Sayfa 1

1
Dr. Leemon Baird, Mance Harmon ve Paul Madsen
İnternetin güven katmanı
Hedera: Herkese Açık Bir Hashgraph
Ağ ve Yönetim Konseyi
WHITEPAPER V.2.0 SON GÜNCELLEME 29 AĞUSTOS 2019 DAHA FAZLA GÖZDEN GEÇİRME VE GÜNCELLEME KONUSU

Sayfa 2

2
BEYAZ KAĞIT
Vizyon
Herkes için güvenilir, güvenli ve güçlendirilmiş bir dijital gelecek inşa etmek.
Misyon
Kendimizi güvenilir ve güvenli bir çevrimiçi dünya oluşturmaya adadık
bu sizi güçlendirir.
Çalışabileceğiniz, oynayabileceğiniz, satın alabileceğiniz, satabileceğiniz, yaratabileceğiniz ve sosyal olarak etkileşim kurabileceğiniz yer.
Dijital topluluklarınızda güvenliğiniz ve mahremiyetinizin olduğu yerler.
Başkalarıyla etkileşim kurarken kendinizden emin olduğunuz yer.
Bu dijital geleceğin herkese açık olduğu yer.
Merhaba gelecek.

---

3. Sayfa

3
YÖNETİCİ ÖZETİ
Yönetici Özeti
Dağıtılmış defter teknolojileri (DLT), mevcut pazarları bozma ve dönüştürme potansiyeline sahiptir.
birden çok endüstri. Ancak bize göre daha önce aşılması gereken beş temel engel var.
dağıtılmış defterler, işletmeler tarafından geniş çapta kabul edilebilir ve benimsenebilir. Bu yazıda inceleyeceğiz
bu engeller ve Hedera Hashgraph'ın neden geniş bir uygulama yelpazesini desteklemek için uygun olduğunu tartışın
ve dünyanın ilk kitlesel olarak benimsenen halka açık defteridir.
1.
PERFORMANS - DLT için en zorlayıcı kullanım durumları yüz binlerce gerektirir
saniyede işlem sayısı ve çoğu saniye cinsinden ölçülen fikir birliği gecikmesi gerektirir.
Bu performans ölçütleri, mevcut kamu DLT'sinin ötesinde büyüklükteki siparişlerdir.
platformlar başarabilir.
2.
GÜVENLİK - Herkese açık DLT platformları trilyonlarca dolar transferini kolaylaştıracaksa
bilgisayar korsanları tarafından hedef alınacaklar ve bu nedenle mümkün olan en güçlü ağa ihtiyaçları olacak
güvenlik. Mümkün olan en güçlü güvenliğe sahip olmak, fikir birliği algoritmasıyla başlar
kendisi, resmi olarak matematiksel olarak kanıtlanmış güvenlik özellikleri ile. Güvenlik açıkları
ve saldırı vektörleri hafifletilmemelidir; tamamen ortadan kaldırılmalıdır. Geliştirmek
performans ölçütleri, bazı genel DLT platformları,
ademi merkeziyetçilik ve bunu yaparken potansiyel olarak güvenliği tehlikeye atıyor.
3.
YÖNETİŞİM - Genel amaçlı bir kamu defteri, temsilciler tarafından yönetilmelidir
her biri birinci sınıf uzmanlığa sahip geniş bir pazar ve coğrafi sektör yelpazesinden.
Ağ yönetişiminden sorumlu olanlar teknik uzmanlığa ihtiyaç duyarlar, böylece

platformun temelindeki yazılımı yetkin bir şekilde yönetin. İşe ihtiyaçları var ve
kuruluşun iş operasyonlarını yönetebilmeleri için ekonomi uzmanlığı ve
kripto para birimi. Değişen düzenleyici süreçte gezinmeye yardımcı olmak için yasal uzmanlığa ihtiyaçları var
çevre. Başka bir deyişle, ağ, merkezi olmayan bir grup tarafından yönetilmelidir.
dünyadaki her pazarı temsil eden, küresel olarak tanınan endüstri liderleri.

4.

KARARLILIK - Kararları uygulamak için teknik ve yasal mekanizmalar olmadan
yönetim organı, kamu DLT platformları kaosa dönüşme riski altındadır. Güçlü güvenlik ve
olgun yönetişim, gerekli güveni sağlayan istikrarlı bir platform sağlayacaktır
ve üzerinde ticari veya hassas uygulamalar geliştirenler arasında güven.

5.

MEVZUATA UYGUNLUK - Hükümetlerin,
halka açık defterleri ve ilişkili defterleri kullanan kullanıcılara, kuruluşlara ve geliştiricilere yönelik politika hedefleri
kripto para birimleri ve belirteçler. Herkese açık olarak dağıtılmış bir defterin yetkin olması gerektiğini düşünüyoruz
ekosisteminin tüm üyelerinin yürürlükteki yasalara uyması için gerekli araçları sağlamak
ve Avrupa Birliği'nin Genel Veri Gizliliği Yönetmelikleri (GDPR) gibi düzenlemeler ve
Yaptırım taraması yürütmek ve Bilin'i kolaylaştırmak için uygun kimlik yönetimini etkinleştirin
Müşteriniz (KYC) ve Kara Para Aklamayı Önleme (AML) kontrolleri.

---

4. sayfa

4

YÖNETİCİ ÖZETİ

DLT endüstrisini ileriye taşımak ve etkinleştirmek için gerekenler
tam potansiyelinin farkına varmak için mi?
Yüksek performansın birleşimini sağlayan bir platform,
güçlü güvenlik, etkili yönetişim, teknik ve yasal
platformun kararlılığını sağlamak için kontroller ve etkinleştirilecek araçlar
mevzuata uygunluk. Ancak o zaman ana akım olduğunu düşünüyoruz
pazarlar, onu benimsemek için yeterince DLT platformuna güvenecek.

5.Sayfa

5

HEDERA HASHGRAPH KONSEYİ

Hedera ile tanışın - herkese açık bir hashgraph ağı
ve ihtiyaçları karşılamak için tasarlanmış yönetim organı
ana akım pazarların.

Hedera ağı, birden fazla endüstride ve çeşitli sektörlerde önde gelen küresel işletmelerden oluşan bir konsey tarafından yönetilecektir.
coğrafyalar. Vizyonu, merkezi partilere ihtiyaç duymadan, güvenilir ve emniyetli bir siber uzaydır.
aşırı etkiye sahip. Lisanslama ve yönetişim modeli, çatallaşma riskini ortadan kaldırarak kullanıcıları korur,
kod tabanının bütünlüğünü korumak ve temeldeki yazılım kodunu incelemek için açık erişim sağlamak.
Platform yönetişimi, bir vadesi olacak olan Hedera Yönetim Konseyi aracılığıyla dağıtılacaktır.
sınırlı, dönüşümlü yönetim üyeleri kümesi, her biri aşağıdakilerle ilgili temel kararlar üzerinde eşit oy hakkına sahiptir:
platform. 1
Hedera ağı, benimsenmesini kısıtlayan faktörleri çözen dağıtılmış bir defter platformudur.
genel kullanıma açık DLT.

1.

PERFORMANS - Platform, karma grafik dağıtılmış fikir birliği algoritması üzerine kurulmuştur,

Dr. Leemon Baird tarafından icat edildi. Karma grafik fikir birliği algoritması mükemmele yakın sağlar
bant genişliği kullanımında verimlilik ve sonuç olarak yüz binlerce
tek bir parçada saniye başına işlem (tam olarak bağlı, eşler arası bir düğüm ağında)
ağ). Başlangıçta, Hedera ağının 10.000 işleyebileceğini tahmin ediyoruz.
saniyede kripto para birimi işlemleri. Mutabakat gecikmesi saniye cinsinden ölçülür,
dakika, saat veya gün.

2.

GÜVENLİK - Hashgraph, dağıtılmış güvenlik alanında altın standardına ulaşır
fikir birliği: asenkron Bizans Hata Toleransı (aBFT). Kullanan diğer platformlar
Koordinatörler, liderler veya performansı iyileştirmeye yönelik iletişim zaman aşımları genellikle
Dağıtılmış Hizmet Reddi (DDoS) saldırılarına karşı savunmasız. Hashgraph bunlara karşı dayanıklıdır
fikir birliği algoritmasına karşı saldırı türleri çünkü böyle bir lider yok. Başarmak
Bu ölçekte güvenlik seviyesi, dağıtılmış sistemler alanında temel bir ilerlemedir.
Birçok uygulama, işlemlerin mutabakat sırasının gerçek sırayla eşleşmesini gerektirir.
işlemlerin ağ tarafından alındığı. Tek bir parti için mümkün olmamalı
ağa işlem akışını önlemek veya işlemlerin sırasını etkilemek için
nihai ağ konsensüsü. Adil bir fikir birliği algoritması, bir kullanıcının gönderebilmesini sağlar
ağa yapılan bir işlem varsa, işlem ağ tarafından alınacak ve
alındığı sıra adil bir sipariş olacaktır. Hashgraph, benzersiz bir şekilde
ağ tarafından alınan fiili sipariş işlemleri mutabakat sırasına yansıtılacaktır.
Başka bir deyişle, hashgraph hem Adil Erişim hem de Adil Sipariş sağlar.
Karma grafik konsensüs algoritması için aBFT'nin ve adalet özelliklerinin resmi kanıtları,
Haziran 2016'dan beri halka açık incelemeye sunulmuştur. Ayrıca, hashgraph algoritması
Bir matematik kanıtı tarafından ABFT olarak valide Ekim 2018 yılında Coq sistemi kullanılarak
bilgisayar tarafından kontrol 2

3.

YÖNETİŞİM - Hedera ağı, en fazla 39 liderden oluşan bir konsey tarafından yönetilecektir.
küresel işletmeler. Hedera Konseyi üyeleri süreçte gerekli deneyimi getirecek ve
önceki halka açık defter platformlarında bulunmayan iş uzmanlığı. Konsey
üyelik, (i) bir dizi endüstriyi ve coğrafyayı yansıtacak şekilde, (ii) sahip olmak üzere tasarlanmıştır.
son derece saygın markalar ve güvenilir pazar konumları ve (iii) rekabeti kapsamak için
perspektifler.
Yönetişim şartları, tek bir Konsey üyesinin denetime sahip olmamasını sağlar ve
hiçbir küçük üye grubu, bir bütün olarak vücut üzerinde aşırı etkiye sahip olmayacaktır.

4.

KARARLILIK - Hedera, istikrarı sağlamak için hem teknik hem de yasal kontrollere güvenir
platformun.
Hedera teknik kontroller iki yeteneği etkinleştirir.
ben)
İlk olarak, hashgraph teknolojisi, yazılım istemcilerinin
Hedera hashgraph defterinin soyağacı, bir
paylaşılan durum mekanizması. Bir ağ düğümünün
Hedera hashgraph platformunun resmi sürümü, değişiklikler yapın ve ardından
bu değişikliklerin geçerli olarak kabul edilmesini sağlayın. Orijinal hashgraph platformu
ve kopya bağımsız olarak değiştirilir, yazılım istemcileri Hedera'yı
platform hangisinin geçerli ve hangisinin olmadığını bilecektir.
ii)
İkincisi, hashgraph teknolojisi Hedera için bunu mümkün kılar
Ağ düğümlerinde yapılacak yazılım değişikliklerini belirleme konseyi,
tam olarak bu değişikliklerin ne zaman kabul edileceğini ve bunların

kabul edilmiştir. Hedera Konseyi bir yazılım güncellemesi yayınladığında,
ağ düğümlerinin yazılımı tam olarak otomatik olarak güncellenir.
aynı an. Geçersiz yazılıma sahip herhangi bir düğüm (yani, yüklenmemiş olan
yazılım güncellemesi) artık defteri değiştiremez veya
dünya, defterin versiyonunu meşru olarak kabul ediyor.
Hedera yasal kontrolleri, platformun rakip bir platforma geçmemesini sağlar ve
kripto para.
iii)
Hedera kod tabanı, Hedera Yönetim Konseyi tarafından yönetilecektir ve
Yayımlanması beklenen Sürüm 1.0 ile genel inceleme için yayınlanacaktır.
2020. Açık kaynak olmayacak ancak kaynak kodunu herkes okuyabilecek,
yeniden derleyin ve doğru olduğunu doğrulayın. Kullanmak için herhangi bir lisans gerekmeyecektir.
Hedera platformu. Kullanan yazılımı yazmak için herhangi bir lisans gerekmeyecektir.
Hedera platformunun hizmetleri. Akıllı oluşturmak için herhangi bir lisans gerekmeyecek
Hedera platformunun üstünde sözleşmeler. Hedera üzerine inşa edilen uygulamalar
platform açık kaynak veya tescilli olabilir. Herhangi bir lisans gerektirmezler
veya Hedera'dan herhangi bir onay. Hedera, kodu herkese açık hale getirecek
karma grafik kullanarak kararlılık sağlarken, onu gözden geçirecek (Sürüm 1.0'da)
Yazılım, çatalları önlemek için savunma amaçlı patentler. Bu şekilde Hedera sağlayacaktır
piyasaların talep ettiği istikrarı sağlayacak şeffaf bir kod tabanı

---

7. Sayfa

halka açık bir defterin genel kabulü için.
Teknik ve yasal kontrollerin kombinasyonu, yönetim organına ihtiyaç duyulan mekanizmaları sağlar.
anlamlı yönetişimi mümkün kılmak ve geniş tabanlı sistemler için gerekli olduğunu düşündüğümüz
istikrarı sağlamak
Benimseme.
5.
MEVZUATA UYGUNLUK - Hedera teknik çerçevesi kontrollü
ağ durumunun değişkenliği ve ek veri talep etme veya ekleme potansiyeli
kimlik sertifikaları gibi işlemler. Bu özellikler gelecekteki işlevselliği etkinleştirir
kişisel verilerin ve diğer yüklenen dosyaların silinmesi ve onaylanmış kimliğin dahil edilmesi gibi
mekanizmalar - tümü isteğe bağlı ve son kullanıcıların kontrolü dahilinde. İle çalışmak niyetindeyiz
düzenleyiciler ve işletmelerin kendi kurallarını yerine getirmesine izin verecek bu tür araçların
geliştirilmesini teşvik eder.
tüketicinin korunması ve yasal uyumluluk yükümlülükleri.
1 Swirlds, Inc., karma grafik konsensüs algoritmasının patent başlıklarını elinde tutan bir Delaware
şirketidir. Swirlds kalıcıdır
Hedera Yönetim Konseyi üyesi.
2 aBFT'nin ispatları dahil olmak üzere karma grafik algoritmasının tam tanımı için Ek 3'e
bakın. Ayrıca bkz. Https://www.hedera.com/blog/coq-
kanıtı-tamamlandı-carnegie-mellon-profesör-onaylar-karma-fikir birliği-algoritması-asenkron-bizans-
hataya dayanıklıdır
resmileştirilmiş aBFT kanıtına erişim için.

---

8. Sayfa

Sayfa 9

9
GİRİŞ
Karma grafik veri yapısı ve fikir birliği algoritması,
dağıtılmış fikir birliği için yeni platform. Bu giriş, bir
karma grafiğin nasıl çalıştığına ve bazı özelliklerine genel bakış.
Dağıtılmış bir fikir birliği algoritmasının amacı, bir topluluğun
bazı kullanıcıların sırasına göre bir anlaşmaya varacak
Kullanıcılar, tek bir üyeye güvenilmediğinde işlem üretti
Herkes tarafından. Bu şekilde, güven oluşturmak için bir sistemdir.
bireyler zaten birbirlerine güvenmiyor. Hashgraph bunu başarır
temelde yeni bir yol.
Blok zinciri, büyüdükçe sürekli budanan bir ağaç gibidir - bu budama
blokların dallarının kontrolden çıkmasını engellemek ve
defterin yalnızca bir blok zincirinden oluştuğundan emin olun. Karma grafikte
yeni büyümeyi budamayla, bu tür bir büyüme defterin gövdesine geri dokunur.

Sayfa 10

10
GİRİŞ
Hem blockchain hem de hashgraph defterlerinde, herhangi bir kullanıcı bir
sonunda bir konteynere ("blok") konulacak olan işlem
ve daha sonra dağıtılmış ağa yayılacaktır.
Blok zincirinde, kapların bu "bloklarının" bir
tek, uzun zincir. Aynı anda iki blok oluşturulursa,
ağ düğümleri sonunda devam etmek ve atmak için bir zincir seçecektir
diğeri, blok zinciri "çatalı" nın iki farklı zincire bölünmesidir. Bu
Dallarından biri hariç hepsine sahip olan büyüyen bir ağaç gibi
kesildi.
Hashgraph'da, her işlem konteyneri,
defter - hiçbiri atılmaz - bu nedenle blok zincirlerinden daha verimlidir.
Tüm dallar sonsuza kadar var olmaya devam eder ve birlikte örülür.
tek bir bütün.
Dahası, yeni konteynerler çok hızlı gelirse blockchain başarısız olur,
çünkü yeni dallar budanabileceklerinden daha hızlı filizlenir. Bu
blok zincirinin çalışma kanıtı veya başka bir mekanizmaya ihtiyaç duymasının nedeni budur
büyümeyi yapay olarak yavaşlatmak için. Hashgraph olarak, hiçbir şey
atıldı. Hashgraph veri yapısında herhangi bir zarar yoktur
hızla büyüyor. Her üye işlem oluşturabilir ve
istedikleri zaman konteynerler.
Son olarak, hashgraph, olasılığın budanmasını gerektirmediğinden
"Çatallar" (her işlem konteyneri,
defter), hashgraph daha güçlü matematiksel garantiler sağlar,
Bizans anlaşması ve adalet gibi. Dağıtılmış veritabanları
Paxos gibi Bizanslılar, ancak ülkedeki adaleti garanti etmiyorlar.
işlemlerin sıralanması. Blockchain ne Bizans ne de adildir.
hashgraph algoritması *adil, hızlı, Bizans, ACID* olmayı başarır
uyumlu, verimli, ucuz, zaman damgalı ve DoS dirençli.

Sayfa 11

11
VERİM
Verim
MALİYET

Bir hashgraph dağıtılmış defterinin çalıştırılması, blockchain dağıtılmış defterlere kıyasla daha ucuzdur.
enerji yoğun çalışma kanıtından kaçınır. Hashgraph düğümlerini çalıştırmak isteyen kişiler ve kuruluşlar
pahalı özel maden ocakları satın almanıza gerek kalmayacaktır. Bunun yerine, hashgraph düğümlerini çalıştırabilecekler
bu tür özel madencilik teçhizatlarından daha ucuz olan hazır donanım aracılığıyla.

VERİMLİLİK

Hashgraph, blockchain topluluğunda kullanıldığı için% 100 etkilidir. Blok zincirinde iş
bazen daha sonra bayat olarak kabul edilen ve düğüm ağı tarafından atılan bir blok madenciliği israf edilir.
Karma grafikte, bir işlem "bloğunun" eşdeğeri asla eskimez. Hashgraph ayrıca verimlidir
bant genişliği kullanımında. Verilen tüm düğümleri bilgilendirmek için gereken bant genişliği miktarı ne olursa olsun
işlem (bu işlem için bir zaman damgası üzerinde fikir birliğine varılmasa bile), hashgraph ekliyor
mutabakat zaman damgası elde etmek için çok küçük bir ek bant genişliği ek yükü ve
sırayla işlemler. Ek olarak, karma grafik oylama algoritması herhangi bir ek
düğümlerin işlemlerin onaylanmasına (veya sayılacak oylar) oy vermesi için mesajlar gönderilecektir.
ağ düğümlerinin işlemin kendisinden öğrendiği mesajların ötesinde.

THROUGHPUT

Hashgraph *hızlıdır* . Yalnızca bant genişliği ile sınırlıdır. Her ağ düğümü, aşağıdakileri yapmak için yeterli bant genişliğine sahipse
saniyede belirli sayıda işlemi indirip yükleyin, ağ bir bütün olarak kapatabilir
saniyede bu kadar çok işlem. Hızlı bir ev internet bağlantısı bile bir hashgraph'ı etkinleştirebilir
düğüm, tüm küresel VISA kart ağına eşit işlem hacmini işleyecek kadar hızlı olacak.

Sayfa 12

12

VERİM

AŞAĞIDAKİ ŞEMALAR HASHGRAPH TEKNOLOJİSİ İÇİN PERFORMANS SONUÇLARI VERİYOR
TEST KOŞULLARI ALTINDA.

Önceki sayfalardaki grafikler, barındırılan hashgraph düğümleri kullanılarak gerçekleştirilen testlerin sonuçlarını gösterir.
Amazon AWS m4.4xlarge bulut sunucuları tarafından. Şekil 1, tek bir bölge (Virginia) için performansı göstermektedir, Şekil
2, kıta Amerika Birleşik Devletleri'nin zıt taraflarında 2,000 mil aralıklı iki bölge için sonuçları gösterir.
(Virginia ve Oregon) ve Şekil 3, 8 bölgeye (Virginia, Oregon, Kanada, Sao Paulo,
Avustralya, Seul, Tokyo ve Frankfurt).
Grafikteki her satır, sağında gösterilen farklı sayıda örnek (bilgisayarlar) içindir.
çizgi. Her durumda, örnekler kullanılan bölge sayısına eşit olarak dağıtıldı.
Yatay eksen, defterin elde ettiği saniyede 100 baytlık işlem sayısıdır
uzlaşma. Bu deneylerde, bu işlem hacmi 50.000 tps'nin altından neredeyse 500.000'e kadar değişmektedir.
tps. Çizgilerin çoğunda soldan ikinci nokta 10.000 tps'dir.
Dikey eksen, bir düğümün ilk kez bir işlem oluşturduğu andan başlayana kadar geçen ortalama saniye sayısıdır.
kesin fikir birliği sırasını ve bunun için fikir birliği zaman damgasını bilir. Bu sadece bir ilke varmanın zamanı değil
onay -% 100 kesinliğe ulaşılana kadar geçen süredir.
Tüm deneylerde bu gecikme 11 saniyenin altındaydı. Çeşitli deneylerde gecikme süreleri vardı.
0,04 saniyeden az.
Grafiklerde, aktarım hızı, gecikme süresi, bilgisayar sayısı ve
coğrafi dağılım. Saniyede 50.000 işlemle çalışan 32 bilgisayar için, mutabakat kesinliği

Ağ, tüm dünyaya yayılmış 8 bölgeye yayıldığında 3 saniyede ulaşılır. Ne zaman
ağ ABD genelinde yalnızca 2.000 mil uzanıyor, bu 1,5 saniyeye düşüyor
0.75 saniye.
Gecikmeyi kredi kartlarının gerektirdiği 7 saniyenin altında tutmak isteniyorsa
Saniyede 200.000 işlem, sekiz bölgede 32 bilgisayar kullanmak veya 64 bilgisayar kullanmak
mümkündür
iki bölgede veya bir bölgede 128 bilgisayar kullanın.
Bu testlerin yalnızca işlem sırası üzerinde fikir birliğine varmak için olduğuna dikkat etmek önemlidir.
zaman damgaları. İşlemleri işleme süresini içermezler. Örneğin, her işlem
dijital olarak imzalandığında, bu sonuçlar, büyük bir işlem gücüne ihtiyaç duyulabileceğini
göstermektedir.
Saniyede yüz binlerce dijital imzayı doğrulayın. GPU uygulamalarının
yardımcı olabilir.
Ek olarak, bir işlem büyük bir dosyayı saklama isteği ise, bant genişliği sınırlamaları yavaşlayacaktır.
ağın bu işlemi işleme yeteneği. Dosya depolama işlemleri için ağ fiyatlandırması
büyük dosyaların kayıt defterinde saklanmasını nispeten pahalı hale getirecek şekilde
yapılandırılmıştır, bu da herhangi bir
ağı bu şekilde yavaşlatma çabaları.

Sayfa 13

0.01
0.1
1
10
100
0
500.000
400.000
300.000
200.000
100.000
50.000
150.000
250.000
350.000
450.000
64 bilgisayar
32 bilgisayar
16 bilgisayar
8 bilgisayar
4 bilgisayar
2 bilgisayar
128 bilgisayar
400.000 tps
Şekil 1
Hashgraph Gecikmesi ve Aktarım Hızı
1 bölge, m4.4xlarge
L
a
te
n
c
y
(s
e

c
Ö
nd
s)
Aktarım hızı (saniyede 100 bayt işlem)
13
VERİM

Sayfa 14

0.01
0.1
1
10
100
0
500.000
400.000
300.000
200.000
100.000
50.000
150.000
250.000
350.000
450.000
şekil 2
Hashgraph Gecikmesi ve Aktarım Hızı
2 bölge, m4.4xlarge
L
a
te
n
c
y
(s
e
c
Ö
nd
s)
Aktarım hızı (saniyede 100 bayt işlem)
64 bilgisayar
32 bilgisayar
16 bilgisayar
8 bilgisayar
4 bilgisayar
128 bilgisayar
14
VERİM

Sayfa 15

0.01
0.1
1

10
100
0
500.000
400.000
300.000
200.000
100.000
50.000
150.000
250.000
350.000
450.000
Figür 3
Hashgraph Gecikmesi ve Aktarım Hızı
8 bölge, m4.4xlarge
Aktarım hızı (saniyede 100 bayt işlem)
L
a
te
n
c
y
(s
e
c
Ö
nd
s)
64 bilgisayar
32 bilgisayar
16 bilgisayar
8 bilgisayar
15
VERİM

Sayfa 16

1 6
DEVLET VERİMLİLİĞİ
Bir ağ işlemi gerçekleştiğinde, saniyeler içinde ağdaki tüm düğümler bu işlemin nerede olduğunu bilecektir.
% 100 kesinlikle işlem geçmişine yerleştirilmelidir. Daha da önemlisi, her düğüm
diğer her düğümün bunu bildiğini bilin. Bu noktada ağ, yalnızca
işlem ve, gelecekteki denetim veya uyum için gerekmedikçe, işlem verilerini atın. Yani, asgari düzeyde
kripto para sistemi, her düğümün yalnızca her ağ hesabının mevcut bakiyesini depolaması gerekir
bu boş değil. Düğümlerin, sonuçlanan işlemlerin tam geçmişini hatırlaması gerekmez.
bu dengeler "oluşum" a kadar uzanır.
VERİM

Sayfa 17

17
GÜVENLİK
Güvenlik

KRİPTOGRAFİ
Tüm Hedera ağ iletişimleri TLS 1.2 ile şifrelenir, tüm işlemler dijital olarak imzalanır ve
karma grafik, kriptografik karmalar kullanılarak oluşturulur. Tüm algoritmalar ve anahtar boyutları seçildi
CNSA Suite güvenlik standardıyla uyumlu olmak. Bu, ABD'yi korumak için gerekli standarttır
hükümet Çok Gizli bilgiler. AES-256, RSA 3072, SHA-384 ve ECDSA kullanımını belirtir ve
Mükemmel ileri gizlilik için geçici anahtarlarla birlikte p-384 ile ECDH.
ASENKRON BİZANS HATA TOLERANSI
Karma algoritma asenkron Bizans Hata Toleranslı (aBFT). Bu teknik bir terim anlamı
hiçbir tek düğümün (veya küçük düğüm grubunun) ağın fikir birliğine varmasını engelleyemeyeceği ve
bir kez ulaşıldığında fikir birliğini değiştirin. Her Hedera ağ düğümü sonunda bir noktaya ulaşacaktır.
ağın fikir birliğine vardığından emin "bilir". Blockchain platformlarının garantisi yoktur
Bizans anlaşması, çünkü bir düğüm hiçbir zaman anlaşmaya varıldığına dair kesinliğe ulaşmaz. Daha doğrusu
sadece zamanla artan bir olasılık vardır. Blok zinciri de Bizans dışıdır çünkü öyle değildir.
ağ bölümleriyle otomatik olarak ilgilenir - yani, bir grup madenci internetin geri kalanından izole edilmişse,
birden çok zincir ("çatal"), işlemlerin sırasına göre birbirleriyle bu çatışmayı büyütebilir.
"Bizans Arıza Toleranslı" (BFT) teriminin bazen daha zayıf bir anlamda kullanıldığını belirtmek gerekir.
diğer fikir birliği algoritmaları tarafından kötü niyetli davranışa karşı direnç. Onu orijinal haliyle, daha güçlü anlamıyla kullanıyoruz.
(1) bazı saldırganların fikir birliğini durdurmak veya tersine çevirmek için işbirliği yapacağını ve (2) bazı saldırganların
hatta internetin kendisini kontrol edin (bazı sınırlamalarla) ve mesajların teslimini yavaşlatın veya engelleyin, ağ
sonunda fikir birliğine varacak ve her düğüm sonunda fikir birliğine varıldığını bilecek. Hashgraph
Bizans, bu daha güçlü tanımla bile. Saldırganlar, toplam hbar hissesinin 1 / 3'ünden daha azına sahip olduğu sürece,
mutabakatı durduramazlar ve hatta işlem zaman damgalarını veya mutabakat sırasını çarpıtamazlar.
Ağ ve iletim hakkında yapılan varsayımlara bağlı olarak farklı BFT dereceleri vardır.
mesajların.
BFT'nin en güçlü biçimi, eşzamansız BFT'dir - yani ağ,
Kötü niyetli kişiler ağı kontrol edebilir ve kendi seçtikleri mesajları silebilir veya yavaşlatabilirlerse.
sadece varsayımlar, 2 / 3'ten fazlasının protokolü doğru bir şekilde izlediği ve mesajların
İnternet üzerinden bir düğümden diğerine tekrar tekrar gönderilirse, sonunda biri geçecek ve en sonunda
başka bir irade vb. Bazı sistemler kısmen eşzamansızdır ve yalnızca saldırganlar bunu yaparsa güvenlidir.
çok fazla güce sahip değildir ve mesajların zamanlamasını çok fazla değiştirmeyin. Örneğin, kısmen
asenkron sistem, mesajların geçtiği varsayımı altında Bizans'ı kanıtlayabilir.
on saniyede internet. Bununla birlikte, bu varsayım botnetlerin, Dağıtılmış Hizmet Reddi gerçeğini göz ardı etmektedir.
saldırılar ve kötü niyetli güvenlik duvarları.
Matematiksel kanıtlar dahil, karma grafik veri yapısını ve algoritmasını açıklayan tam bir teknik rapor
Hashgraph'ın asenkron BFT olduğu, Ek'te yer almaktadır.

---

1 8

ASİT UYUMLULUĞU
Karma grafik ACID uyumludur. ACID (Atomisite, Tutarlılık, İzolasyon, Dayanıklılık) bir veritabanı terimidir,
ve dağıtılmış bir veritabanı olarak kullanıldığında karma grafiğe uygulanır. Bir düğüm ağı ulaşmak için onu kullanır

işlemlerin gerçekleştiği sıra üzerinde bir fikir birliği. Fikir birliğine vardıktan sonra, her düğüm
bu işlemler, her birini mutabakat sırasına göre göndererek, o düğümün veritabanının yerel
kopyasına. Eğer
yerel veritabanı bir veritabanının (ACID) tüm standart özelliklerine sahiptir, bu durumda ağ bir bütün
olarak
aynı özelliklere sahip tek, dağıtılmış bir veritabanına sahip olduğu söylenebilir. Blok zincirinde hiçbir
zaman bir
Konsensusa ulaşıldığını bildiğiniz an, bu nedenle ACID uyumlu olmayacaktır.

DAĞITILMIŞ HİZMETİN ENGELLENMESİ SALDIRI DİRENCİ

Hizmet Reddi (DoS) saldırısının bir biçimi, bir saldırganın bir
anlamsız mesajlar içeren ağ, bu düğümün diğer (geçerli) görevleri ve rolleri yerine getirmesini
engeller.
Dağıtılmış Hizmet Reddi (DDoS), bu DoS'yi farkında olmadan genişletmek için genel hizmetleri veya
cihazları kullanır.
saldırı - onları daha da büyük bir tehdit haline getiriyor.
Bir DLT ağında, bir DDoS saldırısı, fikir birliği tanımına katkıda bulunan düğümleri hedefleyebilir.
ve potansiyel olarak bu fikir birliğinin kurulmasını engelleyebilir.
Karma grafik DDoS dirençlidir çünkü tek bir düğümü veya özel bir düğüme sahip az sayıda düğümü
güçlendirmez.
fikir birliği oluşturmada haklar veya sorumluluklar. Hem Bitcoin hem de hashgraph bir
DDoS saldırılarına dirençli bir yol. Bir saldırgan, bir düğümü veya madenciyi veri paketleriyle
doldurabilir.
geçici olarak internet bağlantısını kesin. Ancak ağ bir bütün olarak normal şekilde çalışmaya devam
edecek.
Bir bütün olarak sisteme yapılacak bir saldırı, düğümlerin büyük bir kısmının paketlerle
doldurulmasını gerektirir.
hangisi daha zor. Blok zincirine dayalı olarak önerilen bir dizi alternatif vardır.
"Liderler" veya "round robin" modelleri. Bunlar, Bitcoin'in iş kanıtı maliyetlerinden kaçınmak için
önerildi,
ancak DDoS saldırılarına duyarlı olma dezavantajına sahiptirler. Saldırgan mevcut lidere saldırırsa
düğüm seçer seçilmez yeni lidere saldırmaya geçerse, saldırgan donabilir
tüm sistem aynı anda yalnızca bir düğüme saldırırken. Hashgraph bu sorunu ortadan kaldırırken,
iş kanıtı enerji gereksinimlerinden kaçınmak.
.
GÜVENLİK

Sayfa 19

19
ADİLLİK
Adalet
Hashgraph adildir çünkü lider düğümü veya madencinin belirlemesi için özel izinler verilmemiştir.
bir işleme atanan fikir birliği zaman damgası. Bunun yerine, işlemler için mutabakat zaman damgaları
algoritmada otomatik bir oylama süreci ile hesaplanır ve düğümlerin toplu olarak ve
fikir birliğini demokratik olarak kurmak. Adaletin üç yönünü birbirinden ayırabiliriz.

FUAR ERİŞİM

Hashgraph temelde adildir çünkü hiçbir tek düğüm bir işlemin
sistemi, hatta onu çok geciktirir. Bir veya birkaç kötü niyetli düğüm belirli bir işlemi engellemeye
çalışırsa
ağın geri kalanına teslim edilmekten ve böylece fikir birliğine eklenmelidir,
düğümlerin birbirleriyle mesajları ilettiği karma grafik dedikodu protokolü,
işlem bu blokaj etrafında akar.

ADİL ZAMAN HATLARI

Hashgraph, her işleme bir mutabakat zaman damgası verir.
ağ düğümleri bu işlemi aldı. Bu fikir birliği zaman damgası adil, çünkü bir
kötü niyetli düğüm onu bozmak ve o zamandan çok farklı kılmak. Her işlem atanır

her bir düğümün onu ilk aldığını söylediği zamanların medyanı olan bir fikir birliği süresi. Alınan
burada, belirli bir düğümün işlemi başka bir düğümden ilk kez geçirdiği zamanı ifade eder.
dedikodu. Bu fikir birliğinin bir parçası ve Bizans olmanın tüm garantileri de öyle. İkiden fazla ise-
Katılan düğümlerin üçte biri dürüst ve bilgisayarlarında güvenilir saatler var, ardından zaman damgası
kendisi dürüst ve güvenilir olacaktır, çünkü dürüst ve güvenilir bir düğüm tarafından üretilir veya
dürüst ve güvenilir düğümler tarafından oluşturulan iki kez. Çünkü hashgraph hepsinin medyanını
alıyor
bu zamanlarda, fikir birliği zaman damgası sağlamdır. Saatlerden birkaçı biraz kapalı olsa bile, hatta
birkaçı
düğümler kötü niyetle çok uzak zamanlar verir, fikir birliği zaman damgası önemli ölçüde etkilenmez.
Bu fikir birliği zaman damgası, bazı eylemleri gerçekleştirmeye yönelik yasal bir zorunluluk gibi
şeyler için yararlıdır.
belirli bir zamana göre. Bir olayın son teslim tarihine kadar olup olmadığı konusunda bir fikir birliği
olacaktır ve
zaman damgası, bir saldırganın manipülasyonuna karşı dirençlidir. Blok zincirinde, her blok bir zaman
damgası içerir,
ancak yalnızca tek bir saati yansıtır: bu bloğu çıkaran madencinin bilgisayarındaki saat.

FUAR İŞLEM SİPARİŞİ

İşlemler, zaman damgalarına göre sıralanır. Çünkü atanan zaman damgaları
bireysel işlemler adil, sonuçta ortaya çıkan sipariş de öyle. Bu, bazı kullanım durumları için kritik
öneme sahiptir.
Örneğin, Alice ve Bob'un her ikisinin de bir hisse senedinin mevcut son payını almaya çalıştıkları bir
borsa hayal edin.
aynı fiyata aynı anda hisse senedi. Blok zincirinde, bir madenci bu işlemlerin her ikisini de koyabilir
tek bir blokta ve hangi sırayla gerçekleşeceklerini seçme özgürlüğüne sahip. Ya da madenci belki
yalnızca Alice'in işlemini dahil etmeyi seçin ve Bob'u gelecekteki bir bloğa erteleyin. Hashgraph'da
yol yok
tek bir düğümün bu işlemlerin mutabakat sırasını gereksiz şekilde etkilemesi için. Alice'in
yapabileceği en iyi
daha iyi bir internet bağlantısına yatırım yapmak ve böylece işleminin Bob'dan önce herkese
ulaşmasını sağlamaktır. Bu
rekabet etmenin adil yolu.

Sayfa 20

20

YÖNETİM

Yönetim

Halka açık bir defter için bir yönetişim modeli, bir kamu defterinin evrimini kontrol eden kuralları ve
politikaları tanımlayacaktır.
düğüm yazılımı, madeni para basımı ve ağ katılımcılarını teşvik eden ödül modeli. Orada
çıkarları ve motivasyonları dengelenmesi gereken çok sayıda paydaştır: ağ düğümü operatörleri,
platformda uygulamalar geliştiren geliştiriciler, bu uygulamalara güvenen işletmeler,
bu uygulamalar ve ilgili düzenleyici kurumlar.
Hedera Yönetim Kurulu, 39 üyeye sahip olan bir limited şirkettir.
farklı endüstrilerden ve coğrafyalardan tanınmış şirketler. Hedera'nın lisanslama ve yönetişim modeli
çatal riskini ortadan kaldırarak, kod tabanının bütünlüğünü garanti ederek ağ kullanıcılarını korur ve
temeldeki yazılım kodunu incelemek için açık erişim sağlamak. Yönetişim modeli kapsamında, tüm
Yönetim
Üyeler eşit oy haklarına sahip olacak ve her bir Yönetici Üye (Swirlds hariç)
tek bir Yönetici Üyenin veya Yönetim Üyelerinin hiçbir grubunun
merkezi kontrol.
Hedera ağının, izinsiz veya izinsiz kullanım için aşamalı bir plana sahip izinli bir yönetişim modeli
vardır.
açık fikir birliği.
Yönetişim kararlarının Hedera üyeleri tarafından alınmasıyla yönetişime izin verilir.

Yönetim Kurulu. Konsey, Konsey üyeliği için politika belirler, ağ kurallarını belirler,
platformun para hazinesi ve platform kod tabanındaki değişiklikleri onaylar. Yönetişim modelimiz
1968'de kurulan ve daha sonra kurulan National BankAmericard Inc. tarafından kullanılan orijinal
modele dayanmaktadır.
VISA olarak yeniden adlandırıldı. Yönetişim modelimizi, Yönetim Kurulu Üyelerine güvence verecek
şekilde tasarlıyoruz.
Hedera platformunun çıkarına en uygun olanı yapmak için güvenilebilir ve gereksiz yere
etkilenmemelidir.
bireysel Konsey üyeleri veya düğüm operatörleri. Hedera, Yönetim Üyelerine ek olarak,
katılımcı kuruluşlar, danışmanlık hizmetleri sunarak Hedera ağ ekosistemine katkıda bulunurlar.
uygundur, ancak bu tür kuruluşlar oy kullanma ayrıcalıklarına sahip olmayacaktır.
Açık fikir birliği modeli, düğümlerin ağa katıldığı ve bir ağa ulaştığı süreçle ilgilidir.
platformdaki işlemlerin sırası konusunda fikir birliği. Model, aşağıdakilerin konsolidasyonunu
önlemek için tasarlanmıştır.
Sonunda milyonlarca kişiyle merkezi olmayan bir ağın ortaya çıkmasını teşvik ederek fikir birliği
üzerinde güç
düğüm sayısı. Kripto para birimini taklit ederek sisteme saldırmak için birkaç kişinin hile yapmasını
önler,
defteri uygunsuz bir şekilde değiştirmek veya işlemlerin mutabakat sırasını etkilemek. Engelliyoruz
belirli bir düğümün hashgraph algoritması içindeki oyları, düğüme göre ağırlıklandırarak gizli anlaşma
madeni para hissesi. Açıkça ifade edilirse, her düğüm Hedera yerel para biriminin her bir madeni
parası için bir oy atar.
(hbars) sahibi. Başlangıçta Hedera ağındaki tüm düğümler Konsey üyeleri tarafından işletilecek,
böylece mutabakat izinli olarak başlayacaktır. Ağ kullanımı arttıkça, Konsey yeni düğümlere izin
verecektir.
operatörlerin ağa katılmaları ve hashgraph'ı sürdürmedeki hizmetleri için ödeme almaları. Sayısı
düğümlerin zaman içinde büyüyerek oylama ayrıcalıklarının birçok kişiye dağıtılmasını sağlaması
bekleniyor.
düğümler. Stake etme modelinin tam bir tartışması aşağıdaki bölümde yer almaktadır.
Açık fikir birliğine sahip bu izinli yönetişim sistemi, yalnızca
kapalı sistem. Bu, küresel bir DLT platformunun başarısı için çok önemlidir.

Sayfa 21

21
YÖNETİM
İZİN VERİLEN YÖNETİM
Hedera yönetişim modelini, Konseyin,
ağ oldukça. Konsey üyeleri eşit yönetim haklarına ve sınırlı şartlara sahip olacak ve
yönetişim ademi merkeziyetçi. Müzakere ve münazara tüm Konsey üyelerine açık olacak ve
Yok.
Yönetim Üyeleri, Hedera operasyonlarının gözetimini sağlayan komitelere de katılacaklardır.
Komiteler, bunlarla sınırlı olmamak üzere, bir Teknik Yönlendirme ve Ürün Komitesi, bir Finans
Komite ve Hukuk ve Düzenleme Komitesi. Yönetim Üyeleri,
geniş bir iş sektörü yelpazesi ve hedefimiz, toplu olarak üyeliğin katkıda bulunacağıdır.
Hedera komitelerine sektör lideri temsilcilik.

Sayfa 22

22
İSTİKRAR
istikrar
Bitcoin ve Ethereum'un yaşadığı sert çatallar muhtemelen ağ etkisine zarar verdi.
Piyasada karışıklık ve belirsizlik yaratarak karşılık gelen para birimlerinin sayısı. Benzer şekilde,
Altcoinlerin patlaması (ve çoğunun şüpheli meşruiyeti ve değeri),
kripto para birimlerini benimsemeyi düşünen işletmelere ve tüketicilere gerekli güven.

Tarihsel olarak, açık kaynak yazılım geliştiricileri tek bir temeli korumanın değerini anlamışlardır. kodlama ve topluluktan en iyi fikirlerin bütünün yararına dahil edilmesini sağlama.
Bununla birlikte, açık kaynaklı bir projeyi bir kripto para birimi ile birleştirirken, geleneksel teşvik yapı alt üst edildi. En yaygın şekilde benimsenen dağıtılmış defter teknolojileri
aynı zamanda en çok bölünenlerdir. Bu dinamik, sektörde kaosa neden olur ve doğrudan
halka açık defterlerin ana akım piyasalar tarafından benimsenmesi.
Hedera teknik ve yasal kontroller, platformun rakip bir platforma geçmemesini sağlar ve
kripto para.

Sayfa 23

23
İSTİKRAR
Teknik kontroller
İMZALANMIŞ DEVLET KANITLARI
Tüm düğümler, durumun bir kopyasını tutar. Örneğin, her düğüm tüm ağın dengelerini bilir katılımcıların kripto hesapları. Algoritmanın her turunun sonunda, her düğüm yeni
o turda ve öncesinde alınan tüm işlemleri işleyerek belirtiniz. Her düğüm daha sonra dijital olarak bu paylaşılan durumun bir karmasını imzalar, bir işleme koyar ve ağda dedikodu yapar. Sonra bu imzaları diğer tüm düğümlerden toplar.
Bir müşteri durumun bazı yönlerini talep ettiğinde, tüm düğümler küçük bir
Müşteriye (veya başka birine kanıtlamak için toplanan imzaları ve diğer kriptografik materyalleri içeren dosya)
taraf) döndürülen verilerin gerçekten gerçek, fikir birliği durumu olduğunu.
Devlet bir Merkle ağacı olarak düzenlenmiştir, bu nedenle üçüncü bir tarafa küçük bir parçadan oluşan bir kanıt verilebilir.
devletin yanı sıra oradan Merkle ağacının köküne giden yol (bu köşelerin kardeşleri dahil)
ağaç) artı imzalar ve genel anahtarlar için bir adres defteri geçmişi.
Aşağıdaki şema, üçüncü bir tarafın aşağıdakilerden birinden aldığı durumdan nasıl emin olacağını temsil etmektedir.
düğümler gerçekten de tüm ağın fikir birliği durumunu temsil eder.

Sayfa 24

24
İSTİKRAR
LEDGER KİMLİĞİ
İspat ayrıca, her düğümün hissesi ile birlikte tüm düğümlerin ortak anahtarlarının bir listesi olan bir "adres defteri" içerecektir. Bir
üçüncü şahıs, eyaletteki (veya eyaletin bir kısmındaki) imzaları kontrol etmek için bu adres defterine ihtiyaç duyacaktır.
Kanıt ayrıca bir "adres defteri geçmişi" içermelidir. Bu, her adres defterinin bulunduğu bir adres defteri dizisidir.
önceki adres defterinden düğümler tarafından imzalanmıştır. Verilen herhangi bir adres defteri, daha fazlasını kontrol eden bir dizi düğüm tarafından imzalanmalıdır.
ağın düğüm listesine ve önceki hisseye göre, platformun paralarının 2 / 3'ünden daha fazla
adres defteri. Bu adres defteri zinciri, başlangıçtaki düğümler tarafından imzalanan başlangıç adres defterine kadar uzanır.
defteri yaratan.
Genesis adres defterinin karması önemlidir. Defterin benzersiz bir tanımlayıcısı görevi görür. Defterin "adı" dır.
TAŞIMA ÇATALLARI
Az sayıda düğüm ağdan ayrılmak ve mevcut olanın çatalı olan yeni bir defter oluşturmak istiyorsa, bu düğümler bunu yapmak için teknik beceriye sahiptir ve hatta yeni defterlerinin ilk durumunu aynı olacak şekilde oluşturabilirler.

eski deftere. Yani bu bir çatal. Ancak, adres defterine kadar geriye giden bir adres defteri geçmişi oluşturamazlar.
genesis adres defteri, her adres defterinin düğümleri bir sonrakini imzalar, çünkü düğümlerin çoğunluğu (kim
çatallanmıyorsa) çatallanan düğümlerin azınlığı için adres defterini imzalamayacaktır. Bu, yeni çatalı zorlar
yeni bir adres defterine ve dolayısıyla yeni bir benzersiz tanımlayıcıya ve dolayısıyla yeni bir ada sahip olur. Sonuç olarak, bunlar
çatalı yaratmak kimseyi çatalın meşru defter olduğunu düşünmeye ikna edemez.
Bir müşteri, deftere göndermek üzere bir düğüme bir işlem gönderdiğinde, müşteri,
düğüm, işlemlerinin paylaşılan durumu doğru bir şekilde etkilediğinin şifreli kanıtıdır. Alice transfer olduğunda
kripto para biriminden Bob'a, her ikisi de işlemin başarılı olduğuna dair kriptografik bir kanıt alabilecek.
Bu ispat, kaynak adres defterine geri gelen imzaları içerir. Yani sadece transferin
oluştuğunda, doğru defterde gerçekleştiğini doğrularlar. Bir defter çatallanırsa, hiçbir müşterinin hangisi olduğu konusunda kafası karışmaz.
Bir defada yalnızca bir defter bu ada sahip olabileceğinden, uğraştıkları defter.
Ayrıca, ağın hbar hissesi iki düğüm grubu arasında 50/50 bölüşürse, hiçbir grup
düğümler, genesis adres defterine bir bağlantı olduğunu kanıtlayabilecektir. Çataldan ziyade, tam olacaktır
bir defterin yapısökümü ve iki yeni defterin yaratılması. Bu, defterin değerini büyük ölçüde azaltır
düğümlere, çünkü orijinaline erişmek isteyen müşterilerden artık ücret kazanamayacaklardı.
defter. Ve orijinal kripto para birimlerinin tümü, çok gerçek anlamda var olmaktan çıkar. Bu muazzam bir
çatallanmayı caydırıcı.
Bu şekilde, Hedera defterinin kullanıcıların kafasını karıştıracak aldatıcı bir çatalını etkili bir şekilde oluşturmak imkansızdır. Hatta
dürüst olmayan düğümler, kullanıcıları kopyanın doğru olduğunu düşünmeye ikna etmek için Hedera defterinin çatallı bir kopyasını oluştururlarsa
meşru defterde, kullanıcılar defterin geçerli olmadığını bilirlerdi çünkü meşru olmayan çatalı barındıran düğümler
geçerli bir devlet kanıtı sağlayamama. Ve düğümlerin açıkça çatallı bir kopya oluşturması için çok az teşvik vardır, çünkü
Kullanıcılardan geçersiz bir sürüme geçmeleri için çok fazla talep olması olası değildir. Bu yüzden güçlü teşvikler var
Herhangi bir yasal teşvikin dışında bile çatallardan kaçının.
Çatalları önleyen kriptografik kanıtlar ve benzersiz tanımlayıcılar da güvenli parçalama için kritik öneme sahiptir.
Parçaların birbirlerine mesajlar göndermesine izin verirler ve verilen bir parçadan gelen mesajın gerçekten doğru olduğundan emin olurlar.
bu parçanın fikir birliği.

Sayfa 25

İSTİKRAR
Yasal Denetimler ve Şeffaflık
Hedera kod tabanı, Hedera Yönetim Konseyi tarafından yönetilecektir. Kod tabanının 1.0 sürümü, 2020'de beklenen "açık inceleme" olacak, yani herkesin kaynak kodunu okuyabileceği,
yeniden derleyin ve doğru olduğunu doğrulayın.
Hedera platformunu kullanmak için herhangi bir lisans gerekmeyecektir. Bunu sağlayan yazılımları yazmak için herhangi bir lisans gerekmez.
Hedera platformunun hizmetlerini kullanır. Üstüne akıllı sözleşmeler oluşturmak için herhangi bir lisans gerekmeyecek
Hedera platformu. Hedera platformu üzerine inşa edilen uygulamalar açık kaynak veya tescilli olabilir.

Hedera'dan herhangi bir lisans veya onay gerektirmezler. Platform API'leri kullanılarak geliştirilen yazılım
hiçbir şekilde ipotek altına alınmayacaktır. Yazılım geliştiriciler, üzerinde tam sahiplik ve takdir yetkisine sahip olacaktır.
Hedera platformunu kullanan uygulamaları için seçtikleri lisans.
Swirlds, hashgraph mutabakat algoritmasındaki fikri mülkiyet haklarına sahiptir. Hedera
Yönetim Konseyi, hashgraph fikir birliği algoritmasını kullanmak için Swirlds'den bir lisansa sahiptir ve ilgili
Hedera dağıtılmış halka açık defter platformu için teknoloji. Bu lisans karşılığında Hedera
Yönetim Konseyi, Swirlds'e ağ gelirinin% 10'unu ödeyecek (aylık minimumlar ile) ve Swirlds
Hedera coinlerinin% 5'ine sahip. Swirlds, hashgraph teknolojisinin kullanım için lisans gerektirmeye devam edecek.
özel, izinli ağlar, ancak üzerinde çalışan dağıtılmış uygulamalar için lisans gerekmez.
Hedera'nın halka açık platformu. Hedera ve Swirlds, hashgraph ile ilişkili patent haklarını kullanacaktır.
kod tabanının çatallanmasını ve rakip bir
platform ve para birimi. Geliştiriciler, Hedera'nın üzerine dağıtılmış uygulamalar oluşturmakta özgürdür
ilişkili yerel belirteçlerle platform.
Özetle Hedera, yazılım kodunun açık bir incelemesini eşzamanlı olarak benimseyecek ve aynı zamanda
Lisansı kontrol ederek platforma ve kripto para birimine istikrar. Bu şekilde Hedera,
şeffaf kod tabanı, piyasaların ana akımın benimsenmesi için talep ettiği istikrarı garanti eder.

Sayfa 26

MEVZUATA UYGUNLUK

Mevzuata uygunluk
Hükümetlerin politika hedeflerini kullanıcılara, kuruluşlara ve geliştiricilere genişletmeye devam etmesini bekliyoruz.
halka açık defterleri ve ilgili kripto para birimleri ve jetonları kullanmak. Bunu temel bir hedef olarak görüyoruz
Hedera ağının, ekosisteminin tüm üyelerinin uyması için gerekli araçları sağlayabileceğini
Avrupa Birliği Genel Verileri gibi mevcut rejimler dahil olmak üzere geçerli yasa ve yönetmelikler
Gizlilik Düzenlemeleri (GDPR) ve kara para aklamayı önleme (AML) yükümlülükleri. İle çalışmaya devam edeceğiz
yeni ve değişen yasa ve yönetmeliklere uyumu sağlamak için düzenleyiciler. Aşağıdaki bölümler
Yasal uyumluluğa giden bir yola izin veren Hedera ağının bazı temel unsurlarının ana hatlarını çizin.

KENDİNE ÖZEL

Diğer dağıtılmış defterlerin çoğunda olduğu gibi, Hedera hesabının durumunu etkileyen tüm işlemler hesabın özel anahtarı ile imzalanmalıdır. Bu, kendi sahipliklerini elinde tutan son kullanıcıların
özel anahtar hesapları üzerinde tek kontrole sahip olmak ve hiçbir fonun saklama sorumluluğunu Hedera'ya bırakmamak,
geliştiriciler veya işletmeler. Hatta kripto para birimi işlemleri bile olmadan tamamen eşler arasıdır.
hbarları ele geçiren aracılar. Geliştiriciler cüzdanlar ve uygulamalar tasarlayıp oluşturabilir
Özel anahtarların ve fonların kendi kendine saklanmasını kullanan veya özel anahtarları barındırmayı seçen Hedera ağında
kullanıcılarının anahtarlarını ve bu tür gözetim ilişkisinden kaynaklanan yasal yükümlülüklere uymaktadır.

VERİ KENDİNE BAĞIMSIZLIK

Diğer dağıtılmış defterlerin çoğunun aksine, Hedera ağı kontrollü değişkenlik uygular. Ne zaman veri Hedera ağında yayınlandığında, yayıncı ileride silinmek üzere bir yetkilendirme politikası tanımlayabilir
ve / veya hangi anahtarların bu yetkilere sahip olduğunu belirleyerek değişiklik. Bu, geliştiricilerin GDPR kapsamındaki "silme hakkı" gerekliliğiyle uyumlu olabilecek veya kullanıcılarının

hangi verilerin ne kadar süreyle herkese açık olduğu konusunda tam kontrol sağlayın.

GİZLİLİK YÖNETİMİ

Hedera ağı, kullanıcıların kendi kimliklerini ve işlem gereksinimlerini yönetmelerine de olanak tanır. Tarafından
varsayılan olarak hesaplar, diğer dağıtılmış defterlerin çoğu gibi takma addır. Ancak Hedera teknolojisi
çerçeve, kullanıcıların gerçek kimliklerini eklemelerine izin veren gelecekteki uygulamaları destekleyebilir (iddia edildiği gibi
Sertifika Yetkilisi olarak hareket eden bir akredite taraf tarafından) mantıksal olarak genel muhasebe hesaplarına bağlı olmak için
Bu hesabı fonları taşımak için kullanırken, uygun KYC kontrollerinin yapılabileceğini bir karşı taraf tam kimlik kanıtı (tam yasal ad dahil) veya belirli kimlik özellikleri talep etmeyi seçebilir
(yaş gibi) ağda bir işlemi kabul etmek için uyum programlarıyla tutarlı.
Kullanıcı, kişisel bilgilerinin kontrolünde kalır ve kimlik kanıtı sunup sunmayacağı veya
karşı tarafın özellikleri; karşı taraf, uyumluluk yükümlülüklerini yerine getirme kontrolünde kalır bir işlem yapmadan önce.
Sistem, bir kullanıcının mekanizmadan yararlanmayı açıkça seçmesi gerektiğinden ve eğer yapmazlarsa, hesap işlemleri takma ad olarak kalacaktır. Ancak bu seçim önleyebilir
belirli finansal işlemlere girmekten alıkoyuyorlar.

Sayfa 27

BÖLÜM
2 7

Sistem, aşağıdakilerin uygun dengesini sağlayacak şekilde tasarlanmıştır:

1.
Hükümet görünürlüğü
2.
Güvenlik
3.
Kullanıcı gizliliği

Yeni bir banka hesabı oluştururken sürücü ehliyeti göstermeye benzer, modelin bir kullanıcı eki vardır tanınmış bir kimlik sağlayıcısı tarafından kendi hesabına oluşturulmuş bir dijital sertifikanın karması. Bu ek
ağa gönderilen bir işlem şeklini alacaktır.
Bu işlem:

1.
Hem kullanıcının özel anahtarı hem de kimlik sağlayıcının özel anahtarı ile imzalanması gerekebilir
2.
Daha sonra hash'i ayırmak için hangi tarafların yetkili olduğunu belirleyebilir (ve böylece, kimlik ve hesap arasındaki bağlayıcılık).

Hesap ve sertifika arasındaki ek, kullanıcı tarafından iptal edilmediği sürece
veya kimlik sağlayıcı, hesabın bilinen bir kullanıcıya bağlı olduğunu belirlemek için kullanılabilir.
fonlar bu hesaba girer veya çıkar. Uygunsa ve uygun olduğunda, kimlik sağlayıcı bağlayıcılığı iptal edebilir
sadece ağa imzalanmış bir işlem göndererek.
Nasıl çalışabileceğine bir örnek olarak, Hedera hesabından şu hesaba para göndermeye çalışan bir kullanıcıyı düşünün:
bir ABD bankası. Kullanıcı, bankaya hem sertifikayı hem de hesap adresini sağlar. Banka
hesabı arar ve hesabın sertifika için karşılık gelen hash'e sahip olduğunu onaylar,
ve sertifikanın güvenilir bir kimlik sağlayıcı tarafından verildiği. Sadece tüm bu kontroller onaylandıysa
banka işlemi yetkilendirir ve fonları kabul eder. Banka tarafından sorulabilir
ilgili hükümetin sertifikayı ve işlem ayrıntılarını gerçek zamanlı olarak (belki
transfer miktarına göre) veya bir programa göre.

PARA AKLAMA

Hedera ağını kullanan bazı geliştiriciler ve kuruluşlar, kara para aklamayı önleme raporlarına sahip olabilir
yükümlülükler. Bu tür varlıklar için, ağ üzerindeki kimlik sertifikaları ve aynadan gelen ağ verilerinin kullanımı
düğümler bir uyum programının temelini oluşturabilir. Aşağıda daha ayrıntılı olarak tartışıldığı gibi yansıtma düğümleri,
sonunda herkes tarafından çalıştırılabilecek ve ağ etkinliğinin "salt okunur" gözlemcisi olarak hizmet verecek. Böyle olan
yansıtma düğümleri, ağdaki tüm genel veriler görüntülenebilir, depolanabilir ve inceleme yapmak için analiz edilebilir
ve şüpheli davranışları işaretleyin.
Hedera, Distributed Ledger Foundation'ın kurucu üyesidir ve daha geniş kapsamlı DLT ile çalışacaktır.
topluluk ve hükümetler, düzenleyici gereksinimlerin karşılanmasını sağlarken,
Gizlilik ve güvenlik.
Hedera, genel muhasebe defterinin ana piyasa tarafından benimsenmesinin önündeki beş temel engeli doğrudan çözüyor
teknoloji: Performans, Güvenlik, Kararlılık, Yönetişim ve Yasal Uygunluk. Hashgraph
veri yapısı ve fikir birliği algoritması, sınıfının en iyisi, benzersiz bir performans kombinasyonu sağlar
ve güvenlik. Hedera platformu ve Hedera Yönetim Konseyi şeffaflık sağlayacak, açık
yenilik, platform istikrarı, KYC ve AML'yi etkinleştirmeye yönelik araçlar ve küresel, sektörler arası uzmanlık
küresel olarak dağıtılmış bir ağ ve kripto para birimi için yönetişim ve karar verme sağlar.

Sayfa 28

2 8
Bölüm 2
Mimari
MİMARİ

Sayfa 29

MERKEZİLEŞTİRİLMİŞ UYGULAMA
HEDERA HASHGRAPH AĞI
İNTERNET
CÜZDAN
KRİPTO PARA
AKILLI
SÖZLEŞMELER
UZLAŞMA
HİZMET
DOSYA
HİZMET
29
MİMARİ

Sayfa 30

3 0
İNTERNET KATMANI
Hedera ağ düğümleri, TCP / IP bağlantılarıyla iletişim kuran internetteki tüm bilgisayarlardır.
Mükemmel iletme gizliliği için geçici anahtarlarla TLS şifrelemesiyle korunur. Düğümler şu şekilde adreslenmektedir:
Sembolik adlar yerine IP adresi ve bağlantı noktası, bu nedenle DNS sistemine yapılan saldırılar,
ağ.
HASHGRAPH CONSENSUS KATMANI

Düğümler, istemcilerden işlemleri alır ve bunları ağda bir dedikodu protokolü ile paylaşır.
Ardından tüm düğümler, bir fikir birliği zaman damgası üzerinde anlaşmaya varmak için karma grafik fikir birliği algoritmasını çalıştırır.
her işlem ve tarihteki mutabakat sırası için. Her düğüm daha sonra
paylaşılan durumun kopyasını değiştirmek için mutabakat sırasındaki işlemler. Bu şekilde, tüm düğümler bir
özdeş fikir birliği durumu (herhangi bir parça içinde).

HİZMET KATMANI

KRİPTO PARA

Kripto para birimi hızlı olacak şekilde tasarlanmıştır, bu da düşük ağ ücretlerine yol açar.
küçük mikro dönüşümler pratik. Hedera platformu geniş ölçekte çalışırken, herhangi bir kullanıcı ağda bir düğüm çalıştırabilecek ve bunu yapmak için kripto para birimi ödemeleri kazanabilecek.
Herhangi bir kullanıcı, herhangi bir isim olmaksızın sadece bir anahtar çifti oluşturarak bir hesap oluşturabilir.
veya ekli adres. İsteğe bağlı olarak, bir kullanıcının karma eklemesine izin vermek için provizyonlar yapılır
kimlik sertifikalarının. Bunlar herhangi bir üçüncü taraf sertifika yetkilisinden gelebilir veya kullanıcının seçtiği kimlik yetkisi. Bu, yasal uyumluluğa izin vermek için tasarlanmıştır,
Know Your Customer ile bir yargı alanında kullanılacak kripto para birimi hesapları için
(KYC) veya Kara Para Aklamayı Önleme (AML) yasaları. Yönetmelikte daha fazla ayrıntı verilmiştir.
Uyum bölümü.

DOSYA DEPOLAMA

Dosya sistemi, kullanıcıların tam olarak neyin depolandığına dair fikir birliği ile bilgileri depolamasına izin verir.
ve neyin saklanmayacağı. Kırıktaki her düğüm aynı dosyaları depolar, bu nedenle
düğümlerden biri çökerse kaybolur. Depolanan bilgiler yalnızca şunlar tarafından silinebilir:
izin verildi. Bu şekilde, dosya sistemi bir iptal hizmeti olarak hareket edebilir. İçin
Örneğin, gelecekte, bir kullanıcıya Bakanlıktan bir sürücü belgesi verilebilir.
Motorlu Taşıtlar (DMV) ve hem kullanıcı hem de DMV dijital olarak imzalayan işlemi
deftere bir hash koyar. Her ikisi de lisansın karmasını kaldırma hakkına sahiptir.
kullanıcı, o kişiye geçerli bir lisansa sahip olduğunu kanıtlamayı seçebilir.
Lisans dosyasının bir kopyası, böylece kişi hash'in hala içinde saklanıp saklanmadığını kontrol edebilir.
defter. DMV lisansı iptal ederse, dünyaya şunu göstermek için hash'i de siler.
lisans artık geçerli değil. Kullanıcı hash'i imza olmadan yeniden saklamaya çalışırsa
DMV'den, hash'in yalnızca DMV'siz kullanıcı tarafından saklandığı açık olacaktır.
işbirliği ve kullanıcının araba kullanma hakkının geçerli bir kanıtı olarak kabul edilmeyecektir.
MİMARİ

Sayfa 31

Dosyalar aslında Merkle ağaçları olarak saklanır, ancak geliştiricilere izin vermek için Java sınıfları sağlarız.
onları manipüle etmek için.
Geliştiricilere bir Merkle ağacını bir dosya sistemiymiş gibi kullanmaları için Java kodu veriyoruz.
Dizinleri, alt dizinleri ve dosyaları görürler. Ve dosya içeriğini ve dizini değiştirirler
isimler, nesneleri hareket ettirin ve kopyalayıp yapıştırın. Yine de, altında, hepsi bir
Merkle ağacı otomatik olarak. Bu, bir dosyanın fikir birliğinin parçası olduğuna dair kanıtlar sunmamızı sağlar.
durum. Kullanıcılar ayrıca Hedera dosya sisteminde tüm bir dizini depolayabilir.
Yalnızca Merkle ağaçlarını depolamakla kalmıyoruz, Merkle DAG'lerini de depoluyoruz, yani iki dosya varsa
ortak bazı baytlar, ortak baytların yalnızca bir kopyasını depolayabiliriz.
Bir dosyaya hash'i ile erişilebilir, böylece insanlar onun değişmez olduğu gerçeğine güvenebilirler.

Ancak bir Dosya Kimliği de vardır. Sahibi yeni bir dosya oluşturabilir ve Dosya Kimliğini
eski dosya yerine yeni dosyayla ilişkilendirilir. Bu şekilde kullanıcıların
her zaman bir dosyanın en son sürümünü bulun. Karma yerine sadece Dosya Kimliğine erişirler.
Böylece dosyalar aynı anda hem güvenli bir şekilde değişmez hem de güvenli bir şekilde
değiştirilemez.
Bir dosyaya hash'i ile erişiliyorsa, o zaman asla değişmez. Dosya Kimliği ile erişiliyorsa,
daha sonra en son sürüm bulunur.

AKILLI SÖZLEŞMELER

Hedera defteri, Solidity'de yazılmış akıllı sözleşmeleri çalıştırabilir. Şu anda, büyük kitaplıklar
Solidity akıllı sözleşme kodu mevcuttur ve Hedera'da değiştirilmeden çalıştırılabilir. Bunlar izin verir
Hedera'nın üzerine kolayca inşa edilebilecek dağıtılmış uygulamalar için.

UZLAŞMA

Hedera Mutabakat Hizmeti, akıllı sözleşmelere etkili bir alternatif sunacak ve
dağıtılmış uygulamalar oluşturmak için dosya sistemi. Müşteriler Hedera'ya mesaj gönderir
belirli konularda zaman damgası ve sipariş için. Bu sıralı mesajlar akacak
mutabakat sırasına göre işlenmek üzere ayna düğümlerinin müşterilerini veya düğümlerini yansıtmak
için.
fikir birliği hizmeti, dağıtılmış uygulamalara yerel hıza doğrudan erişim sağlar,
karma grafik konsensüs algoritmasının güvenlik ve adil sipariş garantileri,
Hedera defterine tam güven. Hedera platformunun fikir birliği hizmetiyle ilgili tüm ayrıntılar,
başlangıçta mevcut olmayacak, ancak platformun sonraki bir aşamasında eklenecek
geliştirme, Ek 2'de mevcuttur.

Sayfa 32

Yansıtma ağı

Hedera ayna ağı, aynı gereksinimleri ve çoğunu koruyacak bir düğümler kümesidir.
ana Hedera ağının işlevselliği İşlevsellikteki temel fark, ayna düğümlerinin
ağın defterine dahil edilecek işlemleri gönderme yeteneğine sahip değildir. Yansıtma düğümleri
dedikodu yapacak, fikir birliğini hesaplayacak ve imzaları doğrulayacak, ancak oluşturamadıkları için
olaylar, ayna düğümlerinin karma grafik yapısı üzerinde hiçbir etkisi yoktur. Bu nedenle
gönderemezler
mutabakat için işlemler ve oylama gücü yok. Yansıtma düğümleri "salt okunur" düğümler olarak
düşünülebilir
bu işlemler, Hedera API aracılığıyla bir ayna düğüme gönderilemez. Yansıtma düğümleri ücretsizdir
oluşturdukları yeni hizmet türlerini sağlamak için ek API'ler geliştirin.
Yansıtma ağı, defterin durumunu çok daha fazla kullanıcıya ulaştırmanın etkili bir yolunu
sağlayacaktır.
ve ana sistemin performansı üzerinde büyük bir etkisi olmadan kısa bir süre içinde dApp'ler
ağ. Sonuç olarak, dApps, üzerindeki işlemleri dinlemek için kendi yansıtma düğümlerini barındırmayı
seçebilir.
ana ağ ve buna göre yanıt verin. Örneğin, akıllı bir sözleşme uygulayan bir dApp,
bir ayna düğümü barındırın, akıllı sözleşmesindeki olayları dinleyin, diğer işlemleri filtreleyin ve
yanıtlayın
buna göre.

Sayfa 33

Parçalama

Başlangıçta, Hedera ağı, Yönetim Kurulu Üyeleri tarafından hepsi bir arada işletilen az sayıda düğüm
olacaktır.
tek bir parça. Hedera Yönetim Konseyi büyüdükçe ve diğerleri düğümleri çalıştırmaya başladıkça, ağ

Birden fazla parçayı doğrulamak için yeterli sayıda düğüm kazanır. Parçalama performans avantajları sağlayabilir
her düğümün her işlemi işlemesi gerekmediğinden. Mutabakat sonuç olarak paralel olarak ilerleyebilir. Kırıklar
birbirlerine güvenecek, bu nedenle bir parça, kripto para birimini taşıma veya çeşitli
başka bir parça tarafından yapılan kaynaklar - bu taleplerin, tarafların mutabakatını yansıttığı kanıtlanabildiği sürece
parça istiyor. Bu, çoklu parçalı defterin bir bütün olarak asenkron Bizans hatasına ulaşmasına izin verecektir.
hoşgörü ve çift harcamaları veya defterin diğer çelişen durumlarını önlemek için, çünkü her birey
parça bu özelliklere sahip olacak ve aralarındaki tüm mesajlar,
bu parçanın fikir birliği.
Plan, düğümlerin rastgele bir şekilde farklı parçalara gruplanacağı ve bunların içinde fikir birliği sağlanacağıdır.
işlemler normal şekilde kurulacaktır. Her parça, tümü düğümlerin bir alt kümesinden oluşacaktır.
tüm defterin durumunun bir alt kümesi olacak aynı durumu paylaşın. İşlemler yerleştirilecek
normal şekilde ayrı ayrı parçalarda mutabakat düzenine dönüşür - bir parça içindeki tüm düğümler katkıda bulunur
yalnızca bu parçadan kaynaklanan işlemler için fikir birliğine. Düğümlerin parçalara atanması
her gün bir parçaya yeni düğümler atayan bir ana parça tarafından rastgele gerçekleştirilecek ve ayrıca
her bir parçanın toplamda büyük miktarda hbar'a sahip olmasını sağlamak için düğümleri parçalar arasında gerektiği gibi hareket ettirir
ve bir parça içindeki hiçbir düğümün bu toplam miktarın büyük bir kısmına sahip olmayacağını.
Parçalar, farklı parçaların düğümleri arasında mesaj alışverişi yoluyla iletişim kuracak.
Bu tür tüm mesajlar itilir (çekme yerine). Her parça (düğümleri) bir giden giden kuyruğu tutacaktır.
diğer kırıkların her birine mesaj. Her parça, son mesajın sıra numarasını hatırlayacaktır
diğer kırıkların her birinden işlendi. Alfa parçasından şu adrese aktarım için bir mesaj gönderilecek:
Beta'daki düğümlerle rastgele iletişim kuran Alfa düğümlerinden oluşan Beta parçası ve bunun bir parçası olduğunun kanıtı
Alfa parçasının fikir birliği durumu. Beta düğümlerinden biri ile yanıt verene kadar bunu yapmaya devam edecekler
Beta parçası paylaşılan durumunun, bu mesajın
Alındı ve işlendi. Bu şekilde, farklı parçalardaki adresleri etkileyen işlemler
her bir parçanın durumuna ve böylece tüm defterin tüm durumuna uygun şekilde kaydedilir.
Daha fazla ayrıntı, Sharding ekinde verilmektedir.

Sayfa 34

3 4
3. bölüm
Kriptoekonomi
KRİPTOEKONOMİ

Sayfa 35

Stake etme ve vekil stake etme
Hedera defteri, her bir düğümün etki alanı üzerindeki etkisinin olduğu bir teminat kanıtı fikir birliği mekanizması kullanır.
fikir birliği, kendisine yatırdığı kripto para birimi miktarıyla orantılıdır. Bir işlem doğrulandı
ve ikiden fazla toplam hisseyi temsil eden düğümler tarafından doğrulandıktan sonra konsensusa yerleştirilir:
ağın toplam hbar sayısının üçte biri (hbar sayısı 50 milyar olarak sabitlenmiştir). Bu önemli
ağın çalışmaya devam etmesi için kripto para biriminin çoğunun gerçekte stake edildiğinden emin olmak için.

Ağın ilk aşamasında, Hedera Hazinesi toplamın üçte ikisinin üzerinde "vekaleten pay alacak"
Konsey Üyeleri tarafından barındırılan düğümlere hbar sayısı.
Hbar'lar daha geniş çapta dağıtıldıktan sonra (böylece tek bir kullanıcı veya kullanıcı grubu denetimi
ele geçiremez.
tüm hbar'ların üçte biri kadar), ağ herkesin bir düğümü barındırmasına izin verecektir (yani, izinsiz
olacaktır.
ağ). O anda, bir düğüm ağa katıldığında, yapabileceği bir veya daha fazla hesabı bildirmelidir.
kontrol edin ve bu hesaplar için özel anahtarlara sahip olduğunu kanıtlayın. O andan itibaren, içindeki
hbar miktarı
bu hesaplar, hashgraph sanal oylama algoritmasında oylarını ağırlıklandırmak için kullanılacaktır. Ek
olarak,
bu ödeme, bu hesaplardaki hbar miktarıyla orantılı olacak şekilde, bir düğüm olarak hizmet etmesi için
ödenecektir.
Bu hbarları herhangi bir zamanda harcamak hala ücretsizdir. Sonuç olarak, bağlı kanıtı potansiyel bir
caydırıcı
İlişkili likidite kaybı korkusuyla riske girmek istemeyen düğümlerin riskli modellerinden kaçınılır.
Ek olarak, "vekil staking" adı verilen bir mekanizma, hbar'lara sahip olan ancak bir
yine de bu hbar'ları hisseden ve ağa katkıda bulunmak için az miktarda hbar kazanmak için düğüm
hesaplarını bir düğüme "vekil stake ederek" işlem. Bu, başka bir hesap kredisi vermek anlamına gelir
hbar'ları ve fikir birliğine katkıda bulunduğunda düğümün bu hisseyi kullanmasına izin veriyor. İçin
ödemeler
Düğümü çalıştırmak (yatırılan miktarla orantılı olarak) daha sonra düğüm ve sahibi arasında bölünür.
hbarlar vekil kazanıyor. Vekâlet edilen hbarlar hala onların kontrolü altındadır.
sahip. Sahip, proxy staking'i istediği zaman kapatabilir veya başka bir düğüme yönlendirebilir. Onlar
ayrıca, vekil ile stake edilmiş hbar'ları herhangi bir zamanda harcayabilecektir, ancak bu, miktarı
azaltacaktır.
stake etme karşılığında ödeme alırlar. Hbar'ların proxy stake edildiği düğümün harcama
yapamayacağını unutmayın
o hbarlar. Ağ kullanıcıları için bu proxy staking özelliği başlangıçta kullanılamayacak ve eklenecektir.
platformun geliştirilmesinin sonraki bir aşamasında.
Bir düğümün, fikir birliğini etkileyebilmesi veya ücret ödeyebilmesi için hesabında en azından bazı
hbar'ların olması gerekir.
deftere işlem gönderme ile ilişkili.

Sayfa 36

SAHİP
DÜĞÜM
VEKİL
HİSSE
PROXY HİSSE
DÜĞÜM ÖDEMELERİ
VEKİL ÖDEMELERİ
HİSSE
SAHİP OLANLAR
PROXIED
36
KRİPTOEKONOMİ
Vekil stake etme modeli aşağıda gösterilmiştir.
Bir düğümün fikir birliğine yönelik hissesi,
hem sahip olduğu hem de sahip olduğu hbarları yansıtır
staked ve hbarlar ona vekalet etti.
Bununla ilgili ödemeler
stake etme, düğüm arasında paylaşılacaktır
ve bu vekil stake etme hesapları. İçinde
uygulama, bir düğümün olması bekleniyor

birçok hesap hisselerini buna vekalet ediyor.
Proxy stake etme, düğümleri çalıştırmayanların,
hbar'larının bir düğümün oyuna göre ağırlığı. Ağ, bu uygulamayı teşvik ederek işi daha da zorlaştırır.
kötü bir aktörün tüm hissenin üçte birinden fazla nüfuz kazanması için. Ve düğümleri çalıştıranlar,
gelirlerini artırmak için.

Sayfa 37

Ödemeler ve ücretler

Kullanıcılar, kripto para birimi transferi veya ürün ekleme gibi faaliyetler için Hedera platformunu kullanmak için ücret öderler
deftere. Hedera ağı yüksek verimliliğe sahip olduğundan ve çalışma kanıtı gerektirmediğinden, ücretlerin bugün piyasadaki diğer halka açık DLT platformlarının küçük bir kısmı olacağını tahmin ediyoruz.

Hedera defterindeki düğümler, hesaplama, bant genişliği ve depolama kaynakları için tazmin edilir.
fikir birliği oluşturmada ve hizmet sağlamada kullanmak. Birkaç tür ödeme ve ücret vardır:

1.
DÜĞÜM ÜCRETİ - Platformda bir işlemi tamamlamak isteyen bir kullanıcı veya uygulama gönderecektir
tek bir düğüme karşılık gelen işlem, daha sonra bu işlemi gönderecektir
ağa. Bunu yaparken, düğüm az miktarda kaynak ve enerji harcayacaktır.

Düğüm Ücretleri, bu kaynaklar için düğümleri telafi eder ve düğümleri bunu üstlenmeye teşvik eder
kiritik rol. Başlangıçta, Hedera Yönetim Konseyi Düğüm Ücretlerinin miktarını belirleyecek,
ancak Düğüm Ücreti tutarları eninde sonunda belirlenmek üzere her bir düğüme bırakılacaktır. Düğüm ücretleri ödenir
son kullanıcılar tarafından doğrudan kullanıcının işlemini gönderen düğümün hesabına
ağ.

2.
AĞ ÜCRETİ - Ağa bir işlem gönderildikten sonra, işlem ağa iletilir.
herhangi bir dijital imzayı doğrulayan düğümler. İşlem daha sonra iletilir
ağ ulaşırken geçici olarak hafızasında depolayan diğer düğümlere
uzlaşma. Kullanıcılar, bunun için katılan tüm düğümleri telafi eden bir Ağ Ücreti öder
işlem üzerinde fikir birliği hesaplama faaliyeti. Doğrulamak için gerekli kaynaklar
işlem, işlemin ayrıntılarına göre değişebilir, ancak genellikle
işlemin dosya boyutu ve dijital imza sayısı. Ağ Ücretleri kullanıcılar tarafından ödenir
Hedera Hazine hesabına aktarılır ve bu toplanan tutarların bir kısmı daha sonra
Katılımcı düğümlere Düğüm Ödül Ödemeleri olarak günlük olarak dağıtılır.

3.
HİZMET ÜCRETİ - Hizmet Ücretleri, devam eden bakım yükü için düğümleri telafi eder
veya işlemi desteklemek. Örnek olarak, bir dosya depolama işlemi için tüm düğümler
dosyayı sabit disklerinde belirli bir süre ve Hizmet Ücretini depolayacak
bu işlem, dosyanın boyutunu ve depolandığı süreyi yansıtacaktır. Bir
bir akıllı sözleşme işlevinin yürütülmesini talep eden işlem, Hizmet Ücreti olacaktır
bu hesaplamayı gerçekleştirmek için ağ düğümlerinin ihtiyaç duyduğu işlem gücüne dayanır
ve herhangi bir ilişkili depolama yükü, örneğin, sözleşmenin yürütülmesinin sonuçlarının
depolanması.

Hizmet Ücretleri, kullanıcılar tarafından bir Hedera Hazine hesabına ödenir ve bunun bir kısmı
toplanan miktarlar daha sonra her gün katılımcı düğümlere Düğüm olarak dağıtılır
Ödül Ödemeleri.

Üç farklı ücret türü, hangi hesaptan olduklarını gösteren aşağıdaki şemada gösterilmektedir.
alınır ve bunlara eklenir. Müşteriler, düğüm ücretlerini doğrudan istedikleri düğüme öderler
işlemlerini gerçekleştirin. Müşteriler ağ ücretlerini aynı düğüme öderler, ancak bu ücretler
Hedera Hazinesi. Müşteriler hizmet ücretlerini doğrudan Hedera'ya öderler. Tüm ücret ödemeleri,
ağ, ödemeye yetki veren dedikodulu bir işlem üzerinde fikir birliğine varıyor.

Sayfa 38

38

KRİPTOEKONOMİ

Hedera, işlemleri işleyen tüm düğümler adına hizmetleri ve işlem ücretlerini toplar ve hizmetlerin yerine getirilmesi. Hedera, toplanan ücretleri, düğümlere teşvik ödemelerini finanse etmek için kullanır:

DÜĞÜM ÖDÜLÜ ÖDEME - Hedera hesabından düğümlere günde bir kez ödeme yapılır. onları düğüm görevi görmeye teşvik edin. Ödeme alabilmek için, bir düğümün tam gün boyunca çevrimiçi olması gerekir.

Hedera Yönetim Konseyi tarafından tanımlanan eşikler (örneğin, düğümün en az bir her bir olay, bu 24 saatlik süre boyunca turların en az% 90'ına kadar). Bir düğüm, orantılı olarak ödenecek

Stake ettiği kripto para birimi miktarı (hem kendisine aittir hem de başkaları tarafından kendisine vekil verilir).

Ücret modeli, maliyetleri ve riskleri uygun şekilde tahsis etmek için tasarlanmıştır.

Sayfa 39

39

KRİPTOEKONOMİ

En büyük kaynak maliyetleri, hizmet ücretleri ve bu kaynak maliyetleri (örneğin, büyük bir dosyanın depolanması) ile ödenir.

müşteri tarafından uygun ödeme yapılana kadar asla tahakkuk etmez. Örnek olarak, bir müşteri ödemek zorundadır

üzerinde dosyayı oluşturan işlem sırasında 30 gün önceden bir dosyanın saklanması için ağ.

Dedikodu yapmanın ve işlemlerin kendileri üzerinde fikir birliğine varmanın daha küçük kaynak maliyetleri ödenir

ağ ücretleri için. Bir işlemi gönderen düğüm, önce ödeme yapan hesabın

ücretler yeterli kaynağa sahiptir, ancak kısa vadede bakiyenin bu seviyenin altına düşmesi gibi küçük bir risk vardır.

işlemin mutabakata göre işlenmesi için geçen süre. Bu durumda ağ,

kaynakları harcamış, ancak bu çaba için ödeme yapılmayacaktır.

Böylece sistemin her seviyesinde maliyetler ödenir ve ekonomik teşvikler hizalanır.

Bir istemci, bazı hizmetleri gerçekleştirmek için ağa bir işlem göndermeye yardımcı olması için bir düğümle iletişim kurduğunda

müşteri için, müşteri işlem için bir işlem ücreti parametresi şart koşar - bu maksimum değerdir Müşterinin talep edilen hizmet için ödemeye razı olduğu miktar.

Düğüm, çeşitli işlemlerin tutarlarını belirlemek için işlemi analiz ederek bir ön kontrol gerçekleştirir. ağ kaynakları (bant genişliği, CPU, depolama, vb.) ilişkili hizmetin gerektireceği ve bunları çoğaltır. Toplam işlem ücretini belirlemek için yayınlanmış bir ücret çizelgesindeki katsayılara göre miktarlar. Düğüm

hesaplanan bu işlem ücretini müşterinin öngörülen maksimum işlem ücretiyle ve

işlemin ağa gönderilmesi gerekip gerekmediğini belirlemek için müşterinin bakiyesi.

İşlem gönderildikten sonra, tüm düğümler bunu mutabakat sırasına göre işler, işlemi hesaplar ücret, müşteri hesabının hala yeterli bakiyeye sahip olup olmadığını belirleyin ve varsa, işlemi mutabakat devleti ve son olarak ücretleri yukarıda açıklandığı gibi işleme koyun.

Ücretler, düğümün bir işlemi doğru bir şekilde göndermesini teşvik eder, aksi takdirde ödeme yapılmaz.

Hizmet ücreti, yalnızca hizmetin gerçekleştirilmesi durumunda ödenir, böylece müşteriye yönelik risk minimum düzeydedir. Ve çünkü

hizmet yalnızca ödeme gerçekleşirse gerçekleştirilir, Hedera ağı için bir risk yoktur.

Sayfa 40

Ölçeklendirme Yol Haritası
Aşağıdakiler, ağın konsantre düğümlerden büyümesini beklediğimiz aşamalardır ve
yaygın düğümler ve kazık için risk. Bu aşamalar farklı olmayacak, ancak beklenenleri temsil edecek
ağın evrimi ve para birimi.

FAZ 1

Madeni paraların çoğunu Hedera Hazinesi elinde tutuyor ve Hazine "vekaletname" yapmaya
başlayacak.
Hedera Konseyi Üyeleri tarafından yönetilen düğümlere "madeni paralar". Bazı madeni paralar
Hedera Hazinesi, ağda kullanılmak üzere genel nüfusa da dağıtılacaktır.
Hedera tarafından sağlanan cüzdan yazılımını kullanan kişiler, madeni paralarını da
Konsey Üyesi tarafından yönetilen düğümler.

FAZ 2

Hedera Yönetim Kurulu Üyelerine ek olarak, diğer güvenilir taraflar da
düğümleri ayağa kaldırabilir. Hedera Treasury ve Hedera tarafından sağlanan cüzdan yazılımı
kullanılır
hbar sahipleri tarafından (varsayılan olarak) hem Konsey Üyesi düğümlerine hem de
bu ek güvenilir düğüm operatörleri. Zamanla madeni paraların dağılımı
daha fazla sayıda düğüme daha geniş bir şekilde yayılır. Daha fazla para olmaya devam ediyor
Hedera Hazinesinden ağ kullanıcılarının genel nüfusuna dağıtılır.

3. AŞAMA

İlgilenen bireyler bir Müşterini Tanı sürecinden geçebilir ve ardından
ayrıca düğümleri ayağa kaldırın ve Hedera Hazinesinden ve varsayılan olarak jetonların stake
edilmesini alın
Hedera cüzdan yazılımı. Hedera'dan daha fazla para dağıtılmaya devam edecek
Genel nüfusa Hazine. Anonim kişiler düğümleri çalıştırmaya başlayabilir ve
vekil ile stake edilen paraları alır. Hedera Hazinesi ve Hedera cüzdan yazılımı,
bu anonim düğümlere proxy paraları, ancak bu düğümler proxy
3. taraf cüzdan yazılımından paralar.

4.AŞAMA

Madeni paralar geniş çapta dağıtıldıkça ve rakip cüzdan yazılım programları ortaya çıktıkça,
Hedera Yönetim Konseyi'nden bağımsız, vekil madeni paralar için bir pazar olacak.
Sonunda tüm madeni paralar geniş çapta dağıtılır, bir cüzdan yazılımı pazarı vardır ve
vekil staking için rekabet eden düğüm pazarı.
Bu şekilde, tüm madeni paralar Hedera Hazine hesabında ve ilk Hedera cüzdan yazılımında başlar.
varsayılan olarak sadece Hedera Yönetim Konseyi üyelerine vekaleten verilir. Ancak zamanla her iki
madeni para
ve proxy kullanımı, milyonlarca düğüme dağıtılıncaya kadar daha geniş ve daha geniş bir dağıtım elde
eder ve
hesaplar.

Sayfa 41

TEŞEKKÜRLER
Teşekkür
Danışmanlarımız Natalie Furman'ın katkılarını ve yardımlarını minnetle kabul ediyoruz,
Tom Trowbridge, Edgar Seah, Jordan Fried, Christian Hasker, Arlan Harris, Paul Bugeja, Alex
Godwin,
Ken Anderson, Patrick Harding, Zenobia Godschalk, George Samman, Sam Brylski, Tom Sylvester ve
Rachel Epstein.

ve kaynaklar uygun ve güvenilir kabul edilir, ancak bunların doğruluğu veya
tamlık.
Bu belge bir menkul kıymet teklifi veya satışı teşkil etmez. Herhangi bir teklif veya satış yalnızca şuna göre gerçekleşir:
kesin teklif belgeleri.
Bu belgede öngörüldüğü şekliyle proje geliştirme aşamasındadır, değiştirilebilir ve olmayabilir
tüm yargı bölgelerinde mevcut olmalıdır. Başarıyla ilgili hiçbir beyan veya garanti verilmez veya
herhangi bir planın, gelecekteki projeksiyonların veya beklentilerin makul olup olmadığı. Bu belge herhangi bir
herhangi bir tavsiye veya teklife herhangi bir amaçla güvenilmemelidir. Bu belge İngilizce olarak düzenlenmiştir
sadece. Herhangi bir çeviri yalnızca referans amaçlıdır ve Hedera Hashgraph, LLC veya herhangi biri
tarafından onaylanmamıştır.
Diğer kişi. Bu belgenin İngilizce versiyonu, herhangi bir tutarsızlık ölçüsünde geçerlidir.
tercüme. Lütfen gerekli her türlü profesyonel tavsiyeyi alın.

Sayfa 42

4 2
Ekler
EKLER

Sayfa 43

4 3
Ek 1: Takım
EKLER
DR. LEEMON BAIRD, KURUCU KURUCU, CTO VE BAŞ BİLİMCİ
Leemon, hashgraph dağıtılmış fikir birliği algoritmasının mucididir,
ve Hedera'nın Kurucu Ortağı ve Baş Bilim Adamıdır. 20 yılı aşkın
teknoloji ve başlangıç deneyimi, Profesör olarak görev yaptı.
ABD Hava Kuvvetleri Akademisi'nde ve kıdemli bir bilim insanı olarak Bilgisayar Bilimi
birkaç laboratuvarda. Aşağıdakiler de dahil olmak üzere çeşitli girişimlerin Kurucu Ortağı olmuştur.
her ikisi de satın alınan iki kimlik ile ilgili girişim. Leemon
Doktora derecesini Bilgisayar Bilimleri alanında Carnegie Mellon Üniversitesi'nden aldı.
ve hakemli dergilerde birden fazla patenti ve yayını vardır ve
bilgisayar güvenliği, makine öğrenimi ve matematikte konferanslar.
MANCE HARMON, KURUCU VE CEO
Mance, deneyimli bir teknoloji yöneticisi ve girişimcidir.
çok uluslu alanda 20 yıldan fazla stratejik liderlik deneyimi
şirketler, devlet kurumları ve yüksek teknoloji girişimleri ve Co-
Hedera'nın kurucusu ve CEO'su. Önceki deneyimi,
Ping Identity'de Mimarlık ve Laboratuvar Başkanı, iki şirketin Kurucusu ve CEO'su
1,7 milyar ABD doları gelirle ürün güvenliğinden sorumlu üst düzey yönetici olan teknoloji girişimleri
organizasyon, çok büyük ölçekli bir yazılım programı için Program Yöneticisi
Füze Savunma Ajansı adına Siber Güvenlik Kurs Direktörü
ABD Hava Kuvvetleri Akademisi'nde ve Makine Öğrenimi alanında araştırma yapan bilim insanı
Wright Laboratuvarı'nda. Mance, Bilgisayar Bilimi alanında MS aldı.
Massachusetts Üniversitesi ve Bilgisayar Bilimleri alanında Lisans derecesi
Mississippi Eyalet Üniversitesi.
NATALIE GRUNFELD FURMAN, GENEL MÜŞAVİR
Natalie, Hedera'nın Genel Danışmanıdır. Önceden kıdemliydi
Paul Hastings LLP'de, pratiğinin entelektüel konulara odaklandığı
mülkiyet, haksız rekabet ve mahremiyet ve aleniyet hakları. Önce
hukuk fakültesi, kariyerine Silikon Vadisi'nde başladı ve stratejik

yüksek teknolojili girişimlere tavsiyeler. Strateji ve İşletme Direktörü idi
Bir çevrimiçi grup iletişimi başlangıcındaki geliştirme,
Yahoo! Inc. ve bir teknoloji için İş Geliştirme Direktörü
küresel bir işbirliğine dayalı tedarik zinciri platformu geliştiren girişim. Natalie
Lisans derecesini Antropoloji dalında Stanford Üniversitesi'nden onur derecesi ile aldı.
ve Columbia Üniversitesi Hukuk Fakültesi'nden doktorası.

Sayfa 44

CHRISTIAN HASKER, PAZARLAMA BAŞKANI

Christian, kurumsal yazılım alanında yirmi yıllık deneyime sahiptir.
pazarlama dahil olmak üzere girişimlerde ve büyük şirketlerde çeşitli roller,
ürün yönetimi, ürün pazarlaması ve satış yönetimi ve
Hedera'nın Pazarlama Direktörüdür. Önceden yardımcıydı ...
DataStax'ta Pazarlama Başkanı, sorumlu olduğu yer
geliştirici eğitimi ve açık kaynak Apache Cassandra topluluğu
hiper büyüme dönemindeki girişimler. Doğuştan bir İngiliz, Christian'ın
Manchester Üniversitesi ve London College of
Müzik.

LIONEL CHOCRON, BAŞ ÜRÜN SORUMLUSU

Lionel, 20 yılı aşkın deneyimiyle deneyimli bir ürün yöneticisidir.
kurumsal ürünleri pazara sunma ve bunları geliştirme deneyimi
Hedera'nın Baş Ürün Sorumlusu. O katılır
Oracle, Endüstri ve Gelişen Teknolojiden Sorumlu Başkan Yardımcısı olarak,
ve gelişmekte olan teknoloji (Blockchain, IoT, AI) çözüm çabalarına öncülük etti.
endüstriler. Bundan önce, Başkan Yardımcısı ve Genel Müdür olarak görev yapmıştır.
Cisco, Cisco'nun hızla büyüyen
Nesnelerin İnterneti (IoT) işi. Daha önce AT'de rol aldı.
Kearney, Bain & Company ve BNP Paribas. Lionel, UC'den MBA derecesine sahip
Berkeley's Haas School of Business, McGill'den Mühendislik Yüksek Lisansı
Ecole des Mines Üniversitesi'nden Mühendislik alanında lisans derecesi.

MEHERNOSH (NOSH) MODY, KIDEMLİ BAŞKAN YARDIMCISI, MÜHENDİSLİK

Nosh, mühendislik müdürü olarak 25 yıllık deneyime sahiptir ve
teknoloji yöneticisi ve Mühendislik Kıdemli Başkan Yardımcısıdır
Hedera. Önceden Trend Micro'da Ar-Ge Direktörü olarak görev yaptı.
TippingPoint, geliştirme ve yenilikten sorumlu
TippingPoint Saldırı Önleme Sistemleri. Trend Micro'dan önce,
Britestream Networks dahil olmak üzere çok sayıda girişimde Ar-Ge'yi yönetti
ve Coretrace Corp. Nosh, Texas Üniversitesi'nden bir MBA ve
Massachusetts Üniversitesi'nden Bilgisayar Bilimleri Yüksek Lisansı.

Sayfa 45

ATUL MAHAMUNI, ÜST BAŞKAN YARDIMCISI, ÜRÜN

Atul, ürün yönetimi konusunda uzun yıllara dayanan deneyime sahiptir ve
Hedera Ürününün Kıdemli Başkan Yardımcısı. Önceden yardımcıydı-
Blockchain SaaS Uygulamaları ve Nesnelerin İnterneti (IoT) SaaS Başkanı
Uygulamalar, Oracle'da PaaS Platformu. Bundan önce üründe görev yaptı
Cisco, Juniper Networks'de yönetim, strateji ve geliştirme rolleri,
ve Nokia.

ZENOBIA GODSCHALK, KIDEMLİ BAŞKAN YARDIMCISI, KURUMSAL İLETİŞİM

Zenobia, yüksek teknoloji PR ve yardım konusunda 20 yılı aşkın deneyime sahiptir.

şirketler yeni kategoriler oluşturur ve bunlara hükmeder ve Kıdemli Başkan Yardımcısıdır.
Hedera Kurumsal İletişim Başkanı. Daha önce, öyleydi
yatırım bankası Morgan Keegan'da satış tarafı analisti.
The Wall Street Journal'ın 1 Numaralı Yazılım Analisti ekibinin bir parçası.
Bundan önce, kurumsal iletişim başkanı olarak görev yaptı.
Marc Andreessen ve Ben tarafından kurulan Opsware, Inc. (NASDAQ: OPSW)
HP tarafından 1.6 milyar dolara satın alınan Horowitz. Zenobia mezun oldu
Stanford Üniversitesi Ekonomi ve Psikoloji alanında lisans ve
Endüstri Mühendisliği.

JORDAN FRIED, KIDEMLİ BAŞKAN YARDIMCISI, İŞ GELİŞTİRME

Ürdün bir DLT müjdecisidir ve kendini kanıtlamış bir kripto-kapitalisttir ve
Hedera'nın İş Geliştirmeden Sorumlu Kıdemli Başkan Yardımcısı. O oldu
daha önce Buffered VPN'in Kurucu Ortağı ve CEO'suydu, en hızlı büyüyen
2017 yılının ilk çeyreğinde satın alınan çevrimiçi kişisel VPN hizmeti. Ürdün,
Hive.org ve Buffer App gibi şirketlerde yatırımcı ve
Entrepreneur Magazine, Inc.com, Wired.com, Time Magazine'de yer aldı,
ve Success.com.

EKLER

ASYA PASİFİK BÖLGESİ BAŞKANI EDGAR DENİZİ

Edgar, erken aşama teknoloji şirketlerinde melek yatırımcı ve
Hedera için İş Geliştirmede Asya Pasifik Bölgesi. O oldu
eski Varlığa Dayalı Ticaret ve Sendikasyon Başkanı ve Eş Başkanı
Asya için Bank of America Merrill Lynch'te Varlığa Dayalı Menşei. Sonra
Bu, Eğitim Fırsatı Sponsorları başlatmak için Gana'da yaşadı.
Afrika, gelir getiren, kar amacı gütmeyen bir liderlik geliştirme programı
genç Afrikalılar için. Edgar, lisans derecesini Carnegie Mellon Üniversitesi'nde (Phi
Beta Kappa).

BRETT MCDOWELL, YÖNETİCİ, YÖNETİM KONSEYİ

Brett, 20 yılı aşkın BT endüstrisi koalisyon deneyimini beraberinde getiriyor ve
Hedera Yönetiminin Kurucu İcra Direktörü ve Başkan Yardımcısı
Konsey. Kantara Girişimi'nde kurucu yönetici rolleri vardı.
IDESG, DMARC.org ve FIDO Alliance'ta halen danışman olarak görev yapmaktadır.
Ek olarak, çok paydaşlı kapsamlı bir yönetişim deneyimine sahiptir,
MAAWG, NCSA yönetim kurulunda veya danışma kurulunda görev almış,
StopBadWare ve PCI SSC, diğer endüstri koalisyonları arasında. Brett bir
UMASS Dijital Yönetim Merkezi'nde bir ABD üyesi
Federal Rezerv Bankası'nın Mobil Ödemeler Sektörü Çalışma Grubu ve
InterCon'dan 2019'un En İyi 50 Teknoloji Lideri ödülünün sahibi.

KEN ANDERSON, BAŞ GELİŞTİRİCİ SAVUNUCUSU

Ken, dağıtılmış ekonomi konusunda tutkuludur ve Baş Geliştirici'dir
Hedera'nın savunucusu. 20 yıllık seri girişimci
sistem tasarımı ve yazılım mimarisinde deneyim. O inşa etti
ödüllü mühendislerden oluşan bir ekip ve geçici CTO olarak danışıldı.
yeniden yapılanma dönemlerinde çeşitli şirketler. O da başardı
TM Forum'un REST API tasarım yönergelerine katkıda bulunan, şimdi kullanılıyor
trilyonlarca küresel telekom endüstrisi boyunca. Ken mezun oldu
California Eyaletinden Yönetim Bilişim Sistemleri alanında BBA ile
Üniversite ve Amerika Birleşik Devletleri Ordusunda İstihbarat Çavuşuydu.

Ek 2: Parçalama
Başlangıçta ağ, tek bir parça içinde nispeten az sayıda düğümden oluşacaktır. Ağ olarak büyüdükçe, birden çok parçayı desteklemek için yeterli düğüm kazanır. Bu parçalar şu şekilde çalışacaktır.
Bir işlem her zaman belirli bir parçaya gönderilir. Bir parça içindeki her düğüm bunların hepsini alır shard'ın işlemleri ve her düğüm aynı paylaşılan durumu korur. Her parça, her ikisini de depolayabilir kripto para birimi hesapları ve dosyaları. Her parça akıllı sözleşmeler çalıştırabilir.
Bir parça, işlemleri için bir fikir birliği sırasına ulaşmak için karma grafik fikir birliği algoritmasını kullanır. Her biri
parça, diğer parçaların her birinin fikir birliği kararına güvenebilmelidir. Bu nedenle, her parça rastgele seçilen düğümlerden oluşmalı ve asla güvenilmeyecek kadar büyük olmalıdır.
Kötü niyetli düğümlerin sahip olduğu hisseli kripto para biriminin 1 / 3'üne sahip.
Bir işlem yalnızca belirli bir parça içindeki kaynakları içeriyorsa, o zaman mutabakat sırasındaki nokta ulaşıldığında işlem etkisini gösterir. Örneğin, bir işlem kripto para birimini hareket ettirebilir
aynı parça içindeki iki hesap arasında. Veya bu parça içindeki bir dosyayı kaydedip bunun için ödeme yapabilir
o kırıkta bir hesap. Bu durumlarda, kripto para birimi transferleri veya dosya, şu adreste hemen depolanır:
mutabakat sırasına göre işlemin gerçekleştiği nokta.
Bir işlem farklı parçalarda kaynakları içeriyorsa, parçalar arası mesajları tetikleyecektir. İçin Örneğin, kripto para birimi hesabı Alice Shard Alpha'da ise ve Bob hesabı shard Beta'da ise, o zaman Alice, kripto para birimini Alice'den Bob'a taşımak için bir işlem oluşturur ve imzalar. O gönderiyor Alfa parçasındaki bir düğüme işlem ve Alpha'daki tüm düğümler, siparişin sırası konusunda fikir birliğine varır. Şurada
mutabakat sırasında bu olayın meydana geldiği noktada, Alice'in hesap bakiyesi miktar kadar azaltılır gönderilir ve Beta parçasına bir mesaj oluşturulur. Her parça bir giden kuyruğu tutar
diğer kırıkların her birine gönderilecek mesajlar. Böylece bu yeni mesaj, Alpha'nın
Mesajların Beta'ya gönderilmesini sağlar. Belirli bir kuyruktaki her mesajın 64 bitlik bir sıra numarası vardır,
ağ ilk oluşturulduğunda sıfırdan başlar ve daha sonra gönderilen her yeni mesajla birlikte artar.
Her Alpha üyesi, rastgele aralıklarla, giden herhangi bir mesajda herhangi bir mesaj olup olmadığını kontrol edecektir.
kuyruklar ve kuyruklardan birini göndermeye çalışın. Amaçlanan mesajların olduğunu gördüklerinde Beta, rastgele bir Beta üyesini çağıracaklar ve onlara sıradaki tüm mesajları,
bu kuyruğun Alpha için mevcut imzalanmış durumunun bir parçası olduğunun kanıtı.
Bir Beta üyesi, Alpha üyesinden böyle bir mesaj listesi aldığında, Beta üyesi
Beta'ya, mesajların ve bunların imzalamanın bir parçası olduklarının kanıtı olan bir işlem gönderir durum. Zaten bir mesajın gönderildiğini görürlerse, tekrar göndermezler, ancak
bazen aynı mesaj aynı anda iki kez gönderilebilir. Bu durumda dizi
sayılar eşleşecek, böylece kopya yok sayılacak ve herhangi bir zarar verilmeyecektir.
EKLER

Sayfa 48

4 8
İki belirli parça arasındaki tüm mesajlar sıra numarası sırasına göre işlenecektir. Alpha ise Beta'ya bir mesaj gönderir ve Beta içindeki bir işleme eklenir, sıra ne zaman kontrol edilir
işlem fikir birliğine varır. Sırayla bir sonraki mesaj ise, etkisi gerçekleştirilir.
hemen. Sıra numarası bir veya daha fazla başka mesajın atlandığını gösteriyorsa, o zaman
hiçbir etkisi yoktur ve dikkate alınmaz. Bu durumda, diğer mesajlar sonunda fikir birliğine varacak ve ardından
atlanan mesaj tekrar gönderilecek ve etkisi olacaktır.
Beta, Alpha'dan beklenen bir sonraki sıra numarasıyla birlikte bir mesajı işlediğinde,
Alfa'dan işlenmiş olan mesajların sayısını artırır. Yani her parça
diğer kırıkların her biri için tek bir numara tutar; bu, ondan en son sıra numarasıdır
işlenmiş diğer parça.

Alpha mesajı Beta'ya gönderdikten sonra, bu mesaj giden sırada kalır ve
defalarca gönderilecek. Sonunda, bir Apha üyesi, göndermek için bir Beta üyesiyle iletişime geçecektir.
bu mesaj, ancak mesajın zaten işlendiğine dair bir kanıt alacaktır. Bu kanıt
imzalı durumun Beta'nın Alpha'dan alınan mesajlar için sıra sayısını içerdiğini ve
sayı artık kuyruktaki mesajdan daha yüksek. Bu noktada, Alpha üyesi
bir işlemde kanıtlar ve dedikoduları Alpha'ya iletir. Mutabakat sırasına ulaştığında, bu noktada mesaj, paylaşılan durumda giden sırasından silinir.
Alice'den Bob'a kripto para transferi örneği için "kesinlik" var diyebiliriz
Transferin geçerli olduğunu, Alice'in yeterli paraya sahip olduğunu ve Bob'un kesinlikle alacağını bildiğimizde
para kaynağı. Bu aktarım Ayşe'nin Bob'dan bir ürün satın alması için ise, o zaman kesinlik, zamanın olduğu bir noktadır.
Bob'un ürünü Alice'e vermesi için güvenlidir. Kesinliğe kadar geçen süre aslında fikir birliği süresi kadar kısadır.
tek bir parça. Bu ilk işlem üzerinde fikir birliğine varıldığında, Alpha'nın
Beta'ya bir mesaj gönderirseniz, bu Beta onu işleyecek ve Bob'un hesabının transferi alacaktır. Yani kesinlik, fikir birliği kadar hızlıdır.
Bir kaynak hesaptan iki hedef hesaba transfer ise, kesinlik yine de aynı hızdadır. Yakında
ilk işlem fikir birliğine vardığında, yeterli paraya sahip olup olmadığı ve
iki mesaj gönderilecektir.
Ancak, tek bir işlem iki kaynak hesaptan bir hedef hesaba aktarılacaksa ve
kaynak hesaplar farklı parçalardaysa, kesinlik daha yavaş olacaktır. Çünkü dahil etmesi gerekecek başka bir mesaj türü: "bekletme", daha sonra bir "bırakma" izler.
Örneğin, alfa parçasındaki Alice'den 2 jeton ve 3 jeton transfer etmek için bir işlem oluşturulduğunu varsayalım.
Bob'dan Beta parçasında, 5 jeton Gama parçasında Gina'ya aktarılıyor. Bu olması amaçlanmıştır atomik, böylece Alice ve Bob transfer için yeterli paraya sahip olmadıkça hiçbir şey olmayacak.
Bunu başarmak için, işlem hem Alice hem de Bob tarafından imzalanmalı ve
Alfa parçası. Fikir birliğine ulaştığında, Alice'in hesabında 2 jeton üzerinde "bekletme" yapılmasına neden olur.
Bu, hesabın 2 madeni parasının geçici olarak dondurulduğu anlamına gelir. Donmuş haldeyken Alice hala özgür
para almak ve para aktarmak, ancak bakiyesini azaltacak herhangi bir transfer yapamamak
2 madeni paradan daha azına.
EKLER

Sayfa 49

4 9
Alpha, Alice için 2 jeton tutarken aynı zamanda Beta'ya bir mesaj göndererek bir
Bob için 3 jetonluk. Alpha'dan geldiği için bu mesajın Bob tarafından imzalanmasına gerek yoktur.
ve Alpha, Bob'un işlemi imzaladığını zaten kontrol etti.
Mesaj alındığında ve fikir birliğine vardığında, Beta, Bob'un hesabını bekletmeye çalışacaktır.
3 jeton için. Yeterli parası varsa başarılı olur. 3'ten az bozuk parası varsa başarısız olur ve bekletilmez ona hiç. Beta daha sonra Alpha'ya beklemenin başarılı olup olmadığını belirten bir mesaj gönderir.
Alpha, tutmanın başarılı olduğuna dair bir yanıt aldığında, Alpha, Alice'in hesabını 2 düşürür.
jeton (bu aynı zamanda tutmayı da kaldırır), Beta'ya Bob'un hesabını 3 düşürmesini söyleyen bir mesaj gönderir.
jetonlar (tutucusunu kaldırır) ve Gina'nın hesabını 5 jeton artırmak için Gamma'ya bir mesaj gönderir.
Öte yandan, Beta'nın mesajı, Bob'un yeterli jetonu olmadığı için bekletmenin başarısız olduğunu söylüyorsa, o zaman
Alpha, Alice'in hesabındaki bekletmeyi kaldırır ve tüm işlemin başarısız olduğunu düşünür.
Üç dengeden hiçbiri değişmez.
Tüm bunlar Alpha'nın ilk işlemi gerçekleştirmesiyle başladığında, Alpha'nın
tüm sürece kaç mesajın dahil edileceğini hesaplayın, bu örnekte 4 mesaj. Alfa

bu nedenle, işlemin ücretini içeren bir hizmet ücretinin yetkilendirilmesini içerdiğini kontrol edecektir.
bu 4 mesajı gönderme hizmeti. Hedera daha sonra otomatik olarak düğümlere ödeme yapar.
işlenen (ve yineleme olarak göz ardı edilmeyen) her bir ileti hareketini oluşturdu. Bu davranır
düğümlerin diğer parçalara mesaj gönderme işini yapması için teşvik olarak
onlardan alındı ve bu mesajları ve onayları içeren işlemlerin oluşturulması.
EKLER

Sayfa 50

5 0
Ek 3: Mutabakat Hizmeti
EKLER

Sayfa 51

Öz
Consensus Service kavram kanıtı kullanım örneği, özel Hyperledger Fabric ağları sağlıyor
ihtiyaç duyulmadan blok zinciri işlemlerinin geçerliliği ve sırası konusunda merkezi olmayan fikir birliği ile
RAFT 1 veya Kafka 2 yapılandırmak için
sipariş hizmeti. Ek kullanım durumları şunları içerir, ancak bunlarla sınırlı değildir:
finansal piyasalar, eşleşen motorlar (Uber veya AirBnb'de kullanılanlar gibi) veya tedarik zinciri görüşmeleri
(örneğin, birkaç rakip parça tedarikçisinin parçaları için teklif veren birkaç rakip fabrika).
Hedera Mutabakat Hizmeti, dağıtılmak üzere mesajların adil sırasını senkronize eder.
merkezi bir saate güvenmeden sistemler.
1 "Bir RAFT Sipariş Hizmetini Yapılandırma ve Çalıştırma,"
https://hyperledger-fabric.readthedocs.io/en/release-1.4/raft_configuration.html
2 "Bir Kafka Sipariş Hizmeti Getirmek,"
https://hyperledger-fabric.readthedocs.io/en/release-1.4/kafka.html
DAĞITILMIŞ BİR LEDGER'DA TÜMÜ
AĞ KAYITLARI VE ONAYLARI
HER İŞLEM.
51
EKLER

Sayfa 52

Giriş
Hedera Consensus Service, ilk Dağıtılmış Defter Teknolojisi (DLT) ağ hizmetidir.
yalnızca olayların geçerliliğini ve sırasını ve zaman içindeki olayların geçmişine şeffaflık sağlamak
kalıcı bir işlem geçmişi gerektirmeden. Sonuç olarak, Hedera Mutabakat Hizmeti
hızlı, adil ve güvenli bir fikir birliğinin faydalarını diğer tüm halklardan daha düşük bir maliyetle sağlar
dağıtılmış defter ağı.
Finansal hizmetler, IoT veya tedarik zincirinde olsun - olayların zamanlaması ve sırası her şeyi belirler
finansal işlemlerden anlamlı varlık kaynağına. Uygulamalar mantık yürütmelidir
belirli bir zamanda, belirli bir sırada meydana gelen olaylara dayanır. Çoğu durumda,
Bu uygulamaların, denetimden her şey için bu siparişin geçmişine zamanında geri bakması gerekir.
uzlaşmaya.
Günümüzde bu uygulamalar, tek bir varlık tarafından gerçekleştirilen denetleme, eşleştirme ve sıralamaya dayanmaktadır.
Bu, onları ağ kesintisine yatkın hale getirir 3 , az sayıda tarafın gizli anlaşması riski altında 4 ve
merkezi altyapı sağlayıcılarının maliyet modeline tabidir 5 . Özel dağıtılmış defter bile
ağlar, geri kalanına fikir birliği sağlamak için bir veya birkaç taraf tarafından işletilen düğümlere güvenir.

ağ 6 . Her yaklaşım, kasıtsız olarak maliyet ve operasyonel risk nedeniyle ekonomik risk oluşturmaktadır.
hizmet kesintisi veya kasıtlı manipülasyonu.
Dağıtılmış defter alanında, protokoller bu sorunu provizyon yoluyla çözmeyi amaçlamaktadır.
iki özellik:
1 Olayların geçerliliği ve düzeni konusunda merkezi olmayan fikir birliği.
2 Zaman içindeki olayların geçmişine şeffaflık.
İlk değer, bir olayın meydana geldiği zaman üzerinde anlaşmaya varacak düğümlerin varlığına dayanır,
nihayetinde zaman içindeki olaylar için bir fikir birliği düzeni üretir. R3'ün Corda'sı gibi dağıtılmış defterler,
Hyperledger Fabric veya Ethereum'un kurumsal sürümü, bilinen ve güvenilir düğümleri dağıtır kurumlar tarafından işletiliyor, siparişi sağlamak için tek bir tarafa güveniyor veya yavaş ve pahalı halka güveniyor
İş kanıtı aracılığıyla bir blok üreticisi seçmek için Bitcoin veya Ethereum gibi defterler 7 . Başvurular bir işlemin kesinliğinin onaylanması için dakikalar hatta saatler beklemeye zorlanabilir. Orada uzlaşmayı merkezileştirmeye gerek kalmadan dağıtılmış ve hızlı bir uzlaşma için pazar ihtiyacıdır süreç.
Şirketler İçin '12 Saatlik Soruna' Neden Olan 3 Gps Hatası
Chris Baraniuk - https://www.bbc.com/news/technology-35491962
4 Bozuk Yönetişim? Son Eos Skandalı Hakkında Bildiklerimiz
Stephen O'Neal - https://cointelegraph.com/news/corrupt-governance-what-we-know-about-recent-eos-scandal
5 Cloud Pub / sub | Google Cloud
https://cloud.google.com/pubsub/
6 Sipariş Hizmeti¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer/ordering_service.html ve Noterler¶
7 "Son araştırmalar, PoW tabanlı blok zincirlerinin performansının geliştirilemeyeceğini gösteriyor güvenliklerini etkilemeden ”- https://eprint.iacr.org/2016/555.pdf

---

Sayfa 53

8 Bitcoin Blockchain Boyutu 2010-2019 | İstatistik
https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/
İkinci değer, herhangi bir bireyin veya kuruluşun bağımsız olarak olup olmadığını ve ne zaman olduğunu doğrulama becerisidir.
bir olay meydana geldi. Bu, çoğunlukla token hesap bakiyelerini izlemek veya
bir varlığın menşei. Geleneksel blok zincirleri, tüm olayların depolanmasına dayanır.
ağ. Bu model, hesap bakiyelerinin basit bir şekilde sorgulanmasına izin verir, ancak performansı 10-20 ile sınırlar
tps ve defterin büyümeye devam edeceği anlamına gelir (tek başına bitcoin, yazım tarihi itibariyle 200 GB'ın üzerindedir
bu kağıt). 8
Hedera, merkezi olmayan konsensüsün optimize edilmiş performansını sağlamak için benzersiz bir çözüm sunar
Hedera hükümleri aracılığıyla zaman içinde işlem geçmişini sürdürmeye gerek kalmadan
Mutabakat Hizmeti. Hedera Mutabakat Hizmeti, Hedera genel ağını ve temelini kullanacaktır.
Doğrulamayı kaldırırken hızlı, adil ve güvenli fikir birliği için karma grafik fikir birliği algoritması ve Mirror Network kullanan bilgisayarlara farklı uygulamalar için depolama gereksinimleri.

Sayfa 54

Hedera Yönetişimi
ve Ademi Merkeziyetçiliğe Giden Yol
Hedera kamu ağı, bir ölçekte merkezi olmayan hizmetler sunmak için sıfırdan inşa edilmiştir.
kurumsal ve tüketici uygulamaları için gereklidir. Bu, ağın tam ademi merkeziyetçiliğini içerir
operasyonlar, yüksek performans ve garantili kesinlik.
Merkeziyetsizleştirme
Hedera kamu ağı, 39 dönem sınırlı, çok sektörlü ve
ağın istikrarını ve büyümesini sağlamak için çok bölgeli büyük işletmeler. Başlangıç olarak hareket ediyorlar
Düğüm işleminden önce düğüm operatörleri, uzun vadede herkese açık hale gelir. Bu, ağın kendisinin
ve sağladığı hizmetler, küçük bir grubun arzusu üzerine hile veya manipülasyona eğilimli değildir.
varlıklar veya madenciler. Bu, doğal afet kurtarma ile çoklu bulut / çoklu veri merkezi hizmeti olarak işlev görür
ve herhangi bir uygulama tarafından kullanılabilen yüksek kullanılabilirlik. Hedera Mutabakat
Hizmeti şunları sağlar:
tek bir bulut sağlayıcısına güvenmek yerine merkezi olmayan bir ağda işlem siparişi verme veya
küçük grup özel düğüm operatörleri.
Verim
Verimlilik, bugün merkezi olmayan genel ağların çoğunda darboğaz oluşturmaya devam ediyor. Hashgraph
% 100 kesinlik ile daha hızlı fikir birliği sağlar ve liderleri seçmeye gerek kalmadan
düğümlerin alt kümesi veya herhangi bir şekilde ağın güvenliğini tehlikeye atabilir. Hedera
Konsensüsü
Hizmet, bir başvuru tarafından sunulan herhangi bir işlem türü için bu avantajı
genişletecektir. Uzlaşma
her biri on ila yüzbinlerce işlemi işlerken birkaç saniye içinde gerçekleşir.
ikinci. Bu performans düzeyi, tüm ölçeklendirilmiş tüketici veya kurumsal uygulamalar için gereklidir.
MERKEZİLEŞTİRME
VERİM
SONUÇ

Sayfa 55

Son olarak, ana ağ tarafından oluşturulan sıra kesindir ve doğrulanabilir. Mutabakat zaman damgaları açık
Hedera ana ağı, Eşzamansız Bizans hatası nedeniyle oluşturulduktan sonra% 100 kesindir
Hoşgörü (ABFT) doğası. Bu, belirli bir işlemin zaman damgasının nihai olduğu ve
değişiklik. Herhangi bir istemci uygulaması, kayıt için ağı sorgulayabilir (
mutabakata eklenen işlemle ilgili önemli bilgileri yakalamak için düğümler) ve isteğe bağlı olarak
karşılık gelen bir durum kanıtı isteyin (kriptografik olarak güvenli ve kalıcı bir iddia)
kaydın doğruluğuna göre ağ) bu zaman damgasını onaylamak için. Ek olarak, Konsensüs
Hizmet işlemleri, ek yazılım çalıştıran ayna düğümlerinde depolanacaktır. Kullanıcılar yansıtmayı çalıştırabilir
düğümlerin kendileri, durum provaları için bir yansıtma düğümünü sorgulayın veya birden çok ayna arasındaki kayıtları doğrulayın
tek bir düğüm operatörüne güvenmeye gerek kalmadan tam siparişi doğrulamak için düğümler.
ikinci. Bu performans düzeyi, tüm ölçeklendirilmiş tüketici veya kurumsal uygulamalar için gereklidir.
Kesinlik

Sayfa 56

Adil İşlem Sırası

Hashgraph'ın birincil işlevi, merkezi olmayan bir ortamda adil bir işlem sırası hesaplamaktır.
çevre. Başlıca farklılaştırıcılardan biri, bireylerin veya küçük grupların
siparişi manipüle etmekten alıkonuldu, adaleti sağladı. 9
Hedera halka açık defter, hashgraph fikir birliği algoritmasını ve HBAR kripto para birimini kullanarak
başlangıçta üç hizmet sağlar: Cryptocurrency, Smart Contract ve File Service. Hashgraph kullanır
Ağın zaman damgası üzerinde fikir birliğine varması için dedikodu ve sanal oylama hakkında dedikodu yapmak
herhangi bir varlık veya grup etrafında merkezileştirmeden bant genişliği kullanımının etkinliğine sahip herhangi bir olayın
varlıklar. Hbarlar, madeni paranın herhangi bir sahibinin, tarafından sağlanan hizmet için ödeme yapmasını sağlayan ağ parasıdır.
ağ ve ayrıca stake etme süreci boyunca ağın güvenliğini sağlar (bağlama etkisi
sanal oylama dahilinde tutulan jeton miktarına).
Hedera düğümleri arasındaki dedikodu, hangi düğümün gönderildiğine bakılmaksızın aynı hızda gerçekleşir
işlem ve belirli bir işlem için daha fazla ödeme yapılarak artırılamaz. Bu farklı
uygulamaların işlemlerinin olması için daha fazla ödeme yapmasına izin veren diğer genel ağ modelleri
önce işlenir. Benzer şekilde, fikir birliğinde liderler kavramı olmadığından,
düğümler, fikir birliği düzenini kendi lehlerine gereğinden fazla etkilemek için işbirliği yapabilir.
İşlemler ağa yayılır ve birkaç saniye içinde nihai mutabakata varılır. Eğer
bir uygulama, tek bir düğümün işlemi geri kalanına göndermekten alıkoyması konusunda endişeleniyor.
ağ daha sonra birden fazla düğüme gönderebilirler. Bu senaryoda yalnızca ulaşılacak ilk işlem
fikir birliği korunacak ve diğerleri göz ardı edilecektir.
Hedera'nın Diğer Hizmetleri
Hedera, ademi merkeziyetçiliğin değerini herhangi bir uygulama oluşturucuya ifşa etmek için üç ilk hizmet oluşturdu:
1 Cryptocurrency: aralarında düşük maliyetli ve hızlı bir değer aktarım yöntemine erişin
aracılara güvenmeden hesaplar. Cryptocurrency Hizmeti kullanılabilir
ödeme uygulamaları, veri satın alımları ve güvenilen diğer birçok kullanım durumu için
hızlı değer aktarımı.
2 Akıllı Sözleşmeler: bir güvenmeye gerek kalmadan kodu belirleyici olarak yürütün.
uygulama operatörü. Adil pazarlar oluşturun, belirteçleri yayınlayın ve iş mantığını programlayın
Sağlamlık ve güvenilir güvenlik ve adil siparişten yararlanmak için Hedera'da dağıtın.
3 Dosya Hizmeti: herhangi bir düğüm veya kullanıcının erişmesi veya
verilerin durumunun mutabakat zaman damgasından yararlanmak için karmaşıklaştırılmış verileri depolayın
zamanın bir noktasında. Merkezi olmayan kayıtlar, kayıtlar ve diğer herkese açık veriler oluşturun
Dosya Hizmetinde.
9 https://www.hedera.com/whitepaper

Sayfa 57

Bu hizmetler, büyük işletmelerin, bağımsız geliştiricilerin ve tüketicilerin
endüstriler ve coğrafyalar genelinde uygulamalar. Ortak olarak SDK'lar aracılığıyla tüketilebilirler
programlama dilleri ve her türden uygulamayı desteklemesi amaçlanmıştır.
Mutabakat Hizmetini Genişletmek
Mutabakat Hizmeti, işlemlerin tam geçmişini yaymak için başka bir özelliğe ve
birçok katılımcı için sonuçlar: ayna ağı. Consensus Service tarafından sipariş edilen mesajlar
ayna düğümleri tarafından alınır. Geliştiriciler, her biri için ek yazılım uygulamayı seçebilirler.
ayna düğümü. Bir yansıtma düğümü, belirli konular için tüm mesajları depolayabilir (tanımlayıcılar
bir mesajı belirli bir uygulama veya ağ ile ilişkilendirme). Tüm mesajları saklayabilir (dizeleri

belirli bir işlemi temsil eden baytlar). Veya tüm işlemlerin kayıtlarını bile depolayabilir.
defterde fikir birliğine vardı. Her şey depolanırsa, benzer bir şey oluşturabilir.
Hedera defteri asla bu geçmişi tutmasa da geleneksel blok zinciri.
Hedera ayna ağı (mirrornet), durumu yaymaya adanmış paralel bir ağdır.
Hedera ana ağı (ana ağ). Bu yayılma, gereksiz eklenmeden gerçekleştirilir.
ana ağı zorlayın. Ve gelecekte herkes bir ana ağ düğümünü barındırabilecekken, yansıtma düğümleri işletmelerin Hedera'nın işlevselliğini ana ağ üzerinde ciddi bir etki yaratmadan genişletmesine izin verir.
Mirrornet, aynı gereksinimleri ve çoğunu koruyan bir düğümler kümesidir.
ana ağın işlevselliği. İşlevsellikteki temel fark, ayna düğümlerinin
fikir birliğine katılmak. Ana ağdan bilgi alırlar ancak bilgi göndermezler
ona. Ayna düğümleri, diğer ayna düğümleriyle dedikodu yapmaya devam eder ve fikir birliğini hesaplayıp doğrulayacaktır.
imzalar, ancak ana ağ üzerinde hiçbir etkisi yoktur. Bu nedenle gönderemezler
mutabakat için işlemler ve oylama gücü yok. Yansıtma düğümleri, yalnızca okunabilir düğümler olarak düşünülebilir.
bu işlemler Hedera API aracılığıyla bir ayna düğüme gönderilemez. Yansıtma düğüm operatörleri
Hedera, bu ağ hizmetlerini, adaleti getiren dördüncü bir hizmetle genişletir.
Hashgraph fikir birliği algoritması tarafından Hedera Consensus Service'e sağlanır.
Bu hizmet mesajları alır ve onlara fikir birliği zaman damgaları atar ve
fikir birliği düzeni.
AYNA
DÜĞÜMLER
101010
010101
101010
101010
010101
101010
101010
010101
101010
57
EKLER

Sayfa 58

geliştirdikleri yeni hizmet türlerini sağlamak için ek API'ler geliştirmekte özgürdür. Beta
yansıtma düğümlerinin sürümü Mayıs 2019'da daha fazla gecikmeyle (örneğin bir dakika) tamamlandı, ancak
tam yansıtmalı düğümlerin gecikme süresi saniye olacaktır.
Consensus Service'ten yararlanan bireyler veya özel ağlar tarafından işletilen yansıtma düğümleri, belirli bir konuya sahip işlemler için olayları ve kayıtları filtreleyebilir ve alabilir. Yapacaklar
daha sonra uygulamalarıyla ilgili olayların tam geçmişini saklayabilirler.
58
EKLER

Sayfa 59

HEDERA AĞI
HEDERA HASHGRAPH
KRİPTO PARA
HİZMET
AKILLI SÖZLEŞME
HİZMET
DOSYA

HİZMET
UZLAŞMA
HİZMET
HEDERA SDK
Mimari
Bu bölüm, Hedera genel ağındaki Mutabakat Hizmetinin mimarisini açıklayacaktır.
Mutabakat Hizmetinin, aralarında ve arasında birlikte çalışabilirliği nasıl sağlayabileceğine dair genel bir bakışla
Hyperledger Fabric tabanlı herhangi bir ağ.
Hedera Consensus Hizmet Mimarisi
Hedera Mutabakat Hizmeti, Hedera tarafından sağlanan dördüncü temel hizmettir. Diğer hizmetler gibi,
Mutabakat Hizmeti, ortak programlamada çok sayıda SDK aracılığıyla açığa çıkarılacaktır.
diller ve protobuf kullanan Hedera API (HAPI). Bu, uygulamaların
hem SDK soyutlamalarını hem de daha düşük seviyeli API'leri kullanan ağ hizmetleri.
İstemci uygulaması bir mesaj (bir bayt dizisi) gönderir ve ona bir konu (bir kimlik numarası) verir.
mesaj, bir finansal varlığa teklif gibi bir işlemin ilgili ayrıntılarını veya hatta
yalnızca başka bir yerde depolanan verilerin karması. Konu, aynı konudaki mesajların
birlikte sınıflandırılır. Müşteri uygulaması, hbar cinsinden bir işlem ücreti ödeyecektir.
Konsensüs Hizmetinin kullanımı.
Hedera kamu defteri, fikir birliğine varıldığını belirten bir kayıt döndürecektir.
ulaşıldığı zaman damgası ve verilen konu için olayın sıra numarası. Sekans
numara, uygulamanın mesajın sırasını diğer mesajlara göre yorumlamasına izin verir
aynı konuyla. Sonuç, o konu için şimdiye kadarki tüm mesajların çalışan bir karmasını da içerecektir. Bir
çalışan hash, o konu için şimdiye kadarki tüm mesajların parmak izi görevi gören birkaç bayttır.
Konular, HAPI tarafından tanımlanan bir işlemin yürütülmesi ile oluşturulur ve bu, konunun
oluşturuldu, sahibin anahtarları belirlenecek, konuya mesaj gönderebilecek veya konu silebilecek olanların anahtarları
belirtilecek ve konunun ID numarasını döndürecektir.
Şekil 1A: Kamusal Ağ

Sayfa 60

Uygulamada, Konsensüs Hizmetinin bir grup ayna düğüm operatörü ve kullanıcısı tarafından kullanılmasını bekliyoruz.
özel veya tescilli verileri işleyen, ancak hızlı olandan yararlanan bir uygulamadan yararlananlar
sipariş verme, merkezi olmayan güven ve bir kamu düzeni hizmetinin değişmez kaydı.
Ağı kurmak için, kuruluşlar bir veya daha fazla yansıtma düğümü yapılandıracak,
üzerinde istemci uygulamaları ve anahtarlara sahip olanların bunu yapmasına izin veren bir veya daha fazla anahtar yapılandırın.
grubun ne yaptığını görün. Grup ayrıca, tanımlamak için kullanabilecekleri bir konu da tanımlayacaktır.
grupları ile ilgili işlemler. Bu konu, istemcinin gönderdiği mesajlara eklenecektir.
uygulama Hedera genel ağına gönderilecektir.
Şekil 1B: İşlem Sipariş Süreci
Yukarıdaki şekil Hedera Konsensüs Hizmetine bir işlem gönderme sürecini özetlemektedir.
İstemci uygulaması, Hedera SDK'yı kullanarak bir işlem oluşturacak ve
mesaj ve konu. Mesaj, bir eylemi açıklayabilir veya sadece bir karma içerebilir veya başka herhangi bir
istemci uygulamasıyla ilgili bayt dizisi. Her uygulamanın bir veya daha fazla konu kullanması gerekecektir.
Diğer Hedera ağ hizmetleri gibi, işlem de tek veya birden fazla ana ağa gönderilebilir
düğümler. Ana ağ düğümü, işlemin gerekli bilgilere (imzalar) sahip olup olmadığını kontrol edecektir.

ödeme, girdiler) ve müşteri uygulamasına işlemin sahip olduğu bir alındı bildirimi iade edin
ön kontrol ile tanıştı. Aşağıda örnek bir işlem gösterilmektedir:
MÜŞTERİ
UYGULAMA
SDK
ARAYÜZ
MAINNET
DÜĞÜM
AYNA
DÜĞÜM
İstemci uygulaması
işlemi gönderir
bir mesajla
ve konu.
1
Hedera düğümü
ön kontrolü döndürür
onay.
2
Hedera düğümü dedikoduları
ağa olay.
3
Hedera ağı belirler
olayın düzen ve fikir birliği zaman damgası.
4
Hedera düğümü ile işlem kaydı oluşturur
yük, konu, sipariş ve fikir birliği zaman damgası.
5
Yansıtma düğümü dinler
belirli bir konunun kayıtları.
6
Yansıtma düğümü ayrıştırır
ödeme detayları
düzen oluşturmak için.
7
İstemci uygulaması
ayna ile iletişim kurar
mantık tabanlı yürütmek için düğüm
işlem emri üzerine.
8

Sayfa 61

13
Ana ağ düğümü, ağın geri kalanına olayı dedikodu yaparak ağın
karma grafik konsensüs algoritmasını kullanan olay için bir fikir birliği zaman damgası. Daha sonra bir kayıt olacak
mesaj, konu, sıra, çalışan karma ve fikir birliği zaman damgasını içeren oluşturulur.
Mutabakat zaman damgası, ulaşıldıktan sonra% 100 nihai haldedir ve genellikle birkaç saniye içinde ulaşılır.
Ayna düğümü, tüm bilgileri ana ağdan alır ve bu nedenle işlemi öğrenir.
ve konsensüs zaman damgalarıyla birlikte, çalışan bir hash ile birbirine bağlanmış fikir birliği düzeni. Ayrıca

üçüncü bir tarafa, söz konusu kişi için alınan mesajların tam listesini kanıtlayabilecek durum kanıtları oluşturun.
konu ve hangi sırayla ve hangi zaman damgalarıyla.
Ayna düğümü, uygulamanın iş mantığını uygulayan yazılımı çalıştırır. Alacaktı
sipariş edilen bir işlemin sonuçları ve eşleşen teklifler gibi sonuçları uygulamaya döndür ve
bir borsada sorar, menkul kıymet jetonlarını hesap sahipleri arasında aktarır veya durumu günceller
bir nakliye ve lojistik sağlayıcısı için iyi.
Bu özellik, Cryptocurrency Hizmetini kullanmaya benzer bir performans ve maliyet profiline sahip olacaktır.
(İşlem başına <0,001 ABD doları). Kesinliğe birkaç saniye içinde ulaşılır.
Uygulama, hem ayna ağının hem de Hedera kamu ağının dağıtımından yararlanır.
Herhangi bir kullanıcı bir veya birden fazla yansıtma düğümünden kayıt alabilir ve durum provalarını kontrol edebilir 10
bunu onaylamak için
ana ağ, bu fikir birliği zaman damgası ve bir işlemin sırası üzerinde anlaştı. Bu gerçek bir
doğru şeyi yaptığını doğrulamak için yansıtma düğümünün zaman denetimi. Ayrıca herhangi bir kullanıcı bir yansıtma düğümü çalıştırabilir ve
sırayla ve doğru sonuçlar hakkındaki gerçeği hemen öğrenecekti.
Hyperledger Fabric Birlikte Çalışabilirliği
Hedera Consensus Service kavram kanıtı kullanım senaryosu, özel Hyperledger Fabric sağlar
blockchain işlemlerinin geçerliliği ve sırası konusunda merkezi olmayan fikir birliğine sahip ağlar
bir RAFT 11 veya Kafka 12 yapılandırma ihtiyacı
sipariş hizmeti.
Hyperledger Fabric, düzenleyici adı verilen bir tür düğüm içerir ("sipariş verme" olarak da bilinir)
node ”), diğer düğümlerle birlikte bir **sipariş hizmeti** oluşturan bu işlem sıralaması yapar .
Fabric'in tasarımı **deterministik** fikir birliği algoritmalarına dayandığından, bir eşin doğruladığı herhangi bir blok
sipariş hizmeti tarafından üretilen nihai ve doğru olduğu garanti edilir. 13 Teşvik etmeye ek olarak sonluk, zincir kod çalıştırma onayını (eşlerde gerçekleşen)
sipariş, Fabric'e performans ve ölçeklenebilirlik açısından avantajlar sunarak
yürütme ve sıralama aynı düğümler tarafından gerçekleştirildiğinde ortaya çıkar.
Hyperledger Fabric v1.4.1'den itibaren yeni olan Raft, bir çökme hatası toleranslı (CFT) sipariş hizmetidir.
Raft protokolünün etcd'de uygulanması. Raft, bir liderin
düğüm seçilir (kanal başına) ve kararları takipçiler tarafından kopyalanır. 14
10 Durum Kanıtı: Ağın çoğunluğundan kriptografik olarak güvenli, taşınabilir bir iddia
fikir birliğine giren bir işlem veya sonuçlanan durum hakkında bazı gerçeklere göre düğümler
11 Bir Sal Sipariş Hizmetinin Yapılandırılması ve Çalıştırılması¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/raft_configuration.html
12 Kafka Tabanlı Bir Sipariş Hizmeti Getirmek¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/kafka.html
13 Sipariş Hizmeti¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer/ordering_service.html
14 Sipariş Hizmeti¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer/ordering_service.html

---

Sayfa 62

RAFT'nin kurulması ve yönetilmesi Kafka tabanlı sipariş hizmetlerinden daha kolaydır (diğer bir seçenek de
Hyperledger Fabric), hala iki dezavantajı var:
1 Yapılandırma Karmaşıklığı: Yapılandırma sürecinde birbiriyle ilişkili dört adım vardır.
Hyperledger Fabric sipariş düğümü 15'i ve yeni bir
bir Raft kümesine düğüm. 16

2 Bizans Hata Toleransı: Bir Bizans hatası, bileşenlerin
kötü niyetli davranmak. Ağın kendisinin olabileceği durumu bile içerir.
bir saldırgan tarafından kontrol edilebilir. 17
Raft, Fabric'in
Bizans hataya dayanıklı (BFT) sipariş hizmeti, ancak Bizans hatası değil
bugün hoşgörülü. 18
KUMAŞ FİŞİ
& KUMAŞ ŞARKILARI
MAINNET
DÜĞÜMLER
AYNA
DÜĞÜMLER
Bildir
4
Düğümler arasındaki işlemlerin dedikodusu
ana ağ ve ayna düğümleri ile
fikir birliği zaman damgası hesaplanıyor
ve devlet kanıtı üretme.
2
1
MÜŞTERİ
UYGULAMA
SDK
ARAYÜZ
Onaylanan yayınlar
Hedera düğümüne mesajlar
seçim (veya rastgele)
Siparişi herkese yayınla
kayıtlı Eşler. Eşler şunları yapabilir:
herhangi birine veya çoğuna kayıt ol
ayna düğümleri.
3
Fabric ağ üyeleri tarafından çalıştırılır
Konsey / halk tarafından yönetilir
Bizans - Hyperledger Fabric ağı
Hedera'nın ABFT doğasını hatırlıyor
mainnet, çünkü herhangi bir Fabric eşi,
herhangi bir ana ağ veya ayna ile iletişim kurun
ağ düğümü. Kötü niyetli olmayan herhangi bir düğüm,
aynı sicile ve devlet kanıtına sahip olmak
bir işlem için. Kötü niyetli düğümler
hemen görünür hale gelir çünkü
kayıtları çelişecektir.
Bu nedenle, yalnızca bir ayna ağı düğümü
sistemin çalışması için
dürüst ol.
Şekil 1C: Hyperledger Yapısı / Hedera Konsensüs Hizmeti Birlikte Çalışabilirliği
Hedera Mutabakat Hizmeti, küresel, hataya dayanıklı ve uygun maliyetli hale getirecek bugün inşa edilen herhangi bir Hyperledger Fabric ağı için sipariş servisi mevcuttur. 19
15 Sipariş Düğümü Kurma¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer_deploy.html
16 Bir Sal Sipariş Hizmetinin Yapılandırılması ve Çalıştırılması¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/raft_configuration.html
17 Bizans Fayı
https://en.wikipedia.org/wiki/Byzantine_fault

18 Sipariş Hizmeti¶
https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer/ordering_service.html
19 Giriş
https://hyperledger-fabric.readthedocs.io/en/release-1.2/whatis.html

---

Sayfa 63

Önceki sayfadaki şema, herhangi bir Hyperledger'ı etkinleştirmek için mimariyi göstermektedir.
Hedera Konsensüs Hizmetini kullanmak için kumaş ağı. Bunu yaparken, Hyperledger Fabric ağı
şunları yapabilir:
Hedera kamu ağının Bizans doğasını miras alır.
1. adımda, müşteri uygulaması Hedera ağına onaylanmış bir mesaj yayınlayacaktır.
işlem, Hyperledger Fabric meslektaşları tarafından onay politikası kullanılarak onaylanmış olacaktır.
İstemci uygulaması, işlemi herhangi bir ana ağ düğümüne veya hatta birden fazla ana ağ düğümüne
gönderebilir.
işlemin ağa gönderildiğine dair daha yüksek bir güven derecesi ister.
İşlem, herhangi bir bayt dizisi olarak geçirilebilir (işlemin hash değeri, benzersiz işlem
id, vb.) ve işlemi belirli bir gruba ait olarak tanımlayan bir konu içerecektir.
Kumaş ağı. İşlem daha sonra Hedera ağından bir fikir birliği zaman damgası alır,
sipariş edilmek üzere hazırlanıyor.
Ayna düğümleri, fikir birliği zaman damgasını hesaplamak için ana ağ düğümlerinden de dedikodu
alırdı.
ve kendileri bir devlet kanıtı oluştururlar. Bir veya daha fazla ayna düğüm daha sonra siparişi bir
Hyperledger Fabric Peers'in kayıtlı kümesi. Bu işlemler daha sonra yapılandırılır ve saklanır
ile ilgili sıralı işlemlerin kurcalamaya karşı korumalı zincirini oluşturmak için çalışan bir karma
kullanmak
Kumaş ağı.
Herhangi bir Yapı eşi, herhangi bir ana ağ veya ayna ağ düğümü ile iletişim kurabilir. Kötü niyetli
olmayan herhangi bir düğüm,
bir işlemin aynı kayıt ve durum kanıtına sahip olmak. Kötü niyetli düğümler ortaya çıkacak
hemen çünkü geçerli durum kanıtları sağlayamayacaklardı.
Hedera Mutabakat Hizmeti, herhangi bir Fabric ağına işlem sipariş etme yeteneği sağlar.
tek tek veya çalıştırılması gerekmeyen küresel bir düğüm ağı kullanarak yüksek verim
Fabric ağının üyeleri tarafından güveniliyor. Bu, Fabric tabanlı işletim maliyetini düşürecektir.
çözümler, veri merkezi kesintilerine karşı dayanıklılığı artırın ve kimin olduğunu belirleme ihtiyacını
ağ başına özel Fabric sipariş hizmetlerini çalıştırır.

Sayfa 64

işlemlerinin tanımlanmasını zorlaştıracak konular.
Kullanım Örneği
Bir Fabric ağ güvenlik belirteci örneğini ve ardından bir
Hedera'nın kullanımını göstermek için bu yazıda merkezi olmayan borsa
Konsensüs Hizmeti çalışıyor.
Özel Ağ Jetonu İhracı
Hyperledger Fabric tabanlı özel bir ağ, aralarında menkul kıymetler ticareti için bir token verebilir.
düzenlenmiş endüstriler. Bu, belirli bir
yalnızca izinli yatırımcıların varlığı satın alabileceği veya takas edebileceği mülk.
Üyeler veya ağ yöneticisi bir konu oluşturur ve konu kimliğini herkese iletir.
ağ üyeleri, böylece hem ağı hem de jetonu tanıyabilirler.
ilişkili işlem. 20
A kullanıcısı bir belirteci B kullanıcısına aktardığında, istemci uygulaması otomatik olarak

işlem kimliğini belirtin ve doğru olanı belirlerken bir işlemin ileti yükünde gönderin.
konu. İşlem, kullanıcının müşteri uygulaması tarafından imzalanacak ve Hedera'ya gönderilecektir.
genel ağ.
Kayıt, mesajın siparişiyle birlikte iade edildiğinde, istemci uygulaması,
kullanıcılar arasında aktarım, şimdi işlemin ne zaman yapıldığına dair adil ve nihai bir fikir birliği
zaman damgasına sahip
oluştu. Uygulama, geniş ölçekte hangi transferlerin önce geleceğini ve hangilerinin
zaman damgalarına bağlı olarak geçersiz olabilir. Kullanıcılar yansıtma düğümünü veya
Ana ağ, belirli bir işlemin kaydını onaylamak için doğrudan veya daha fazla bakmak için yansıtma düğümlerini kullanın
Uygulamanın doğru bir şekilde dağıtıldığından emin olmak için zamanında geri dönün.
Aynı ağ, ağlar arasında güvenlik belirteçlerinin atomik değişimini de destekleyebilir. Kullanıcı söyle
Bir jeton 2 için jeton 1 ticareti yapmak için bir anlaşmaya varıldı, bir jeton düzenlenmiş ve başka bir düzenlemeye tabi tutulmuş
ağ ve şu anda kullanıcıya ait C.
Jetonları değiş tokuş etmek için, her kullanıcı her ağda bir katılımcı olacaktır. Bu kullanım durumunda bu gerekli olabilir çünkü her iki ağ da yatırımcıların
doğrulandı.
Her bir belirteç, daha sonra her ağda konuşlandırılan akıllı bir sözleşmede kilitlenir.
Hedera genel ağındaki bir işlemden hem kullanıcılardan gelen imzalar hem de bir zaman damgası. Her biri
kullanıcı, bir tarafından tetiklendiğinde jetonları yeni sahibine aynı anda açmayı (aktarmayı) kabul edecektir.
Hedera Konsensüs Hizmetine gönderilen ve bir mutabakat zaman damgası ile iade edilen işlem.
20 Ağın farklı gizlilik gereksinimleri vardır. Bazı ağlar dönüşümlü veya daha anonim kullanmayı seçebilir
64
EKLER

Sayfa 65

https://www.npr.org/2014/04/01/297686724/on-a-rigged-wall-street-milliseconds-make-all-the-difference
Fabric-Hedera mimarisi, özel bir ortamda izinli varlık ticaretinin faydalarını sağlar.
ağ ve Hedera kamu ağının merkezi olmayan güveni ve değişmezliği. Kullanıcılar yapar
işlem emrinin merkezi bir tarafça manipüle edilmesi konusunda endişelenmenize gerek yoktur ve hizmetin bağımsız düğümlerden kaynaklanan kesinti sürelerini sürdürebileceğine dair güven.
Hisse Senedi Piyasası Siparişi
Hisse senedi piyasaları tipik olarak finansal firmaların bir milisaniye elde etmek için milyonlar harcamasına neden olan davranışları teşvik eder.
tekliflerini iletmeleri veya borsaya talep etmeleri için geçen süre açısından avantaj sağlar. 21
Bu
Bazı firmaların finansal bir ilerleme sağlamak için diğerlerini ön plana çıkardığı kötü niyetli davranışları teşvik eder.
Hedera üzerine inşa edilen borsalar, tüm piyasa katılımcılarına adalet sağlayacaktır.
Bir borsa, jetona benzer şekilde özel bir ağda bir uygulama olarak oluşturulabilir
ticaret kullanım durumu yukarıda veya doğrudan bir ayna düğümünün veya bir dizi ayna düğümünün üstünde. Bu ayna
düğümler, ana ağdan mesaj almalarına izin veren yazılımı çalıştırır.
fikir birliği zaman damgası ve düzen. Sadece ilgili konuyla ilgili gönderilen mesajları dinleyebilirler.
borsa üstüne inşa edildi.
Uygulamanın bir kullanıcısı teklifini sunacak veya Hedera Konsensüs Hizmetine
rastgele bir işlem kimliği kullanarak anonimleştirilmiş bir şekilde veya düz metin teklif veya talep olarak. Mesaj
belirli bir pazara veya hatta varlık sınıfına ait olduğunu tanımlayan bir konu dahil edin.
Mesaj bir fikir birliği emri ve zaman damgası alacak ve tek kişiye veya

borsayı çalıştıran çoklu ayna düğümleri. Ayna düğümleri yalnızca
Depolama yükünü azaltmak için doğru konuya sahip mesajlar. Yerel bir veritabanı
sıralı mesajlarla yapılandırılmıştır.
Uygulama, teklifleri eşleştirmek için bu veritabanını kullanabilir ve fikir birliğine dayalı olarak sorabilir.
verimli ve adil bir hisse senedi piyasası işletmek için zaman damgaları.
Bir kullanıcı bir ana ağ düğümüne güvenmiyorsa, kullanılan bu düğüm yerine bir veya daha fazla başka düğüme gönderebilir.
tek bir doğruluk kaynağı tarafından darboğazla karşılaşmak. Bir kullanıcı bir yansıtma düğümüne güvenmiyorsa, o kullanıcı
ondan bir durum kanıtı isteyebilir veya işlemlerin kayıtları için başka herhangi bir ayna düğümünü isteyebilir ve hatta
kullanıcılar seçerse ana ağdan bir durum kanıtı isteyin. Kullanıcılar yansıtma düğümünü bile çalıştırabilir
ayrıca borsa sonuçlarını doğrulamak için kendileri.
Herhangi bir dürüst düğüm, doğru ve diğerinin yanlış olduğunu kriptografik olarak kanıtlayabilir.
21 'Hileli' bir Wall Street'te Milisaniyeler Farkı Yaratıyor

Sayfa 66

Bu kullanım durumundaki yalancılar (kullanıcılar, ikiz düğümler) hemen gösterilecektir çünkü iki düğümün sonuçları
birbirleriyle çatışacak. Bu kötü niyetli kullanıcıların genel fikir birliğini etkilemesinin önündeki engel aynı zamanda halka açık bir ağın kullanılmasıyla süreç çok daha yüksektir. Tek bir varlık (veya hizalanmış bir grup)
Fikir birliğini somut olarak etkilemek için var olan tüm hbarların en az 1 / 3'üne ulaşması gerekir. İçinde
daha küçük özel ağlar bu engel, hem daha az katılımcı hem de daha az katılımcı olması nedeniyle daha düşüktür.
Proof-of-stake güvenlik mekanizması.
Büyük olasılıkla borsa uygulamalarının yukarıdaki mimariye gizlilik katması muhtemeldir.
bazı bilgiler gizlidir. Bu durumda uygulama, mesajı şifreleyebilir ve
Hedera'ya. Sadece uygun taraflar mesajı okuyabilirken, Hedera sadece
bazı mesajların işlendiğini bilin.
Uygulama daha sonra teklifleri ve talepleri karşılaştırmadan önce anahtarını kullanarak mesajın şifresini çözer.
Bu, borsa için gerçek mahremiyet sağlar.

Sayfa 67

Ek Fırsatlar
Önceki iki kullanım durumu, yalnızca Hedera Konsensüsünün potansiyel kullanım durumlarının yüzeyini çiziyor
Hizmet. Yolculuk selamlama uygulamaları, hizmeti gerçek anlamda bir taksi talebi ile arzı eşleştirmek için kullanabilir.
zaman. Tedarik zincirleri, varlık transferleri için doğru ve adil bir zaman damgası elde etmek için hizmeti kullanabilir
tedarik zinciri boyunca. Parça üreticileri, hizmeti malların gerçek zamanlı işlemleri için kullanabilir. IoT
Üreticiler, sensörlerden okunan veriler üzerinde fikir birliği zaman damgası almak için hizmeti kullanabilir
Dünya çapında.

Hedera Mutabakat Hizmeti, uygulama oluşturucular kutusunda, yararlanma için başka bir araç sağlar.
ademi merkeziyetçiliğin gücü.

Sayfa 68

Sonuç
Hedera Mutabakat Hizmeti, hızlı, adil, güvenli ve merkezi olmayan fikir birliğinin değerini
herhangi bir uygulama - özel defter tabanlı olsun ya da olmasın. Kuruluşlar ve bireyler ihraç edebilir
ve ticaret yapabilir
Herhangi bir uygulama için işlemlerin adil küresel sıralanmasını kullanarak özel defterler arasındaki
belirteçler.
Hedera Mutabakat Hizmeti, özel ağları işletme maliyetini düşürür,
hem gizlilik hem de ölçeklenebilirlik ve hem özel defterler hem de özel defterler için güven modelini
geliştirir
merkezi sunucular.
Diğer Hedera ağ hizmetlerinde olduğu gibi, Mutabakat Hizmetinin değeri en çok
her boyutta veya odakta kuruluştan geliştiriciler tarafından ağ üzerinde oluşturulan çeşitli uygulamalar
tarafından.
Uzun vadede bu, ortak bir hizmetten yararlanan birbirine bağlı uygulamalar ağını etkinleştirecektir.
Kullanıcı tabanları içinde ve arasında işlemlerin sıralanması.

Sayfa 69

6 9
Ek 4: Hashgraph

Sayfa 70

SWIRLDS HASHGRAPH KONSENSUS ALGORİTMASI:
FUAR, HIZLI, BİZANS HATA TOLERANSI
LEEMON BAIRD
31 MAYIS 2016
SWIRLDS TECH RAPORU SWIRLDS-TR-2016-01
Öz. Yeni bir sistem olan *Swirlds hashgraph fikir birliği algoritması* pro-
garantili Bizans hata toleransı ile çoğaltılmış durum makineleri için pozlandı.
Bir saldırganın manipüle etmesinin zor olması anlamında *adalet* sağlar.
mutabakatta ilk olarak iki işlemden hangisinin seçileceğini belirlemek
sipariş. Tam bir eşzamansızlığa sahip, lider yok, turnuva sırası yok, kanıtı yok.
iş, birinci olasılıkla nihai fikir birliği ve yokluğunda yüksek hız
hataların. Katılımcıların yapmadığı bir dedikodu protokolüne dayanmaktadır.
sadece işlemler hakkında dedikodu yapın. Bunlar *dedikodu hakkında dedikodu* . Birlikte inşa ediyorlar
tüm dedikodu olaylarını yansıtan *hashgraph* . Bu Bizans anlaşmasına izin verir
sanal oylama yoluyla elde edilecek . Alice, Bob'a oy göndermez
internet. Bunun yerine Bob, Alice'in göndereceği oyu hesaplar.
Alice'in bildiklerine dair bilgisi üzerine. Bu adil bir Bizans anlaşması sağlar
çok az iletişim ek yükü ile tüm işlemler için toplam siparişte
işlemlerin ötesinde.
Anahtar Kelimeler: Bizans, Bizans anlaşması, Bizans hata toleransı, tekrarlanmış
devlet makinesi, adil, adalet, karma, dedikodu hakkında dedikodu, sanal oylama, Swirlds
İçindekiler
Şekiller Listesi

1. Giriş
2
2. Temel kavramlar
4
3. Dedikodu hakkında dedikodu yapın: hashgraph
5
4. Konsensüs algoritması
6
5. Bizans hata toleransının kanıtı
12
6. Adillik
19
7. Genellemeler ve geliştirmeler
20
8. Sonuçlar
24
Referanslar
25
9. Ek A: İşlevsel formda fikir birliği algoritması
26
1 Revizyon tarihi: 16 Şubat 2018
1
70
EKLER

Sayfa 71

Şekiller Listesi
1
Yönlendirilmiş bir grafik olarak dedikodu tarihi
5
2
Karma grafik veri yapısı
7
3
Güçlü bir şekilde görmenin illüstrasyonu.
8
4
Sözde kod: Swirlds hashgraph fikir birliği algoritması
11
5
Sözde kod: divideRounds prosedürü
12
6
Sözde kod: karar verme prosedürü
13
7
Sözde kod: finalOrder prosedürü
14
1. Giriş
Dağıtılmış veritabanlarının çoğu zaman, aşağıdakilerle çoğaltılmış durum makineleri olması gerekir: Bizans hata toleransı. Bazı yazarlar "Bizans" terimini zayıf bir
saldırganların gizlice işbirliği yapmayacağını veya iletişimin
zayıf asenkron [1]. Bu yazıda "Bizans" kuvvetli

orijinal tanımının anlamı [2]: üyelerin yaklaşık 1 / 3'üne kadar
saldırganlar, gizlice işbirliği yapabilir ve dürüst olanlar arasındaki mesajları silebilir veya geciktirebilirler.
mesajda sınır tanımayan üyeler gecikir. Saldırganlar,
Dürüst bir üye varsa, herhangi bir zamanda herhangi bir mesajı geciktirmek ve silmek için şebeke
art arda başka bir üyeye mesajlar gönderirse, saldırganların sonunda izin vermesi gerekir
bir üzerinden. Güvenli dijital imzaların mevcut olduğu varsayılmaktadır, bu nedenle saldırganlar
tespit edilemeyecek şekilde mesajları değiştirir. Güvenli hash fonksiyonlarının mevcut olduğu varsayılmaktadır.
hangi çarpışmalar asla bulunamayacak. Bu makale Swirld'leri önermekte ve tanımlamaktadır.
hashgraph mutabakat algoritması ve Bizans hata toleransını kanıtlar.
güçlü tanım.
Hiçbir deterministik Bizans sistemi tamamen eşzamansız olamaz.
FLP teoremi [3] ile sınırlı mesaj gecikmeleri ve hala fikir birliğini garanti eder.
Ancak kesin olmayan bir sistemin problemlerle fikir birliğine varması mümkündür.
yetenek bir. Karma grafik fikir birliği algoritması tamamen eşzamansızdır,
belirsizdir ve olasılık bir ile Bizans anlaşmasına ulaşır.
Paxos [4] veya Raft [5] gibi bazı sistemler, onları
Bir saldırgan, web sitesinde bir hizmet reddi saldırısı başlatırsa, büyük gecikmelere karşı savunmasızdır.
mevcut lider [6]. Çoğu sistem tek bir kötü istemci tarafından bile geciktirilebilir
[7]. Aslında, ikinci makale, bu tür güvenlik açıklarına sahip sistemlerin
"Bizans fayı" yerine "Bizans fayı hayatta kalabilir" olarak tanımlanmalıdır.
hoşgörülü". Hashgraph konsensüsü bir lider kullanmaz ve inkar etmeye dirençlidir.
üyelerin küçük alt kümelerine hizmet saldırıları.
Bitcoin gibi diğer sistemler, iş kanıtı blok zincirlerine dayanmaktadır [8]. Bu
yukarıdaki tüm sorunlardan kaçınır. Ancak bu tür sistemler Bizans olamaz çünkü
bir üye, ne zaman fikir birliğine varıldığını asla kesin olarak bilemez; sadece sahipler
zamanla artmaya devam eden bir güven olasılığı. İki blok mayınlıysa
eşzamanlı olarak, bu durumda zincir, topluluk hangi
genişletmek için şube. Bloklar yavaş eklenirse, topluluk her zaman
daha uzun dalı eklerseniz, sonunda diğer dal büyümeyi durdurur ve
"bayat" olduğu için budanmalı ve atılmalıdır. Bu anlamda verimsizliğe yol açar

---

Sayfa 72

bazı blokların düzgün bir şekilde çıkarıldığını, ancak yine de atıldığını. Aynı zamanda bunun anlamı topluluğun yapabilmesi için blokların ne kadar hızlı çıkarıldığını yavaşlatmak için gereklidir.
dalları, yeni dalların filizlenmesinden daha hızlı budayın. Bunun amacı budur
işin kanıtı. Madencilerin zor hesaplama problemlerini çözmelerini talep ederek
bir blok çıkarmak için, tüm ağın yeterince uzun olmasını sağlayabilir
ortalama olarak madencilik etkinlikleri arasındaki gecikmeler. Hashgraph fikir birliği algoritması
"zincir" in sürekli dallara ayrıldığı bir blok zincirine eşdeğer,
hiçbir bloğun bayat olmadığı ve her madencinin yapmasına izin verilen herhangi bir budama
iş kanıtı olmadan ve% 100 verimlilikle saniyede çok sayıda yeni blok madencilik yapın.
İş kanıtı blok zincirleri, elektriğin ekstra bilgisayarlarda boşa harcanmasını da gerektirir.
ve belki de o pahalı madencilik teçhizatı satın alınabilir. Süresi dolan bir süre kanıtı
sistem [9] boşa harcanan elektriği önleyebilir (belki de madencilik maliyeti olmasa da)
kuleler), sanki uzun süre geciken güvenilir donanım yongaları kullanarak
iş kanıtı hesaplamaları yapmak. Ancak bu, tüm katılımcıların
çipi oluşturan şirkete güvenin. Çip satıcılarına böyle bir güven, bazılarında var
FreeBSD'nin yalnızca güvenmemek için değiştirildiği durumlar gibi diğer durumlarda değil

güvenli rasgele sayılar için donanım RDRAND komutunda, çünkü "biz
onlara artık güvenemiyorum ”[10].
Bizans anlaşma sistemleri, Bizans anlaşması için geliştirilmiştir.
yukarıdaki sorunlardan kaçının. Bu sistemler genellikle birçok mesajı değiş tokuş eder
üyelerin oy kullanması. For *n* üyeleri tek EVET / HAYIR soru karar vermek, bazı
sistemler , ağ üzerinden *O* (*n*) mesajlarının gönderilmesini gerektirebilir . Diğer sistemler
gerektirebilir *O* (*n*
2) veya hatta *O* (*n*
3) ikili karara göre ağı geçen mesajlar
[11]. Tek bir EVET / HAYIR kararı için bir algoritma daha sonra karar vermeye genişletilebilir
oy trafiğini daha da artırabilecek bir dizi işlem için toplam sipariş.
Hashgraph, tüm oylama sanal olduğu için ağın her yerine oy göndermez.

Sayfa 73

2. Temel kavramlar
Karma grafik fikir birliği algoritması aşağıdaki temel kavramlara dayanmaktadır.
• *İşlemler* - herhangi bir üye herhangi bir zamanda imzalı bir işlem oluşturabilir. Herşey
üyeler bunun bir kopyasını alır ve topluluk Bizans anlaşmasına varır
bu işlemlerin sırasına göre.
• *Adalet* - küçük bir grup saldırganın haksız yere
Konsensüs olarak seçilen işlemlerin sırasını etkiler.
• *Dedikodu* - bilgi, her üyenin bir başkasını tekrar tekrar seçmesiyle yayılır
üye rastgele ve onlara bildikleri her şeyi anlatmak
• *Hashgraph* - kimin kime ve kime dedikodu yaptığını kaydeden bir veri yapısı
Hangi düzen.
• *Dedikodu hakkında dedikodu yapın* - hashgraph, dedikodu protokolü aracılığıyla yayılır.
Dedikodu yapılan bilgi dedikodunun kendisinin tarihidir, bu yüzden öyle
"Dedikodu hakkında dedikodu". Bu, ötesinde çok az bant genişliği kullanır
sadece işlemleri dedikodu yapmak.
• *Sanal oylama* - her üyenin bir hashgraph kopyası vardır, böylece Alice şunları yapabilir:
Koşuyor *olsalardı* Bob'un ona hangi oyu *göndereceğini* hesaplayın
oy göndermeyi içeren geleneksel bir Bizans anlaşma protokolü.
Yani Bob'un gerçekten oy vermesine gerek yok. Her üye ulaşabilir
Tek bir oylama olmaksızın herhangi bir sayıda karar üzerinde Bizans anlaşması
hiç gönderiliyor. Tek başına hashgraph yeterlidir. Yani sıfır bant genişliği
sadece hashgraph'ı dedikodu yapmanın ötesinde kullanılır.
• *Ünlü tanıklar* - Topluluk, *n* işlemin bir listesini
O (*n* log *n*) üzerinde ayrı Bizans anlaşma protokolleri çalıştırarak sipariş verin
" *x* olayı *y* olayından önce mi geldi ?" şeklinde farklı evet / hayır soruları Bir
çok daha hızlı bir yaklaşım, yalnızca birkaç olayı seçmektir (karma grafiğin köşeleri),
tanık olarak adlandırılmalı ve hashgraph'ın *ünlü* olması için bir tanık tanımlanmalıdır.
çoğu üyenin bunu oluşturulduktan hemen sonra aldığını gösterir. Sonra
Bizans anlaşması protokolünü sadece tanıklar için yürütmek yeterlidir,
her tanık için tek soruyu "bu tanık ünlü mü?" bir Zamanlar
Ünlü tanıkların kesin seti üzerinde Bizans anlaşmasına varıldı,
hashgraph'dan tüm olaylar için adil bir toplam sipariş elde etmek kolaydır.
• *Kesinlikle* görülüyor - karma grafiğin herhangi iki köşesi *x* ve *y* verildiğinde,
olmak hemen olup hesaplanan *X* güçlü görebilir *y* tanımlanan,
birden fazla yönden geçen yollarla birbirine bağlıysa doğru olmak
yeterli üye. Bu kavram, anahtar lemmanın kanıtlanmasına izin verir:
Alice ve Bob, Carol'ın verilen bir oylamadaki sanal oyunu hesaplayabilirse

soru, sonra Alice ve Bob aynı cevabı alır. Bu lemma oluşturur
Bizans anlaşmasının matematiksel kanıtının geri kalanının temeli
bir olasılıkla.

Sayfa 74

Alice!
Bob!
Carol! Dave!
Ed!
Zaman!
Şekil 1. Yönlendirilmiş bir grafik olarak dedikodu tarihi. Herhangi birinin tarihi
dedikodu protokolü, her üyenin
bir köşe sütunudur. Alice, Bob'dan dedikodu aldığında,
dedikodu olayının temsil edildiğini ona bildiği her şeyi anlatmak
Alice sütunundaki bir tepe noktasıyla, iki kenar aşağıya doğru
Alice ve Bob'un hemen önceki dedikodu olaylarına.
3. Dedikodu hakkında dedikodu yapın: hashgraph
Hashgraph fikir birliği bir dedikodu protokolü kullanır. Bu, böyle bir üye anlamına gelir
Alice, Bob gibi rastgele başka bir üye seçeceği için
Bob'a şu ana kadar bildiği tüm bilgileri söyleyin. Alice daha sonra farklı bir
rastgele üye. Bob defalarca aynı şeyi yapıyor ve diğer tüm üyeler
aynı. Bu şekilde tek bir üye yeni bilgilerden haberdar olursa,
her üye farkına varana kadar toplulukta katlanarak hızlı yayılır
o.
Herhangi bir dedikodu protokolünün geçmişi, aşağıdaki gibi yönlendirilmiş bir grafikle gösterilebilir.
Şekil 1. Alice sütunundaki her köşe bir dedikodu olayını temsil eder. Örneğin,
Alice sütunundaki en üstteki olay, Bob'un Alice ile dedikodu senkronizasyonu gerçekleştirdiğini
gösterir
Bob'un bildiği tüm bilgileri ona gönderdiği. Bu tepe noktasında iki
aşağı doğru kenarlar, Alice için hemen önceki dedikodulara bağlanır ve
Bob. Zaman grafikte yukarı doğru akar, bu nedenle daha düşük köşeler tarihteki önceki olayları temsil
eder.
Tipik bir dedikodu protokolünde, bunun gibi bir şema yalnızca
protokol; herhangi bir yerde hafızada saklanan gibi gerçek bir grafik yoktur.
Hashgraph mutabakatında, bu grafik gerçek bir veri yapısıdır. Şekil 2 illus-
bu veri yapısını inceliyor. Her *olay* (köşe) bellekte bir dizi olarak saklanır.
byte, yaratıcısı tarafından imzalanmıştır. Örneğin, Alice'in (kırmızı) bir olayı gerçeği kaydeder
Bob'un ona bildiği her şeyi gönderdiği bir dedikodu eşleştirmesi yaptığını. Bu
olay Alice tarafından oluşturulur ve onun tarafından imzalanır ve diğer iki hash değerini içerir.
olaylar: son olayı ve Bob'un dedikodu senkronizasyonundan önceki son olayı. Kırmızı olay
Alice'in oluşturmayı seçtiği herhangi bir işlemin *yükünü* de içerebilir .
an ve belki de Alice'in iddia ettiği saat ve tarih olan bir zaman damgası
onu yarattı. O olayın diğer ataları (gri) içinde yer almıyor
bu, ancak kriptografik karmalar kümesi tarafından belirlenir. Veri yapıları
Karma grafikleri, ver-
tices bir dosya ağacının versiyonlarıdır ve kenarlar değişiklikleri temsil eder. Ama Git hiçbir şeyi
saklamıyor

Üyelerin nasıl iletişim kurduğunun kaydı. Karma grafik farklı bir amaç içindir.
Üyelerin nasıl iletişim kurduğunun geçmişini kaydeder.
Dedikodu protokolleri, çeşitli bilgi türlerini aktarmak için yaygın olarak kullanılmaktadır.
Kullanıcı kimlikleri hakkında dedikodu yapmayı veya işlemler hakkında dedikodu yapmayı veya
blockchain blokları hakkında dedikodu yapmak veya diğer bilgiler hakkında dedikodu yapmak
dağıtılması gerekiyor. Peki ya protokol dedikodu hakkında dedikodu yapacak olsaydı?
Ya üyeler hashgraphın kendisini transfer etmek için dedikodu yapıyorlarsa? Bob ne zaman
Alice'e dedikodu yaptı, ona bildiği tüm olayları verecekti ve yaptı
değil.
Bir hashgraph'ı dedikodu yapmak, katılımcılara çok fazla bilgi verir. Eğer bir
bir olayın yüküne yeni işlem yerleştirilirse, hızla herkese yayılır.
üyeler, her üye öğrenene kadar. Alice işlemi öğrenecek. Ve
Bob'un işlemi tam olarak ne zaman öğrendiğini bilecektir. Ve o bilecek
Carol tam da Bob'un bu işlemi öğrendiğini öğrendiği zaman.
Böyle bir muhakemenin derin zincirleri, tüm üyelerin bir kopyası olduğunda mümkün hale gelir.
karma grafik. Karma grafik yukarı doğru büyüdükçe, farklı üyeler
tepeye yakın yeni olayların biraz farklı alt kümeleri, ancak bunlar hızla
karma grafiğinde tam olarak aynı olayları daha düşük bir seviyeye getirme eşiğinde. Ayrıca,
Alice ve Bob her ikisinin de belirli bir etkinliğe sahip olması durumunda,
ayrıca her ikisinin de tüm ataları vardır. Ve alt grafiğin tüm kenarları üzerinde anlaşacaklar
bu ataların. Tüm bunlar, güçlü algoritmaların yerel olarak çalışmasını sağlar.
Bizans hata toleransı için.
Bu güç, çok az iletişim yükü ile birlikte gelir. Bir topluluk ise
basitçe oluşturdukları imzalı işlemleri dedikodu yapmak, belli bir miktar var
bant genişliği gerekli. Bunun yerine bir hashgraph'ı dedikodu yaparlarsa ve yeterince varsa
tipik bir olayın en az bir işlem içerdiği işlemler, ardından ek yük
minimumdur. Alice, oluşturduğu bir işlemi imzalamak yerine,
bu işlemi içermek için yarattığı olay. Her iki durumda da, o sadece bir tane gönderiyor
imza. Her iki durumda da işlemin kendisini göndermesi gerekir. Tek ekstra
ek yükü, iki karmayı göndermesi gerektiğidir. Ama bu bile büyük ölçüde olabilir
sıkıştırılmış. Şekil 2'de Alice, Carol'a kırmızı olayı göndermeyecektir.
önceki tüm atalarına sahiptir (Alice'ten veya biriyle daha önceki bir senkronizasyondan)
Başka). Dolayısıyla, Alice'in iki mavi ana olayın iki karmasını göndermesine gerek yoktur.
Carol'a bu olayın Alice tarafından bir sonraki olay olduğunu ve
diğer ebeveyn, Bob tarafından üçüncü olanıdır. Uygun sıkıştırma ile bu,
çok az bayt olarak gönderilir, mesajın boyutunun yalnızca yüzde birkaçını ekler
gönderildi.
4. Konsensüs algoritması
Her üyenin her olayı bilmesini sağlamak yeterli değildir. Aynı zamanda
olayların ve dolayısıyla işlemlerin doğrusal bir sıralaması üzerinde anlaşmak için gerekli
olayların içine kaydedilir. Çoğu Bizans hata toleransı protokolü
lider, üyelerin birbirlerine oy göndermesine bağlıdır. Yani n üyenin kabul etmesi için
tek bir EVET / HAYIR soruda $O(n^2)$ gönderilecek oylama mesajları
ağ, her üyenin diğer üyelere oylarını söylediği gibi. Bunlardan bazıları
protokoller, herkese gönderilen oyların makbuzlarını gerektirir, bu da onları $O(n^3)$. Ve onlar
birden fazla oylama turu gerektirebilir, bu da oylama sayısını daha da artırır
mesaj gönderildi.

Sayfa 76

Alice!
Bob!
Carol! Dave!
Ed!
Şekil 2. Karma grafik veri yapısı. Alice bir *olay* yaratır
(kırmızı) Bob'un onunla dedikodu senkronizasyonu yaptığı durumu kaydediyor
ve ona bildiği her şeyi anlatıyor. Etkinlik bir karması içeriyor
iki ebeveyn olayı (mavi): öz-ebeveyn (koyu mavi) aynı
yaratıcısı Alice ve diğer ebeveyn (açık mavi) Bob tarafından. Aynı zamanda
Alice'in seçtiği tüm yeni işlemlerin yükünü içerir
o anda ve Alice tarafından bir dijital imza oluşturun. Diğer
ata olayları (gri) kırmızı olayda saklanmaz, ancak
tüm karmalar tarafından belirlenir. Diğer öz-atalar (karanlık
gri) öz-ana bağlantı dizileri ile ulaşılabilenlerdir ve
diğerleri (açık gri) değildir.

Hashgraph konsensüsü herhangi bir oy gönderilmesini gerektirmez. Her üyenin bir
hashgraph'ın kopyası. Alice ve Bob aynı karma grafiğe sahipse,
herhangi bir deterministik fonksiyona göre olayların toplam sıralamasını hesaplayabilir
bu hashgraph ve ikisi de aynı cevabı alacak. Bu nedenle, fikir birliği
oylama mesajları gönderilmeden bile elde edildi.

Elbette, Alice ve Bob herhangi bir veride tam olarak aynı karma grafiğe sahip olmayabilir.
an. Genellikle eski etkinliklerde eşleşeceklerdir. Ama son zamanlarda
olaylar, her biri diğerinin henüz görmediği olaylara sahip olabilir. Ayrıca orada
zaman zaman topluluğa yerleştirilmesi gereken yeni bir etkinlik olabilir
karma grafikte daha düşük (önceki) bir konumda. Hashgraph fikir birliği algoritması
Bu sorunu en iyi *sanal oylama* olarak düşünülen bir sistem kullanarak ele alır .

Alice hashgraph *A* ve Bob hash hashgraph *B'ye* sahip olduğunu varsayalım . Bu karma grafikler
herhangi bir anda biraz farklı olabilir, ancak her zaman *tutarlı* olacaktır .

Tutarlı, eğer *A* ve *B'nin* her ikisi de *x* olayını içeriyorsa, her ikisinin de
x için tam olarak aynı atalar kümesi ve her ikisi de tam olarak aynı kümeyi içerecek
bu atalar arasındaki sınırlar. Alice *x'i* biliyorsa ve Bob bilmiyorsa ve her ikisi de
dürüst ve aktif katılımcılarsa, Bob'un *x'i* öğrenmesini bekleriz.

dedikodu protokolü aracılığıyla oldukça hızlı. Mutabakat algoritması şunu varsayar:
eninde sonunda olacaktır, ancak ne kadar hızlı olacağı konusunda herhangi bir varsayımda bulunmaz.
olmak. Protokol tamamen eşzamansızdır ve varsayımlarda bulunmaz
zaman aşımı süreleri veya dedikodunun hızı veya ilerlemenin yapıldığı hız hakkında.

Alice, bir dizi hesaplayarak *A'daki* olayların toplam sırasını hesaplayacaktır.
seçimler . Her seçimde, *A'daki* bazı olayların bir
oylanır ve *A'daki* bazı olayların o oyu aldığı kabul edilir. Alice yapacak

---

Sayfa 77

(a)!
(b)!
(c)!
(d)!
Şekil 3. Güçlü görmenin resmi. Her bir karma grafikte
üstteki sarı olay turuncu olaylardan birini *güçlü* bir *şekilde görebilir*

alt sırada. Vardır , $n = 5$ üye, en az bir tamsayı, böylece
$2n/3$'ten büyük 4'tür. (d) 'de, bir olay (turuncu) bir atadır
farklı yaratıcılar tarafından 4 ara etkinliğin her biri (kırmızı), her biri
sarı olayın atasıdır. Bu nedenle sarı
turuncu olayı kuvvetle görebiliyorsunuz. Diğer karma değerlerin her biri
grafikler, farklı bir turuncu olay için aynısını gösterecek şekilde renklendirilmiştir.
sarı olayın en az 4 kırmızı ile gördüğü alt sıra
Etkinlikler. Tüm 4 turuncu olay ve sarı olayın her iki ebeveyni
oluşturulmuş bir r turu varsa, $r + 1$ turunda sarı oluşturulur ,
çünkü yaratılan $2n/3$ taneden fazlasını güçlü bir şekilde görebilir .
r turunda farklı üyeler . Her olayın şu şekilde tanımlandığını unutmayın:
Bir ikisi de *atası* ve bir *öz-atası* kendisinin.
Birden fazla seçimi hesaplayın ve belirli bir etkinlik bazı seçimlere katılabilir
ama diğerleri değil ve farklı seçimlerde farklı oylar verebilir. Olay
Bob tarafından yaratılmışsa, Bob'un belirli bir seçimde belirli bir şekilde oy kullanmasından
bahsedeceğiz.
Ancak gerçek üye Bob işin içinde değil. Bu tamamen Alice'in
yerel olarak performans sergiliyor, burada Bob'un *kendisine* hangi oyu *göndereceğini* hesaplıyor ,
eğer gerçek Bob internet üzerinden ona oy gönderiyor olsaydı.
Bu sanal oylamanın çeşitli faydaları vardır. Bant genişliğinden tasarruf etmenin yanı sıra,
Üyelerin oylarını daima kurallara göre hesaplamalarını sağlar. Alice
dürüstçe, sanal Bob için dürüst olan sanal oyları hesaplayacaktır. Hatta
eğer gerçek Bob bir hilekâr ise, sanal Bob oylamasını yaparak Alice'e saldıramaz
yanlış.
Bob farklı bir şekilde hile yapmayı deneyebilir. Bob bir olay oluşturur varsayalım x a ile
önceki olayına işaret eden belirli kendi ebeveyn hash'i z . Sonra Bob yeni bir
olay y , ancak ona kendi ebeveyn hash'i vermek yerine *z'nin* kendi ebeveyn hash'ini verir.
x olması gerektiği gibi. Bu, hashgraph'daki Bob tarafından yapılan olayların artık
olması gerektiği gibi bir zincir olun. Şimdi bir ağaç olacaklar, çünkü o yarattı
çatal . Bob , Alice'e *x'e* ve *y'den* Carol'a dedikodu yaparsa , o zaman bir süre Alice ve Carol
çatalın farkında olmayabilir. Ve Alice için sanal oyu hesaplayabilir x olduğuna
Carol'ın y için sanal oyundan farklı .
Hashgraph fikir birliği algoritması, konsepti kullanarak bu saldırıyı engeller.
bir devletin diğerini *görmesi* ve bir devletin diğerini *güçlü* bir *şekilde görmesi* kavramı .
Bunlar *ata* ve *öz-ata* tanımlarına dayanmaktadır öyle ki her olay
kendisinin hem atası hem de öz-atası olarak kabul edilir.
Bob, her ikisi de diğerinin atası olmayan iki x ve y olayı yaratırsa ,
Bob çatallayarak hile yaptı. Eğer bir olay *w'nin* atası *x'e* sahipse ama yoksa

---

Sayfa 78

bilgisi y , ardından olay, bir ata olarak *ağırlık* olabilir *bkz* etkinlik x . Ancak, her ikisi de eğer x ve y
w'nin atalarıdır , o zaman w ikisini de veya başka herhangi bir olayı görmeyecek şekilde tanımlanır
aynı yaratıcı tarafından. Diğer bir deyişle, W görebilir x ise x buna bilinir ve herhangi bir çatal
o yaratıcı tarafından bilinir.
Varsa n üyeleri, daha sonra bir olay w olabilir *kuvvetle bakın* bir olay x eğer w görebilirsiniz
Her biri *x'i* görebilen farklı üyelerden $2n/3$ olaydan fazlası . Bu kavram
Şekil 3'te gösterilmektedir. Aynı karma grafiğin dört kopyası gösterilmektedir, her biri
alt sırada turuncu renkli farklı bir olay. (D) 'de, sarı olay
üstte, her biri turuncu rengi görebilen farklı üyelere ait 4 kırmızı etkinliği görebilir
altta olay. Bu aynı zamanda (a), (b) ve (c) için de doğrudur;

5 kırmızı etkinlik. Ancak güçlü bir şekilde görmek için yalnızca 4 tanesine ihtiyaç vardır, çünkü bu örnekte
n = 5 üye ve 2 *n* / 3'ten büyük en küçük tam sayı 4'tür.
Bu konsept, Bizans hata toleransına ulaşmak için bir anlaşma protokolüne izin verir
herhangi bir gerçek oylama olmaksızın, sadece yerel sanal oylama yoluyla.
Sanal oylamada, *x* etkinliği bazı EVET / HAYIR sorularına oy verdiğinde (örn.
başka bir olay meşhurdur), oy tamamen
x'in ataları . Bu oy, yalnızca *x'ten* nesline gönderilmiş olarak kabul edilir
Olay *w* eğer *w* kuvvetle görebilirsiniz *x* . 5. bölümde *x* ve *y* açıksa
yasadışı bir çatalın farklı dalları varsa, *w* en fazla *x* ve
y , ama ikisi birden değil. Ayrıca, karma grafikler *A* ve *B* tutarlıysa, o zaman değildir
güçlü görmek bir olay için olası *x* de , *A* ve başka etkinlik güçlü bkz *y* içinde
B . Bu lemma, Bizans ispatının temel taşıdır. Bunu bile sağlar
bir saldırgan çatal atarak hile yapmaya çalışırsa, yine de farklı
üyeler farklı siparişlere karar verir. Tarihsel olarak, bazı Bizans anlaşmaları
algoritmalar, üyelerin her oylama için herkese "makbuz" göndermesini gerektirdi
Alice'e karşı savunmak için Bob ve Carol'a tutarsız oylar gönderiyorlar.
Bu saldırı ile hashgraph forking saldırısı arasında bazı benzerlikler var,
ve makbuz kullanımı ile güçlü bir şekilde görme arasında.
Bu tanımlar göz önüne alındığında, tam hashgraph konsensüs protokolü verilebilir.
Şekil 4, 5, 6 ve 7'deki algoritmalarla.
Şekil 4'teki ana algoritma, iletişimin çok basit olduğunu göstermektedir:
Alice, rastgele başka bir üye Bob'u seçer ve tüm olayları ona dedikodu yapar.
o bilir. Bob daha sonra bu dedikodunun gerçeğini kaydetmek için yeni bir olay yaratır.
Bu basit dedikodu protokolü Bizans Hata Toleransı ve düzeltmeleri için yeterlidir.
doğruluk. Ancak verimliliği artırmak için çeşitli şekillerde genişletilebilir.
Alice ve Bob birbirlerine hangi olayları bildiklerini söyleyebilir, sonra Alice
Bob'a bilmediğini bildiği tüm olayları gönderir. Protokol yeniden
Alice'in bu olayları topolojik sırayla göndermesini isteyin, böylece Bob her zaman bir
olayın ebeveynleri olayı almadan önce. Protokol, daha sonra bile söyleyebilir
Alice, Bob ile senkronize olur, ardından Bob hemen Alice ile senkronize olur. Çoklu
senkronizasyonlar
aynı anda olabilir, bu nedenle Alice aynı anda birkaç üyeyle senkronize olabilir
birkaç üye onunla senkronize oluyor. Bunlar ve diğer optimizasyonların tümü kullanılabilir,
ama bu basit olan yeterli.
Her senkronizasyondan sonra üye, mutabakatı belirlemek için üç prosedürü çağırır.
mümkün olduğu kadar çok olay için sipariş. Bunlar iletişim içermez; yalnızca
yerel hesaplamalar yeterlidir. Bu prosedürlerde, her bir *for* döngüsü ziyaretleri olayları
içinde *topolojik sırayla* bir olay her zaman ebeveynler sonra ziyaret edilir. İlk olarak
Algoritmanın döngüsü *için* , eğer x tüm tarihteki ilk olaysa, o zaman

---

Sayfa 79

ebeveynler veya önceki turlar, bu nedenle x.round = 1 ve x.witness = TRUE olarak ayarlanmalıdır.
Algoritma aynı zamanda sabit bir *n* kullanır ; bu, toplamdaki üye sayısıdır.
nüfus ve *C* gibi 2'den daha küçük bir tamsayı sabit daha büyük olduğu , *c* = 10.
Aşağıdaki algoritmada Bizans anlaşması bir olasılıkla garanti edilmektedir.
Atalarının bir işlevi olarak her olay için bir yuvarlak sayı tanımlamak kullanışlıdır.
DivideRounds'da (Şekil 5), bilinen her olaya bir tam sayı *yuvarlak sayı* atanır
(tanım 5.2) atalarının yuvarlak sayılarının bir fonksiyonu olarak. Karma grafikler
Şekil 3, bunun nasıl yapıldığını gösterir. Alt sıradaki tüm olaylar yuvarlak olsaydı
r ise , o zaman bu şekillerdeki diğer olayların tümü de *r* turu olur , hariç

r + 1 turu olacak sarı olay. Sarı olay,
sonraki tur, *r* + 1, çünkü 2 *n* / 3 olaydan fazlasını güçlü bir şekilde görebilir .
yuvarlak *r* . Tarihteki ilk olay 1. tur olarak tanımlanmıştır, bu nedenle gelecekteki tüm turlar
buna göre belirlenir. Her olay sonunda hem olacaktır *yuvarlak oluşturulur* ve
bir *tur alınan* numara. Oluşturulan tura *tur* veya *tur* da denir.
numarası .
Herhangi bir üye için, her turda oluşturdukları ilk etkinliğe
tanık . Sanal oyları gönderen ve alan yalnızca tanık olaylarıdır. Bu
Şekil 6'da gösterilen karar verme prosedüründe gerçekleşir. Bu prosedür,
Bizans anlaşması gerçekleşir. Her tanık için *ünlü* olup olmadığına karar verir .
Bir sonraki turdaki birçok tanığın görmesi durumunda bir tanık meşhurdur ve öyledir.
pek çoğu yapamazsa ünlü değil. Bizans anlaşması protokolü,
her tanık, ünlü olup olmadığını belirlemek için. *R* turundaki bir *x* tanık için, her tanık
r + 1 turunda eğer görebilirse *x'in* ünlü olduğunu oylayacaktır . 2 *n* / 3'ten fazlası aynı fikirde ise
Ünlü olup olmadığına, o zaman toplum karar verdi ve seçim bitti. Eğer
oy daha dengelidir, ardından gerektiği kadar çok tur için devam eder.
her tanık, tanıkların çoğunluğuna göre normal bir tur oylamasında
önceki turda güçlü bir şekilde görebileceğini. Saldırganlara karşı savunmak için
interneti kontrol edebilir, tanıkların oy kullanabileceği periyodik *bozuk para turları* vardır
sözde rastgele. Bu, bir saldırganın tüm mesajları kontrol edebildiği anlamına gelir.
oyları dikkatlice bölmek için internette dolaşmak, hala bir şans var
topluluk 2 *n* / 3 eşiğini rastgele geçecek . Ve böylece anlaşma
sonunda bir olasılıkla ulaşıldı.
Şekil 6'da, algoritma hattı ise çalışma devam edecektir *"ise, d = 1"* idi
değiştirildi *"ise, d = 2"* . Bu revize edilmiş algoritmada, her seçim bir tur başlayacaktı
sonra. İkisi aşağıda birleştirilse bile çalışmaya devam ederdi.
hibrit algoritma. Her turda, önce tüm seçimlerini *"d = 1"* işaretiyle çalıştırın.
O turdaki her tanığın şöhretine karar verilirse ve 2 *n* / 3 veya daha az üye
o turda ünlü tanıklar yarattı, sonra sadece o tur için seçimler
d = 2 kontrolü kullanarak tümü yeniden çalıştırın . Bu hibrit algoritma için, buradaki tüm teoremler
Bizans Hata Toleransının kanıtı da dahil olmak üzere kağıt doğru olmaya devam edecektir.
Yeni seçimleri tetikleyen turlar için uzlaşma süresi uzar
biraz (belki% 20 oranında). Ancak bu pratikte çok nadiren olur ve
yapıldığında, adaleti sağlamak için ünlü tanıkların sayısını artırabilir.
Belirli bir turdaki her tanığın
meşhursa, bir fikir birliği zaman damgası ve bir zaman damgası belirlemek için bunu kullanmak
kolaydır.
eski olaylarda mutabakat toplam sırası. Bu findOrder prosedürü ile yapılır, bulundu
Şekil 7'de.

Sayfa 80

paralel olarak iki döngü çalıştırın:
döngü
bilinen tüm olayları rastgele bir üye ile senkronize et
son döngü
döngü
senkronizasyon almak
yeni bir etkinlik oluştur
çağrı divideRounds
çağrı decideFame
arama findOrder

son döngü
Şekil 4. Swirlds hashgraph konsensüs algoritması. Her biri
üye, rastgele seçilen diğer üyeleri defalarca arar ve
bunlarla senkronize olur. Giden senkronizasyonlara paralel olarak, her üye
gelen senkronizasyonları alır. Alice, Bob ile senkronize olduğunda, hepsini gönderir
Bob'un bilmediğini bildiği olaylar. Bob bu etkinlikleri ekler
karma grafiğe, yalnızca geçerli imzalara sahip olayları kabul ederek
Sahip olduğu ebeveyn olaylarının geçerli karmalarının lekelenmesi. Bilinen tüm olaylar
daha sonra mermilere bölünür. Sonra her mem-
her turda ("tanıklar") ünlü olarak belirlenir
veya sanal oylama ile tamamen yerel Bizans anlaşması yoluyla
ing. Daha sonra, yeterli olan olaylarda toplam sipariş bulunur.
bilgi mevcuttur. İki üye bağımsız olarak bir
bir olay için tarihteki pozisyonu atamaları garanti edilir.
aynı pozisyon ve daha fazla yerde olsa bile, asla değiştirmemesi garantilidir.
oluşum devreye girer. Ayrıca, sonunda her olay atanır.
böyle bir pozisyon, bir olasılıkla.
Önce *alınan tur* hesaplanır. Olay *x* , eğer öyleyse, alınan bir *r* turuna sahiptir .
tüm eşsiz ünlü tanıkların soyundan geldiği ilk raunttur,
ve her tanığın şöhreti *r'ye* eşit veya daha düşük raundlar için belirlenir . (
seti *eşsiz ünlü tanıklar* bir turda setinde aynı olacak şekilde tanımlanır
ünlü tanıklar, ancak belirli bir üyeden tüm ünlü tanıkların çıkarılması
o üyenin o rauntta birden fazla ünlü tanığı varsa).
Ardından *alınan süre* hesaplanır. *X* olayının alınan bir tur olduğunu varsayalım .
r ve Alice eşsiz ünlü tanık yarattı *y* yuvarlak içinde *r* . Algoritma *z* bulur ,
y'nin x'i öğrenen en eski öz-ataları . Let *t* zaman damgası olması
Alice içine koymak *z* diye oluştururken *z* . O halde *t* ,
Alice, *x'i* ilk kez öğrendiğini iddia ediyor . *X* için alınan süre , hepsinin medyanıdır
bu tür zaman damgaları, *r* turundaki eşsiz ünlü tanıkların tüm yaratıcıları için .
Daha sonra fikir birliği sırası hesaplanır. Tüm olaylar alındıklarına göre sıralanır
yuvarlak. İki etkinlik aynı alınan tura sahipse, bunlar kendilerine göre sıralanır.
zaman aldı. Hala bağlar varsa, bunlar imzaya göre sıralanarak koparılır,
imza XORing tarafından tüm benzersiz imzalarla beyazlatıldıktan sonra
kabul turunda ünlü tanıklar.

---

prosedür bölme
her olay için *x*
r ← *x'in* ebeveynlerinin maks. turu (veya yoksa 1)
eğer *x* kuvvetle fazla görebilirsiniz 2 *N* / 3 yuvarlak *r* tanıklar
x.round ← *r* + 1
Başka
x.round ← *r*
x.witness ← (x'in kendi ebeveyni yok)
veya (x.round> x.selfParent.round)
Şekil 5. divideRounds prosedürü. Bir olay olur olmaz x
biliniyorsa, buna x.round bir yuvarlak sayı ve boole
değer x. tanıklık bir "tanık" olup olmadığını gösteren hesaplanır,
o turda bir üyenin oluşturduğu ilk etkinlik.
5. Bizans hata toleransının kanıtı
Bu bölümde bir dizi yararlı tanım ve ardından birkaç kanıt yer almaktadır.

Güçlü Gören Lemma'dan (lemma 5.12) Bizans Fayına doğru inşa
Tolerans Teoremi (teorem 5.19). İspatlarda olduğu varsayılmaktadır.
N elemanları (*n*> 1), en az 2 *N* / 3 dürüst ve en fazla *N* / 3
dürüst olmayan Ayrıca dijital imzaların ve kripto para birimlerinin
grafik karmaları güvenlidir, bu nedenle imzalar taklit edilemez, imzalı mesajlar
tespit edilmeden değiştirilebilir ve karma çarpışmalar asla bulunamaz. Senkronizasyon
dedikodu protokolünün, Alice Bob'a tüm olayları gönderdiğinde
Bob yalnızca geçerli bir imzası olan ve geçerli karmalar içerenleri kabul eder.
sahip olduğu olaylara karşılık gelir. Sistem tamamen asenkron. Bu
Alice ve Bob'un dürüst üyeler için eninde sonunda
Bob ile senkronize edin ve Alice tekrar tekrar Bob'a bir mesaj göndermeye çalışırsa, sonunda
müttefik başarılı. Ağ güvenilirliği veya ağ hakkında başka hiçbir varsayımda bulunulmaz.
hız veya zaman aşımı süreleri. Özellikle, saldırganın tamamen kontrol etmesine izin verilir.
ağ, mesajları keyfi olarak siler ve geciktirir, kısıtlamaya tabidir
dürüst üyeler arasında defalarca gönderilen bir mesajın eninde sonunda
bir kopyası olsun.

Tanım 5.1. Bir olay, *X* bir olarak tanımlanır *ata* olayı *y* ise *X* olduğu *y* ya da bir
ana *y* ya da bir ebeveyn bir üst *y* , vb. Aynı zamanda bir olan *öz atası* ait *y* eğer
X ise *Y* , ya da bir kendi kendine üst *y* ya da bir kendi kendine ebeveynin kendinden üst *y* ve
benzerleri.

Tanım 5.2. Bir *x* olayının *turda oluşturulan sayısı* (veya *turu*) şu şekilde tanımlanır:
olmak *r* + *i* , burada *r* , *x'in* ebeveynlerinin maksimum yuvarlak sayısıdır (veya eğer varsa 1)
) anne hayır ve *ben* eğer 1 olarak tanımlanır *x* kuvvetle 2'den fazla görebilirsiniz *n* / 3 tanık
r turunda (veya yapamazsa 0).

Tanım 5.3. *Yuvarlak alınan sayı* (ya da *yuvarlak alınan* bir olayın) *x* olduğu
tüm eşsiz ünlü tanıkların soyundan geldiği ilk tur olarak tanımlanmıştır.
x .

Sayfa 82

prosedür karar
her olay **için** önceki turlardan daha sonraya doğru sırayla x
x.famous ← KARARSIZIM
her olay için y önceki raundlardan sonraya doğru sırayla
eğer x.witness **ve** y.witness **ve** y.round > x.round
d ← y.round - x.round
s ← turdaki tanık olaylar dizisi
y.round-1, y kuvvetlice görebilir
v ← s cinsinden çoğunluk oyu (beraberlik için DOĞRUDUR)
t ← s içindeki v oyu ile olay sayısı
Eğer d = 1 olarak
// seçimin ilk turu
y.vote ← x'i görebilir mi?
Başka
Eğer d mod c > 0
// bu normal bir raund
eğer t> 2 * n / 3
// süper büyükse, o zaman karar ver
x.famous ← v
y.vote ← v
y döngüsünden çıkmak
Başka

// başka, sadece oy ver
y.vote ← v
Başka
// bu bir madeni para turu
eğer t> 2 * n / 3
// süper üstünlük ise, o zaman oy verin
y.vote ← v
Başka
// başka bir yazı tura atmak
y.vote ← *y* imzasının orta biti
Şekil 6. Karar verme prosedürü. Her tanık olayı için
(yani, x.witness'in doğru olduğu bir x olayı), fa- olup olmadığına karar verin
mous (yani, x.famous'a bir boole atayın). Bu karar verildi
sanal oylamaya dayalı bir Bizans anlaşma protokolü ile. Her biri
üye yerel olarak kendi hashgraph kopyası üzerinde çalıştırır.
ek iletişim yok. Hashgraph'daki olayları ele alır
sanki birbirlerine oy gönderiyorlarmış gibi, hesaplama
bir üyenin bilgisayarına tamamen yereldir. Üye oy verir
her turun tanıklarına, birkaç tur boyunca
Nüfusun 2 / 3'ü aynı fikirde. X'in şöhretini bulmak için bunu yeniden çalıştırın
x.famous bir
değer.
Tanım 5.4. *X* ve *y* aynı yaratıcıya sahipse , olay çifti (*x, y*) bir *çataldır* ,
ama ikisi de ötekinin atası değildir.

Sayfa 83

prosedür bul
için her olay x
y olayı olmayacak şekilde bir r turu **varsa**
y. tanıklık = TRUE olan r turunda veya öncesinde
ve y.famous = UNNDECIDED
ve x her turun atasıdır r eşsiz ünlü
şahit
ve bu, r'den önceki herhangi bir raunt için geçerli değildir
sonra
x.roundReceived ← r
s ← her olayın ayarlayın z öyle ki z
bir yuvarlak benzersiz ünlü bir öz-atası
tanık, ve x, z'nin bir atasıdır ama değil
z'nin kendi ebeveyninin
x.consensusTimestamp ← medyan
s'deki tüm olayların zaman damgaları
TAVSİYE EDİLMEDEN ALINAN tüm olayları **geri** döndür,
Tura göre sıralandı Alındı, sonra bağlar sıralandı
zaman damgası, ardından beyazlatılmış imza ile
Şekil 7. findOrder prosedürü. Bir kez tüm tanıklar
Yuvarlak *r* , ünleri karar verdik ünlü tanıkların kümesini bulmak
o turda, daha sonra o setten herhangi bir ünlü tanığı çıkarın.
bu setteki diğer kişilerle aynı yaratıcıya sahip. Kalan
ünlü tanıklar, *eşsiz ünlü tanıklardır* . Gibi davranırlar
Yargıçlar, daha önceki olaylara alınan bir tur atamak ve onaylamak için

sus zaman damgası. İlk turda bir olayın "kabul edildiği" söyleniyor
daha önce de olsa, tüm eşsiz ünlü tanıkların onu aldığı yer
turlar tüm tanıkların şöhretine karar verdi. Zaman damgası
bu olayların zaman damgalarının medyanında bu mem-
bers önce aldı. Bunlar hesaplandıktan sonra olaylar
alınan tura göre sıralanır. Herhangi bir bağ, fikir birliği ile sınıflandırılır
zaman damgası. Kalan bağlar beyazlatılmış imzalar tarafından sınıflandırılır.
ture. Beyazlatılmış imza, XORed imzasıdır.
kabul edilen turdaki tüm eşsiz ünlü tanıkların imzaları.
Tanım 5.5. Bir *dürüst* üyesi diğer her ile sonsuz sık senkronize etmeye çalışır
üye, her senkronizasyondan sonra geçerli bir olay oluşturur (en son kendi ebeveyninin karmalarıyla)
ve diğer-ebeveyn) ve asla birbiriyle çatal olan iki olay oluşturmaz.
Tanım 5.6. Bir olay *x* olabilir *bkz* olay *y* ise *y* bir atası *x* ve
x'in ataları, *y'nin* yaratıcısı tarafından bir çatal içermez .

Tanım 5.7. Bir olay *x* olabilir *kuvvetle bkz* olay *y* eğer *x* görebilirsiniz *y* ve bir var
seti *S* üyelerin 2/3 ten fazlasına göre olayların öyle ki *x* her etkinliği görebilen
içerisinde , *S* , ve her olay *S* görebilir *y* .
Tanım 5.8. Bir *tanık* , bir turda bir üyesi tarafından oluşturulan ilk olaydır.
Tanım 5.9. Bir *ünlü tanık* olmaya karar verilmiş bir şahittir *ünlü*
topluluk tarafından, burada açıklanan algoritmaları kullanarak. Gayri resmi olarak, topluluk
bir tanığın ünlü olduğuna karar verme eğilimindedir, eğer birçok üye onu başlangıcına kadar görürse
sonraki tur. Bir *benzersiz ünlü tanık* olmayan bir ünlü şahittir
aynı turda yaratılan diğer ünlü tanıklarla aynı yaratıcı. İçinde
çatallanma olmaması, her ünlü tanık aynı zamanda eşsiz bir ünlü tanıktır.
Tanım 5.10. Karma grafikleri *A* ve *B* , içerdiği herhangi bir olay *x* için *tutarlıdır.*
her iki karma grafikte de, her ikisi de *x* için aynı ata kümesini içerir.
bu atalar arasında ebeveyn ve kendi kendine ebeveyn kenarları.
Lemma 5.11. *Tüm üyelerin tutarlı hashgraphları vardır.*
İspat: İki üyenin *x* olayını içeren karma grafikleri varsa , o zaman aynı
x içinde bulunan iki karma . Bir üye, senkronizasyon sırasında bir etkinliği kabul etmeyecek
bu üyenin o etkinlik için zaten her iki ebeveyni de yoksa, her iki karma grafik de
x için her iki ebeveyni de içermelidir . Kriptografik karmalar olduğu varsayılır
güvenli, bu nedenle ebeveynler aynı olmalıdır. Tümevarım yoluyla, *x'in* tüm ataları
aynı olmalı. Bu nedenle, iki karma grafik tutarlıdır.
D
Güçlü görme kavramının amacı , aşağıdaki lemmayı doğru kılmaktır.
Bu lemma tüm ispatın temelidir, çünkü tutarlılık sağlar.
oylama ve farklı üyelerin asla tutarsız hesaplamayacağına dair garantiler için
tamamen sanal oylamayla bile sonuçlar.
Lemma 5.12 (Güçlü Gören Lemma) **.** *Olay çifti* (*x, y*) *bir çatal ise ve*
x, A hashgraph'ındaki z olayı tarafından güçlü bir şekilde görülür, bu durumda y,
A ile tutarlı olan herhangi bir B hashgraphındaki herhangi bir olay.
Kanıt: Kanıt çelişkidir. Varsayalım olay *ağırlık* olarak *B* güçlü görebilir *y* .
Kuvvetle görme Tanım olarak, bir dizi var olmalıdır *S A* olayların *A* o
z görebilir ve hepsi *x'i* görebilir . Bir dizi olmalı *S B* olayların *B* o *w*
bkz olan ve her görebilir *y* . O zaman *S A* , birden fazla kişi tarafından oluşturulan olayları içermelidir
2 *n* / 3 üye ve *S B de* öyle olmalıdır , bu nedenle birden fazla örtüşme olmalıdır
Her iki sette de etkinlik oluşturan *n* / 3 üye. *N* / 3'ten az olduğu varsayılmaktadır
üyeler dürüst değil, bu yüzden yaratmış en az bir dürüst üye olmalı

Her iki etkinlik *S A* ve *S B* . Let *m,* böyle bir parça olabilir ve bunların etkinlikleri *q bir ∈ S A* ve *q, B ∈ S B* . Çünkü *m* dürüst, *q, A* ve *q B* , birbiriyle çatal olamaz yani biri diğerinin öz-atası olmalıdır. Genelliği kaybetmeden, izin *q bir* olmak *q B'nin* öz-atası . Hashgraphs *A* ve *B* tutarlıdır ve *q, B* içinde *B* , yani atası *q A* da *B'de* olmalıdır . O zaman *B'de , x q A'nın* bir atasıdır ve bu bir *q B'nin* atası , dolayısıyla *x , q B'nin* atasıdır . Ama *y* aynı zamanda *q B'nin* de atasıdır . Yani ikisi de *x* ve *y q B'nin* atalarıdır ve birbirlerinin çatallarıdır, bu nedenle *q B* ikisini de göremez onlardan. Ancak o aykırı olduğuna varsayım *q B* görebilir *y* de *B* . Bu bir çelişki, böylece lemma kanıtlanmıştır.

D

Her an, tüm üyeler tutarlı hashgraph'lara sahip olacaktır. İki hash-grafikler tutarlıdır ve her ikisi de bir *x* olayı içerir, bu durumda ikisi de

---

Sayfa 85

x için aynı atalar kümesi . Bu, *x'in* her özelliği üzerinde anlaşmalarına neden olacaktır. bu tamamen atalarının bir işlevidir. Bu, oluşturulmuş turunu içerir. bir tanıktır, hangi olayları görebilir, hangi olayları güçlü bir şekilde görebilir ve nasıl her seçimde oy kullanır (eğer tanık ise). Bu mülklerin çoğu için bu doğrudan tanımdan izler. Aşağıdaki lemma da bunun doğru olduğunu kanıtlıyor oluşturulan tur için.

Lemma 5.13. *Karma grafikler A ve B tutarlıysa ve her ikisi de x olayını içeriyorsa, her ikisi de aynı turda oluşturulan sayıyı x'e atayacaktır.*

İspat: Tutarlı karma grafiklerin her ikisi de *x* içeriyorsa, ikisi de Tarihteki ilk olay da dahil olmak üzere tüm atalarının aynı kümesi. Sonra kanıt tümevarım gereğidir: ilk etkinliğin raund sayısı üzerinde anlaşırlar, ki bu 1 ile tanım. Ve eğer ikisi de keyfi bir *y* durumu içeriyorsa ve turda anlaşırsa tüm atalarının sayıları, o zaman maksimum yuvarlak sayı üzerinde anlaşacaklar *r* ebeveynlerinin *y* olup olmadığı ve kabul edecektir *y* kuvvetle görebilirsiniz 2'den fazla *n* / 3 farklı üyeler tarafından *r* turunda oluşturulan tanıklar ve bu nedenle *y* yuvarlak sayısı . Bu nedenle, tüm etkinliklerin yuvarlak sayısı üzerinde anlaşacaklar *x* dahil paylaşırlar .

D

Farklı üyeler biraz farklı karma grafiklere sahip olabilir ve bu nedenle biraz farklı seçimler. Ancak, tüm oylar tutarlı olacaktır. Bir hash-Grafik, Alice'in belirli bir seçim için belirli bir turda belirli bir oyu Bob'a gönderdiğini gösterir. daha sonra herhangi bir tutarlı hashgraph aynı oyu göstermeli veya hiç oy göstermemelidir Alice'ten Bob'a o rauntta. İki tutarlı hashgraph için imkansızdır o turda Alice'e iki farklı oy göstermek için. Bu aşağıda gösterilmiştir lemma.

Lemma 5.14. *Karma grafikler A ve B tutarlıysa ve algoritma çalışıyorsa A, üye m* 0 *tarafından yapılan bir r etkinliğinin m* 1 *üyesine bir oy v A gönderdiğini gösterir . r* + 1 *tur ve B üzerinde çalışan algoritma, üyeye göre bir r turu olayının m,* 0 *, bir oy v gönderir B elemanı m bir etkinliğe* 1 *tur r* + 1 *ve v, bir = v B .*

Kanıt: Algoritma , *y* güçlü bir şekilde görebiliyorsa, yalnızca *x* olayından *y* olayına bir oy gönderir *x* . Tutarlı karma grafiklerin çatal olan iki olaya sahip olması mümkün değildir. Güçlü Gören lemma (lemma 5.12). Bu nedenle, iki oy , her ikisinde de aynı *x* olayından gelmelidir. hashgraphs. Bir olayın oyu tamamen atalarının bir işlevi olarak hesaplanır, bu nedenle İki hashgraphs oylama üzerinde anlaşmaya gerekir ve *v A = v B* .

D

Belirli bir EVET / HAYIR sorusuyla ilgili Bizans anlaşması birden fazla
sanal oylama turları. Belirli bir üye seçim hesaplamalarını şu tarihte bitirir:
r turu normal bir tursa (bozuk para turu değilse) ve bir tur *r* + 1 olayı ise
r turunda aynı şekilde oy veren üyelerin 2 *n* / 3'ünden fazlasını kuvvetle görüyor . Eğer
bu gerçekleşirse, her aktif üye seçimlerini *r* veya *r* + 1 turunda sona erdirir.
(veya *R* + 2 ise *r* + 1, bir madeni para yuvarlak) ve aynı şekilde karar verecektir. Diğer bir deyişle,
Aşağıdaki lemma, eğer birisi bir EVET / HAYIR sorusuna karar verirse, o zaman
herkes hemen ardından Bizans mutabakatına ulaşır.
Lemma 5.15. *Karma grafikler A ve B tutarlıysa ve A, bir Bizans*
r ve B turunda v sonucuyla anlaşma seçimi r'den önce karar vermemişse, o zaman
B, v'ye r + 2 *turunda veya öncesinde karar verecek .*

Sayfa 86

İspat: Kararlar jeton turlarında alınamaz , bu nedenle *r* normal bir tur olmalıdır. Eğer *bir*
v oyuna karar verir , bu, *r* turundaki bazı tanıkların bir setten *v* oyu aldığı anlamına gelir.
2'den fazla *n* / 3 üye içeren üye sayısı *S.* Çünkü oylama tutarlıdır
(önceki lemmaya göre), *A* ve *B'deki* diğer tüm *r* turu etkinlikleri oy alacak
2'den fazla *n* / 3 üyeden, çoğunluğu aynı zamanda *S'de olacak ,* çünkü
büyüklüğü daha iki alt kümesi 2'den *N* / 3 boyutunda bir dizi çekilen *n* her biri olmalıdır
unsurlarının çoğu diğeriyle ortaktır. Bu nedenle, her tur *r*
Her iki tanık *A* ve *B* için oy verecek *v* (ve bazı karar verebilir *v*). Yuvarlak *r* + 1 ise
normal bir raundsa, o raunttaki *A* ve *B'deki* her etkinlik oybirliğiyle alınır.
v oyları ve karar verecek *v* . Yuvarlak Eğer *r* + 1 bir sikke yuvarlaktır, o zaman tüm alacak
oybirliğiyle *v'nin* oyları , bu nedenle hiçbiri bozuk paraları çevirmeyecek ve hepsi *v* oylayacak ve
sonra hepsi
r + 2 turunda *v'ye* karar verin .
D
Aşağıdaki teorem, Bizans hata toleransının herhangi bir
tek EVET / HAYIR soru.
Teorem 5.16. *Herhangi bir tek EVET / HAYIR sorusu için nihai fikir birliğine varılır.*
1 olasılıkla müttefik.
İspat: Herhangi bir üye soruya karar verirse, o zaman tüm üyeler aynı kararı verecektir.
2 tur içinde, son lemmaya göre. Yani fikir birliğinin başarısız olmasının tek yolu,
hiçbir üye karar vermez çünkü hiçbir tanık 2 *n* / 3 den fazla eşleşme almaz
oylar. Bununla birlikte, madeni para turunda, böyle bir üstünlük henüz elde edilmemişse,
sonra tüm dürüst üyeler oylarını rastgele seçerler ve sıfırdan farklı bir
herkesin aynı oyu seçme olasılığı. Para turları periyodik olarak sonsuza kadar gerçekleşir,
bu yüzden en sonunda dürüst üyeler, bir olasılıkla oybirliği yapacaklar,
ve ardından 2 tur içinde fikir birliğine varılacaktır.
D
Hashgraph mutabakat algoritmasında, karar vermek için Bizans anlaşması kullanılır.
belirli bir turdaki her tanığın ünlü olup olmadığı. Her tur garantilidir
aşağıdaki lemma ile ünlü en az bir tanığa sahip olmak.
Lemma 5.17. *Herhangi bir r yuvarlak numarası için, en az bir tane olan herhangi bir karma grafik için*
r +3 *turundaki olay, r turunda karar verilecek en az bir tanık olacaktır.*
mutabakat algoritması ile ünlü olmak ve bu karar herkes tarafından alınacaktır.
r + 3 *turunda veya öncesinde tanık olun .*
Korumalı: Let *S r* +3 yuvarlak tek bir tanık içeren bir resim grubu olabilir , *r* bir hashgraph +3,
en azından böyle bir tanığı var. Her *i* <*r* + 3 için, *S i* hepsinin kümesi olsun
Yuvarlak şahitler *i* her güçlü en az bir tanık ile görülür *S i* + 1 .

Durum 2 $n / 3 <| S i |$ Tüm $i \leq r + 2$ için $\leq n$, çünkü varoluş
$i + 1$ turundaki bir olayın 2'den fazla $n / 3$ garantisinin raundda güçlü bir şekilde görülmesi
i ve n üyenin hiçbiri belirli bir turda birden fazla tanık yaratamaz.
bu kuvvetle görülür (Strongly Seeing lemma, lemma 5.12 tarafından). Kesinlikle görmek
görmek anlamına gelir, yani $S r + 1$'deki her olay , içindeki olayların üçte ikisinden fazlasını görür.
$S r$. Bu nedenle, ortalama olarak, *S r'deki* her olay, üçte ikiden fazlası tarafından görülür.
$S r + 1$'deki olaylar . Hepsi ortalamanın altında olamaz, bu yüzden en az bir tane olmalı
S r'deki olay (buna *x diyelim*) $S r + 1$'deki olayların üçte ikisinden fazlası tarafından görülür .
Dolayısıyla $S r + 1$'in üçte ikisinden fazlası, *x'in* ünlü olduğu seçiminde EVET oyu verecek .
Bu nedenle, $S r +2$'deki her olay, HAYIR oyundan daha fazla EVET oyu alacaktır.
şöhreti x ve dolayısıyla oy verecek x ünlü olmak (ve ya karar olmayabilir
bu x ünlü). Bu nedenle, $S r + 3$'teki etkinlik için oybirliği ile oy verilecektir.

Sayfa 87

x o karar neden olacak ünlü olmak x ünlüdür. Bu nedenle, her
$r + 3$ turunda bir etkinliğe sahip olan üye , önce *x'in* her iki durumda da ünlü olduğuna karar
verecektir.
yuvarlak $r + 2$ veya $r + 3$.
D
Lemma 5.18. *Karma grafik A, x olayını içermiyor, ancak tüm*
x'in ebeveynleri ve hashgraph B, x'in A'ya eklenmesinin sonucudur ve x bir tanıktır
r turunda oluşturulur ve A'nın r turunda şöhreti olan en az bir tanığı vardır.
karar verildiğinde (ünlü veya ünlü olmadığı için), x'in "ünlü değil" olduğuna karar verilecek
B.
Kanıt: Let *w* de tanıklık *A* tanık biri için ün karar
yuvarlak r . Atalarının hiçbiri *ağırlık* görebilir x bir yoktur, çünkü, X in A . Yani
onlar da görmez x in B onlar tutarlı aynı ataları var çünkü,
hashgraphs. Bu nedenle, $r + 1$ turunda tanık olan *w'nin* atalarının hepsi
ünü oylayacamaya YOK x in B . Atalarından Yani w içinde $r + 2$ karar verecek x ise
B'de ünlü değil .
D
Son 3 lemma / teorem göz önüne alındığında, her turun sonunda olacağını biliyoruz.
tüm tanıklarını evrensel fikir birliği ile ünlü veya ünlü değil olarak sınıflandırmak,
Tanıklardan en az birinin ünlü olmasıyla. Ondan sonra ünlüler
o tur için tanıklar, daha fazla olay eklense bile asla değişmeyecektir.
hashgraph. Bu ünlü tanıklardan oluşan bir grup, bu nedenle, bir yargıç olarak hareket edebilir.
onlara ulaşan tüm olayların toplam düzeni ve bir fikir birliği zaman damgası
her olayda.
Teorem 5.19 (Bizans Hata Tolerans Teoremi) **.** *Her x olayı bir*
dürüst üyeye sonunda toplam siparişte bir fikir birliği pozisyonu atanacaktır.
1 olasılıkla olayların sayısı.
Kanıt: Tüm dürüst üyeler eninde sonunda dürüst tanımına göre *x'i* öğrenecekler.
ve interneti kontrol eden saldırganların nihayetinde
herhangi iki dürüst üyenin iletişim kurmasına izin verin. Bu nedenle, sonunda olacak
tüm eşsiz ünlü tanıkların *x'in* soyundan geldiği bir raunt olun . Bu nedenle
Bu turda, ya da muhtemelen daha önceki bir yuvarlak olacak r nerede tüm ünlü
tanıklar *x'in* torunudur . Sonra *x'e* alınan bir r turu atanır ve a
bu üyelerin ilk aldığı zamanın medyanının fikir birliği zaman damgası ve
tarihteki fikir birliği yeri sabitlenecektir. Üstelik daha sonra yapmak mümkün değil
mutabakat düzeninde *x'ten* önce gelecek yeni bir *y* olayı keşfeder . Çünkü
Konsensüs tarihinde daha erken geldiyse, *y* turun daha az kabul edilmesi gerekirdi

daha büyük veya eşit *r* . Yani anlamına geleceğini yuvarlak tüm ünlü tanıklar *r* şırası
y aldı . Ancak ünlü tanıklar bir kez bir turda tanındığında, hepsi
ataları da biliniyor, bu yüzden onlar için yeni atalar keşfetmenin bir yolu yok
hashgraph büyüdükçe gelecekte. Dahası, bir tur için mümkün değil
gelecekte yeni ünlü tanıklar kazanmak için, bir zamanlar bilinen tüm ünlülerin
o raunttaki tanıklar biliniyor. Tüm yeni yuvarlak *r* içinde keşfedilir tanık
gelecek olacak *olup* bilinen yuvarlak bir atası *r* (1 + tanık olan
2 *n* / 3'ten fazla var) ve bu nedenle hemen fikir birliğine varılacak
ünlü değil. Bu nedenle, bir olay toplam sıralamada bir yer atandığında,
pozisyonunu asla değiştirmeyecek, ne bilinen başka bir olayla değiş tokuş yapmayacak, ne de
daha sonra keşfedilen ve önüne eklenen yeni olaylarla.
D
87
EKLER

Sayfa 88

SWIRLDS HASHGRAPH CONSENSUS ALGORİTMA - SWIRLDS-TR-2016-01
19
6. Adillik
Dağıtılmış fikir birliğine yönelik mevcut sistemlerin çoğu, kendi
işlemlerin mutabakat sıralaması. Bunu görmek için önce bir borsayı düşünün.
tek bir sunucu tarafından çalıştırılır. Alice ve Bob, bu sunucuya bir teklif verir.
Alice bunu Bob'dan hemen önce gönderiyor. Sunucu *adilse* , Alice'in
Bob'dan önce gerçekleşen işlem. Bazı uygulamalar için tam sıra
önemli değil, ancak bir borsa için bu kararın
adil yapılmalıdır.
Şimdi, tek bir sunucunun olmadığı dağıtılmış bir eşler arası sistemi düşünün.
ancak kimin işleminin ilk olduğu konusunda fikir birliğine varacak bir topluluk var.
Uzlaşı kararının adil olması yine de kritik derecede önemli olabilir. Ama ne
"adil" kelimesinin tanımı olmalı mı?
İşlem emriyle ilgili "adil" karar, hangisinin
ilk işlem oluşturuldu. Ama bu kötü olur. Alice yaratmış olabilir
Bob'dan bir saniye önce ormandaki bir kulübedeyken yaptığı işlem,
internet bağlantısı kesildi. O zaman topluluk yalnızca Bob'un
işlem ve Bob'un ilk olduğunu varsayar. Bir yıl sonra, Alice nihayet
ormandan çıkar ve internete yeniden katılırsa, topluluk
"adil" olmak için tarihi revize edin. Bu pek çok soruna neden olur. Böylece
ideal bir adalet tanımı olmaz. Bir gereklilik olması gerekir
işlem aslında ilk olarak sayılması için topluluğa gönderilir.
"Adil" karar, işlemin gerçekleştirilme sırasını yansıtan şekilde tanımlanabilir.
eylemler mevcut *lidere* ulaştı . Ama bu da kötü olur. Lider olabilir
Paxos algoritması tarafından seçilen bir üye olun. Veya hangi üye olursa olsun
şu anda döngüsel bir sistemde bir dönüş var. İş kanıtı sisteminde,
İlk önce bir bulmacayı çözmeyi başaran madenci olun. Her durumda lider,
Alice'in veya Bob'un işlemlerini bir süre için keyfi olarak görmezden gelmeye karar verirseniz,
birini geciktirmek, işlemlerini diğerinin peşinden gelmeye zorlamak. Eğer hedef
güven dağıtılmışsa, tek bir kişiye güvenilemez.
"Adil" karar, her bir işlemin ilk
tüm topluluğun belirli bir kısmına ulaştı. Bu biraz daha iyi.
topluluk, işlemlerin ilk kez bir
sanal sunucu, burada "sunucuya ulaşmak",
bir bütün olarak topluluk. Ancak yine de sorunlar var. Adil seçim tanımlanmışsa
hangi işlem önce topluluğun en az yarısına ulaşırsa o zaman orada
Carol önce Alice'i görürse, Dave önce Bob'u görürse ve diğer herkes
soru üzerinde eşit olarak bölün. Carol ve Dave'in ikisi de saldırganlarsa bu başarısız olur.

topluluğa gördüklerini söylemeden önce bilgisayarlarını kalıcı olarak kapatın.
Bu durumda, topluluk asla adil bir fikir birliğine varamaz çünkü
Carol ve Dave'i oy kullanmaları için sonsuza kadar bekleyecekler.
Daha iyi bir tanım, Alice'i ilk olarak kabul etmenin "adil" olduğunu söylemek olabilir.
Topluluğun önemli bir kısmı, Bob'dan önce Alice'in işlemini aldı ve
topluluğun bu bölümü daha sonra diğerlerinin çoğuyla iletişim kurmaya devam etti
hızlı bir şekilde. Bu tanıma göre, Alice ve Bob işlemlerini
dedikodu ağı neredeyse aynı anda ve her ikisi de aynı şekilde yayıldı
oran, o zaman fikir birliği her iki şekilde de gidebilir ve yine de adil kabul edilebilir. Ancak,
Alice, Bob'dan önceki işleminde dedikodu yapıp, süresi boyunca onu yenerse
tek bir dedikodu senkronizasyonundan kaynaklanırsa, her iki işlem de yayıldıkça

---

Sayfa 89

katlanarak, sonunda her senkronizasyonda ulaşılan üye sayısını ikiye katlayarak
2 üzerinde / nüfusun 3'te Bob önce Alice duyar ve 1'den az / 3 tercih edecektir
Bob. Yani bu durumda, fikir birliği içinde Alice'i Bob'a tercih etmek adil olur.
hashgraph mutabakat algoritması bu anlamda adildir. Çevrimiçi olan üyeler
ve düzenli olarak katılmak, *ünlü tanıklar olarak* adlandırılan bir dizi olay oluşturacaktır ve
mutabakat kararı, "ilk" işlemin hangi işlem olduğuna
ilk olarak bu setin çoğunluğuna ulaştı. Küçük bir üye grubu çevrimdışıysa veya
geri kalanıyla iletişim kuramayacakları şekilde bölümlenir, o zaman yapmazlar
ünlü tanıklara sahip olmak ve bu nedenle onlara ulaşan bir işlemin olması,
topluma bir bütün olarak ulaşmış olmak. Ancak bu setteki üyeler
geri kalanıyla iletişim kurduktan sonra ünlü tanıklar olarak sayılacaklar ve
ilk olarak "topluluğa" kimin ulaştığına karar vermeye yardımcı olacaktır.
Bu sisteme karşı olduğu kabul edilmeyecek saldırılar var.
fikir birliği sisteminin başarısızlığı, çünkü bunlar karşı eşit derecede etkili olacaktır.
tek sunuculu bir çözüm. Örneğin, Bizans delilleri saldırganların
interneti kontrol edebilir ve rastgele mesajları geciktirebilir. Saldırganlar gerçekten sahip olsaydı
bu güçle, Alice'in internetle olan bağlantısını olabildiğince uzun süre kesebilirler.
Bob'un bir işlemi göndermesi ve kaydetmesi gerekir. Bu,
bir hizmet reddi saldırısı başlatarak gerçek internet, her bilgisayarı
Alice'in iletişim kurmasını engellemek için Bob'dan gelen paketler. Elbette,
bu aynı zamanda Alice merkezi bir sunucuyla iletişim kuruyor olsaydı da etkili olurdu.
fikir birliğinin başarısızlığından çok internetin bir başarısızlığı olarak düşünülebilir
sistemi.
Benzer şekilde, Bob daha fazla bant genişliği satın alarak Alice'e göre avantaj elde edebilir.
dedikodularının daha çok insana daha hızlı ulaştığını. Alice'in 8 katı bant genişliğine sahipse,
Alice'in gönderdiği zamanda ilk olarak 8 üyeye işlemlerini gönderebilsin.
1'e çıkarsa, yaklaşık 3 dedikodu senkronizasyonunun zamanından bir avantaj elde edebilir. Bu değil
bir başarısızlık olarak kabul edildi. Mesajı gerçekten dünyaya ulaşırsa, o zaman
bunun için krediye sahip olmalı. Bu, mevcut borsalara benzer.
şirketler, biraz daha hızlı bağlantılar için büyük meblağlar harcarlar.
merkezi sunucuya daha hızlı ulaşın. Dolayısıyla fikir birliği algoritması dikkate alınmaz
Bu durumda "haksız" çünkü merkezi bir sunucu gibi davranıyor.

7. Genellemeler ve geliştirmeler

7.1. **delil kanıtı.** Şimdiye kadar her üyenin eşit olduğu varsayılmıştır. The
yukarıdaki algoritmalar, " üyelerin 2 *n* / 3'ünden fazlasına" bağlı olan şeylere atıfta bulunur
ve "ünlü tanık olaylarının en az yarısı". Ayrıca bir fikrini de kullanıyorlar
Bir sayı kümesinin "medyanı". Kanıt, Bizans yakınsamasını daha fazla olduğunda gösterir.
üyelerin 2 *n* / 3'ünden fazlası dürüst.

Üyelerin eşitsiz olmasına izin vermek için algoritmayı değiştirmek kolaydır. Her üye
kendileriyle ilişkili bir pozitif tam sayıya sahip olduğu varsayılabilir.
"Bahis". Daha sonra oylar ağırlıklı oylama ile değiştirilir ve medyanlar
oyların seçmen hissesi ile orantılı olarak ağırlıklandırıldığı ağırlıklı medyanlarla.
Yukarıdaki tüm tanımlarda, algoritmalarda ve ispatlarda "2'den fazla *n* / 3
üye "toplam hissesi 2 *n* / 3'ten fazla olan bir dizi üye anlamına gelir , burada
n tüm üyelerin toplam hissesidir ". "Olayların zaman damgalarının medyanı"
S "," S'deki zaman damgalarının ağırlıklı medyanı olur ve
S'deki her olayın yaratıcısının hissesi ". Ağırlıklı medyan şu şekilde düşünülebilir:

Sayfa 90

S'deki her *y* olayı almak ve *y'nin* zaman damgasının birden çok kopyasını içine koymak
kopya sayısı yarattı üyesinin hissesini eşit bir çanta, *y* .
Ardından çantadaki zaman damgalarının medyanını alın.
Bizans ispatı, saldırganlar 1 / 3'ten az olduğu sürece uygulandı.
nüfusun. Bu yeni tanımlarla, artık saldırganlar
birlikte tüm üyelerin toplam hissesinin 1 / 3'ünden daha az bir hisseye sahiptir .
Bu yeni teminat kanıtı sistemi, ağırlıksız sistemden daha geneldir.
Yine de ağırlıksız sistemi uygulamak için sadece her şeyi vererek kullanılabilir.
üye hissesi 1'dir. Ancak daha iyi davranış sağlamak için de kullanılabilir. İçin
Örneğin, pay, bir üyenin sahip olduğu dereceyle orantılı olabilir.
güvenilir. Belki bir şekilde soruşturulan üyeler,
diğerlerinden daha güvenilir. Veya üyelere daha fazla ağırlık vermek için kullanılabilir.
bir bütün olarak düzgün çalışan sisteme daha fazla ilgi duymak. Bir kripto para birimi
her üyenin coin sayısını kendi hissesi olarak kullanabilir.
daha fazla madeni para ile sistemin sorunsuz çalışmasını sağlamaya daha fazla ilgi
duyulmaktadır. Veya
bir topluluk, karşılıklı güvene sahip bir grup üye tarafından başlatılabilir, her biri
eşit hisse verilir. Ardından, mevcut her üyenin davet etmesine izin verilebilir.
davet edenin kısıtlamasına tabi olarak, katılacak pek çok yeni üye
hisselerini davetli ile paylaşmalıdır. Bu, bir Sybil saldırısının cesaretini kırabilir.
bir üye çok sayıda çorap kuklası hesabını davet ediyor.
oylama.
"Pay kaydı", üyelerin listesi ve her birinin sahip olduğu hissenin miktarıdır.
üye. Şimdiye kadar, hisse sicilinin evrensel olarak bilindiği varsayıldı,
ve değişmez. Bu varsayımı gevşetmek kolaydır.
Payı değiştiren belirli bir işlem şekli olduğunu varsayalım.
kayıt. Topluluk, başlangıçta kurallar koyabilir, hangisinin böyle olduğuna hükmedebilir.
işlemler geçerlidir. Örneğin, her üyenin diğerini davet etmesine izin verilebilir.
üye, toplamda en fazla 10 yeni üye. Ya da belki davet eden birini
yeni bir üye aynı anda yeni üyeye kendisinin bir bölümünü vermelidir
kazık. Böyle bir işlemin geçerliliği, işin tam sırasına bağlı olabilir.
mutabakat sırasındaki işlemler. Örneğin, kural yalnızca bir yeni
üye davet edilebilir ve Alice, Carol'ı davet eder, aynı anda Bob, Dave'i davet eder.
daha sonra, fikir birliği sıralamasında hangi davet önce gelirse, başarılı olur ve
diğeri başarısız olur.
Bunların tümü barındırılabilir. Konsensüs algoritması bittiğinde,
Yuvarlak hangi soruyu ciding *r* ilkleri ünlüdür, o anda o olur
tam olarak hangi olayların *r* turu alacağını bulmak ve hesaplamak
mutabakat sırasındaki kesin konumları. O sırada işlemlerin her biri
bu olaylarda işlenebilir ve hangilerinin olduğunu görmek için kurallara bakılabilir.

geçerlidir ve geçerli işlemler uygulanabilir. Bu, hisse senedini değiştirebilir.
Bahis kaydı değişirse, algoritma herkes için yeniden çalıştırılmalıdır.
r ve sonraki *raunttaki* olaylar . Bu, hangi olayların hesaplamalarını değiştirebilir?
güçlü bir şekilde görülüyor, olay turu sayıları, hangi olayların tanık olduğu ve
ünlü tanıklar.
Not hangi karar verirken yuvarlak olduğunu *r* tanıklar, hesaplamalar ünlüdür
eski bahis kaydı kullanılarak yapılır. *R* turu için oylama birkaç kez devam edebilir
hepsi eski hisselerini kullanarak geleceğe doğru ilerliyor. *R* turu yerleştikten sonra,

---

Sayfa 91

Gelecek turlar değişecek ve *r* + 1 turu ünlü tanıklar için hesaplamalar
yeni hisse kaydı kullanılarak yapılacaktır.
Bu yaklaşım, tüm üyelerin tam olarak hangi menfaatin olduğu konusunda hemfikir olmasını sağlar
herhangi bir hesaplama için kayıt kullanılıyor. Bu onların her zaman
bu hesaplamaların sonuçları üzerinde hemfikir olun. Ve Bizans anlaşması hala olacak
birinci olasılıkla garantilidir.
7.2. **imzalı durum.** Sistemin bir başka iyileştirmesi de imzalanmış durumlara sahip olmaktır.
R turundaki her tanığın ünlü olup olmadığı konusunda fikir birliğine varıldığında
ya da değil, geçmişte alınan her olay için toplam sipariş hesaplanabilir.
yuvarlak *r* veya daha azdır. Ayrıca, diğer tüm etkinliklerin (bunlara dahil olanlar dahil)
daha Alınan yuvarlak büyüktür olacaktır) henüz bilinmiyor *r* . Diğer bir deyişle,
bu noktada, *r* raunduna kadar olan tüm olaylar için tarih dondurulur ve değişmez . Bir
üye bu nedenle bu etkinliklerden tüm işlemleri alabilir ve onları besleyebilir
mutabakat sırasına göre bir veritabanına yerleştirin ve sonra ulaşılan durumu hesaplayın
bu işlemlerin işlenmesi. Her üye aynı fikir birliğini hesaplayacak
düzen, böylece her üye aynı durumu hesaplayacaktır. Bu bir *fikir birliği halidir* .
Her üye bu devletin karmasını alıp dijital olarak imzalayabilir ve
yeni bir işleme imza. Kısa süre sonra, her üye tarafından teslim alınacak
fikir birliği durumu için birçok imzayı dedikodu yapın. İmzalar alındıktan sonra
nüfusun en az 1 / 3'ü, bu fikir birliği durumu, imza seti ile birlikte,
sistem için resmi bir mutabakat devleti olan *imzalı bir devlet* oluşturur .
r turunun başlangıcı . Toplum dışındaki kişilere verilebilir ve yapabilirler.
imzaları kontrol edin ve bu nedenle devlete güvenin. Bu noktada bir üye şunları yapabilir:
durumu oluşturmak için kullanılan tüm işlemleri silmekten ve
bu işlemleri içeren tüm olaylar. Sadece devletin kendisinin olması gerekir
tuttu. Bunu birkaç dakikada bir yapmak mümkün olabilir, bu nedenle asla
depolanan çok sayıda işlem ve olay. Yalnızca fikir birliği kendisini ifade eder. Nın-nin
elbette, bir üye eski olayları, işlemleri ve durumları korumakta özgürdür, belki
arşiv veya denetim amaçlı. Ancak sistem hala değişmez ve güvenlidir.
Herkes bu eski bilgiyi bir kenara atarsa.
Nüfusun 1 / 3'ünden daha azının dürüst olmadığı varsayıldığında,
devletin en az bir dürüst imzaya sahip olduğu garanti edilir ve bu nedenle güvenilebilir
fikir birliği algoritmasında bulunan topluluk fikir birliğini temsil eder. Eğer
üye grubu (veya hissesi) zamanla değişebilir, ardından bu hisse senedi kaydı (ve
tarihi) de devletin bir parçası olacaktır. 1/3 eşiği değiştirilebilir
2 / 3'ten fazla gibi başka bir şeyle ve sistem yine de çalışırdı.
7.3. **Etkili dedikodu.** Dedikodu protokolü, bant genişliğini çok verimli kullanır.
Her olayın içerdiği yeterli sayıda işlemin oluşturulduğunu varsayalım.
en az bir işlem. Noktadan noktaya kullanarak herhangi bir çoğaltılmış durum makinesinde
İnternet gibi ağ, her üyenin her birini alması gerekecektir.
imzalanan işlem bir kez ve ayrıca imzalanan her işlemi ortalama bir kez göndermek için.

Hashgraph dedikoduları için, imzanın
işlemin kendisi için değil, işlemi içeren olay. Tek
ek yük, iki karma ve zaman damgası artı sayım dizisidir
senkronizasyonun başlangıcında. Ancak, hash'lerin kendilerinin gönderilmesi gerekmez
internet. Sadece olayı yaratanın kimliğinin gönderilmesi yeterlidir,
ve diğer ebeveyninin sıra numarası.

Sayfa 92

Örneğin, Alice tarafından oluşturulan 100. olayın başka bir ebeveyni olduğunu varsayalım.
Ed'in 50. olayı. Alice tarafından bu olay bir senkronizasyon sırasında Bob'dan Carol'a gönderilirse,
Bob, olayda Carol'a iki karmayı göndermeyi atlayabilir. Bunun yerine söyleyebilirdi
Carol, bunun Alice tarafından bir olay olduğunu ve diğer ebeveynin Ed'in 50. olayı olduğunu söyledi.
Bob yalnızca baş harflerine göre sahip olmadığı Carol etkinliklerini gönderdiği için
önemli, Carol bunun Alice'in son olaydan beri 100. olayı olması gerektiğini bilecek
Alice tarafından Alice'in 99. olayı olduğunu biliyor. Böylece Bob'un
öz-ebeveynin hash'i ve sıra numarası 100'ü göndermek zorunda değildir.
sadece Alice tarafından olduğu gerçeğini göndermek zorunda. Benzer şekilde, diğerini de göndermesi gerekir.
ebeveyn Ed'e ait ve bu Ed'in 50. etkinliği. Yani iki büyük karma yerine,
Bob basitçe üçlüyü gönderiyor (Alice, Ed, 50). Biraz özenle, kimlikler
ve sıra numaraları, her biri bir veya iki bayta sıkıştırılabilir, böylece üçlü
yalnızca 3 ila 6 bayt gerekir. Bu, imzaya kıyasla küçük bir ek yüktür (ki
512 bitlik bir imza için 64 bayttır) ve olay içindeki işlemler (belki
ortalama 100 bayt veya daha fazla). Dolayısıyla, her olay en az bir işlem içeriyorsa,
o zaman bir hashgraph'ı dedikodu yapmak için neredeyse hiçbir ek yük yoktur, sadece dedikodu yapmanın ötesinde
işlemlerin kendileri.
Ve oylama sanal olduğu için, başka bir bant genişliği maliyeti yoktur.
fikir birliğine varmak. Bu anlamda, hashgraph mutabakatı için gereken bant genişliği
teorik sınıra çok yakın;
imzalı ve tarihli işlemleri kendileri gönderin.
Yalnızca işlemleri gönderen bir sistem, bant genişliğinden tasarruf edebilir.
Uygulama zaman damgalarına ihtiyaç duymadıysa işlemlere zaman damgaları eklemek.
Hashgraph fikir birliği aynı şeyi yapabilir. Bu durumda, bir
olay, kendi ebeveyninin "zaman damgası" artı bir olan bir tam sayı olacaktır.
Bob, Carol'a bir olay gönderdiğinde, bu sıra numarası şu şekilde hesaplanabilir:
Carol, bu yüzden Bob'un bunu internet üzerinden göndermesine gerek yok.
Yalnızca işlem gönderen bir sistem, gruplandırarak da bant genişliğinden tasarruf edebilir
aynı oluşturucu tarafından yapılan birkaç işlemi bir araya getirerek ve yalnızca tek bir işaret iliştirerek
işlem başına bir tane yerine listenin niteliği. Hashgraph aynı şeyi yapabilir,
birkaç işlemi tek bir etkinliğe koyarak ve böylece yalnızca tek bir
liste için imza.
Dolayısıyla, hashgraph mutabakatının bant genişliği gereksinimleri,
her durumda teorik asgari.
7.4. **Hızlı seçimler.** Algoritmanın ikinci kısmı bir Bizans anlaşmasıdır.
şöhrete karar verme adımı. İlginç bir özelliği var. Bir grup üye olduğunda
tümü çevrimiçi ve tüm katılımcılar düzenli olarak, Bizans sözleşmesi uygulanacaktır.
neredeyse tüm seçmenlerin aynı oylarla başladığı bir dizi seçime. Yani
yuvarlak çünkü *r* 1 Tanık kuvvetle yuvarlak birçok göreceksiniz *r* a nedenle, tanıklar
turun yaklaşık iki "dedikodu dönemi" sürmesi beklenebilir.
bir mesajın tüm toplulukta yayılması için geçen süredir. Bu

Çevrimiçi *n* üye varken, *log* 2 (*n*) eşitlemesi yapma zamanı olmalıdır . Bir
Yuvarlak *r* + 1 tanık *x* yuvarlak ün üzerinde oy EVET *R* tanık *y* , değil
için gerekli *x* kuvvetle görmek *y* . Bu sadece görebilirsiniz *y* . Beklenirdi ki
y tek bir dedikodu döneminde tüm çevrimiçi üyelere yayılır. Bu yüzden orada
onlara iki dedikodu içinde yayılma olasılığı çok yüksek
dönemler. Yani pratikte, herkes çevrimiçiyken ve katılırken,

Sayfa 93

tanıklara neredeyse her zaman, birçok tura gerek kalmadan hemen karar verilir
oylama.
Benzer şekilde, *Y* , bir yuvarlak *r* tanık, ama uykuda bir üyesi tarafından oluşturulmuş
ve sonra *r* turunun bitiminden hemen önce uyandığında , büyük olasılıkla
yuvarlak *r* +1 tanıklar *y için* HAYIR oyu verecek ve seçim hemen sona erecek.
Tek bir senkronizasyonun süresine göre küçük bir zaman penceresi vardır.
hangi bir üyenin uyanması ve *y* yaratması raund *r* + 1 tanıklara neden olabilir
eşit bir oy dağılımıyla başlamak için. Çevrimiçi üyelerin hepsi seçiyorsa
birbirlerini rastgele ve sık sık senkronize ederseniz, böyle bir sonuç bir
3 turdan fazlası için sadece birkaç yüzde olasılıkla yaklaşık 3 turda karar
mermi ve 6 turdan fazlası için yüzde onda birinden az. Bir saldırgan
İnterneti tamamen kontrol ederse, bunun üstel olarak sürüklenmesine neden olabilirler
birçok tur. Bu, sabit bir beklenen raund sayısına düşürülebilir.
"orta bit" yerine kriptografik bir "paylaşılan para" protokolü kullanarak
imza ”yukarıdaki algoritmada açıklanmıştır. Ortadaki bit şunun gibi olması amaçlanmıştır
saldırganın yapamayacağı bağımsız bir rastgele yazı tura atan her üye
önceden tahmin edin. Paylaşılan bir madeni para protokolü aynıdır, ancak tüm üyelerin
aynı "rastgele" sonuçla sonuçlanır. Bu ek, teorik
en kötü durum beklenen süre. Ancak böyle bir ekleme, muhtemelen değere değmeyecektir.
pratikte çaba. Bir saldırgan, interneti gerçek anlamda koruyacak kadar kontrol edebiliyorsa,
dürüst üyelerin uzun bir süre birbirleriyle rastgele senkronize olmalarını, sonra
saldırgan muhtemelen dürüst kullanıcıların erişimini engelleme gücüne sahiptir.
hiç internet. Dolayısıyla, paylaşılan bir madeni para burada sadece teorik olarak ilgi çekiyor gibi
görünüyor.
Ancak paylaşılan bir madeni para kullanmak her zaman bir seçenektir.
7.5. **Etkili hesaplamalar.** Algoritmanın ilk bölüm adımı, bir
Yeterince güçlü bir şekilde görüp görmediğine bağlı olarak bir olaya *r* veya *r* + 1 turu
yuvarlak *r* olaylar. Bu nedenle, bir *r* tanık olayının *x* olup olmadığını hesaplamak gerekir.
keyfi bir *y* olayıyla güçlü bir şekilde görülebilir . Aşağıdakiler hesaplamanın bir yoludur
bu cevap.
Her olaya sıra numarasından bir büyük olan bir sıra numarası verin
kendi ebeveyninin. *Y* için bir dizi ve *x* için bir dizi *saklayın* . *Y* dizisi hatırlar
y'nin atası olan her üye tarafından son olayın sıra numarası . The
dizi için *x* , her üye tarafından ilk olayın sıra numarasını hatırlar
bu, *x'in* soyundan gelir . İki diziyi karşılaştırın ve içinde kaç tane eleman bulun.
Y dizisi daha büyük olan ya da karşılık gelen elemanına eşit *x* dizisi. Eğer
2'den fazla *n* / 3 eşleşme varsa, *y* kesinlikle *x'i* görür . Karşılaştırması
X ve *Y* diziler (daha fazla çekirdek kullanmak için), ambalaj çoklu kullanım ile hızlandırılabilir
montaj kullanarak (ALU'yu daha verimli kullanmak için) tek bir tam sayıya birden çok öğe
dil (CPU vektör talimatlarına erişmek için) veya GPU (daha fazla vektör için)
paralellik).
8. Sonuçlar
Swirlds hashgraph veri yapısına dayalı yeni bir sistem sunulmuştur.

ture ve Swirlds hashgraph fikir birliği algoritması. Adil, hızlı, Bizans
hata toleranslı ve sanal oylama sayesinde son derece verimli bant genişliği. Algo-
rithm, şekillerde zorunlu bir dil kullanılarak sözde kodda verilmiştir, ancak
işlevsel bir biçimde tarif etmek de çok doğal. Ek,
kısa ve ilgi çekici olabilecek işlevsel bir biçimde algoritma.

Sayfa 94

Referanslar
[1] Miguel Castro ve Barbara Liskov. Pratik Bizans hata toleransı. In *Proceedings Üçüncü İşletim Sistemleri Tasarımı ve Uygulaması Sempozyumu* , OSDI '99, sayfalar 173–186, Berkeley, CA, USA, 1999. USENIX Association.
[2] Leslie Lamport, Robert Shostak ve Marshall Pease. Bizans generalleri sorunu. *ACM Trans. Program. Lang. Syst.* , 4 (3): 382–401, Temmuz 1982.
[3] Michael J. Fischer, Nancy A. Lynch ve Michael S. Paterson. Dağıtılmanın imkansızlığı bir hatalı işlemle fikir birliği. *J. ACM* , 32 (2): 374–382, Nisan 1985.
[4] Leslie Lamport. Yarı zamanlı parlamento. *ACM Trans. Comput. Syst.* , 16 (2): 133–169, Mayıs 1998.
[5] Diego Ongaro ve John Ousterhout. Anlaşılır bir fikir birliği algoritması arayışı içinde. İçinde *2014 USENIX Yıllık Teknik Konferansı (USENIX ATC 14)* , sayfalar 305–319, Philadelphia, PA, Haziran 2014. USENIX Derneği.
[6] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi ve Dawn Song. Bft'nin bal porsuğu protokoller. Cryptology ePrint Arşivi, Rapor 2016/199, 2016. http://eprint.iacr.org/.
[7] Allen Clement, Edmund Wong, Lorenzo Alvisi, Mike Dahlin ve Mirco Marchetti. Yapımı Bizans hataya dayanıklı sistemler, bizans hatalarını tolere eder. In *6 USENIX Proceedings Ağa Bağlı Sistem Tasarımı ve Uygulaması Sempozyumu* , NSDI'09, sayfalar 153-168, Berkeley, CA, ABD, 2009. USENIX Derneği.
[8] Satoshi Nakamoto. Bitcoin: Eşler arası elektronik nakit sistemi. internete gönderildi Kasım, 2008, 2008. http://bitcoin.org/bitcoin.pdf.
[9] Giulio Prisco. Intel, Hyper-
defter projesi. *Bitcoin Magazine* , Nisan 2016.
[10] Dağ-Erling Smorgrav. FreeBSD üç aylık durum raporu. FreeBSD.org'da yayınlandı, 2013. http://www.freebsd.org/news/status/report-2013-09-devsummit.html#Security.
[11] Miguel Miguel Correia, Giuliana Santos Veronese, Nuno Ferreira Neves ve Paulo Verissimo. Eşzamansız mesaj geçirme sistemlerinde Bizans mutabakatı: bir anket. *Uluslararası Kritik Bilgisayar Tabanlı Sistemler Dergisi* , 2 (2): 141–161, 2011.

Sayfa 95

9. Ek A: İşlevsel formda fikir birliği algoritması
Bir olay bir demettir *e = {p, h, t, i, s}* burada:
p = yük (*e*) = işlem listesi gibi "yük" verileri
h = karmalar (*e*)
= olayın ebeveynlerinin karmalarının bir listesi, önce kendi ebeveyni
t
= zaman (*e*)
= oluşturucunun, olayın oluşturulmasına ilişkin talep ettiği tarih ve saat
ben

= *yaratan* (*e*) = yaratıcının kimlik numarası
s = *sig* (*e*)
= oluşturucunun *{p, h, t, i}* dijital imzası
ebeveynler (*x*) = x olayının ebeveynleri olan olaylar kümesi
selfParent (*x*) = x olayının kendi ebeveyni veya none yoksa
n = popülasyondaki üye sayısı
c = bozuk para turlarının sıklığı (*c* = 10 gibi)
d = seçim başlamadan önce ertelenen raundlar (*d* = 1 gibi)
E = hashgraph'daki tüm olayların kümesi
E 0
= E ∪{ ∅ }
T = tüm olası (*saat, tarih*) çiftlerinin kümesi
B = *{true, f alse}*
N = *{* 1 , 2 , 3 , ...*}*
ebeveynler: *E* → 2 *E*
selfParent: *E* → *E* 0
ata: *E* × *E* → B
özAta: *E* × *E* → B
manyCreators: 2 *E* → B
bkz: *E* × *E* → B
kesinlikleBakınız: *E* × *E* → B
parentRound: *E* → N
roundInc: *E* → B
yuvarlak: *E* → N
tanık: *E* → B
fark: *E* × *E* → I
oylar: *E* × *E* × B → N
Kırık Gerçek: *E* × *E* → R
karar: *E* × *E* → B
oy: *E* × *E* → B
oy: *E* × *E* → B
ünlü: *E* → B
uniqueFamous: *E* → B
Karar verilen: N → B
roundAlındı: *E* → N
Alınan zaman: *E* → T

Sayfa 96

9. Ek A: İşlevsel formda fikir birliği algoritması
Bir olay bir demettir *e = {p, h, t, i, s}* burada:
p = *yük* (*e*) = işlem listesi gibi "yük" verileri
h = *karmalar* (*e*)
= olayın ebeveynlerinin karmalarının bir listesi, önce kendi ebeveyni
t
= *zaman* (*e*)
= oluşturucunun, olayın oluşturulmasına ilişkin talep ettiği tarih ve saat
ben
= *yaratan* (*e*) = yaratıcının kimlik numarası
s = *sig* (*e*)
= oluşturucunun *{p, h, t, i}* dijital imzası

ebeveynler (x) = x olayının ebeveynleri olan olaylar kümesi
selfParent (x) = x olayının kendi ebeveyni veya none yoksa
n = popülasyondaki üye sayısı
c = bozuk para turlarının sıklığı (c = 10 gibi)
d = seçim başlamadan önce ertelenen raundlar (d = 1 gibi)
E = hashgraph'daki tüm olayların kümesi
E 0
= E $\cup \{ \emptyset \}$
T = tüm olası (*saat, tarih*) çiftlerinin kümesi
B = *{true, f alse}*
N = { 1 , 2 , 3 , ...}
ebeveynler: $E \rightarrow 2\ E$
selfParent: $E \rightarrow E$ 0
ata: $E \times E \rightarrow$ B
özAta: $E \times E \rightarrow$ B
manyCreators: $2\ E \rightarrow$ B
bkz: $E \times E \rightarrow$ B
kesinlikleBakınız: $E \times E \rightarrow$ B
parentRound: $E \rightarrow$ N
roundInc: $E \rightarrow$ B
yuvarlak: $E \rightarrow$ N
tanık: $E \rightarrow$ B
fark: $E \times E \rightarrow$ I
oylar: $E \times E \times$ B $\rightarrow$ N
Kırık Gerçek: $E \times E \rightarrow$ R
karar: $E \times E \rightarrow$ B
oy: $E \times E \rightarrow$ B
oy: $E \times E \rightarrow$ B
ünlü: $E \rightarrow$ B
uniqueFamous: $E \rightarrow$ B
Karar verilen: N $\rightarrow$ B
roundAlındı: $E \rightarrow$ N
Alınan zaman: $E \rightarrow$ T

EKLER

Sayfa 97

ata (x, y)
= $x = y \vee \exists z \in$ ebeveynler (x) , ata (z, y)
selfAncestor (x, y) = $x = y \vee$ (selfParent (x) = 0 $\wedge$ selfAncestor (selfParent (x) , y))
manyCreators (S) = $| S | > 2\ n / 3 \wedge \forall x, y \in S,$ ($x = y = \Rightarrow$ yaratıcı (x) = yaratıcı (y))
bkz. (x, y)
= ata (x, y) $\wedge \neg$ ($\exists a, b \in E,$ yaratıcı (y) = yaratıcı (a) = yaratıcı (b) $\wedge$
ata (x, a) $\wedge$ ata (x, b) $\wedge \neg$ özAta (a, b) $\wedge \neg$ özAta (b, a))
kesinlikleBkz. (x, y)
= bkz. (x, y) $\wedge$ ($\exists S \subseteq E,$ manyCreators (S)
$\wedge$ ($z \in S = \Rightarrow$ (bkz. (X, z) $\wedge$ bkz. (Z, y))))
parentRound (x)
= maks ({ 1 } $\cup$ { yuvarlak (y) | $y \in$ ebeveynler (x) })
roundInc (x)
= $\exists S \subseteq E,$ manyCreators (S)
$\wedge$ ($\forall y \in S,$ round (y) = parentRound (x) $\wedge$ kesinlikleBkz. (X, y))

yuvarlak (*x*)
= parentRound (*x*) + {
1 eğer roundInc (*x*)
0 aksi halde
tanık (*x*)
= (selfParent (*x*) = 0) ∨(round (*x*) > round (selfParent (*x*))
fark (*x, y*)
= yuvarlak (*x*) - yuvarlak (*y*)
oylar (*x, y, v*)
= | {*z* ∈ E | fark (*x, z*) = 1 ∧ şahit (*z*) ∧ kesinlikleBkz. (*x, z*) ∧ oy (*z, y*) = *v*} |
fractTrue (*x, y*)
=
oylar (*x, y, doğru*)
(oylar (*x, y, doğru*) + oylar (*x, y, yanlış*))
karar (*x, y*)
= (selfParent (*x*) = 0 ∧ karar vermek (selfParent (*x*) , *y*)) ∨ (tanık (*x*) ∧ tanık (*y*)
∧ fark (*x, y*) > *d* ∧ (fark (*x, y*) mod *c*> 0) ∧ (∃*v* ∈ *B*, oy (*x, y, v*) >
2 *n*
3)))
copyVote (*x, y*)
= (¬ tanık (*x*)) ∨ (selfParent (*x*) = 0 ∧ karar (selfParent (*x*) , *y*)
oy (*x, y*)
=
□
□□□□□□□□□
□□□□□□□□□
oy (selfParent (*x*) , *y*)
copyVote (*x*) ise
bkz. (*x, y*)
eğer ¬ copyVote (*x*) ∧ fark (*x, y*) = *d*
1 = ortaBit (imza (*x*)) eğer ¬ copyVote (*x*) ∧ fark (*x, y*) = *d*
∧ (fark (*x, y*) mod *c* = 0)
∧ (1
3 ≤ fractTrue (*x, y*) ≤
2
3)
fractTrue (*x, y*) ≥
1
2
aksi takdirde
ünlü (*x*)
= ∃*y* ∈ *E*, karar *ver* (*y, x*) ∧ oy (*y, x*)
uniqueFamous (*x*) = ünlü (*x*) ∧ ¬∃*y* ∈ *E*, *y* = *x* ∧ ünlü (*y*)
∧ yuvarlak (*x*) = yuvarlak (*y*) ∧ yaratıcı (*x*) = yaratıcı (*y*)
Karar verildi (*r*) = ∀*x* ∈ *E*, ((yuvarlak (*x*) ≤ *r* ∧ tanık (*x*)) = ⇒∃*y* ∈ *E*, karar (*y, x*))
yuvarlandı (*x*) = min ({*r* ∈ N | yuvarlar Karar verildi (*r*) ∧ (∀*y* ∈ *E*,
(yuvarlak (*y*) = *r* ∧ benzersizFamous (*y*)) = ⇒ata (*y, x*)
alınan zaman (*x*)
= medyan ({ zaman (*y*) | *y* ∈ *E* ∧ ata (*y, x*) ∧
(∃*z* ∈ *E*, round (*z*) = roundAlınan (*x*) ∧ uniqueFamous (*z*)
∧ selfAncestor (*z, y*}) ∧ ¬ (∃*w* ∈ *E*, selfAncestor (*y, w*) ∧ ata (*w, x*)) })