Sayfa 1

Taslak

Holochain

ölçeklenebilir ajan merkezli dağıtılmış bilgi işlem

TASLAK (ALPHA 1) - 15.02.2018

Eric Harris-Braun, Nicolas Luck, Arthur Brock 1

1 *Ceptr, LLC*

ÖZET: Ölçeklenebilir, aracı merkezli dağıtılmış bir bilgi işlem platformu sunuyoruz. Biz kullanıyoruz dağıtılmış sistemleri karakterize etmek için biçimcilik, bazı mevcut dağıtılmış sistemlere nasıl uygulandığını gösterin
ve veri merkezli bir modelden aracı merkezli bir modele geçmenin faydalarını gösterin.
Holochain sisteminin ayrıntılı bir biçimsel spesifikasyonunu, bir analiziyle birlikte sunuyoruz.
sistemik bütünlük, evrim için kapasite, toplam sistem hesaplama karmaşıklığı,
kullanım durumları ve mevcut uygulama durumu.

I.GİRİŞ

Dağıtılmış bilgi işlem platformları yeni bir
iki temelin ortaya çıkmasıyla yaşayabilirlik seviyesi
şifreleme araçları: güvenli hash algoritmaları ve
açık anahtarlı şifreleme. Bunlar çözümler sağladı
dağıtılmış hesaplamadaki temel sorunlara: doğrulanabilir,
durumu düğümler arasında paylaşmak için kurcalamaya dayanıklı veriler
dağıtılmış sistem ve veri kaynağının onayı
dijital imza algoritmaları aracılığıyla. İlki elde edildi
tekdüze veri depolarının yeniden olduğu karma zincirler ile
özünde kurcalamaya karşı korumalı (ve böylece güvenle
düğümler arasında paylaşılabilir) önceki hash değerlerini dahil ederek
sonraki girişlerdeki girişler. İkincisi,
veri karmalarının kriptografik şifrelemesini birleştirmek
ve genel anahtarları adres olarak kullanmak
böylece sistemdeki diğer ajanların
verilerin kaynağını matematiksel olarak doğrulayın.

Hash zincirleri bağımsız problemi çözmeye yardımcı olsa da
nazikçe hareket eden ajanlar durumu güvenilir şekilde paylaşıyor, iki görüyoruz
kullanımlarında derinlere sahip çok farklı yaklaşımlar
sistemik sonuçlar. Bu yaklaşımlar şeytani
günümüzün iki kanonik dağıtılmış sistemi tarafından oluşturulur:

1. git[1]: Git'te, tüm düğümler hash zincirlerini güncelleyebilir
uygun gördükleri gibi. Paylaşılan örtüşme derecesi
zincir girişlerinin durumu (commit nesneleri olarak bilinir)
tüm düğümler arasında git tarafından yönetilmez, bunun yerine eski
açıkça çekme taleplerinde bulunan aracının eylemi ile
ve birleştirme yapmak. Bu yaklaşım ajanı diyoruz.
merkezlidir çünkü düğümlere izin vermeye odaklanır
bağımsız olarak gelişen veri gerçeklerini paylaşın.
2. Bitcoin[2]: Bitcoin'de (ve genel olarak blok zincirinde),
"sorun", anlamlandırma sorunu olarak anlaşılıyor
bir işlem bloğunun nasıl seçileceğini öğrenin
madencilikte yaşanan birçok varyant
düğümler (müşterilerden işlem topladıkça
farklı siparişler) ve bu tek değişkeni işlemek-
küresel olarak paylaşılan tek zincire karınca. Biz buna diyoruz

1 https://git-scm.com/about

2 https://bitcoin.org/bitcoin.pdf

yaratıcılığa odaklandığı için veri merkezli yaklaşım
Tüm düğümler arasında tek bir paylaşılan veri gerçekliği sağlamak.

Bu temel orijinal duruşun,
doğrudan doğruya en önemli sınırlamada sonuçlanır.
blockchain: ölçeklenebilirlik. Bu sınırlama yaygın olarak bilinmektedir
3 ve birçok çözüm sunuldu 4. Holochain ...
doğrudan kök veriye hitap ederek ileriye doğru bir yol sunar.
blok zinciri yaklaşımının merkezli varsayımları.
II. ÖNCEKİ ÇALIŞMA
Bu makale büyük ölçüde kriptodaki son çalışmalara dayanmaktadır.
grafik dağıtılmış sistemler ve dağıtılmış karma tablolar
ve çok etmenli sistemler.
Ethereum: Ahşap [EIP-150] , DHT: [Kademlia] Benet
[IPFS]
YAPILACAKLAR: tartışma ve daha fazla referans burada
III. DAĞITILMIŞ SİSTEMLER
A. Biçimcilik
Dağıtılmış bir basit genelleştirilmiş model tanımlıyoruz
sistem Ω aşağıdaki gibi karma zincirleri kullanarak:
1. N, {n 1 , n 2 , ... n n } par- öğeler kümesi olsun
sistemde ticipating. N elemanlarını çağırın
düğümler veya aracılar.
2. Her düğüm düğümünün , öğeler içeren bir S n kümesinden oluşmasına izin verin
{σ 1 , σ 2 , ...}. Devletin S n unsurlarını çağırın
düğüm n. Bu yazının amaçları doğrultusunda biz-
sume iσ i ∈ S n : σ i = {X i , D i } X i a olmak üzere
karma zinciri ve D, karma olmayan zincir verileri kümesi
elementler.
3. H, kriptografik olarak güvenli bir hash işlevi olsun.
3 çeşitli kaynaklar ekleyin
Burada 4 dipnot daha var

---

4. Bir durum geçiş fonksiyonu olalım:
τ (σ ben , t) = (τ X (X ben , t), τ D (D ben , t))
(3.1)
nerede:
(a) τ X (X i , t) = X ben + 1 burada
X ben + 1 = X ben ∪ {x i + 1 }
= {x 1 , ..., x i , x i + 1 }
(3.2)
ile
x ben + 1 = {h, t}
h = {H (t), y}
y = {H (x j) | j <i}
(3.3)
Ha başlığını çağırın ve sıranın nasıl olduğuna dikkat edin
başlıkların sayısı bir zincir oluşturur (genel olarak ağaç
durum) her başlığı bir öncekine bağlayarak
başlık (lar) ve işlem.
(b) D ben + 1 = τ D (σ ben , t)
5. V (t, v) ile birlikte t alan bir fonksiyon olsun.
ekstra doğrulama verileri v, t'nin geçerliliğini doğrular ve
yalnızca geçerli t için bir geçiş işlevi çağırırsa. Telefon etmek

V bir doğrulama işlevi.
6. I (t) t işlemini alan bir fonksiyon olsun,
bunu bir V işlevi kullanarak değerlendirir ve geçerliyse kullanır
S dönüştürmek için τ. Girdi veya uyarıcıyı ara I
işlevi.
7. P (x) işlem oluşturabilen bir işlev olsun
t ve tetikleme fonksiyonları V ve τ ve P'nin kendisi
durum değişiklikleri veya zamanın geçişi tarafından tetiklenir.
P'yi işleme işlevini çağırın.
8. C, N'deki tüm düğümlere izin veren bir kanal olsun
iletişim kurmak için ve her bir düğümün bir
benzersiz adres A n . C'yi ve haberleşen düğümleri arayın ...
ağ üzerinden iletişim kurun.
9. E (i) fonksiyonları değiştiren bir fonksiyon olsun
VİP. E'yi evrim işlevi olarak adlandırın.
Açıklama: Bu biçimcilik, ayrı ayrı modellememize izin verir.
ajanların temel yönlerini toplayın.
İlk önce temsilcinin durumunu bir kriptografa ayırıyoruz.
ically sabitlenmiş hash-chain kısım X ve başka bir kısım
keyfi verileri D tutar. Sonra yukarı süreci böleriz-
devletin iki aşamaya tarihlenmesi: 1) yeninin doğrulanması
doğrulama işlevi V (t, v) aracılığıyla işlemler t,
ve 2) S iç durumunun fiili değişimi (ya X
veya D) durum geçiş fonksiyonları τ X ve τ D aracılığıyla .
Son olarak, 1) durum geçiş tetikleyicilerini birbirinden ayırıyoruz.
dış olaylardan kaynaklanan uyaranlar, I (t) aracılığıyla alınan,
ve 2) bir düğümün dahili işlemesi P (x) ile sonuçlanan
dahili olarak oluşturulan bir işlemle V ve τ çağrısında.
Dağıtılmış sistemlerin bazı temel özelliklerini tanımlıyoruz:
1. N'de işlevlerinden herhangi birinin
T, V, P ve E, olma özelliklerine sahiptir.
hem güvenilir şekilde biliniyor hem de aynı olduğu biliniyor
bu düğüm kümesi için: saygı duyulan güvenilen düğümler
çok bilinen işlevlere.
2. Mesaj gönderen özelliğe sahip bir C kanalını çağırın
taşıma sırasında tam olarak gönderildiği gibi ulaşacağına güvenilebilir:
güvenli.
3. Bir düğümün A n adresinin bulunduğu bir C kanalını çağırın
n, A n = H (pk n) 'dir, burada pk n ,
düğüm düğüm ve tüm mesajların bir
gönderen tarafından imzalanan mesajın dijital imzası:
doğrulanmış.
4. Karması ile erişilebilen bir veri öğesini çağırın
içerik adreslenebilir.
Bu yazının amaçları doğrultusunda güvenilmez olduğunu varsayıyoruz
düğümler, yani bağımsız olarak hareket eden ajanlar yalnızca kendi
kendi kontrolü ve güvensiz bir kanal. Biz bunu ...
kriptografik araçların varoluş nedeni
yukarıda bahsedilen, bireysel düğümlerin
tüm sistem bu varsayım altında. Kriptografi
anında durum verilerinde görünür hale getirir.
sistemdeki diğer düğüm, işlevlerin bir sürümünü kullanır
kendisinden farklı. Bu özellik genellikle şu şekilde anılır:
güvenilmez bir sistem. Ancak, sadece şu anlama geldiği için
güven odağının devlet verilerine kaydırıldığını,

diğer düğümlerden ziyade, buna sistemik güven diyoruz
içsel veri bütünlüğü üzerine. Ayrıntılı bilgi için IVC'ye bakın
dağıtılmış sistemlerde güven üzerine tartışma.
B. Veri Merkezli ve Ajan Merkezli Sistemler
Bu tanımı kullanarak Bitcoin şu şekilde anlaşılabilir:
sistem Ω bitcoin burada:
1. ∀n, m ∈ N: X n
!
= X m nerede
!
= araç zorunludur.
2. V (e, v) e bir bloktur ve v,
"İş kanıtı" hash-crack algoritması ve V con-
firmalar v'nin geçerliliğini, yapısını ve geçerliliğini
e çift harcama kurallarına göre5.
3. I (t, n) müşterilerden gelen işlemleri kabul eder ve ekler
daha sonrası için bir blok inşa etmek için onları D'ye (mempool)
V () tetiklemede kullanın.
4. P (i), "kanıtı" içeren madencilik sürecidir.
çalışma ”algoritması ve V () ve τ X ile oluşturur
hash kırıldığında.
5 işaretçi buraya

---

5. E (i) resmi olarak tanımlanmamıştır ancak haritası çıkarılabilir
gayri resmi olarak,
Bitcoin yazılımının yeni sürümlerini yüklemek için düğümler
eşya.
İlk nokta, Bit-
madeni para (ve genel olarak Blockchain uygulamalarının) stratejisi
Aksi halde karşılaşılan sorunları çözmek veya önlemek için
merkezi olmayan sistemlerde ve bu,
tüm düğümlerin sahip olması gereken bir ağ durumu oluşturun.
aynı (yerel) zincir.
Buna karşılık, Ω git için herhangi bir
X n , X m düğümlerinde n ve m eşleşiyor, git'in temel amacı olarak
farklı ajanların özerk hareket etmesine ve farklılaşmasına izin vermektir.
nazikçe paylaşılan bir kod tabanında, ki bu imkansız olurdu
eyaletler her zaman eşleşmek zorunda olsaydı.
Biçimciliğin merceğinden diğer bazı yönler
Ω git aşağıdaki gibi anlaşılabilir:
1. yalnızca varsayılan olarak doğrulama işlevi V (e, v)
e'nin yapısal geçerliliğini bir commit ob-
içerik değil ject (git'in de yaptığını unutmayın.
aynı zamanda bir parçası olan taahhütlerin imzalanmasını desteklemek
doğrulama)
2. Ω git için uyarıcı işlevi I (t) aşağıdakilerden oluşur:
kullanıcının kullanabileceği git komutları seti
3. durum geçiş işlevi τ X dahili gittir
bir commit nesnesi ekleyen fonksiyon ve τ D ,
tetiklenen dizine kod ekleyen git işlevi
ekleyerek

4. E, bitcoin'e benzer şekilde , resmi olarak aşağıdakiler için tanımlanmamıştır:
Ω git .
Biçimciliğin daha derinlemesine bir uygulamasını bırakıyoruz
Ω için Git okuyucu için bir excercise olarak, ancak altta
Ω bitcoin ve Ω git arasındaki temel farkı puanlayın
∀n, m ∈ N'nin oluşturucu kısıtlamasında yer alır: X n
!
= X m .
Bunun Ω bitcoin için doğrudan bir sonucu ,
X boyutu , n , Q ve zorunlu olarak tüm düğümler büyür Bitcoin şırası
boyut olarak büyür, oysa bu zorunlu değildir
Ω git'e ve içinde Bitcoin en ölçeklenebilirlik sorunları çekirdeğini yatıyor.
Veri merkezli bir yaklaşımın
Bitcoin için kullanılır. Bu, belirtildiği gerçeğinden kaynaklanmaktadır.
amaç, dijital olarak aktarılabilir "madeni paralar" yaratmaktı, yani
bu özelliği dağıtılmış bir dijital sistemde modellemek
konum olarak bilinen maddenin. Merkezi bilgisayarda
sistemler bu bir sorun olarak bile görünmüyor çünkü
merkezi sistemler,
veri merkezli bir bakış açısıyla düşünün. Bize izin veriyorlar
veri varmış gibi bir tür veri nesnelliğine inanmak,
konumu olan bir yerde oturan fiziksel bir nesne gibi.
Mutlak bir çerçeve açısından düşünmemize izin veriyorlar - sanki
veriler ve / veya zaman dizisi hakkında doğru bir gerçek vardır,
ve "fikir birliğinin" bu konuda bir araya gelmesi gerektiğini öne sürüyor
hakikat. Aslında bu bir bilgi mülkü değildir. Veri
her zaman bir gözlemcinin bakış açısından vardır. Bu
dijital olarak aktarılabilen "madeni paraları" zorlaştıran bu gerçek
tamamen oluşan dağıtık sistemlerde sorun
tanım gereği birden çok görüş noktası.
Dağıtılmış dünyada olaylar
tüm gözlemciler için aynı sıra. Blockchain spesifikasyonu için-
iktisadi olarak, konunun özü budur: hangisini seçmek
blok, farklı işlem alan tüm düğümlerden
ent emirleri, "fikir birliği" için kullanılacak, yani hangi tek
tüm düğümlerde uygulanacak avantaj noktası. Blok zincirleri değil
evrensel bir olay sırasını kaydedin - onlar üretirler
olayların tek bir yetkili sıralaması - dizgi ile
küçük bir yerel görüş noktası parçasını bir araya getirerek
doğrulama kurallarını geçen genel kayıt.
Mutabakat kelimesinin kullanımı en iyi ihtimalle şüpheli görünüyor
sistemik bir gereksinimin açıklaması olarak tüm düğümlerin
aynı X n değerlerini taşır . Özellikle algo-
aynılığın esasen bir dijital
Piyango, pahalı hesaplama ile desteklenmektedir.
birincil tasarım özelliği, hangi düğümün alacağını rastgele hale getirmektir.
V n'yi hiçbir düğümün tercih ettiği e
X n'ye eklenir .
Normalde kullanıldığı şekliyle fikir birliği terimi, kefaret anlamına gelir.
farklılıklar ve işçiliğe ilişkin çalışma
simden ziyade tüm taraflar için geçerli bir perspektif
bir tarafın veri kümesini rastgele seçer. Tersine,
daha aracı merkezli dağıtılmış bir sistem olarak git'in birleşmesi
komutu, daha tanınabilir bir süreç sağlar
fikir birliği, ancak otomatik değildir.

Muhtemelen hash-crack için daha doğru bir terim al-
gorithm Ω uygulanan Bitcoin olurdu “kanıtı şans” ve
çünkü sürecin kendisi fikir birliği değil, aynılıktır. Eğer
veri merkezli bir bakış açısıyla başlıyorsunuz, bu da doğal olarak
tüm temsilcilerin "deneyimini" sadece
birincisi, onları profesyonel bir şekilde çalışmak için tasarlamak çok daha zordur.
gerçekte aleyhte olan gerçek dünya özelliklerine sahip olan cesses
sensus. Tüm düğümleri tutma kısıtlaması belirtiyorsa
aynı bilinçli olarak belirli bir amaç için uygun olarak benimsenmiştir.
poz, bu özellikle sorunlu olmaz. Un-
neyse ki bu veri merkezli bakış açısının mirası,
çoğunlukla bilinçsizce tutuldu ve daha çok kişi tarafından benimsendi
genelleştirilmiş dağıtılmış bilgi işlem sistemleri,
amaç, özellikle "kazmak-
evrensel olarak mutlak bir konuma sahip olan ital madde ”. Süre
kavramsal basitliğin avantajlarına sahip olmak, aynı zamanda
dolaylı olarak ölçeklenebilirlik sorunları yaratır, ancak daha da kötüsü
temsilci merkezli olmanın doğasında bulunan avantajlardan yararlanmak zordur
yaklaşmak.

IV. GENELLEŞTİRİLMİŞ DAĞITILDI HESAPLAMA

Önceki bölümde genel bir biçimcilik tanımlanmıştır.
dağıtılmış sistemler ve git ile Bitcoin'i eski
veri merkezli dağıtılmış bir ajan merkezli
sistemi. Ancak bu sistemlerin hiçbiri gen sağlamaz.
çerçeve olma anlamında eralize hesaplama
bilgisayar programları yazmak veya uygulamalar oluşturmak için.
Öyleyse, IIIA formalizme aşağıdaki kısıtlamaları ekleyelim

---

aşağıdaki gibi:
1. Bir makine M ile ilgili olarak, bazı S n değerleri
şu şekilde yorumlanabilir: çalıştırılabilir kod ve yeniden
kod yürütme sonuçları ve erişilebilir olabilirler
M ve kod. Bu tür değerlere makine deyin
durum.
2. ∃t ve düğümler n, öyle ki I n (t) yürütmeyi tetikleyecektir
bu kodun. Bu tür işlem değerleri çağrılarını çağırın.

A. Ethereum

Ethereum6 şu andaki ilk örneği sağlar:
Blockchain kullanarak genelleştirilmiş dağıtılmış bilgi işlem
model. Ethereum yaklaşımı bir ontolojiden gelir
tek bir fiziksel bileşenin veri kesinliğini kopyalamanın
bilgisayar, dağıtılmış bir demet tabakasının üstüne
günah oluşturma blok zinciri stratejisini kullanan düğümler
kriptografik bir zincirde veri gerçekliği elde edin, ancak kararlılık
hesaplamalar, yalnızca parasal işlemler yerine
Bitcoin'de blokların içine.
Bu yaklaşım, listelenen kısıtlamalara uyuyor
Wood [tarafından tarif edildiği gibi, yukarıda VAP-150] kütle
bu yazının bir özelliği olarak anlaşılabilir
doğrulama işlevi V n () ve açıklanan durum geçişi

σ t + 1 ≡ Y (σ, T) fonksiyonunun bir özelliği olarak
Yukarıdaki kısıtlamalar karşılandı.
Maalesef veri merkezli miras,
Blockchain modelinden Ethereum, hemen göze çarpıyor
yüksek işlem maliyetiyle sunulabilir7 ve ölçeklemede zorluk
ing8.
B. Holochain
Şimdi ajan merkezli bir dis-
düğümlerin yapabildiği haraçlı genelleştirilmiş bilgi işlem sistemi
sisteme bir bütün olarak güvenle katılmaya devam edin
aynı şeyi sürdürmekle sınırlandırılmasalar da
diğer tüm düğümler gibi zincir durumu.
Geniş vuruşlarda: Holochain uygulaması şunlardan oluşur:
benzersiz bir kaynak zincirini koruyan bir aracılar ağı
ortak bir alan uygulamasıyla eşleştirilen işlemlerinin
onaylayan, monoton, parçalanmış, dağıtılmış olarak
Her düğümün doğrulamayı zorunlu kıldığı karma tablosu (DHT)
DHT'deki verilerle ilgili kuralların yanı sıra kanıtlama
kaynak zincirlerinden gelen verilerin nansı.
Holochain tabanlı bir uygulama olan biçimciliğimizi kullanma
Ω hc şu şekilde tanımlanır:
1. n'nin kaynak zincirinde X n'yi çağırın .
6 https://github.com/ethereum/wiki/wiki/White-Paper
7 karşılaştırmalı değerlendirmemize bağlantı
8 Akademik bir makale bulun
2. M, kodu yürütmek için kullanılan bir sanal makine olsun.
3. Tüm X n'lerin ilk girişine izin verin
Han
olmak
özdeş
ve
oluşmak
içinde
the
Ayarlamak
DNA {e 1 , e 2 , ..., f 1 , f 2 , ..., p 1 , p 2 , ...}
nerede
e x , olabilecek girdi türlerinin tanımlarıdır.
zincire eklendiğinde, f x olarak tanımlanan fonksiyonlardır
M üzerinde çalıştırılabilir (biz de
F'yi ayarlayın app = {uygulama 1 , uygulama 2 , ...}) ve p x sistemdir
diğer şeylerin yanı sıra,
uygulamanın beklenen işletim parametreleri
spesifik olmak. Örneğin esneklik faktörü
aşağıda tanımlandığı gibi, bu tür bir özellik olarak ayarlanır.
4. Let ı n her X ikinci girişi olması , n ve bir küme
{p, i} biçiminde, burada p genel anahtar ve i
kullanımı için uygun bilgileri tanımlıyor
bu özel Ω hc . Bu giriş olmasına rağmen
Tüm X için aynı formatın n 's içerik değil
aynı. Bu girdiye aracı kimlik girdisi adını verin.
5. ∀e x ∈ DNA, bir uygulama vardır olsun x ∈ K uygulama olan kutu
girişleri içeren işlemleri doğrulamak için kullanılabilir
e x tipi . Bu seti F v veya uygulama olarak adlandırın
doğrulama işlevleri.

6. Kontrol eden bir V sys (ex, e, v) fonksiyonu olsun.
e giriş tanımında belirtilen formdadır
e x ∈ DNA için. Bu işlevi sistem girişi olarak adlandırın
doğrulama işlevi.
7. Genel doğrulama fonksiyonu V (e, v) ≡ olsun
V x F v (e x) (v) ∧ V sys (e x , e, v).
8. Let F ı K bir alt kümesi uygulama F'den farklı v örneğin
ki ∀f x (t) ∈ F I, orada var olan I (t)
tetikleme f x (t). F I'deki fonksiyonları açığa çıkarın
fonksiyonlar.
9. F uygulamasındaki F v veya F I dahili olmayan herhangi bir işlevi çağırın
işlev görür ve başkaları tarafından çağrılmasına izin verir.
fonksiyonlar.
10. C kanalının kimliğinin doğrulanmasına izin verin.
11. DHT'nin bir au-
kimlik doğrulaması yapılmış kanal aşağıdaki gibidir:
(a) Δ bir küme {δ 1 , δ 2 , ...} olsun, burada δ x bir
anahtarın her zaman karma olduğu {key, value} değerini ayarlayın
H (değer) değer. DHT durumunu Δ arayın.
(b) Bırak
F DHT
işlevler kümesi olmak
{dht put , dht get } nerede:
ben. DHT koymak (δ anahtar değeri) δ ekler anahtarı değeri Ô için
ii. dht get (anahtar) = δ anahtarının değeri , Δ cinsinden değer
(c) x, y ∈ N ve δ i ∈ Δ x ama δ i / ∈ Δ y olduğunu varsayalım .
Y dht get (key) ' i çağırdığında , δ olacağım
X kanalından X kanalından alındı ve eklendi
Δ y .

DHT yeterince olgunlaşmıştır ki, çok sayıda
mülkiyet sağlamanın yolları 11c . Bizim için
alfa sürümünü kiralıyoruz, değiştirilmiş bir sürümünü kullanıyoruz
[LibP2P] 'de uygulandığı şekliyle [Kademlia].
12. DHT hc'nin DHT'yi aşağıdaki gibi artırmasına izin verin :
(a) ∀δ anahtar, değer
∈ Δ değeri sınırlamak
DNA'da tanımlandığı gibi bir giriş türü. Furth-
daha fazla, herhangi bir işlevin dht x (y) çağrısı yapması
Δ'yi değiştiren , doğrulamak için F v (y) 'yi de kullanır
y ve geçerli olup olmadığını kaydeder. Bunu not et
bu doğrulama aşaması iletişim kurmayı içerebilir
y'yi oluşturmakla ilgili kaynak düğümler
bağlamı hakkında daha fazla bilgi toplayın
işlem, bkz. IV C 2.
(b) Yalnızca Δ öğesinin tüm öğelerinin değiştirilmesini zorunlu kılın
monoton olarak, yani elemanlar δ sadece
eklendi to kaldırılmadı.
(c) F DHT'ye A'da tanımlanan işlevleri dahil edin .
(d) δ ∈ Δ kümelerinin daha fazlasını içermesine izin verin
A.'da tanımlanan unsurlar .

(e) d (x, y) simetrik ve tek yönlü olsun
tanımlanmış karma uzaydaki mesafe metriği
H ile, örneğin XOR metriği tanımlı
içerisinde [Kademlia'da] . Bu metriğin
girişler ve düğümler arasında
her ikisinin de adresleri aynı değerlerdir
hash fonksiyonu H (yani δ tuşu = H (δ değeri) ve
Bir n = H (pk n)).
(f) r, ayarlanacak DHT hc'nin bir parametresi olsun
faydalı sayılan özelliklere bağlı olarak
girişlerin birden çok kopyasını muhafaza etmek için cial
verilen uygulama için DHT'de. Çağrı r
esneklik faktörü.
(g) Her düğümün bir M =
{m n , ...} metrik m n diğer düğümler hakkında,
her bir m n , hem bir düğümün hem de doğrudan
bu metriğe göre n deneyimi,
n'nin diğer düğümlerinin deneyiminin yanı sıra.
Tutulan böyle bir metriğin çalışma süresi olmasını zorunlu kılın
zaman yüzdesini takip eden a
düğümün kullanılabilir olduğu deneyimlenir. Ara
bu metrik dedikodularını paylaşan düğümlerin süreci
ayrıntılar için IV C 3'e bakın.
(h) Her düğüm düğümünün sürdürdüğü that n n'yi zorla
bir küme V δ = {n 1 , ..., n q }, en yakın q düğümün δ
n'den görüldüğü gibi, n'den de beklenen
δ tuşunu basılı tutun. Esneklik dikkate alınarak korunur
hesap düğümü çalışma süreleri ve değeri seçme
q böylelikle:
$$\sum_{i=0}^{q} \text{çalışma süresi } (n\ i) \geq r \quad (4.1)$$
çalışma süresi ile (n) ∈ [0, 1].
Verilen bir gruptan bu tür V δ kümelerinin birleşimini çağırın
düğümün perspektifi, örtüşme listesi ve ayrıca
q ≥ r olduğuna dikkat edin.
(i) Her düğüm n'nin her δ x ∈ Δ n'yi atmasına izin ver ,
yakın sayısı (d (x, y) ile ilgili olarak)
düğümler q'dan büyüktür (yani diğer düğümler ise
bunların V oluşturmak mümkün δ DAHİL olmayan setleri
ing n, bu da yeterli olduğu anlamına gelir
δ tutmaktan sorumlu diğer düğümler
Δ m sistemi karşılamak esneklik kümesi bulunması
n depolamaya katılmadan bile r ile δ).
Bunun ağ adaptasyonu ile sonuçlandığını unutmayın.
topoloji ve DHT durumundaki değişiklikler mi-
ağ sayısını düzenleyerek ızgaralar-
eşleştirmek için tüm δ i Δ'lerin geniş yedek kopyaları
r düğüm çalışma süresine göre.
DHT hc'yi doğrulayan, monoton, parçalanmış olarak arayın
DHT.
∈ N ∀n 13. N uygular DHT kabul hc olup,: Δ olduğu
D'nin bir alt kümesi (karma zincir olmayan durum verileri) ve

F DHT n tarafından kullanılabilir, ancak bunların
işlevler doğrudan işlev tarafından KULLANILAMAZ
DNA'da tanımlanan F app .
14. Bırak
F sys
olmak
the
Ayarlamak
nın-nin
fonksiyonlar
{sys commit , sys get , ...} burada:
(a) sys commit (e) sistem doğrulama işlevini kullanır-
e'yi X'e eklemek için V (e, v) ve başarılıysa
dht put (H (e), e) 'yi çağırır .
(b) sys get (k) = dht get (k).
(c) B'de tanımlanan ek sistem işlevlerine bakın .
15. DNA'da tanımlanan F uygulamasındaki işlevlerin
F sys'deki işlevleri çağırın .
16. Keyfi bir mesaj olalım. F sys'e dahil et
fonksiyon sys gönderme (A için çağrıda m)
N gelen işlev uygulamasını tetikleyecek alma (A dan m)
Düğüm n'ye DNA için . Bu mekanizmayı ara
düğümden düğüme mesajlaşma.
17. DNA'daki girişlerin tanımının
giriş türlerini özel olarak işaretleyin. Eğer bir
σ x girişi böyle bir türdeyse, o zaman σ x / ∈ Δ. Not
ancak bu türden girişler şu şekilde gönderilebilir:
düğümden düğüme mesajlar.
18. Sistem işleme fonksiyonu P (i) bir dizi
F uygulamasındaki işlevler sisteme kaydedilecek
çeşitli kriterlere dayalı geri aramalar, örneğin bildirim
DHT'ye reddedilen koyma sayısı, zamanın geçişi vb.
C. Doğrulama Yoluyla Sistemik Bütünlük
Dağıtılmış veri merkezli yaklaşımın çekiciliği
bilgi işlem, bunu kanıtlayabilirseniz

Sayfa 6

tüm düğümler güvenilir bir şekilde aynı verilere sahiptir,
bütünlüğü kanıtlamak için güçlü genel temel
bir bütün olarak sistemin. Bitcoin durumunda,
X işlemleri ve harcanmamış işlemi tutar
düğümlerin gelecekteki işlemleri doğrulamasına izin veren çıktılar
çift harcamaya karşı. Ethereum söz konusu olduğunda, X tutar
makine durumuna işaretçiler için ne kadar önemli. İspat
bu veri kümelerinin tüm düğümlerindeki tutarlılık eğlencelidir.
bu sistemlerin bütünlüğüne zarar verir.
Ancak, varsayımla başladığımız için-
bağımsız olarak dağıtılmış sistemler (bkz. IIIA)
oyunculuk ajanları, herhangi bir ofn kanıtı, m ∈ N: X n
!
= Bir içinde X m
Blockchain tabanlı sistem bir seçim olarak daha iyi anlaşılır

(dolayısıyla bizim kullanımımız
!
=), bu düğümlerde ajanslarını kullanır
diğer düğümlerle etkileşimin ne zaman durdurulacağına karar vermek için
X durumunun artık eşleşmediğini tespit ettiğinde. Bu
"yaptırım kanıtı" olarak da adlandırılabilir ve ayrıca
uygun şekilde çatal olarak bilinir çünkü esasen
ağın bölümlendirilmesinde sonuçlar.
Konunun özü, herhangi bir güven ile ilgili olmalıdır.
sistemde tek ajan var. Gelen [VAP-150] , Bölüm
1.1 (Sürüş Faktörleri) okuduk:
Genel olarak, böyle bir sistem sağlamak istiyorum
Kullanıcılara, ne olursa olsun garanti edilebilir
hangi diğer bireyler, sistemler veya kuruluşlar
etkileşime girerler, bunu mutlak bir kontratla yapabilirler
olası sonuçlara güven ve bunlar
sonuçlar ortaya çıkabilir.
Burada "mutlak güven" fikri önemli görünüyor.
tant ve onu daha resmi olarak anlamaya çalışıyoruz ve
genellikle dağıtılmış sistemler için.
1. Ψ α bir ajanın sahip olduğu güvenin bir ölçüsü olsun
katıldığı sistemin çeşitli yönlerinde,
burada $0 \leq \Psi \leq 1$, 0 güvensizliği temsil eder ve
1 mutlak güveni temsil eder.
2. R n = {α 1 , α 2 , ... olsun. . . } bir dizi yön tanımlayın
bir ajanın ölçtüğü sistem hakkında $n \in N$
güven emin. N'nin gereksinimleri için R n'yi arayın
Ω ile ilgili olarak.
3. ε n (α), n n düğümü için bir eşik fonksiyonu olsun.
A'ya göre N, öyle ki Ψ α <ε (α)
o zaman n sisteme katılmayı bırakacaktır,
veya başkalarının katılımını reddetmek (
çatal).
4. R A ve R C , R'nin bölümleri olsun.
$\forall \alpha \in R A : \varepsilon (\alpha) = 1$
$\forall \alpha \in R C : \varepsilon (\alpha) < 1$
(4.2)
bu nedenle herhangi bir Ψ = 1 değeri, R A'da reddedilir ve herhangi bir
değeri Ψ <ε (α) R reddedilir C . Çağrı R A
mutlak gereksinimler ve dikkate alınan R C
Gereksinimler.
Bu nedenle, sistem özelliklerini resmi olarak ayırdık
(A) ' ya mutlak bir güven duyduğumuza
sadece (R C) 'ye olan güveni düşünmüşlerdir . Hala belirsiz
somut bir güven seviyesi nasıl ölçülür Ψ α . Gerçek olarak-
dünya bağlamları ve gerçek dünya kararları için güven,
esas olarak bir (insan) ajanın bakış açısına bağlıdır,
eldeki veri kümesi ve hatta belki sezgi. Böylece
buna yumuşak bir kriter demeyi daha uygun buluyoruz. İçinde
bu kavramı nesnel olarak anlamak ve ilişkilendirmek için
Woods'un yukarıdaki alıntıda ifade ettiği düşünceye göre,
güven ölçüsünü tanımlayarak ilerliyoruz
açı α, koşullu olasılık olarak
belirli bir bağlamdaki durum:
$\Psi \alpha \equiv P (\alpha \mid C)$

(4.3)
C bağlamının diğer tüm bilgileri modellediği durumlarda,
Temsilciye, temel ve sezgisel varsayım dahil olmak üzere
tions.
Kriptografinin temel örneğini düşünün.
uygulanan asimetrik anahtarlara sahip cally imzalı mesajlar
kriptografik sistemler alanında (temelde
kripto-para birimi terimini hangi paraya çevirir). Merkezi yönü
bu bağlamda bize sağlayan α imza diyoruz
kesin olarak bilme yeteneği, belirli bir mesajın
gerçek yazar Yazar gerçek , yalnızca belirtilen temsilcinin aynısıdır
mesajın meta bilgisindeki yerel olarak mevcut veriler aracılığıyla
kriptografik imza aracılığıyla eşleştirme Yazar yerel .
Bu güveni kazanıyoruz çünkü bunu çok zor buluyoruz
oluşturmak için özel anahtara sahip olmayan herhangi bir aracı
belirli bir mesaj için geçerli bir imza.
α imza ≡ Yazar real = Yerel yazar
(4.4)
Bu yönün çekiciliği, yazarı kontrol edebilmemizdir.
yerel olarak, yani üçüncü bir tarafa ihtiyaç duymadan veya doğrudan
gerçek yazara güvenilir iletişim kanalı. Fakat,
belirli bir kriptografinin bu yönüne olan güven
sistem C bağlamına bağlıdır:
Ψ imza = P (Gerçek Yazar = Yerel Yazar | C)
(4.5)
Bağlamı olasılığını ortadan kaldıracak şekilde kısıtlarsak
bir temsilcinin özel anahtarına erişim sağlayan bir düşman ve
ayrıca hesaplamanın olası (gelecekteki) varlığını da dışlar
kolayca hesaplayabilen veya kaba davranabilen cihazlar veya algoritmalar
anahtarı zorlarsanız, daha sonra (yapılandırılmış) bir yapılandırma atayabiliriz.
1'in dence seviyesi, yani “mutlak güven”. Böyle olmadan
C üzerindeki kısıtlamalar, kabul etmeliyiz ki Ψ imza <1,
hangi gerçek dünya olayları, örneğin Mt.Gox hack'i
2014 yılından itibaren9, temizle.
Bu ilişkileri bu kadar ayrıntılı olarak tanımlamayı hedefliyoruz
herhangi bir R A kümesinin mutlak olduğunu belirtmek için
gereksinimler önemsiz ifadelerin ötesine geçemez -
yerelin içeriği ve bütünlüğü hakkında açıklamalar
ajanın kendisinin durumu. Descarte'nin yolunu takip ederek
9 "Eksik bitcoinlerin çoğu veya tamamı doğrudan
Mt. Zaman içinde Gox sıcak cüzdanı 2011'in sonlarından itibaren başlar ” [Nilsson15]

---

7. Sayfa

her düşüncede güveni sorgulayarak, projelendiriyoruz
meşhur ifadesi cogito ergo sum referansına
şunu belirterek çok aracılı sistemler çerçevesi: Temsilciler şunları yapabilir:
sadece onların
belirli bir uyaranın mevcut olduğunu algılar ve
herhangi bir belirli soyut a priori model olup olmadığı
bu uyaranla çelişmeden eşleşir, yani
bir temsilcinin belirli bir veri parçasını görmesi ve
onu belli bir şekilde yorumlamak mümkün. Her sonuç
uygulama yoluyla bir posteriori çizilmek

Bağlamın karmaşık modelleri şunlara bağlıdır:
içeriğinde bulunan bağlamla ilgili varsayımlar
model. Bu, ajan merkezli bakış açısının kalbidir.
ve iddia ettiğimiz şey her zaman dikkate alınmalıdır
merkezi olmayan çok ajanlı sistemlerin tasarımında,
bir bütün olarak sistemin herhangi bir yönünün
diğer acenteler ve yerel olmayanlar hakkındaki varsayımları içerir
olaylar R C içinde olmalıdır , yani önceden bir güvene sahip olmalıdır
1. <1. Çok etmenli sistemler hakkındaki bu gerçekle yüzleşirken,
mutlak bir gerçeği zorlamak için çok az değer buluyoruz
∀n, m ∈ N: X n
!
= X m ve bunun yerine sorunu çerçeveleriz
gibi:
Bunun için genelleştirilmiş araçlar sağlamak istiyoruz
merkezi olmayan çok ajanlı sistemler bu şekilde kurulabilir
şu:
1. amaca uygun çözümler sırayla uygulanabilir
uygulama bağlamına uygun yapılandırmaya göre optimize etmek için
dences Ψ α ,
2. ac- aracılığıyla herhangi bir ε (α) eşiğinin ihlali
diğer ajanların tıbbı tespit edilebilir ve yönetilebilir
herhangi bir ajan tarafından, öyle ki
3. sistem bütünlüğü, herhangi bir noktada korunur
zaman veya değilse, onu geri kazanmanın bir yolu vardır (bkz.
??).
Bunlara ajan merkezli çözümü algılıyoruz.
sistemin holografik yönetimi olmak için gerekenler-
Sistemin her aracı / düğümü içindeki bütünlük sayesinde
uygulamaya özel doğrulama rutinleri. Bu değer kümeleri
Kimlik kuralları, merkezi olmayan her uygulamanın kalbinde yatar.
uygulama ve uygulamalara göre farklılık gösterirler.
bağlam. Her temsilci, temsilcilerinin kaydını dikkatlice tutar.
gerçekliğin önemli olan kısmının cümle
onlara göre - belirli bir uygulama bağlamında
yüksek güvenirliğe sahip olmak arasındaki ödünleşimi yönetmek zorundadır.
dence eşikleri ε (α) ve düşük kaynak ihtiyacı ve
karmaşıklık.
Örneğin, iki farklı kullanım durumunu ele alalım.
hareketler:
1. yapmaya çalıştığımız bir e-posta mesajının alınması
spam olarak doğrulayın veya onaylayın ve
2. denediğimiz parasal işlem taahhüdü-
çift harcamaya karşı doğrulamak.
Bu bağlamların, bir temsilcinin
farklı şekilde değerlendirmek isteyebilir ve istekli olabilir
doğrulamak için farklı seviyelerde kaynak harcamak. Biz ...
Bu tür doğrulama işlevlerinin olmasına izin vermek için imzalı Holochain
her uygulama için bağlamsal olarak ayarlayın ve bu içeriği ortaya çıkarın
açıkça metinler. Böylece, düşünülebilecek bir
Bilinçli olarak seçimler yapan Holochain uygulaması
ya tümünü ya da par-
Blockchain'lerin tial özellikleri. Holochain, bu nedenle,
bir spesifikasyonu açan bir çerçeve olarak anlaşılabilir.
merkezi olmayan uygulama mimarilerinin trum'u

Blockchain, bir uçta belirli bir örnek olur
bu yelpazenin.
Aşağıdaki bölümlerde hangi kategorileri göstereceğiz
doğrulama algoritmaları mevcuttur ve bunlar nasıl olabilir?
decen oluşturmak için üst üste istiflenmiş
bütünlüğü koruyabilen tralize sistemler-
her ajanın olacağı mutlak bir gerçeği ortaya koyan
kabul etmeye veya düşünmeye zorlandı.

1. İçsel Veri Bütünlüğü

En düşük seviyeli rutinler hariç her uygulama
önemsiz olmayan, yapılandırılmış veri türleri. Yapılandırılmış im-
nasıl yorumlanacağını açıklayan bir modelin varlığını katlar
bir türün örneği olarak ham bitler ve
yapı birbiriyle ilişkilidir. Genellikle bu, cer-
Olası değerler kümesi hakkında varsayımlar. Cer-
Bozuk değer kombinasyonları anlamlı veya sert olmayabilir
bu veri türünün içsel bütünlüğünü geciktirir.
Kriptografik olarak imzalanmış bir örneği düşünün
ileti m = {gövde, imza, yazar}, burada yazar
açık anahtarları şeklinde verilir. Bu veri türü
üç öğenin gövde olduğu varsayımını iletir,
imza ve yazar karşılıklı olarak birbirine karşılık gelir
varsayılan kriptografik algoritma tarafından zorlanıyor
bu türün tanımı ile belirlenecek.
belirli bir örneğin içsel veri bütünlüğü değer olabilir
sadece verinin kendisine bakarak ve kontrol ederek
kriptografik algoritmayı uygulayarak imza
türünün a priori merkezini oluşturan
model. Doğrulama bir sonuç verir true {true, f alse}
bu, içsel verilere olan güvenin,
bütünlük mutlaktır, yani Ψ içsel = 1.
Genel olarak, içsel veri bütünlüğünü tanımlarız
α φ yönü olarak φ işlem türünün , içsel ∈ R A ,
deterministik bir varlığın varlığı ile ifade edilir ve
t ∈ φ işlemleri için yerel doğrulama fonksiyonu V α (t)
başka herhangi bir girişe bağlı değildir, ancak t'nin kendisine bağlıdır.
Mesajın içsel veri bütünlüğünün nasıl oluştuğuna dikkat edin.
yukarıdaki bol miktarda herhangi bir varsayımda bulunmaz.
mesajın gerçek yazarı, yön α imzası olarak
önceki bölüm yapar. Bu tanımla odaklanıyoruz
sistem özellikleri hakkında herhangi bir iddiada bulunmayan yönler
İncelenen temsilci için yerel olmayan riskler,
va'yı oluşturan çıkarımlar dizisinin kökünü oluşturur.
açıklık ve dolayısıyla bir sistemin yüksek seviyesinin güvenilirliği
tutarlı çevresel girdilerdeki yönler ve bütünlük.

---

2. Membranlar ve Kaynak

Dağıtılmış sistemler,
olmayan süreçlerde düğümlerin katılımını kısıtlayın
bu tür bir kısıtlama, sistemik bütünlüğü tehlikeye atacaktır.
Kısıtlamaların düğümlere dayalı olduğu sistemler

kimlik, türüne veya yazara göre bildirilmiş olsun,
ya da düğümlerin davranışlarının geçmişinden derlenmiş,
izin verildiği biliniyor [Swanson15] .
Sistemler
bu kısıtlamaların mülklerine dayanmadığı durumlarda
düğümlerin kendileri izinsiz olarak bilinir.
İzinsiz çok etmenli sistemlerde bir ilke
sistemik bütünlüğe yönelik tehdit Sybil-Attacks'tan geliyor
[Douceur02] , burada bir düşmanın üstesinden gelmeye çalıştığı
sistemin çok sayıda
güvenliği ihlal edilmiş düğümler.
Ancak hem izinli hem de izinsiz
sistemler, katılımı kaplayan mekanizmalar vardır. İçin-
mally:
M (n, φ, z) değerlendiren bir ikili fonksiyon olsun
φ türü işlemlerin n ∈ N tarafından sunulup sunulmadığı
kabul edilecektir ve z keyfi ekstra ise
bu değerlendirmeyi yapmak için gerekli bilgi. Beni ara
zar işlevi ve bunun bir
doğrulama fonksiyonu bileşeni V (t, v) 'den
ilk biçimcilik 5 .
Ω bitcoin ve Ω ethereum söz konusu olduğunda M,
n'nin değeri ve kararını yalnızca
z, işe yarıyor ya da
Sybil'e karşı korumak için yeterli bir geçit olan kazık
Saldırılar.
Bir ab-
çözünen gerçeği ∀n, m ∈ N: X n
!
= X m şunu ortaya çıkarır:
işlem kaynağını atamaz. Ajan merkezli dis-
haraç verilmiş sistemler bunun yerine iki temel gerçeğe dayanmalıdır
veriler hakkında:
1. bir kaynaktan geliyor ve
2. tarihsel sıralaması bu kaynak için yereldir.
Bu nedenle, Ω hc sistem durumu verilerini ikiye böler.
parçalar:
1. her düğüm kendi bütününü korumaktan sorumludur
X n veya kaynak zinciri ve bunu onaylamaya hazır olun
sorulduğunda diğer düğümlere durumu ve
2. diğer düğümlerin bölümlerini paylaşmaktan tüm düğümler sorumludur.
düğümlerin işlemleri ve bu işlemlerin meta
DHT parçasındaki veriler - meta veriler şunları içerir:
geçerlilik durumu, kaynak ve isteğe bağlı olarak kaynağın
tarihsel sırayı sağlayan zincir başlıkları.
Böylece, DHT, başkalarına dağıtılmış erişim sağlar.
işlemler ve bunların geçerliliğine ilişkin değerlendirmeleri
işlemler. Bu, bilginin nasıl tartışıldığına benzer.
sosyal alanlar içinde ve etkileşim yoluyla yapılandırılmış
sosyolojik sosyal teorinin tanımladığı gibi diğerleri
yapılandırmacılık.
DHT'nin özellikleri ile bağlantılı olarak
karma işlevi bize deterministik olarak tanımlanmış bir
düğüm kümesi, yani her işlem için bir mahalle.
Böyle bir işlem kolayca kurulamaz.

belirli bir mahallede topraklar. Resmen:
$\forall t \in \Delta: \exists \eta: H \rightarrow N^r$
$\eta (H (t)) = (n_1, n_2, ..., n_r)$
(4.6)
hash'in H aralığından η işlevi eşlenir
H fonksiyonunu r'yi gereksiz tutan r düğümlerine
t işleminin parçaları (bkz. 12i) .
H (H (t)) düğümlerinin listesine sahip olmak bir temsilcinin
t ile ilgili üçüncü taraf bakış açılarını kendi
ve işlemin kaynağı / kaynakları. Rastgele
H hash fonksiyonunun izlenmesi, bu görüntülemenin
noktalar tarafsız bir örneği temsil eder. r ayarlanabilir
uygulamanın kısıtlamalarına ve seçimine bağlı olarak
maliyetler ve sistem bütünlüğü arasındaki değiş tokuş. Bunlar
özellikler sistem oluşturmak için yeterli altyapı sağlar
tarafından oynamayan düğümleri tespit ederek tem bütünlüğü
kurallar - kaynaklarının geçmişini veya içeriğini değiştirmek gibi
Zincir. Ek C'de, aşağıdakiler için uygun aletleri detaylandırıyoruz:
detaylı analizler dahil olmak üzere farklı bağlamlar
kaynak zinciri geçmişi gereklidir - örneğin finansal
işlem denetimi.
Uygulamanın etki alanına bağlı olarak komşu-
davlumbazlar Sybil-Saldırılarına karşı savunmasız hale gelebilir çünkü
yeterince büyük bir tehlike altındaki düğüm yüzdesi
bir ajan tarafından kullanılan numuneye önyargı katabilir
belirli bir işlemi değerlendirmek için. Holochain ap-
Sybil-Saldırılarını alan adı spe-
cific membran fonksiyonları. Çünkü biz miras almayı seçtik ...
sistem içinde model ajansı kurabilir, izin verebilir
programatik ve merkezi olmayan bir şekilde verilebilir veya reddedilebilir
düzenlenmiş bir şekilde, böylece uygulamaların uygun şekilde
izin verilen ve permis arasındaki spektrumda arazi
siyonsuz.
Ek D'de bazı membran şemaları sunuyoruz
bunun dış zarı için seçilebilir
konuşabilmek için düğümlerin geçmesi gereken uygulama
uygulama içindeki diğer herhangi bir düğüm veya herhangi bir saniye için
uygulama içinde ondary membran. Bu ikincisi
düğümlerin izinsiz ve özel olarak katılabileceği anlamına gelir
Uygulamanın bütünlük olmayan yönlerinde ipate
başka bir koşul olmaksızın kritiktir, ancak sertifika vermeniz gerekir
Membranın uygulamaya geçirilmesi için bazı kriterler
önemli doğrulama.
Böylece, Holochain uygulamaları sistemik giriş
fikir birliği getirmeden dürüstlük ve dolayısıyla
(hesaplama açısından pahalı) mutlak gerçek, çünkü 1)
herhangi bir tek düğüm bağımsız olarak doğrulamak için provenansı kullanır
buna dahil olan kaynaklarla yapılan herhangi bir işlem
işlem ve 2) çünkü her Holochain uygulaması

---

diğerlerinden bağımsız olarak çalışır, doğası gereği

katılmak için uygulamaya özel kurallar tarafından görevlendirildi ve
o uygulamanın ağına katılımın devam etmesi.
Bunların her ikisi de herhangi bir Holochain'in faydasını sağlar.
uygulama, bu doğrulamanın masrafını bir
bağlamsal olarak uygun seviye.

3. Dedikodu ve Dünya Modeli

Şimdiye kadar, doğrulamanın bu kısımlarına odaklandık.
X'in seçimlerini doğrulamak için V yion işlevi kullanılır. Ancak,
dağıtılmış sistemlerde de sistem bütünlüğünü korumak
düğümlerin bilgi paylaşan mekanizmalara sahip olmasını gerektirir
doğrulama kurallarını ihlal eden düğümler hakkında bilgi
böylece katılımdan dışlanabilirler. Orada
ek olarak, içinde yaşamayan kötü davranış biçimleri var
bir işlemin içeriği, ancak işlem modellerinde
sisteme zarar veren davranışlar, örneğin,
hizmet reddi saldırıları.
Holochain, bilgi paylaşmak için düğümler için dedikodu kullanıyor
başkalarının davranışlarıyla ilgili kendi deneyimleri hakkında
düğümler. Gayri resmi olarak bu bilgiyi düğümün
dünya modeli. Bu bölümde doğayı anlatıyoruz
Holochain'in dedikodu protokolleri ve bunların nasıl oluşturulduğu ve
bir düğümün dünya modelini sürdürmek.
Gelen 12f dünya modelinin böyle bir parça açıklanan,
çalışma süresi metriği ve yedeklemeyi sürdürmek için nasıl kullanıldığı
girişlerin dant kopyaları. IVC2'de bir membran tanımladık
bir düğümün bir aktarımı kabul edip etmeyeceğini belirleyen işlev
eylem ve bu işlevin rastgele veriler almasına izin verdi
z. Bu verilerin ana kaynağı bu dünyadan geliyor
model.
Daha resmi:
1. Her düğümün bir dizi M metrik bulundurduğunu hatırlayın
bildiği diğer düğümler hakkında m. Unutmayın
biçimciliğimizin şartları, bu dünya modeli,
her düğümün zincir dışı durum verileri D.
2. m demetlerden oluşan bir demet olsun: ((μ, c) öz , (μ, c) diğerleri)
yeniden ile bir düğüm deneyimini μ kaydeden
belirli bir metriğe spekt ve güvenirlik c
bu tecrübe, hem doğrudan tecrübe edilmiş hem de
Diğer düğümlerden alınan "kulaktan dolma".
3. X n'de saklanan bir girdi sınıfının da kullanılmasına izin verin
imzalı bir beyan görevi gören bir metrik m w olarak
n'nin başka bir düğümle ilgili deneyiminin.
Bu tür girişleri garanti arayın. Bu garantiler ...
Holochain'in standart aletlerini kullanmamızı
menşe bazlı, doğrulanabilir iddialarda bulunmak
ağda yayılan diğer düğümler veya
dedikodu yoluyla olağan DHT yöntemlerinden togonal olarak
bu iddiaları "duyması" gereken düğümlere
düğümlerle etkileşim konusunda kararlar vermek için.
4. ∀m ∈ M , (m) ile G fonksiyonunun bir set döndürmesine izin verin
bir düğümün de-
bu bilgiyi ağırlıklandıran bir olasılıkçı tarafından para cezasına çarptırıldı
bu düğümlerden alınan
m diğer .
5. ∀m ∈ M, (m) ile ilgili G fonksiyonunun bir

Bir düğümün tanımlanmış hakkında dedikodu yapması için önemli düğümler
m özelliklerine göre.
G alt kümelerini tanımlama 6. ile bir uyuşup göre (m)
alçaktan yükseke sahip olmanın ne anlama geldiğiyle ilgili
güven değeri c:
(a) Çekme: hakkında düşük olan düğümlerden oluşur.
güven, daha sık ihtiyaç anlamına gelir
bir düğümün güvenini artırmak için dedikodu. Bu tür düğümler
saygılı olanları içerir
verilen düğüme, yayınlanan girişlerini tutun,
tutmaktan da sorumludur,
o zaman düğüme yakın (yani en düşük k-
paket) ve yönlendirme için dayandığı (ör.
her k-bölümünün bir alt kümesi)
(b) İtme: etrafında yüksek olan düğümlerden oluşur.
güven, daha sık ihtiyaç duyulduğunu ima eder
bununla ilgili bilgileri yaymak için dedikodu yapmak
düğüm. Bu tür düğümler aşağıdakileri içerir:
belirli bir düğümün yüksek güvenilirliğe sahip olduğu bir
kötü oyuncu, yani doğrudan kötü bir deneyim yaşadı
oyunculuk veya kötü aktör dedikodusu aldı
yapabilme konusunda güveninin yüksek olduğu düğümler
o kötü aktör değerlendirmesini yapmak için.
7. YAPILACAK: bir dedikodu tetikleme işlevini açıklayın.
çekmeye karşı çekme ayrımı
dedikodu olur
Dedikodunun hesaplama maliyetleri,
belirli bir uygulamanın izlemesi gereken metrikler
sistem bütünlüğünü korumak için. Bir uygulama için
çok güçlü üyelik membranı belki sadece çalışma süresi
direnci dengelemek için dedikodu yapmak için metrikler gereklidir
lience. Ancak bu da önceden bilgisine bağlı olabilir.
Uygulamaya dahil olan düğümler. İle uygulamalar
çok gevşek üyelik zarlarının bir önemi olabilir
tial metrik sayısı ve karmaşık membran fonksiyonları
önemli miktarda com-
pute çabası. Holochain tasarımı kasıtlı olarak ayrılıyor
bu parametreler yalnızca gevşek bir şekilde belirtilmiştir, böylece uygulama-
Amaca uygun olarak inşa edilebilir.
4. SAKİN ve Mantıksal Monotonluk
YAPILACAKLAR: çok etmenli sistemlerde CALM'ın tanımı,
ve bizim durumumuzda nasıl çalıştığını
V. DAĞITILMIŞ SİSTEMLERDE KARMAŞIKLIK
Bu bölümde profesyonelimizin karmaşıklığını tartışıyoruz.
merkezi olmayan sistemler için oluşturulmuş mimari ve karşılaştırma
gittikçe benimsenen Blockchain modeline.

Merkezi olmayanların karmaşıklığını resmen tanımlayan
çok aracılı sistemler, daha fazlası için önemsiz olmayan bir görevdir.
karmaşık yaklaşımlar önerilmiştir ([Marir2014]).
Olmasının nedeni bu olabilir
topluluklarda belirsizlik ve yanlış anlamalar

Örneğin Bitcoin'in karmaşıklığı ve ölçeklenebilirliği hakkında küfür
[Bitcoin Reddit] .
Bir top parkı karşılaştırması yapabilmek için-
yaklaşımımız ile ondalık dönemdeki mevcut statüko arasında
tralize uygulama mimarisi, modele göre ilerliyoruz
Hem tek bir düğüm için en kötü durum karmaşıklığı
Ω Sistem Düğümünün yanı sıra tüm sistem için Ω Sistem ve
her ikisi de durum geçişlerinin sayısının işlevleri olarak (yani,
işlemler) n ve sistemdeki düğüm sayısı
m.
A. Bitcoin
Ω Let Bitcoin Bitcoin ağı olmak, n sayı
işlem sayısı ve m tam doğrulama düğümlerinin sayısı olabilir
(yani madenciler10) Bitcoin içinde .
Düzenlenen her yeni işlem için, herhangi bir düğüm
işlemin imzasını kontrol etmek zorunda kalacak (aralarında
diğer çekler bkz. [BitcoinWiki]) ve özellikle kontrol edin
bu işlemin çıktısı başka herhangi bir işlemde kullanılmaz
çifte harcamaları reddetme, bu da bir zaman kompleksi ile sonuçlanır.
esneklik
c + n
(5.1)
işlem başına. Big-O gösteriminde zaman karmaşıklığı
işlem sayısının bir fonksiyonu olarak düğüm başına
bu nedenle:
Ω BitcoinNode ∈ O (n 2)
(5.2)
Bir Bitcoin düğümü tarafından ele alınan karmaşıklık, 11
m sistemin toplam düğüm sayısına bağlıdır.
Ancak her düğümün tamamen aynı şeyi doğrulaması gerektiğinden
işlemler kümesi, sistemin zaman karmaşıklığı olarak
işlem sayısı ve düğüm sayısı işlevi
sonuçları olarak
Ω Bitcoin ∈ O (n 2 m)
(5.3)
Bitcoin'in bu ikinci dereceden zaman karmaşıklığının
işlem doğrulama süreci, ana
ağın dedikodu bandını azalttığı için darboğaz
her düğümün her işlemi doğrulaması gerektiğinden genişlik
geçmeden önce. Hala ortalamaya sahip olmak için
10 Basitlik uğruna ve daha düşük bir sınıra odaklanmak için
sistemin karmaşıklığı, olmayan tüm düğümleri ihmal ediyoruz
hafif istemciler gibi ağın çalışması için çok önemlidir ve
doğrulama sürecine dahil olmayan müşteriler
11 Doğası gereği değil - bu, daha fazla katılımcının daha fazla
işlemler ancak her iki değeri de ayrı parametreler olarak modelliyoruz
işlem en az ağın% 90'ını doldurur,
blok boyutu ve süresi 4MB'nin üzerine çıkarılamaz ve
[Croman ve ark. 16] 'ya göre sırasıyla 12s .
B. Ethereum
Ω Let Ethereum Ethereum ana ağ olabilir, bu arada n
işlem sayısı ve m tam sayısı
ağdaki istemciler.
Tek bir işlemi işlemenin zaman karmaşıklığı
tek bir düğümde, kendisine sahip olan kodun bir işlevidir.

verilen işlem artı tarafından tetiklenen yürütme
sabit:
c + f tx ben (n, m)
(5.4)
Bitcoin'e benzer şekilde ve Blockchain de-
tek bir durumu sürdürme kararını imzala (∀n, m ∈ N:
X n
!
= X m , "Ne pahasına olursa olsun bundan kaçınılmalıdır, çünkü
Ortaya çıkacak pislik muhtemelen tüm güveni öldürecektir.
tüm sistem. " [EIP-150]), her düğümün işlenmesi gerekir
gönderilen her işlem bir zaman karmaşıklığına neden olur
düğüm başına ity as
c +
n
∑
i = 0
f tx ben (n, m)
(5.5)
yani
Ω EthereumNode ∈ O (n · f ortalama (n, m))
(5.6)
kullanıcılar ortalama şirketi elinde tutmaya teşvik edilirken
Ethereum tarafından çalıştırılan kodun pleksitesi f avg (n, m)
infazın gazla ödenmesi gerektiğinden küçük ve
blok gaz limiti gibi kısıtlamalardan kaynaklanmaktadır. Diğer
kelimeler, karmaşıklık nedeniyle ∑ n
i = 0 f tx ben (n, m) olmak
sistemin tüm düğümlerine yük, diğer sistemik
özellikler, kullanıcıların karmaşık kod çalıştırmasını engellemelidir
Ethereum'da ağın sınırlarına çarpmamak için.
Yine, her düğümün aynı kümeyi işlemesi gerektiğinden
tüm işlemler, tüm sistemin zaman karmaşıklığı
o zaman bir düğümün m ile çarpımıdır:
Ω Ethereum ∈ O (nm · f tx i (n, m))
(5.7)
C. Blockchain
Yukarıdaki her iki Blockchain sistemi örneğinin
çalışmak için önemsiz olmayan bir hesaplama ek yükü
hiç: iş kanıtı, hash-crack süreci aynı zamanda
madencilik. Bu ek yük ikisinin de bir işlevi olmadığından
işlem sayısı ne de doğrudan
düğümler, karmaşıklık analizinde genellikle ihmal edilir. İle
bugün tüm Bitcoin madencilerinin toplam enerji tüketimi
İzlanda ülkesinden daha büyük olmak [Coppock17] ,

Blockchain'in fikir birliğinin karmaşıklığını ihmal etmek
gorithm aptalca bir hata gibi görünüyor.
Blok zincirleri blok süresini belirler, ortalama süre
sistemin sabit bir parametre olarak iki bloğun arasını doldurun
hash-crack'in farklılığını ayarlayarak homeostazda kalır.

ağın toplam hash oranına göre düzenlenir. Bir
belirli bir madencilik düğümleri kümesine sahip belirli bir ağ ve bir
toplam hash-rate verildiğinde, hash-crack'in karmaşıklığı
sabittir. Ancak sistem büyüdükçe ve daha fazla madenci
çevrimiçi olun, bu da ağların toplam hash değerini artırır
oranını korumak için zorluğun artması gerekir.
ortalama blok zaman sabiti.
Bu yaklaşımla, daha yüksek bir toplam hash avantajı
rate x HR , bir rakibin daha fazla zorluğudur.
önyargılı bloklar oluşturarak sistemi etkilemek (
bu tarafın çift harcama saldırıları yapabilmesini sağlar).
Bu nedenle, Blockchain'ler madenciliği sübvanse etmek zorundadır.
ekonomik olarak iyileştirmek için yüksek x HR beklemede
bir saldırganın güvenilir madencileri alt etmesi mümkündür.
Dolayısıyla, ağlar arasında doğrudan bir ilişki vardır.
toplam güvenilir hash-rate ve onun güvenlik seviyesi
madencilik gücü saldırıları. Bu güven anlamına gelir
Ψ Herhangi bir ajanın sahip olabileceği blok zinciri ,
sistem, sistemin hash-rate x HR'sinin bir fonksiyonudur ve
daha doğrusu, maliyet / iş maliyeti (x HR) pro-
videonuzu izleyin. Sadece belirli bir t işlemine bakıp verilen
herhangi bir bilgisayar korsanı ekonomik olarak yalnızca rasyonel davranır,
Tüm X n'ye eklendiğinde, n'nin bir üst sınırı vardır
içinde
Ψ Blok zinciri (t) <min (1,
maliyet (x HR)
değer (t))
(5.8)
Bu güveni kısıtlamamak için
madencilik süreci ve dolayısıyla mimari
Blockchain'in kendisi, maliyet (x HR) (kurulum dahil)
madencilik donanımının yanı sıra enerji tüketimi)
içinde değiş tokuş edilen değer ile doğrusal olarak büyümesi gerekir.
sistemi.

D. Holochain

Ω HC belirli bir Holochain sistemi olsun, n toplam olsun
tüm halkın12 (yani, DHT'ye koyun) durum geçişleri
(işlemler), Ω HC'deki tüm aracıların toplamda tetiklemesine izin verin ve
sistemdeki ajanların (= düğümlerin) sayısı olalım.
DHT'ye yeni bir giriş koymak, bir
o belirli girişi tutmaktan sorumlu düğüm,
[Kademlia] ya göre bizim durumumuzda bir zaman var
12 özel (bkz: 17) durum geçişi, yani bir lo-
cal X n , tamamen bir düğümün ajansı kapsamındadır ve
sistemin diğer bölümlerini doğrudan etkilemez ve bu nedenle
dağıtılmış olarak Ω HC'nin karmaşıklık analizi için ihmal edilebilir
sistemi
karmaşıklığı
c + ⌈log (m) ⌉.
(5.9)
Durum geçiş verilerini aldıktan sonra bu düğüm,
q komşularıyla dedikodu yapmak r kopyalarına neden olacak
bu durum geçiş girdisinin
sistem - r farklı düğümlerde. Bu düğümlerin her biri,
uygulamaya özel bir mantık olan bu girişi doğrulayın

bunun karmaşıklığına v (n, m) diyeceğiz.
Bir araya geldiğinde bu, sistem genelinde karmaşıklığa neden olur.
ile verildiği gibi durum geçişi
c + ⌈log (m) ⌉
‿

‿‿
‿
DHTlookup
+ q + r · v (n, m)
‿ ‿‿ ‿
doğrulama
(5.10)
aşağıdaki tüm sistem karmaşıklığını ima eder
O-notasyonu
Ω Holochain ∈ O (n · (log (m) + v (n, m))
(5.11)
Şimdi, bu genel sistem karmaşıklığıdır. Or-
karşılaştırmayı mümkün kılmak için,
Holochain genelliği kaybetmeden (yani, bağımlı
Spesifik Holochain uygulaması), bütünün yükü
sistem tüm düğümler tarafından eşit olarak paylaşılır. Daha fazla olmadan
herhangi bir durum geçişi için varsayımlar, olasılık-
belirli bir düğümden kaynaklanması 1
m , yani terim
arama karmaşıklığının m'ye bölünmesi gerektiğinden
düğüm başına ortalama arama karmaşıklığını açıklar. Diğer
her düğümün görmesi gereken Blockchain sistemlerinden
her işlem, eyalet geçişinin büyük çoğunluğu için
belirli bir düğümün dahil olmadığı durumlar.
düğümün açık anahtar karmasının stokastik yakınlığı
girişin hash değeri, düğümün katılımını tetikleyen şeydir.
H hash fonksiyonunun tek tip bir dis-
olasılıkla sonuçlanan hash değerlerinin haraçlanması
belirli bir düğümün, yapamayan r düğümlerinden biri olması
bu girişi 1 olarak atın
m kere r. Ortalama süre
ortalama bir düğüm tarafından işlenen karmaşıklık,
Ω HolochainNode ∈ O (
n
m · (kütük (m) + v (n, m))) (5.12)
N faktörünün
m ortalama sayısını temsil eder
düğüm başına durum işlemleri (yani düğüm başına yük) ve
bu son derece uygulamaya özel bir değer olsa da,
düğümler zorunlu olduğundan, önceden beklenen bir alt sınırdır
en azından ürettikleri durum geçişlerini işlemek-
kendileri.
Mimari tarafından eklenen tek ek yük
Merkezi olmayan bu sistemin,
günlüğün karmaşıklığı (m).
Bilinmeyen ve ayrıca uygulamaya özel kompleks-
doğrulama rutinlerinin ity v (n, m) sebebi olabilir
hala tüm sistemin karmaşıklığını artırıyor. Ve gerçekten
Holochain uygulamalarını bir

doğrulama rutinlerinde çok fazla karmaşıklık var. Bu
Blockchain'in fikir birliği değerini taklit etmek temelde mümkün

---

Sayfa 12

doğrulama düğümünü zorlayarak dation gereksinimi
bir en eklemeden önce diğer tüm düğümlerle iletişim kurar
DHT'yi deneyin. Aynı zamanda tüm düğümlerin yalnızca yarısı olabilir.
Ve kesinlikle çok az şey içeren bir dizi uygulama vardır.
karmaşıklık - veya bir uygulama içindeki belirli durum geçişleri-
çok az karmaşıklık içeren katyon. Holochain'de
uygulama karmaşıklığı gereken yere koyabilir ve
sistemin geri kalanının hızlı ve ölçeklenebilir olmasını sağlayın.
VI . Bölümde gerçek dünya kullanımı sağlayarak devam ediyoruz
vakalar ve önemsiz olmayan Holochain uygulamalarının nasıl olduğunu gösteren
bir doğrulama karmaşıklığıyla başa çıkacak şekilde oluşturulabilir
O (1) sayısı, düğüm başına toplam zaman karmaşıklığına neden olur
O (log (m)) ve bütünlüğe yeterince yüksek güven
iş kanıtı sunmadan.

VI. DURUMLARI KULLANIN

Şimdi, oluşturulmuş uygulamaların birkaç kullanım durumunu sunuyoruz
Holochain'de, kullanım senaryosunun bağlamını göz önünde bulundurarak ve
hem karmaşıklığı hem de bütünlüğün değerlendirmesini nasıl etkiler?
ve dolayısıyla doğrulama tasarımı.

A. Sosyal Medya

Basit bir mikro blog uygulamasını düşünün
Holochain kullanarak:
1. F I = {f gönderi (metin, düğüm), f takip et (düğüm), f oku (metin)}
ve
2. F V = {f isOriginator }
O (1) karmaşıklığını tanımlayın

B. Kimlik

DPKI

C. Para

karşılıklı krediye karşı madeni paraların karmaşıklığı
işlem daha yüksek, karmaşıklık O (n 2) olabilir veya
O (log (n)) holo para birimi teknik incelemesine bakın: [?]

VII. UYGULAMA

Bu yazının yazıldığı sırada tamamen operasyonel bir
sistemin bu yazıda açıklandığı gibi uygulanması,
yazmak için iki ayrı sanal makine içeren
JavaScript veya Lisp'deki DNA işlevleri, kanıtla birlikte
bir dizi uygulamanın konsept uygulamaları
twitter klonu, gevşek benzeri bir sohbet sistemi, DPKI dahil,
ve uygulama oluşturmak için yararlı olan bir dizi karma kitaplık.
1. 30k + satırlık go kodu.
2. DHT: libp2p / ipfs kademlia'nın özelleştirilmiş versiyonu
uygulama.
3. Ağ Aktarımı: uçtan uca dahil libp2p
şifreleme.
4. Javascript Sanal Makinesi: otto
https://github.com/robertkrimen/otto.
5. Lisp Sanal Makineleri: zygomys
https://github.com/glycerine/zygomys.

Ek olarak, bir kıyaslama paketi oluşturduk.
kullanılan işleme, bant genişliği ve depolamayı inceleyin
çeşitli senaryolar ve bunları Ethereum ile karşılaştırdı
benzer senaryolardaki uygulamalar. Bunlar burada görülebilir:
https://github.com/holochain/benchmarks
Henüz büyük boyutlar için ölçeklenebilirlik testleri uygulamadık
ölçek uygulamaları, ancak yol haritamızdadır. YAPMAK
Ek A: DHT hc
1. dht putLink (taban, bağlantı, etiket) temel ve bağlantının olduğu yer
anahtarlar ve etiket keyfi bir dizedir;
demeti {link, tag} anahtar tabanı ile ilişkilendirir.
2. dht getLinks (taban, etiket) burada tabanın bir anahtar tuş olduğu ve
etiket, rastgele bir dizedir ve
etiketi ile tanımlanan temel bağlantı seti.
3. dht mod (anahtar, yeni anahtar) burada anahtar ve yeni anahtar
σ tuşunun değiştiricisi olarak newkey ekleyen anahtarlar ∈ Δ
ve dht putLink'i çağırır (anahtar, yeni anahtar, "değiştirilen").
4. dht del (anahtar) burada anahtar bir anahtar ve σ anahtarını işaretler Δ
silindi.
5. dht için modifikasyon olsun mod & del yeniden .
Ek B: F sys
1. diğer tüm sys işlevleri ...
Ek C: Güven Yönetimi Kalıpları
Uygulama geliştiricilerinin kullanabileceği Holochain'deki araçlar
Değerlendirilen Gereksinimler'de bazıları da kullanılmaktadır
sistem düzeyinde ve küresel olarak parametreleştirilmiş bir
uygulama:
1. TODO'ya karşı imzalama
2. Noterler TODO - "Ağ noterdir."
3. Yayınlama Başlıkları, ör. Zincir geri alma algılaması için
4. Kaynak zinciri incelemesi. YAPMAK

Sayfa 13

5. Engellenen listeler. ör. DDOS, spam, vb.
6. ... daha fazlası burada ...
Ek D: Zarlar
• Davet
Membran için en doğal yaklaşımlardan biri
ajanların kimlik sağladığı bir alanda geçiş
halihazırda
membranda. Bu davetiye olabilir:
- herhangi biri tarafından
- bir yönetici tarafından (bu,
uygulamanın DNA'sı veya içinde paylaşılan bir değişken
DHT - her ikisi de değişebilir veya sabit olabilir)
- birden çok kullanıcı tarafından (sosyal üçgen uygulayarak-
yon)
• Kimlik Kanıtı / İtibar
Diğer uygulamaların / zincirlerin varlığı göz önüne alındığında,
bunlar kimliği eklemek için kullanılabilir ve
o zincirdeki itibar isteyen temsilciye
katılmak. Bu çok önemli bir ayağı gibi göründüğü için

Holochain uygulamalarının ekosistemi,
DPKI (dis-
çalışacak olan açık anahtar altyapısı)
ana kimlik ve itibar platformu olarak.
Bu uygulamanın bir prototipi önceden geliştirilmişti
bu makalenin yazısına.
• Varlık Kanıtı
Kullanım
nın-nin
noter tasdikli
Ulusal
docu-
Acente içindeki ments / pasaport / kimlik kartları
giriş (X'te ikinci giriş).
• Hizmet kanıtı
Bir hizmetin / ana bilgisayarın teslim edildiğinin kriptografik kanıtı
bir uygulamanın oluşturulması. Bundan yararlanmayı planlıyoruz
dağıtılmış bulut barındırma aplikasyonumuzla
üzerine inşa edeceğimiz plikasyon Holo
Holochain. Holo Hosting teknik incelememize bakın:
çok daha fazla ayrıntı [?].
• İşin kanıtı
Başvurunun gerekliliği anonimlik değilse,
kriptografik hash-cracking işi dışında
Blockchain'lerin çoğunda uygulandığında, bu aynı zamanda
yeni üyelerin onaylamalarının istendiği yararlı bir iş olun
topluma övgü ya da kanıtlamak için bir bulmaca
ana bilgi. Örnekler:
- Kanıtlamak için yerel haritalarla ilgili bilgileri test edin
vatandaşlık
- DNA dizilimi
- Protein katlama
- SETI
- Bilimsel makalenin yayınlanması
• Teminat Kanıtı / Ödeme
Temsilcinin onayını almak için depozito veya ödeme.
• Bağışıklık sistemi
Uygulayıcı tarafından oynatılmayan düğümlerin kara listeye alınması
katyon kuralları.
TEŞEKKÜRLER
Steve Sawin'e bu makaleyi incelediği için teşekkür ederiz.
L A TEX 2εdestek ve çok daha fazlası ..... .
[DUPONT] Quinn DuPont. *Algoritmik Deneyler*
Yönetişim: The DAO'nun tarihi ve etnografisi,
Başarısız Merkezi Olmayan Otonom Organizasyon
http://www.iqdupont.com/assets/documents/
DUPONT-2017-Preprint-Algorithmic-Governance.pdf
[EIP-150] Gavin Wood. *Ethereum: Güvenli Merkezi Olmayan*
Genelleştirilmiş İşlem Defteri .
http://yellowpaper.io/
[Kademlia] Petar Maymounkov ve David Mazieres *Kadem-*
lia: Bir Eşler Arası Bilgi Sistemi Tabanı
XOR Metriği
https://pdos.csail.mit.edu/~petar/papers/
maymounkov-kademelerlia-lncs.pdf

[Zhang13] Zhang, H., Wen, Y., Xie, H., Yu, N. *Dağıtılmış Karma Tablo Teorisi, Platformları ve Uygulamaları*
[Croman ve diğerleri 16] Kyle Croman, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Ançizdi Miller, Prateek Saxena, Elaine Shi, Emin Gn Sirer, Dawn Song, Roger Wattenhofer, *Blockchain Ölçeklendirme Üzerine* , Finansal Kriptografi ve Veri Güvenliği, Springer Vergecikme 2016
[Bitcoin Reddit] / u / mike Hearn, / u / awemany, / u / nullc ve diğerleri. https://www.reddit.com/r/Bitcoin/comments/3a5f1v / mike_hearn_on_those_who_want_all_scaling_to_be / csa7exw /? context = 3 & st = j8jfak3q & sh = 6e445294 Reddit tartışması 2015
[Marir2014] Marir, Toufik ve Mokhati, Farid ve Bouchelaghem-Seridi, Hassina ve Tamrabet, Zouheyr ", *Çok* Etmenli *Sistemlerin Karmaşıklık Ölçümü "* , Multiagent Sistem Teknolojileri: 12. Almanya Konferansı, MATES 2014, Stuttgart, Almanya, 23-25 Eylül, 2014. Bildiriler, Springer International Publishing 2014
https://doi.org/10.1007/978-3-319-11584-9_13
[Coppock17] Mark Coppock *THE WORLDS CRYPTOCURRENCY MADENCİLİĞİNDEN DAHA FAZLA ELEKTRİK KULLANAR İZLANDA*
https://www.digitaltrends.com/computing/

Sayfa 14

bitcoin-ethereum-madencilik-kullanım-önemli-elektrik-gücü /
[BitcoinWiki] *Bitcoin Protokolü*
https://en.bitcoin.it/wiki/Protocol_rules#.22tx.22_mesaj Bitcoin Wiki
[IPFS] Juan Benet *IPFS - İçeriğe Yönelik, Sürümlendirilmiş, P2P Dosya Sistemi (TASLAK 3)*
https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX / ipfs.draft3.pdf
[LibP2P] Juan Benet, David Dias *libp2p Spesifikasyonu*
https://github.com/libp2p/specs
[Oxford] Oxford Çevrimiçi sözlüğü
https://en.oxforddictionaries.com/definition/kaynak
[Douceur02] Douceur, John R. (2002). "Sybil Saldırısı"
https://www.microsoft.com/en-us/research/yayın / the-sybil-attack /? from = http% 3A% 2F% 2Fresearch.microsoft.com% 2Fpubs% 2F74220% 2F iptps2002.pdf Uluslararası Peer-To- atölyesi Eş Sistemler. Erişim tarihi: 23 Nisan 2016.
[HoloCurrency] Arthur Brock ve Eric Harris-Braun 2017 *Holo: Küresel Ölçek için Kripto Para Birimi Altyapısı ve Kararlı Değer*
https://holo.host/holo-currency-wp/
[Nilsson15] Nilsson, Kim (19 Nisan 2015). *Eksik MtGox bitcoins ". Erişim tarihi: 10 Aralık 2015.*
http://blog.wizsec.jp/2015/04/

the-eksik-mtgox-bitcoins.html
[Swanson15] Tim Swanson *Hizmet olarak fikir birliği: özet izin verilen, dağıtılanların ortaya çıkması hakkında rapor defter sistemleri* 6 Nisan 2015
https://pdfs.semanticscholar.org/f3a2/2daa64fc82fcda47e86ac50d555ffc24b8c7.pdf