme fırsatları ve zorluklar
and-consortium-blockchains.pdf.html

---