Ripple Labs Inc, 2014

Ripple Protokol Konsensüs Algoritması

David Schwartz
david@ripple.com
Noah Youngs
nyoungs@nyu.edu
Arthur Britto
arthur@ripple.com

Öz

Bizans Generalleri Sorunu için birkaç fikir birliği algoritması varken, özellikle
dağıtılmış ödeme sistemleriyle ilgilidir, çoğu gereksinimden kaynaklanan yüksek gecikmeden
muzdariptir
ağ içindeki tüm düğümler eşzamanlı olarak iletişim kurar. Bu çalışmada bir roman sunuyoruz
Toplu olarak güvenilen alt ağları kullanarak bu gereksinimi aşan fikir birliği algoritması
daha büyük ağ içinde. Bu alt ağlar için gereken "güven" in asgari düzeyde olduğunu gösteriyoruz
ve üye düğümlerin ilkeli seçimi ile daha da azaltılabilir. Ayrıca şunu da gösteriyoruz:
Ağın tamamında anlaşmayı sürdürmek için minimum bağlantı gerekir. Sonuç bir
Bizans başarısızlıkları karşısında hala sağlamlığı koruyan düşük gecikmeli fikir birliği algoritması. Biz
bu algoritmayı Ripple Protokolündeki uygulamasında sunun.

İçindekiler

1. Giriş

Dağıtık fikir birliği sistemlerine ilgi ve araştırma
bir merkez ile son yıllarda önemli ölçüde artmıştır.
dağıtılmış ödeme ağlarına odaklanın. Böyle bir ağ-
işler hızlı, düşük maliyetli işlemlere izin verir.
merkezi bir kaynak tarafından kontrol edilir. Ekonomik iken

böyle bir sistemin faydaları ve dezavantajları değerlidir
kendi içlerinde çok fazla araştırma var, bu çalışma
tümünün dağıttığı bazı teknik zorluklar hakkında
ödeme sistemleri karşı karşıya gelmelidir. Bu sorunlar varken
çeşitli, onları üç ana kategoriye ayırıyoruz: cor-
doğruluk, anlaşma ve fayda.
Doğruluk derken, bunun için gerekli olduğunu kastediyoruz.
farklılıkları ayırt edebilmek için dağıtılmış sistem
doğru ve hileli bir işlem arasında geçiş yapın. Geleneksel olarak
güvene dayalı ayarlar, bu, aralarında güven ile yapılır.
garanti veren kurumlar ve kriptografik imzalar
gerçekten kurumdan gelen bir işlem var
geldiği iddia ediliyor. Dağıtık sistemlerde,
ancak, herhangi birinin kimliği gibi bir güven yoktur.
ve ağdaki tüm üyeler bilinmeyebilir bile.
Bu nedenle, doğruluk için alternatif yöntemler olmalıdır

Sayfa 2

kullanıldı.
Anlaşma, bir sürdürme sorununa atıfta bulunur.
merkezi olmayan bir hesap karşısında tek bir küresel gerçek-
ing sistemi. Doğruluk problemine benzer olsa da,
aradaki fark, kötü niyetli
ağ kullanıcısı bir fraudu oluşturamayabilir
ödünç işlem (doğruluğa meydan okuyan),
bir şekilde birden fazla doğru işlem oluşturun
birbirlerinin farkında değiller ve böylece bir araya gelerek
dolandırıcılık eylemi. Örneğin kötü niyetli bir kullanıcı,
yalnızca yeterli para ile iki eşzamanlı satın alma
hesapları her bir satın alma işlemini ayrı ayrı kapsayacak, ancak
ikisi birlikte değil. Böylece her işlem kendi başına
doğru, ancak bu şekilde eşzamanlı olarak yürütülürse
dağıtılmış ağın bir bütün olarak farkında olmadığını
her ikisinde de açık bir sorun ortaya çıkar ve genellikle
"Çift Harcama Sorunu" [1]. Böylece anlaşma
sorun, yalnızca bir gereklilik olarak özetlenebilir.
küresel olarak tanınan bir dizi işlem vardır:
ağ.
Fayda, biraz daha soyut bir sorundur.
genel olarak dağıtılmış bir ücretin "faydası" olarak tanımlayın
ment sistemi, ancak pratikte çoğu zaman basitleştiren
sistemin gecikmesine. Dağıtılmış bir sistem
hem doğru hem de hemfikir ama bir tane gerektirir
Örneğin, bir işlemin işlenme yılı belli ki
yenilmez bir ödeme sistemi. Kullanımın ek yönleri-
gerekli bilgi işlem gücü düzeyini içerebilir
doğruluk ve anlaşma süreçlerine katılmak
veya bir son kullanıcının yapması gereken teknik yeterlilik
ağda dolandırılmaktan kaçının.
Bu sorunların çoğu çok önceden araştırılmıştı
modern dağıtılmış bilgisayar sistemlerinin ortaya çıkışı,
"Bizans Generalleri Sorunu" olarak bilinen bir sorun
[2]. Bu problemde, her biri kontrol eden bir grup generalin
ordunun bir kısmı ve bir saldırıyı koordine etmelidir.

birbirlerine haberciler göndermek. Çünkü nesil-
als yabancı ve düşmanca bir bölgede, haberciler
hedeflerine ulaşamayabilir (tıpkı bir
dağıtılmış ağ başarısız olabilir veya bozuk veri gönderebilir
amaçlanan mesaj yerine). Ek bir yön
sorunun nedeni, generallerin bazılarının
ya bireysel olarak ya da birlikte komplo kuran hainler ve
böylece bir mesaj oluşturmayı amaçlayan mesajlar gelebilir
sadık nesil için başarısızlığa mahkum olan yanlış plan
als (tıpkı dağıtılmış bir sistemin kötü niyetli üyeleri gibi
sistemi sahtekarlığı kabul etmeye ikna etmeye çalışabilir
işlemler veya aynı gerçeğin birden çok versiyonu
çift harcamayla sonuçlanacak işlem). Böylece
dağıtılmış bir ödeme sistemi her ikisinde de sağlam olmalıdır
standart başarısızlıkların yüzü ve sözde "Bizans"
koordine edilebilecek ve kaynaklanabilecek arızalar
ağdaki birden çok kaynak.

Bu çalışmada, belirli bir uygulamayı analiz ediyoruz:
Dağıtılmış bir ödeme sisteminin tation: Ripple Pro-
tocol. Başarmak için kullanılan algoritmalara odaklanıyoruz
yukarıdaki doğruluk, anlaşma ve fayda hedefleri,
ve hepsinin karşılandığını gösterin (gerekli ve önceden
iyi anlaşılmış olan mayınlı tolerans eşikleri).

Ek olarak, mutabakatı simüle eden bir kod da sağlıyoruz.
parametrelendirilebilir ağ boyutu, numarası ile sus süreci
kötü niyetli kullanıcılar ve ileti gönderme gecikmeleri.

2. Tanımlar, Biçimlendirme ve Önceki iş

Ripple'ın bileşenlerini tanımlayarak başlıyoruz
Protokol. Doğruluğu, anlaşmayı kanıtlamak için ve
faydalı mülkler, önce bu özellikleri biçimlendiriyoruz
aksiyomlar. Bu özellikler, birlikte gruplandığında oluşur
fikir birliği kavramı:
ağ doğru anlaşmaya varır. Sonra vurgularız
fikir birliği algoritmalarıyla ilgili önceki bazı sonuçlar,
ve son olarak Ripple için fikir birliği hedeflerini belirtin
Resmileştirme çerçevemiz dahilindeki protokol.

2.1 Ripple Protokol Bileşenleri

Dalgalanma ağı tanımımıza kesin olarak başlıyoruz.
Aşağıdaki terimleri kullanarak:

• Sunucu: Sunucu, Ripple'ı çalıştıran herhangi bir varlıktır
Sunucu yazılımı (Ripple İstemcisinin aksine
yalnızca bir kullanıcının gönderip almasına izin veren yazılım
fonlar), konsensüs pro-
cess.

• Defter: Defter, tutarın bir kaydıdır
her kullanıcının hesabındaki para birimidir ve temsil eder
ağın "temel gerçeği". Defter
başarılı işlemlerle defalarca güncellenen
mutabakat sürecinden tamamen geçer.

• Son Kapanan Defter: Son kapatılan defter
tarafından onaylanan en son defter
fikir birliği süreci ve dolayısıyla mevcut durumu temsil eder
ağın durumu.

• Açık Defter: Açık defter, mevcut defterdir

bir düğümün çalışma durumu (her düğüm,
kendi açık defteri). Tarafından başlatılan işlemler
belirli bir sunucunun son kullanıcıları açık olana uygulanır
2

---

3. Sayfa

bu sunucunun defteri, ancak işlemler kontr değil
onlar geçene kadar son olarak kabul edildi
mutabakat süreci, bu noktada açık defter
son kapatılan defter olur.
• Benzersiz Düğüm Listesi (UNL): Her sunucu, ana
diğerlerinden oluşan benzersiz bir düğüm listesi içerir.
rıza belirlerken sorgulayan sunucular
sus. Sadece diğer üyelerin oyları
UNL of s, con-
sensus (ağdaki her düğümün aksine).
Böylece UNL, ağın bir alt kümesini temsil eder
toplu olarak alındığında, kullanıcılar tarafından "güvenilen"
ağı dolandırmak için işbirliği yapmamak
iş. Bu "güven" tanımının
UNL'nin her bir üyesinin
güvenilebilir (bkz. bölüm 3.2).
• Teklif veren: Herhangi bir sunucu işlemleri yayınlayabilir
mutabakat sürecine dahil edilecek ve her biri
sunucu her geçerli işlemi dahil etmeye çalışır
yeni bir fikir birliği turu başladığında. Esnasında
fikir birliği süreci, ancak, yalnızca
Bir sunucunun UNL'sindeki sunucular kabul edilir
göre s.

2.2 Biçimlendirme

Hatalı olmayan terimini ağdaki düğümlere atıfta bulunmak için kullanıyoruz.
dürüst ve hatasız davranan işler. Tersine,
hatalı bir düğüm, hatalarla karşılaşan bir düğümdür.
dürüst ol (veri bozulması nedeniyle, uygulama hatası
söylentiler, vb.) veya kötü niyetli (Bizans hataları). Azaltıyoruz
basit bir ikiliye bir işlemi doğrulama kavramı
karar problemi: her bir düğüm içeriden karar vermelidir.
oluşum 0 veya 1 değerinde verilmiştir.
Attiya, Dolev ve Gill, 1984'te [3] olduğu gibi,
aşağıdaki üç aksiyoma göre fikir birliği:
1. (C1): Arızasız her düğüm,
sonlu zaman
2. (C2): Arızalı olmayan tüm düğümler aynı ondalık noktaya ulaşır
sion değeri
3. (C3): 0 ve 1, tümü olmayanlar için olası değerlerdir.
hatalı düğümler. (Bu, önemsiz çözümü ortadan kaldırır
tüm düğümlerin 0 veya 1'e karar verdiği
sunulan bilgiler).

2.3 Mevcut Mutabakat Algoritmaları

Algoritmalar üzerinde pek çok araştırma yapılmıştır.
Bizans hataları karşısında fikir birliğine varmak. Bu
önceki çalışma, tümünün
ağdaki katılımcılar önceden bilinmiyorsa,
mesajların eşzamansız olarak gönderildiği yer (var
tek bir düğümün yapacağı süreye bağlı değil

bir karara varmak için) ve bir tarifin olduğu yerde
güçlü ve zayıf fikir birliği arasında.
Onay üzerine önceki çalışmanın ilgili bir sonucu-
sus algoritmaları Fischer, Lynch ve Patterson'a aittir.
1985 [4], eşzamansız durumda,
feshetmeme her zaman bir uzlaşma olasılığıdır
sus algoritması, tek bir hatalı işlemle bile. Bu
zamana dayalı buluşsal yöntemlerin gerekliliğini ortaya çıkarır.
yakınsamayı sağlamak (veya en azından tekrarlanan yinelemeler)
yakınsama). Bu sezgisel tarama için açıklayacağız
Bölüm 3'teki Ripple Protokolü.
Bir fikir birliği algoritmasının gücü genellikle
hatalı işlemlerin oranı cinsinden ölçülür
tahammül edebilir. Hiçbir çözümün olmadığı kanıtlanabilir.
Bizans Generalleri sorunu (zaten
eşzamanlılık ve bilinen katılımcılar) daha fazlasını tolere edebilir
(n − 1) / 3 Bizans hatasından veya ağın% 33'ünden
kötü niyetli davranmak [2]. Ancak bu çözüm,
teslim edilen mesajların doğrulanabilir gerçekliğini gerektirir
düğümler arasında (dijital imzalar). Üzerinde bir garanti varsa
mesajların taklit edilemezliği mümkündür, örneğin algoritmalar
senkronizasyonda çok daha yüksek hata toleransı ile
durum.
Daha fazla karmaşıklığa sahip çeşitli algoritmalar,
asynda Bizans konsensüsü için önerilmiştir
kronik durum. FaB Paxos [5] tolere edecek (n − 1) / 5
Bir düğüm ağındaki Bizans başarısızlıkları,
ağdaki düğümlerin% 20'sine kadar tolerans
kötü niyetle gizlice gizlice anlaşmak. Attiya, Doyev ve Gill [3] in-
asenkron durum için bir faz algoritması geliştirmek,
tolere edebilir (n − 1) / 4 başarısızlık veya% 25'e kadar
ağ. Son olarak, Alchieri ve ark., 2008 [6] mevcut
BFT-CUP,
bilinmeyen katılımcılarla bile asenkron durum,
(n − 1) / 3 hata toleransının maksimum sınırı,
ancak bağlantısında ek kısıtlamalar var
temel ağ.

2.4 Resmi Konsensüs Hedefleri

Bu çalışmadaki amacımız fikir birliğine varıldığını göstermektir.
Ripple Protokolü tarafından kullanılan algoritma,
her bir defter kapanışında fikir birliği (fikir birliği olsa bile
reddedilen tüm işlemlerin önemsiz mutabakatı) ve
önemsiz fikir birliğine yalnızca bir
Bizans başarısızlıkları karşısında bile olasılık biliniyor.

---

4. sayfa

Ağdaki her düğüm yalnızca teklifleri oyladığından
güvenilir bir düğüm kümesinden (UNL'sindeki diğer düğümler),
ve her düğüm farklı UNL'lere sahip olabileceğinden, biz de
aralarında sadece bir fikir birliğine varılacağını göstermek
UNL üyeliğinden bağımsız olarak tüm düğümler. Bu hedef
ayrıca ağda bir "çatallaşmanın" önlenmesi olarak da anılır: a
iki ayrık düğüm kümesinin her birinin ulaştığı durum
bağımsız olarak fikir birliği ve iki farklı son kapatılan

defterler, her düğüm kümesindeki düğümler tarafından gözlemlenir.
Son olarak, Ripple Protokolünün
(n - 1) / 5 başarısızlık karşısında bu hedeflere ulaşmak,
bu literatürdeki en güçlü sonuç değil, ama biz
ayrıca Ripple Protokolünün birkaç
faydasını büyük ölçüde artıran diğer arzu edilen özellikler.

3. Dalgalanma Konsensüs Algoritması

Dalgalanma Protokolü fikir birliği algoritması (RPCA),
sürdürmek için tüm düğümler tarafından birkaç saniyede bir uygulanır.
ağın doğruluğunu ve mutabakatını sağlamak. bir Zamanlar
fikir birliğine varılır, mevcut defter dikkate alınır
"Kapatılır" ve son kapatılan defter olur. Varsayım
fikir birliği algoritmasının başarılı olduğunu ve
ağda çatal yok, son kapatılan defter
ağdaki tüm düğümler tarafından bakım aynı olacaktır.

3.1 Tanım

RPCA turlar halinde ilerler. Her turda:

• Başlangıçta, her sunucu kendi geçerli tüm işlemleri alır
konsensüsün başlangıcından önce gördü
henüz uygulanmamış yuvarlak (bunlar
sondan itibaren başlatılan yeni işlemleri içerebilir
sunucunun kullanıcıları, yapılan işlemler
önceki bir fikir birliği süreci vb.) ve
olarak bilinen bir liste biçiminde halka açık
"Aday küme".

• Her sunucu daha sonra aday kümelerini birleştirir
kendi UNL'sindeki tüm sunuculardan
tüm işlemlerin.

• Minimumdan fazlasını alan işlemler
"evet" oylarının yüzdesi bir sonrakine geçer
yuvarlak, varsa, yapılan işlemler
Yeterli oy almayanlar ya atılır,
veya başlangıç için aday kümesine dahil edildi
bir sonraki defterde mutabakat süreci.

• Nihai fikir birliği turu minimum
bir sunucunun UNL kabul etme oranının% 80'i
bir işlemde. Bunu karşılayan tüm işlemler
muhasebeye gereksinim uygulanır ve
Defter kapanır, yeni son kapatılan olur
defter.

3.2 Doğruluk

Doğruluğa ulaşmak için, maksimum miktar verildiğinde
Bizans başarısızlıklarının, im-
hileli bir işlemin teyit edilmesi mümkün
fikir birliği sırasında, hatalı düğüm sayısı olmadıkça
bu toleransı aşıyor. Doğruluğunun kanıtı
RPCA daha sonra doğrudan izler: çünkü bir işlem
yalnızca bir sunucunun UNL'sinin% 80'i kabul ederse onaylanır
Bununla birlikte, UNL'nin% 80'i dürüst olduğu sürece dolandırıcılık yok-
ulent işlemler onaylanacaktır. Böylece bir UNL için
ağdaki düğüm sayısı, fikir birliği protokolü
doğruluğu şu kadar uzun süre koruyun:

$$f \leq (n - 1) / 5$$

(1)

f Bizans başarısızlıklarının sayısıdır. Aslında, hatta

(n − 1) / 5 + 1 Bizans başarısızlıkları karşısında, doğru-
ness teknik olarak hala korunmaktadır. Konsensüs yanlısı
cess başarısız olur, ancak yine de bir
hileli işlem. Gerçekten de (4n + 1) / 5 alır
Yanlış bir işlemin onaylanması için Bizans başarısızlıkları
sıkıldı. Buna zayıf için sınır diyoruz
doğruluk ve eski güçlü doğru için sınır-
ness.
Ayrıca, tüm "hileli" işlemlerin
eylemler, mutabakat sırasında onaylansa bile bir tehdit oluşturur.
sus. Bir kullanıcı, içinde iki kez para harcamayı denerse
iki işlem, örneğin, her iki işlem de
mutabakat sürecinde onaylandıktan sonra
ilk işlem uygulandığında, ikinci işlem başarısız olacaktır.
fonlar artık mevcut değil. Bu sağlamlığın nedeni
işlemlerin deterministik olarak uygulandığı gerçeği,
ve bu fikir birliği, ağdaki tüm düğümlerin
deterministik kuralları aynı sete uyguluyor
işlemler.
Biraz farklı bir analiz için şunu varsayalım:
herhangi bir düğümün gizli anlaşmaya karar verme olasılığı ve
hain bir kartele katılmak p c . Sonra olasılığı
doğruluk p ∗ ile verilir , burada:
p
∗ =
⌈ (n − 1
5) ⌉
∑
i = 0
(ni) p i
c (1− p c) n − ben
(2)
Bu olasılık, büyüklüğün olasılığını temsil eder.
hain kartelin% 100'ü maksimumun altında kalacak

5.Sayfa

Bizans başarısızlıklarının eşiği, verilen p c . Bundan beri
olasılık iki terimli bir dağılımdır, p c değerleri daha büyüktür
% 20'den fazla olması beklenen kartel boyutunun daha büyük olmasına neden olur
ağın% 20'sinden fazlası, fikir birliği yanlısı
cess. Uygulamada, bir UNL rastgele seçilmez, ancak
daha ziyade p c . Düğümler olduğundan
anonim değil, kriptografik olarak tanımlanabilir,
kıta karışımından bir UNL düğüm seçmek,
uluslar, endüstriler, ideolojiler vb. değerler üretecek
% 20'den çok daha düşük p c . Örnek olarak, proba
Anti-Defamation League ve Westboro'nun saflığı
Baptist Kilisesi, ağı dolandırmak için gizlice anlaştı.
% 20'den çok daha küçük. UNL olsa bile
nispeten büyük bir p c'ye sahiptir , diyelim ki% 15, olasılığı
doğruluk sadece 200 düğümde bile son derece yüksektir
UNL'de:% 97,8.
Olasılığının nasıl grafiksel bir temsili

yanlışlık, farklılıklar için UNL boyutunun bir fonksiyonu olarak ölçeklenir.
p c'nin ing değerleri Şekil 1'de gösterilmektedir.
dikey eksen, kötü niyetli olma olasılığını temsil eder.
kartel fikir birliğini engelliyor ve dolayısıyla daha düşük değerler
daha fazla fikir birliği başarısı olasılığı vardır. Olabileceği gibi
Hatta p ile, şekilde görüldüğü c yüksek şekilde% 10 olarak,
fikir birliğinin çok hızlı bir şekilde engellenme olasılığı
UNL 100 düğümü geçtikçe önemsiz hale gelir.

3.3 Sözleşme

Anlaşma gereksinimini karşılamak için gösterilmesi gerekir
tüm arızalı olmayan düğümlerin aynı noktada fikir birliğine varması
UNL'lerinden bağımsız olarak işlem kümesi. Dan beri
her sunucu için UNL'ler farklı olabilir, anlaşma
doğruluk kanıtı tarafından doğal olarak garanti edilmez.
Örneğin, üye ile ilgili herhangi bir kısıtlama yoksa-
UNL'nin gemisi ve UNL'nin boyutu daha büyük değil
$0.2 * n$ toplamdan daha fazla burada n toplam , içindeki düğüm sayısıdır
tüm ağ, o zaman bir çatal mümkündür. Bu il-
basit bir örnekle canlandırılmıştır (Şekil 2'de tasvir edilmiştir):
UNL grafiğinde her biri daha büyük iki grup hayal edin
toplam $0.2 * n$'den fazla . Klikler derken, bir dizi düğümü kastediyoruz
burada her düğümün UNL'si aynı düğüm kümesidir.
Bu iki klik herhangi bir üyeyi paylaşmadığı için,
her birinin doğru bir fikir birliğine varması mümkündür
birbirlerinden bağımsız olarak, anlaşmaya aykırı. Eğer
iki kliğin bağlantısı toplamda $0,2 * n$'yi aşıyor ,
o zaman anlaşmazlık olduğu gibi çatal artık mümkün değil-
klikler arasında, fikir birliği olmasını engelleyecekti
gerekli olan% 80 anlaşma eşiğine ulaşıldı.
Bağlantının üst sınırı

Şekil 2. Bunun için gerekli bağlantıya bir örnek
iki UNL kliği arasındaki çatalı önlemek.

kanıtlama anlaşması şu şekilde verilir:

$$|\text{UNL } i \text{ UNL } j| \geq \frac{1}{5} \max(|\text{UNL } i|, |\text{UNL } j|) \quad \forall i, j \quad (3)$$

Bu üst sınır, klik benzeri bir yapı olduğunu varsayar.
UNL'ler, yani düğümler, UNL'leri diğer
bu kümelerdeki düğümler. Bu üst sınır şunları garanti eder:
hiçbir iki grup birbiriyle çelişen işlemlerde fikir birliğine varamaz.
% 80'e ulaşmak imkansız hale geldiğinden
fikir birliği için gerekli eşik. Daha sıkı bir sınır
UNL'ler arasındaki dolaylı kenarlar alındığında mümkündür
hesaba katın. Örneğin,
ağ klik gibi değil, çatal çok daha fazlası oluyor
daha fazla dolaşıklıktan dolayı elde edilmesi zor
tüm düğümlerin UNL'leri.
Herhangi bir varsayımda bulunulmaması ilginçtir.
kesişen düğümlerin doğası hakkında. Kesişen
iki UNL'nin sayısı hatalı düğümler içerebilir, ancak çok uzun
kavşağın boyutu sınırdan daha büyük olduğu için
anlaşmayı garanti etmek için gerekli ve toplam sayı
Hatalı düğümlerin oranı, tatmin etmek için gereken sınırdan daha az
güçlü doğruluk, sonra hem doğruluk hem de anlaşma

elde edilecek. Yani anlaşma bağımlıdır
yalnızca düğümlerin kesişme boyutuna göre,
arızalı olmayan düğümlerin kesişiminin boyutu.

3.4 Fayda

Faydanın birçok bileşeni öznel olsa da,
bu gerçekten de kanıtlanabilir bir yakınsamadır:
sus süreci sonlu bir zamanda sona erecektir.
5

Sayfa 6

Şekil 1. Hain bir kartelin, UNL'nin boyutunun bir fonksiyonu olarak fikir birliğini engelleyebilme olasılığı, çünkü
farklı p c değerleri , UNL'nin herhangi bir üyesinin başkalarıyla işbirliği yapmaya karar verme olasılığı. Burada, daha alçak
değerler daha yüksek bir fikir birliği başarısı olasılığını gösterir.

3.4.1 Yakınsama

Yakınsamayı, RPCA'nın
Defterde güçlü bir doğrulukla fikir birliğine varır,
ve bu defter daha sonra son kapatılan defter olur. Not
teknik olarak zayıf doğruluk hala
algoritmanın yakınsaması, sadece yakınsamadır.
önerme C3 ihlal edildiğinden önemsiz durum ve hayır
işlemler asla onaylanmayacaktır. Sonuçlardan
yukarıda, güçlü doğruluğun her zaman başarıldığını biliyoruz.
(n − 1) / 5 Bizans başarısızlığı karşısında mümkün,
ve sadece bir fikir birliğine varılacağını
UNL-bağlılık con-
dition karşılanır (Denklem 3). Geriye kalan tek şey göstermek
bu koşulların her ikisi de karşılandığında, fikir birliği
sınırlı zamanda ulaşıldı.
Mutabakat algoritmasının kendisi deterministik olduğu için,
ve mutabakattan önce önceden belirlenmiş bir tur sayısı vardır, t
sonlandırılır ve mevcut işlem seti çıkarılır
açıklandı onaylandı veya onaylanmadı (bu noktada bile olsa
hiçbir işlemde% 80'den fazla gerekli kabul edilmez-
ment ve fikir birliği sadece önemsiz fikir birliğidir),
algoritmanın sonlandırılması için sınırlayıcı faktör
düğümler arasındaki iletişim gecikmesidir. Sırayla
bu miktarı sınırlandırmak için düğümlerin yanıt süresi
izlenir ve gecikmesi daha büyük olan düğümler
ön ayarlı bir b tüm UNL'lerden kaldırılır. Süre
bu, uzlaşmanın bir
tb'nin üst sınırı, sınırların
doğruluk ve anlaşma için açıklanan yukarıda olmalıdır
nihai UNL tarafından karşılanacak, tüm düğümlerden sonra
6

---

7. Sayfa

düşürüldü. Koşullar geçerliyse
tüm düğümler için ilk UNL'ler, ancak daha sonra bazı düğümler
gecikme nedeniyle ağdan düştü, doğruluk
ve sözleşme garantileri otomatik olarak geçerli değildir, ancak
yeni UNL'ler tarafından karşılanmalıdır.

3.4.2 Buluşsal Yöntemler ve Prosedürler

Yukarıda bahsedildiği gibi, gecikmeye bağlı buluşsal yöntem en-
Ripple Ağındaki tüm düğümlere zorla
fikir birliği algoritmasının yakınsaması. Ek olarak
bir kaç başka buluşsal yöntem ve yordam daha vardır.
RPCA'ya yardımcı program sağlar.
• Hepsi için zorunlu 2 saniyelik bir pencere vardır
ilk aday kümelerini önerecek düğümler
her turda fikir birliği. Bu giriş yaparken
her bir mutabakat için 2 saniyelik bir alt sınır belirleyin.
sus round, aynı zamanda tüm düğümlerin
makul gecikme, katılma yeteneğine sahip olacaktır.
fikir birliği sürecinde pate.
• Oylar her biri için deftere kaydedildiğinden
fikir birliği turu, düğümler işaretlenebilir ve
bazı yaygın nedenlerle ağdan kaldırıldı,
kolayca tanımlanabilen kötü niyetli davranışlar. Bunlar içinde-
her işlemde "Hayır" oyu veren düğümler,
ve tutarlı bir şekilde işlem öneren düğümler
fikir birliği ile doğrulanmamış.
• Tüm kullanıcılara seçilmiş bir varsayılan UNL sağlanır,
p c'yi en aza indirgemek için seçilmiştir , bölüm
3.2. Kullanıcılar kendi
kendi UNL'leri, bu varsayılan düğüm listesi,
saf kullanıcıların bile bir fikir birliğine katılacağını
doğruluğu ve mutabakatı sağlayan sus süreci-
son derece yüksek olasılıkla.
• Bir ağ bölünmüş algılama algoritması da em-
ağda bir çatallaşmayı önlemek için kullanıldı. Süre
mutabakat algoritması, işlemin
son kapatılan defterdeki bilgiler doğru, doğru
sondan fazla son kullanma olasılığını yasaklamaz
farklı alt bölümlerinde bulunan kapalı defter
zayıf bağlantıya sahip ağ. Denemek ve
böyle bir bölünmenin meydana gelip gelmediğini belirlemek, her düğüm
aktif üyelerinin boyutunu izler
UNL. Bu boyut aniden bir ön ayarın altına düşerse
eşik, bir bölünmenin gerçekleşmiş olması mümkündür.
Durumda yanlış pozitif önlemek için
Bir UNL'nin büyük bir bölümünde geçici
gecikme, düğümlerin "kısmi" yayınlamasına izin verilir
işlem yapmadıkları veya oy kullanmadıkları "doğrulama"
işlemlerde, ancak hala belirli olduğunu beyan edin
oybirliği sürecinde ipating, aksine
bağlantısız bir üzerinde farklı bir fikir birliği süreci
alt ağ.
• RPCA'nın
sadece bir tur fikir birliği, fayda elde edilebilir
birden fazla turdan, her biri bir artışla
Minimum gerekli anlaşma yüzdesini belirlemek,
% 80 şartla final turundan önce.
Bu turlar, gizli düğümlerin algılanmasına izin verir
bu tür birkaç düğümün bir
ağın işlem oranında darboğaz.
Bu düğümler, başlangıçta,
düşük şartlı mermileri yapıyor ama geride kalıyor

ve eşik arttıkça tanımlanmalıdır. İçinde
bir tur fikir birliği durumunda, durum böyle olabilir
çok az işlem% 80 eşiğini aşıyor,
yavaş düğümler bile ayak uydurabilir ve
tüm ağın işlem oranı.

4. Simülasyon Kodu

Sağlanan simülasyon kodu, bir tur
Parametrelendirilebilir özelliklere sahip RPCA (sayısı
ağdaki düğümler, kötü niyetli düğümlerin sayısı, la-
mesajların yoğunluğu, vb.). Simülatör mükemmel bir şekilde başlar
anlaşmazlık (başlangıçta ağdaki düğümlerin yarısı
"evet", diğer yarısı "hayır" önerir), sonra
her birinde gösterilen fikir birliği süreciyle ilerler
ağdaki evet / hayır oylarının sayısını düğümler olarak düzenlemek
tekliflerini kendi tekliflerine göre düzenlerler.
UNL üyeleri. % 80 eşiğine ulaşıldığında,
fikir birliğine varılır. Okuyucuyu eski
tanımlı sabitlerin farklı değerleri ile algılama
aşina olmak için "Sim.cpp" nin başlangıcı
farklı koşullar altında fikir birliği süreci ile.

5. Tartışma

Koşulları karşılayan RPCA'yı tanımladık.
doğruluk, anlaşma ve fayda durumları
yukarıda özetledim. Sonuç olarak Ripple Pro-
tocol, güvenli ve güvenilir işlemleri gerçekleştirebilir
birkaç saniyede: için gereken süre
tamamlanması gereken bir tur fikir birliği. Bu işlemler
ikinci bölümde özetlenen sınırlara kadar kanıtlanabilir şekilde güvenlidir.
en güçlüsü olmasa da 3 numaralı
Eşzamansız Bizans konsensüsü için literatür,
7

---

8. Sayfa

ağda hızlı yakınsama ve esnekliğe izin verir
üyelik. Birlikte ele alındığında bu nitelikler izin verir
Ripple Ağı hızlı ve düşük maliyetli bir şekilde çalışacak
iyi anlaşılmış güvenliğe sahip küresel ödeme ağı
ve güvenilirlik özellikleri.
Ripple Protokolünün
eşitlikte tanımlanan sınırlar olduğu sürece kanıtlanabilir şekilde güvenli
1. ve 3. bölümler karşılandı, bunların
maksimum sınırlar ve pratikte ağ olabilir
önemli ölçüde daha az katı koşullar altında güvenli. O
aynı zamanda tatmin edici olduğunu kabul etmek de önemlidir.
bu sınırlar RPCA'nın kendisinde değildir, ancak
bunun yerine tüm kullanıcıların UNL'lerinin yönetimini gerektirir.
Tüm kullanıcılara sağlanan varsayılan UNL zaten yeterlidir
cient, ancak bir kullanıcı UNL'de değişiklik yaparsa,
yukarıdaki sınırların bilgisi dahilinde yapılmalıdır. İçinde
ek olarak, küresel ağ yapısının bir miktar izlenmesi
Bağlanmanın sağlanması için gereklidir.
denklem 3 karşılandı ve bu anlaşma her zaman
memnun.
RPCA'nın önemli bir adımı temsil ettiğine inanıyoruz
dağıtılmış ödeme sistemleri için yönlendirme, düşük

gecikme, birçok finansal işlem türüne izin verir
daha önce başkalarıyla zor hatta imkansız hale gelmiş,
daha yüksek gecikmeli fikir birliği yöntemleri.

6. Teşekkür

Ripple Labs, tüm insanların
Ripple Protokolünün geliştirilmesinde yer aldı
fikir birliği algoritması. Özellikle, Arthur Britto, onun için
orijinal için işlem setleri üzerinde çalışın, Jed McCaleb
Dalgalanma Protokolü fikir birliği kavramı ve David Schwartz,
"anlaşamama, anlaşmaya varmaktır" konulu çalışması için
uzlaşmanın ”yönü. Ripple Labs ayrıca
Noah Youngs'a hazırlanmadaki çabaları için teşekkür
ve bu makaleyi gözden geçiriyoruz.

Referanslar

[1] Nakamoto, Satoshi. “Bitcoin: Eşler arası bir seçim
tronic nakit sistemi. " 1.2012 (2008): 28.
[2] Lamport, Leslie, Robert Shostak ve Marshall
Bezelye. "Bizans generalleri sorunu." ACM
Programlama Dilleri ve Sys ile İlgili İşlemler
tems (TOPLAS) 4.3 (1982): 382-401.
[3] Attiya, C., D. Dolev ve J. Gill. "Eşzamansız
Bizans Anlaşması. " Proc. 3 üncü. Yıllık ACM
Dağıtık Hesaplama İlkeleri Sempozyumu.
1984.
[4] Fischer, Michael J., Nancy A. Lynch ve Michael
S. Paterson. "Dağıtık uzlaşmanın imkansızlığı
tek bir hatalı işlemle. " ACM Dergisi (JACM)
32.2 (1985): 374-382.
[5] Martin, JP. Ve Lorenzo Alvisi. "Hızlı byzan-
tine fikir birliği. " Güvenilir ve Güvenli Bilgi İşlem,
3.3 (2006) tarihli IEEE İşlemleri: 202-215.
[6] Alchieri, Eduardo AP, vd. "Bizans mutabakatı
bilinmeyen katılımcılarla. " Dağıtık İlkeler
Sistemler. Springer Berlin Heidelberg, 2008. 22-40.