Æternity blok zinciri

Güvenilir, merkezi olmayan ve tamamen işlevsel oracle makinesi

23 Ocak 2017
v0.1

Zackary Hess
zack@aeternity.com
Yanislav Malahov
yani@aeternity.com
Jack Pettersson
jack@aeternity.com

Özet — 2014'te Ethereum'un piyasaya sürülmesinden bu yana merkezi olmayan güvensiz uygulamalara büyük ilgi duymuştur (akıllı sözleşmeler). Sonuç olarak, birçoğu uygulamayı denedi bir blok zincirinin üstünde gerçek dünya verileriyle uygulamalar. Biz uygulamanın durumunu ve kodunu zincir üzerinde depolamanın birkaç nedenden dolayı yanlış.

Son derece ölçeklenebilir bir blok zinciri mimarisi sunuyoruz. oracle'ı kontrol etmek için de kullanılan fikir birliği mekanizması. Bu, kehaneti çok verimli kılar, çünkü katmanlaşmayı önler üst üste bir fikir birliği mekanizması. Eyalet kanalları gizliliği ve ölçeklenebilirliği artırmak için entegre edilmiştir. İçindeki jetonlar kanallar tamamen işlevsel smart kullanılarak aktarılabilir oracle yanıtlarına erişebilen sözleşmeler. Sözleşmeyi saklamayarak zincir üzerinde kod veya durum, akıllı sözleşmeler yapabiliyoruz önemli bir kayıp olmadan analiz etmesi daha kolay ve daha hızlı işlenmesi içinde *fiilen* işlevselliği.

Sentetik varlıklar ve tahmin için pazarlar gibi uygulamalar piyasalar küresel ölçekte verimli bir şekilde uygulanabilir. Birkaç parçalar Erlang'da kavram kanıtı uygulamalarına sahiptir. Devel- cüzdan, adlandırma gibi seçenek araçları ve uygulama esasları kimlik sistemi de sağlanacaktır.

C ONTENTS

I. GİRİŞ
Bu yazının amacı, bir genel bakış sunmaktır.
Æternity blockchain mimarisi ve olası uygulamalar
tions. Gelecekte daha detaylı makaleler yayınlanacak,
özellikle fikir birliği ve yönetişim mekanizmaları için.
Ancak, mimarimizin bütünsel olduğu unutulmamalıdır;
tüm bileşenler modüler bir şekilde birbirine bağlanır ve sinerji oluşturur.
Bu yazının geri kalanı dört bölüme ayrılmıştır. Önce biz
temel teorik fikirleri tanıtacak ve tartışacak
mimarimizi bilgilendiren. İkincisi, tartışacağız

---

temel uygulamaları, diğer olası kullanım durumlarını ve
platformu bir geliştirici olarak nasıl kullanacağınıza dair sezgiler verin.
Üçüncüsü, mevcut kavram kanıtı uygulamasını sunacağız.
Erlang ile yazılmış mentation. Bir tartışma ile sonlandırıyoruz,
olası gelecekteki yönler ve diğerleriyle karşılaştırmalar dahil
teknolojileri.

A. Önceki Çalışma

Blockchain'ler, her şeyden önce Bitcoin yeni bir yol gösterdi
İnternette değer alışverişi yapmak için [1]. Bu var
bir dizi umut verici gelişme takip etti: Ethereum
Turing-complete smart con- yazmanın bir yolunu gösterdi
bir blok zinciri mimarisi [2] ile güvence altına alınmış yollar ; Truthcoin
blockchains [üzerine kehanet alma yapmak için araçlar oluşturdu 3] iken,
GroupGnosis ve Augur bunları nasıl daha fazla yapabileceklerini gösterdi
verimli [4]; Casey Detrio nasıl pazar yapılacağını gösterdi
blok zincirlerinde [5]; Namecoin,
bir alan adı sunucusunun dağıtılmış eşdeğeri [6]; Factom
karmaları depolayan bir blok zincirinin nasıl kullanılabileceğini gösterdi
herhangi bir dijital verinin varlığının bir kanıtı [7] .
Bu teknolojiler söz konusu olduğunda büyük umut vaat ediyor
herkese birinci sınıf mali ve hukuki hizmetler sunmak.
Ancak şimdiye kadar bir araya gelmeyi başaramadılar.
vaadi gerçekten yerine getiren birleşik bütün. Özellikle,
şimdiye kadar tüm çözümler en az birinde eksikti
aşağıdaki hususlar: yönetişim, ölçeklenebilirlik, komut dosyası güvenliği
ve gerçek dünya verilerine ucuz erişim [siteye ihtiyacınız var] . Æternity amaçları
tüm bu açılardan en son teknolojiyi geliştirmek.

II. Æ TERNITY BLOCKCHAIN

Ölçeklenebilirlik eksikliğinin, komut dosyası güvenliğinin
ve mevcut "akıllı kontrolün gerçek dünya verilerine ucuz erişim
tract platformları ”üç temel konuya iniyor. İlk önce
şu anda geçerli olan durum bilgili tasarım akıllı sözleşmeler yapar
platform için yazılmış analizi zor1ve durum bilgisi
sıralı işlem siparişi ile birlikte karmaşık hale getirir
ölçeklenebilirlik [gerekli bilgi] . İkincisi, gerçek
merkezi olmayan, güvenilir ve güvenilir bir şekilde sisteme dünya verileri

güvenilir yol, gerçekleştirmeyi karmaşıklaştırır veya tamamen engeller
pek çok umut vaat eden uygulamadan [alıntı gerekir] . Üçüncüsü, platformlar
sırayla kendilerini güncelleme yetenekleri sınırlıdır
yeni teknolojik veya ekonomik bilgilere uyum sağlamak. Biz
Bu üç sorunun her birinin net bir çözümü olduğuna inanıyorum
keşfedilmesi gereken yollar.
Birincisi, eyalet kanalı teknolojisi ile ilgili son araştırmalar
durumu zincirde tutmanın birçok kullanım durumu için
gerekli [bilgi gerekli] . Çoğu zaman saklamak tamamen mümkündür
eyalet kanallarındaki tüm bilgiler ve yalnızca blok zincirini kullanın
bilgi alışverişinin herhangi bir ekonomik sonucunu çözmek için,
ve anlaşmazlık durumunda bir yedek olarak. Bu öneriler
blockchain mimarisine alternatif bir yaklaşım
Turing-complete akıllı sözleşmeler eyalet kanallarında mevcuttur, ancak
zincir üzerinde değil. Bu, tüm işlemlerden dolayı ölçeklenebilirliği artırır
1 Durum bilgili sözleşmeleri analiz etmenin zorluğu çok açık bir şekilde
"The DAO" yu düşüren yeniden giriş hatasıyla ortaya çıktı. Bu oldu
koda Ethereum'un yaratıcılarından birkaçı tarafından denetlenmiş olmasına rağmen
ve genel topluluk [kaynak belirtilmeli] .
bağımsız hale gelir ve böylece paralel olarak işlenebilir.
Ek olarak, bu, sözleşmelerin asla paylaşılanlara yazmadığı anlamına gelir.
durumu, test ve doğrulamalarını büyük ölçüde basitleştiriyor. Biz
bu tasarımın blok zincirlerinin
veri depolamadan ziyade finansal mantık hakkında; orada var
blok zincirlerini tamamlayan merkezi olmayan depolama çözümleri
mükemmel bir şekilde.
İkincisi, Augur gibi uygulamalar,
gerçek dünya verilerini blok zincirine merkezi olmayan bir şekilde getirin
düzenlenmiş bir yol - esasen bir fikir birliği oluşturma sürecinde
akıllı sözleşmelerin içindeki mekanizma [8], kullanmak yerine
temeldeki blok zincirinin fikir birliği mekanizması. Bu
verimsizliğe yol açar ancak güvenliği artırmaz. The
bundan elde edilen doğal sonuç, blok zincirini genelleştirmektir.
bilgi sağlayabilmesi için fikir birliği mekanizması
sadece bir sonraki iç durumda değil, aynı zamanda eyalette de
dış dünyanın. Bu nedenle,
Blockchain'in fikir birliği mekanizması, sonucunu belirler
karmaşıklık teorisinin kehanet makinesi dediği şeyi çalıştırmak:
Turing'den daha güçlü olan teorik bir makine
makine çünkü yapamayacak bazı soruların cevapları var.
"Futbol maçını kim kazandı
X? " [bilgi gerekiyor.] .
Üçüncüsü, fikir birliği mekanizmasının
sistemin parametrelerini belirlemek için de kullanılabilir.
Bu, değişen dış koşullara uyum sağlamasına izin verir.
yeni araştırmaları ve son gelişmeleri benimsemenin yanı sıra
alan.
Bu bölümün geri kalanı, Æternity blok zincirini tanıtıyor
daha ayrıntılı olarak, hesaplara kısa bir genel bakışla başlayarak,
belirteçler, isimler ve blokların yapısı. Bunu takip eden
devlet kanallarına yaklaşımımızın açıklaması ve akıllı
sözleşmeler ve ardından blok zincirinin nasıl
fikir birliği mekanizması, her ikisi de verimli bir
oracle mekanizması ve sistemi yönetmek. Sonunda biz
Ölçeklenebilirliği birkaç farklı açıdan tartışın.

A. Jetonlar, hesaplar ve bloklar
Sözleşme geliştiricisinin "vatansız" olmasına rağmen
bakış açısına göre, Æternity blok zinciri birkaç
önceden tanımlanmış durum bileşenleri. Şimdi bunları şu şekilde açıklayacağız:
ve her bloğun içeriği. Basit olması için bu bölüm
her düğümün tüm blok zincirini izlediğini varsayar.
Olası optimizasyonlar bölüm II-E'de açıklanmaktadır.
A.1) Erişim belirteci, Aeon: Blok zincirini kullanmak
ücretsiz, ancak kullanıcının aeon adında bir jeton harcamasını gerektirir.
Aeon, tüketilen herhangi bir kaynak için ödeme olarak kullanılır
platformda ve finansal uygulamalar için temelde
platformda uygulanmaktadır.
Aeon'un oluşum bloğundaki dağılımı
Ethereum'da barındırılan akıllı bir sözleşme ile belirlenir. Daha ileri
aeon madencilik yoluyla oluşturulacaktır.
Tüm sistem ücretleri aeon ile ödenir, tüm akıllı sözleşmeler
aeon'a yerleşmek.
A.2) Hesaplar: Her hesabın bir adresi ve bir bakiyesi vardır.
aeon ance ve aynı zamanda her gün artan bir nonce
işlem ve son güncellemesinin yüksekliği. Her hesap

---

ayrıca, olduğu süre için küçük bir ücret ödemek zorunda
açık. Hesap oluşturma ve saklama maliyetleri,
spam ve devlet bloatını caydırır. Silme ödülü
hesaplar, alanın geri kazanılmasını teşvik eder.
A.3) İsim sistemi: Birçok blok zinciri sistemi,
kullanıcıları için okunamayan adresler. Aaron damarında
Swartz'ın işi ve Namecoin, Æternity bir adı taşıyor
hem merkezi olmayan hem de güvenli olan sistem
insan dostu isimleri destekleyen [9]. Blok zincirinin durumu
benzersiz insan dostu dizelerden
sabit boyutlu bayt dizileri. Bu isimler işaret etmek için kullanılabilir
Æternity'deki hesap adresleri veya hash'ler gibi şeyler, ör.
Merkle ağaçları.
A.4) Blok içeriği: Her blok aşağıdakileri içerir
bileşenler:
• Önceki bloğun karması.
• Merkle işlem ağacı.
• Bir Merkle hesap ağacı.
• Merkle adlar ağacı.
• Açık kanallardan oluşan bir Merkle ağacı.
• Cevap vermemiş bir Merkle kahin ağacı
ilgili sorular.
• Bir Merkle kehanet ağacı cevap verir.
• Merkle provalarının bir Merkle ağacı.
• Rastgele sayı üretecindeki mevcut entropi.
Bir önceki bloğun karması, bir
blockchain siparişi. İşlem ağacı hepsini içerir
mevcut bloğa dahil olan işlemler. İle
oybirliği oy ağacı haricinde, tüm ağaçlar tamamen
fikir birliği altında: bir ağaç bir bloktan diğerine değiştirilirse
sonraki, bu değişikliğin yeni bir işlemden kaynaklanması gerekir.
bloğun işlem ağacı ve güncellemenin Merkle kanıtı

bloğun kanıt ağacına dahil edilmelidir. Amacı
kalan üç ağaç umarım
aşağıdaki bölümler.
B. Eyalet kanalları
Dünyadaki en ilginç gelişmelerden biri
Son zamanlarda blockchain alanı, devlet kanallarının alanıdır. Çalışırlar
temel ilkeye göre, çoğu durumda yalnızca insanların
Bir işlemden etkilenen bunun hakkında bilgi sahibi olmanız gerekir. Özünde,
işlem yapan taraflar bir blok zincirinde bazı durumları somutlaştırır,
örneğin bir Ethereum sözleşmesi veya bir Bitcoin multisig. Onlar sonra
bu duruma imzalı güncellemeleri aralarında göndermeniz yeterlidir.
Kilit nokta, bunlardan birinin bunları kullanabilmesidir.
blok zincirindeki durumu güncellemek için, ancak çoğu durumda
onlar değil. Bu, işlemlerin yapılmasına izin verir
bilgi aktarılabildiği ve işlenebildiği kadar hızlı
taraflar tarafından
işlem doğrulandı ve potansiyel olarak sonlandırıldı
blockchain'in fikir birliği mekanizması ile.
Ternity'de, kararlaştırılabilecek tek durum güncellemesi
blok zinciri bir aeon transferidir ve tek aeon
işlem yapan tarafların devredilebilecekleri
zaten kanala yatırıldı. Bu, tüm kanalları
birbirinden bağımsız, anında fayda sağlayan
1
makro Altın f870e8f615b386aad5b953fe089;
2
3
Altın oracle
4
0 1000 ise 0 0 son
5
0
Şekil 1. Altının fiyatı üzerine bir bahsi kodlayan basit bir sözleşme. Dil
IV-A bölümünde sunulacak olan Forth benzeri Chalang kullanılır .
kanallarla ilgili herhangi bir işlemin işlenebilmesi için uygun
paralel olarak, işlem hacmini büyük ölçüde iyileştirir.
Blok zinciri yalnızca nihai sonucu belirlemek için kullanılır
veya ortaya çıkan çatışmaları çözmek için, kabaca benzer
yargı sistemi. Ancak, blok zincirinin davranışı
öngörülebilir olacak, amaçlananın tartışılmasında herhangi bir kazanç olmayacaktır.
bir devlet kanalının sonucu; kötü niyetli aktörler teşvik edilir
doğru davranmak ve yalnızca son durumu
blok zinciri. Hepsi birlikte alındığında, bu işlemi artırır
birkaç büyüklük sırasına göre hız ve hacim
gizlilik olarak.
B.1) Akıllı sözleşmeler: Buna rağmen,
zincir üzerinde yerleşilebilir, aeon, Æternity transferidir
hala yapabilen bir Turing eksiksiz sanal makine içerir.
"akıllı sözleşmeler" çalıştırın. Staj sözleşmeleri kesinlikle
bazı kurallara göre fon dağıtan anlaşmalar,
şirket benzeri sözleşmelerle tam bir tezat oluşturan
örneğin Ethereum. Daha dikkate değer pratik farklılıklardan ikisi
varsayılan olarak, yalnızca ilgili tarafların
belirli bir sözleşme ve yalnızca açık durumu olan taraflar
kanal geçerli bir sözleşme oluşturabilir. Taraflar kabul ederse

sözleşme, imzalarlar ve ileride başvurmak üzere kopyalarını saklarlar.
Yalnızca sonucu şu ise blok zincirine gönderilir.
tartışmalı, bu durumda kod yalnızca bir parça olarak saklanır
hiçbir durumda başka bir durumda gönderilmemiştir. Eğer bu
olur, blok zinciri tokenleri aşağıdakilere göre dağıtır:
sözleşme ve kanalı kapatır.
Örnek olarak, şek. 1 , çok basit bir sözleşmeyi gösterir
belirli bir zamandaki altın fiyatı üzerine bir bahis kodlar. 1. satırda,
Makro Altın, söz konusu kehanetin tanımlayıcısını kaydeder,
altının fiyatı 38 $ / g'ın altındaysa bu doğru olacaktır.
1 Aralık 2016. Sözleşmenin ana metni görüntülenir
2-4. satırlarda: önce altın oracle'ın tanımlayıcısını
Yığın ve oracle kullanarak çağırın;
oracle'ın cevabı yığının tepesinde. Bunu yapmak için kullanıyoruz
koşullu dallanma: oracle true olursa,
Yığına 0 ve 1000, 0 aeon olması gerektiğini belirtir
yandı ve 1000 aeon ilk katılımcıya gitmeli
Kanal. Aksi takdirde, ikinci 0 ile 0 ve 0'a basarız
diğer katılımcının tüm aeon'u aldığını gösterir.
kanal. Sonunda nonce olarak kabul edilen 0'a basıyoruz
Bu kanal durumunun. Gerçek kullanımda, nonce olacaktır
dağıtımda oluşturulur.
Unutulmaması gereken önemli bir nokta, stajyerlik sözleşmeleridir.
kendi durumlarını korumayın. Herhangi bir durum korunur
işlem yapan taraflarca ve icra sırasında girdi olarak sunulur.
Her sözleşme, esasen, bazılarını gerektiren saf bir işlevdir.
3

---

4. sayfa

1
: hashlock
2
takas
3
karma
4
==;
Şekil 2. Basit bir karma blok.
1
makro Taahhüdü a9d7e8023f80ac8928334;
2
3
Taahhüt hashlock çağrısı
4
0 100 değilse 0 50 son
5
1
Şekil 3. Bir aracı aracılığıyla tokenleri güvenmeden göndermek için hashlock kullanma.
girdi ve çıktı olarak yeni bir kanal durumu verir2. Faydalar
genel olarak yazılım geliştirmede saf fonksiyonların kullanılması,
ve özellikle finansal uygulamaların geliştirilmesinde,
akademi ve endüstride kapsamlı bir şekilde belgelenmiştir
onlarca yıldır [10] [kaynak gerek.] .
a) Sözleşme etkileşimi ve çok adımlı sözleşmeler:
Tüm sözleşmeler vatansız ve bağımsız olsa da

birbirlerinden bağımsız olarak, sözleşme etkileşimi ve durumsallık
hashlocking yoluyla hala elde edilebilir [ihtiyaç duyulan sit .] . Basit
hashlock, şek. 2 . 1. satırda bir fonksiyon tanımlıyoruz
yığının bir karma içermesini bekleyen hashlock olarak adlandırılır
h ve bir sır. Onları hash yapmak için 2. satırda değiştirir
3. satırdaki sır, eşitlik operatörünü çağırmadan önce
karma (v) ve h 4. satırda. Bu, sırrı bir
karmanın ön görüntüsü. Bu işlev, tahmin etmek için kullanılabilir
kod dallarının farklı sözleşmelerde yürütülmesi
aynı gizli değerin varlığı.
Basit bir örnek kullanım olarak, hashlock'lar aşağıdakileri mümkün kılar:
güvenmeden göndermek için bir eyalet kanalını paylaşmayan kullanıcılar
diğer aeon, aralarında bir kanal yolu olduğu sürece
onları. Örneğin, Alice ve Bob'un bir kanalı varsa ve
Bob ve Carol'ın bir kanalı var, ardından Alice ve Carol'ın
Bob aracılığıyla işlem yapar. Bunu iki kopya oluşturarak yapıyorlar
Şek. 3 , her kanal için bir tane. The
1. satırdaki taahhüt, Alice'in
seçer. 3. satırda onu yığına itiyoruz ve
hashlock işlevi. Hangi daldan alırsa
çalıştırılan hashlock'un dönüş değerine bağlıdır. bir Zamanlar
Alice, bu sözleşmelerin tüm taraflarca imzalandığını ortaya koyuyor
sırrı, Bob ve Carol'ın kendi
aeon.
Hashlocking, örneğin çok oyunculu oynamak için de kullanılabilir
Şekilde gösterildiği gibi kanallardaki oyunlar . 4. Herkes yapar
aynı yayını yapan oyun yöneticisi olan bir kanal
her kanala sözleşme yapın. 32 numaralı oyun durumunda olduğumuzu varsayalım.
2 Sözleşmelerin oracle'ların cevaplarını okuyabileceğine dikkat edilmelidir.
ve bazı çevre parametreleri, tamamen saf işlevler değildirler.
Ancak, oracle cevapları bir kez verildiğinde asla değişmez ve
oracle'ın hesaplama zenginliğinden kaynaklandığı tartışılabilir.
bir kirlilik olmaktan ziyade makine. Çevre parametreleri kabul edilir
"gerekli bir kötülük" ve ideal olarak uygun şekilde bölümlere ayrılacaktır.
yüksek seviyeli diller.
1
makro Taahhüdü a9d7e8023f80ac8928334;
2
3
Taahhüt hashlock çağrısı
4
State33 yoksa State32 biterse
5
telefon etmek
Şekil 4. Çok oyunculu oynamak için hashlock kullanmanın basitleştirilmiş bir örneği
kanallarda oyun.
State32 işlevi tarafından tanımlanmıştır ve güvenmeden
tüm kanalları aynı anda 33 durumuna güncelleyin.
oyun yöneticisi sırrı ortaya çıkarır, tüm kanallara neden olur
aynı anda güncellemek için.
b) Ölçülü yürütme: Sözleşmenin yürütülmesi ölçülür
Ethereum'un "gas" sına benzer bir şekilde, ancak Æternity iki
ölçümü için farklı kaynaklar, biri zaman için ve diğeri için
Uzay. Her ikisi de aeon kullanımı için parti tarafından ödenir.
yürütmeyi talep eden.

Bu istenmeyen olarak görülebilir, çünkü muhtemelen
blok zinciri ihtiyacına neden olan başka bir taraf
ilk etapta anlaşmazlığı çözmek. Ancak, olduğu sürece
Kanaldaki tüm para bahis için kullanılmaz, bu olabilir
sahip olduğu için sözleşme kodunda etkili bir şekilde geçersiz kılınmalıdır.
fonları bir taraftan diğerine yeniden dağıtma yeteneği. O
aslında tüm fonları kullanmaktan kaçınmak için genellikle iyi bir uygulamadır
işlem yapmak için bir kanalda, çünkü kaybetmeyi caydırır
kanalı kapatırken işbirliği yapacak taraf.
B.2) Örnek: Tüm bu fikirleri aşağıya indirelim
Dünya. Pratikte, Alice ve Bob kullanarak işlem yapmak isterse
Æternity ile ilgili bir devlet kanalı, aşağıdakilerden geçiyorlar
prosedür:
1) Alice ve Bob, nasıl olduğunu belirten bir işlemi imzalar
her biri çok para yatırıyor
kanal ve blok zincirinde yayınlayın.
2) Blok zinciri kanalı açtıktan sonra,
her ikisi de yeni kanal durumları oluşturur, bunları
birbirlerini ve imzalayın. Kanal durumları şunlar olabilir:
kanaldaki fonların yeni bir dağılımı veya
yeni bir dağıtımı belirleyen sözleşme. Her biri
bu kanal durumlarının artan bir nonce vardır ve
her iki tarafça imzalanmış, dolayısıyla bir anlaşmazlık ortaya çıkarsa, en son
geçerli durum, blok zincirine gönderilebilir;
onu zorlar.
3) Kanal iki farklı şekilde kapatılabilir:
a) Alice ve Bob bitirdiklerine karar verirlerse
nihai bakiyeleri üzerinde işlem yapmak ve mutabakata varmak,
her ikisi de bunu gösteren bir işlemi imzalarlar ve
onu kapatacak olan blok zincirine gönderin.
kanal ve kanaldaki parayı yeniden dağıtın
buna göre.
b) Alice için kapanış işlemi imzalamayı reddederse
herhangi bir nedenle, Bob son durumu gönderebilir.
onlardan imzalı ve kanala sahip olma talebinde bulunan
bu durumu kullanarak kapatıldı. Bu bir geri sayım başlatır.
Alice, Bob'un dürüst olmadığına inanıyorsa,
ile bir eyalet yayınlama fırsatı var

---

her ikisinin de imzaladığı daha yüksek bir not
geri sayım bitmeden önce. Eğer öyleyse,
kanal hemen kapanır. Aksi takdirde kapanır
geri sayım bittiğinde.
C. Fikir birliği mekanizması
Æternity, hibrit bir Çalışma Kanıtı ve Teminat Kanıtı kullanır
fikir birliği mekanizması. Blok sırası belirlenecek
Proof-of-Work aracılığıyla. Belirli sistem değişkenleri belirleyici olacaktır.
zincir üzerinde tahmin piyasası sistemi aracılığıyla madencilik
Kullanıcıların katılmaları ve bilgilerini getirmeleri. İçin
PoW algoritması şu anda Tromp'un bir varyantını tercih ediyoruz
Cuckoo Cycle, hafızaya bağlı ve aynı zamanda
daha az gerektirdiğinden, "dolaylı olarak yararlı bir Çalışma Kanıtı"
çalıştırılacak elektrik, ancak bunun yerine başka bir sınırlayıcı faktöre sahiptir,

bellek gecikmesi kullanılabilirliğinden biri. Bu aynı zamanda
akıllı telefonla madencilik yapmak mümkün.
Tromp çalışmaları hakkında şöyle yazıyor:
"[Cuckoo Cycle] anında doğrulanabilir bir hafıza
tarafından yönetilmekte benzersiz olan bağlı PoW
hesaplamadan ziyade gecikme. Bu anlamda min-
Cuckoo Cycle, bir ASIC madenciliği biçimidir.
DRAM yongaları, rastgele
milyarlarca bit okumak ve yazmak.
Gece şarj olan telefonlar bile benim olabilir
verimlilikte büyüklük kaybı emirleri olmadan,
karlılık zihniyetiyle değil oyun oynayarak
piyango, madencilik donanımı ortamı
genişlemenin yanı sıra benimsemeden de yararlanan
ademi merkeziyetçilik. "
Önizleme: Konsensüs mekanizmasının bir şekilde
stajdaki standart rol. Yeni üzerinde anlaşmaya ek olarak
blok zinciri için bloklar, aynı zamanda her iki yanıtı da kabul eder.
oracle soruları ve sistem parametrelerinin değerleri.
Özellikle fikir birliği mekanizması kendi kendini değiştirebilir.
Ancak, bunun tamamen sorunlu olmadığına dikkat edilmelidir.
lematik. Örneğin, basit bir çalışma kanıtı mekanizması
madencilere rüşvet vermek oldukça ucuz olurdu.
kehaneti bozmak. Bu nedenle Æternity bir roman kullanacak
hibrit Proof-of-Stake Proof-of-Work algoritmasından yararlanma
her ikisinin de faydaları. Bundan bağımsız olarak PoW,
yeni aeon belirteçleri çıkarmak için kullanılacak.
Sidenote: Başlangıçta Aeternity'nin yüzde 100 olması amaçlanıyordu
bahis kanıtı blok zinciri. Artık öyle düşünmüyoruz
Merkezi olmayan yüzde 100 PoS sistemi mümkündür.
C.1) Oracles: Çoğu sözleşme için çok önemli bir özellik,
ister metin ister kod olarak kodlanmış olsun,
farklı fiyatlar gibi çevreden gelen değerler
mal veya belirli bir olayın meydana gelip gelmediği. Zeki
bu kabiliyete sahip olmayan sözleşme sistemi, esasen kapalı
sistem ve tartışmasız pek kullanışlı değil. Bu genellikle bir ac-
bir gerçek ve halihazırda bunu deneyen birkaç proje var.
dış verileri merkezi olmayan şekilde blok zincirine getirmek için
yol [8] . Ancak, sağlanan bir gerçeğin doğru olup olmadığına karar vermek
ya da değil, bunlar esasen yeni bir
fikir birliği mekanizmasının üstüne fikir birliği mekanizması.
Üst üste iki fikir birliği mekanizmasını çalıştırmak
her ikisini de ayrı ayrı çalıştırmak kadar pahalıdır. Ek olarak,
güvenliği artırmaz, çünkü en az güvenli olan
yine de saldırıya uğrar ve “yanlış” değerler üretmeye zorlanır. Böylece,
iki fikir birliği mekanizmasını birleştirmeyi öneriyoruz
bir, esasen anlaşmak için kullandığımız mekanizmayı yeniden kullanmak
sistemin durumu hakkında, aynı zamanda
dış dünya.
Bunun çalışma şekli aşağıdaki gibidir. Herhangi bir aeon tutucu
evet / hayır cevabını taahhüt ederek bir kehanet başlatabilir
soru. Bunu yaparken, aynı zamanda
Sorunun cevaplanabileceği zaman dilimi, hangisi
şimdi veya gelecekte bir süre başlayabilir. Kullanıcı
oracle oracle yatırmak için gerekli oracle başlattığında

zaman çerçevesinin uzunluğuna, eğer iade edilirse
kullanıcı gerçek olarak kabul edilen bir cevap verir, aksi takdirde
yanmıştır. Blok zinciri, aşağıdakiler için benzersiz bir tanımlayıcı oluşturur:
cevabı bir kez almak için kullanılabilecek kehanet
mevcut.
Sorunun cevaplanma zamanı geldiğinde,
Oracle'ı başlatan kullanıcı ücretsiz bir cevap verebilir.
Oracle başlatıcısı bir cevap verdiğinde veya
belirli bir süre geçti, diğer tüm kullanıcılar gönderebilir
aynı miktarda aeon yatırarak karşı talepler. Eğer
Sonuna kadar karşı iddiada bulunulmadı.
zaman çerçevesi, başlatan kullanıcı tarafından sağlanan cevap
oracle gerçek olarak kabul edilir ve depozito iade edilir. Varsa
karşı iddialar gönderilir, ardından fikir birliği mekanizması
kehanet cevaplamak için bloklar kullanılacaktır. Bu daha fazlası
pahalı, ancak en az birini alabileceğimizi bildiğimiz için
iki güvenlik mevduatı, onu kullanabiliriz.

D. Yönetişim

Blockchain tabanlı sistemlerin yönetişimi,
geçmişte sorun. Bir sistem yükseltmesi gerektiğinde
tamamlandığında, bu genellikle büyük çatallanmaya yol açan bir sert çatal gerektirir.
tüm değer sahipleri arasında tartışmalar. Gibi basit şeyler bile
kaynak kodda rastgele ayarlanmış bir değişkeni düzeltmek,
Bitcoin'deki blok boyutu tartışmasını gördük, görünüşe göre
kullanıcıların teşviklerinin olduğu bir sistemde çok zor olmak
karar vericilerle uyumlu değil ve nerede olduğu
net bir yükseltme yolu yok. Daha karmaşık olanları da gördük
Tek bir akıllı sözleşme hatasını düzeltmek gibi yönetişim kararları
sistem tarafından hızlı müdahale gerektiren "The DAO" da
geliştiriciler.
Bu sistemlerin temel sorunu kolaylıkla
tanımlanabilir - bir protokol yükseltme için karar verme süreci -
not veya değişim iyi tanımlanmamıştır ve şeffaflıktan yoksundur.
Ternity'nin yönetişim sistemi fikir birliğinin bir parçasıdır. Kullanır
tahmin piyasalarının verimli ve şeffaf bir şekilde işlemesi
olabildiğince.
Dahası, fikir birliği mekanizması bir numara ile tanımlanır.
sistemin nasıl çalıştığını belirleyen değişkenler
ve bunlar her yeni blok tarafından biraz güncelleniyor. Nereden
işlem yapmanın veya bir kahine sormanın maliyeti ne kadar
blok gibi temel parametre değerlerinin modifikasyonları
zaman.

Sayfa 6

Değişkenler hakkında tahmin pazarlarına sahip olarak
protokolü tanımlayın, kullanıcılar nasıl verimli bir şekilde öğrenebilirler
protokolü iyileştirin. Tahminlere sahip olarak pazarlar
potansiyel zor çatallar, topluluğun gelmesine yardımcı olabiliriz
kodun hangi sürümünün kullanılacağı konusunda fikir birliği. Her kullanıcı
hangi metriği optimize etmek istediğini kendisi seçer, ancak
basit varsayılan strateji, değerini en üst düzeye çıkarmak olacaktır.
holdingleri.

E. Ölçeklenebilirlik

E.1) Ağaçları parçalamak: Önceden yapılmış mimari

Şimdiye kadar gönderilen son derece ölçeklenebilir. Çalıştırmak mümkündür
her kullanıcı yalnızca
önem verdikleri ve görmezden geldikleri blockchain devletinin bir parçası
herkesin verileri. Eyaletin en az bir kopyası gerekli
yeni kullanıcıların önemsedikleri kanıt konusunda emin olmaları için
hakkında, ancak bu verileri rastgele birçok
düğümler, böylece her düğümün yükü keyfi olarak küçüktür. Merkle
ağaçlar bir devletin devletin bir parçası olduğunu kanıtlamak için kullanılır
[11]. Belirli düğümlerin bulunduğu bir senaryo hayal etmek kolaydır.
ağaçları takip etme konusunda uzmanlaşmak ve bunun için ödeme almak
ekler ve aramalar.
E.2) Light istemciler: Light istemciler tüm
bloklar. Önce kullanıcı müşterisine geçmişte bir hash verir.
Zayıf olarak da bilinen bir teknik olan tercih ettikleri çatal
öznellik [12]. O zaman müşteri yalnızca indirmeyi bilir
bu hash ile bir blok içeren çatallar. Sadece müşteri
blokların başlıklarını indirir. Başlıklar çok
tam bloklardan daha küçük; çok az işlem işlenir.
Basit olması için, blok başlıklarından hiç bahsetmedik.
Bölüm II-A.4'te blok yapısından bahsederken, ancak
şunları içerir:
• Önceki bloğun karması.
• Tüm devlet ağaçlarının kök karması.
E.3) Durum kanalları ve paralellik: Devlet kanalları
muazzam verim ve içlerinde çoğu işlem var
asla yürütülmez ve hatta blok zincirine kaydedilmez.
Ek olarak, kanallar herhangi bir paylaşılan duruma yazmaz
zincir üzerinde, yani gerçekte kaydedilen tüm işlemler
blok zincirinde paralel olarak işlenebilir. Verilen
bugün satılan çoğu tüketici donanımı, en az dört profesyonel
çekirdeklerden vazgeçildiğinde, bu işlemin
verim kabaca 4 faktörü ile çarpılır.
Dahası, hiçbir zaman karmaşık olmayacak
eşzamanlı etkileşim, bu blok zincirinin parçalanmasının
mimari nispeten kolay olmalıdır. Blockchain'den beri
parçalama hala oldukça deneyseldir, kasıtlı olarak
başlangıçta herhangi bir parçalama tekniğini takip etmemeyi seçti
ternity tasarımı. Ancak gelecekte bu değişirse,
Uzaklık, parçalanması en kolay blok zincirlerinden biri olmalıdır.
E.4) Belirli bir bellekte saniyedeki işlemler yeniden
soru: Protokolü tanımlayan değişkenlerin tümü
fikir birliği ile sürekli güncellenmektedir. Baş harflerinden
varsayılan değerler, başlangıç varsayılan oranını hesaplayabiliriz
saniye başına işlem.
1
Bunun bir taslak olduğunu ve büyük olasılıkla
2
değişiklik.
3
4
Aşağıdaki değişkenleri tanımlıyoruz:
aşağıdaki hesaplamalar:
5
6
B = bayt cinsinden blok \ _boyutu

7
F = bitiş \ _sonuna kadar \ _ bloklar
8
R = saniye cinsinden \ _sona kadar \ _sona kadar
9
T = bayt cinsinden işlem boyutu
10
11
saniye başına işlem = B * F / (T * R)
12
13
B = 1000000 bayt = blok başına 1 megabayt
14
F = 24 * 60 * 2 blok / gün
15
R / F = blok başına 30 saniye
16
R = 24 * 3600 saniye / gün
17
T = işlem başına 1000 bayt
18
19
1000000 * 24 * 60 * 2/1000/24 * 3600
20
= 1000000/1000/30
21
= ca. Saniyede 32 işlem (hızlı
8 içindeki her insanı kaydetmeye yetecek kadar
yıl)
Bir düğümü çalıştırmak için, tüm
kesinlikten bu yana bloklar var ve 100 tane kayıt yapabilmeliyiz
Bir saldırı olması durumunda kat daha fazla bilgi. Tahmin
bu son 2 gündür, sonra 5760 blok vardır.
kesinlik. Yani bellek gereksinimi 5760 * bir megabayttır
* 100 = 576000 megabayt = 576 gigabayt. Ne zaman orada
bir saldırı olmuyor, sadece 5,76'ya ihtiyaç var
blokları depolamak için gigabayt.
III. A ŞEKİLLER
Æternity akıllı sözleşmelerinin vatansız doğası,
Æternity's üzerinde aşağıdaki uygulamaları oluşturmak kolaydır
blok zinciri. Özellikle yüksek hacimli kullanım için uygundur.
durumlarda.
A. Blockchain temelleri
Blockchain temelleri, aeon gibi gerekli ilkellerdir,
cüzdanlar, isimler ve ilgili kavramlar. Modülerleştiriyorlar
başvuru kaynağı olarak kullanılabilen yeniden kullanılabilir bileşenler
dations ve geliştirilebilir.
A.1) Kimlikler: Her hesabın ilişkili bir
benzersiz kimlik numarası. Kullanıcılar benzersiz isimler kaydedebilir ve
isimleri bir veri yapısının Merkle-köküne bağlar. The
veri yapısı, birinin benzersiz kimliğini ve diğerlerini içerebilir
kişinin hesabı hakkında bilgi. Schema.org'u kullanmayı hedefliyoruz
Kişiler veya şirketler gibi şeyleri temsil etmek için JSON biçimi
[13] .
A.2) Cüzdan: Cüzdan , kullanılan bir yazılım parçasıdır

Aeternity ile etkileşim için. Bir cüzdan özel anahtarları yönetir
aeon ve işlemleri oluşturur ve imzalar. Biri kullanabilir
M-cüzdan, kanal işlemlerini göndermek ve uygulamaları kullanmak için
kanal ağı.
A.3) Varoluş kanıtı: Bir işlem türü,
herhangi bir verinin karmasının yayınlanması. Sistem katılımcıları
verinin mevcut olduğunu kanıtlamak için başlıkları kullanabilir
zaman noktası.

---

7. Sayfa

B. Devlet kanalı uygulamaları
Eyalet kanallarındaki akıllı sözleşmeler mikro için mükemmeldir.
web üzerinden yüksek işlem gerektiren hizmetler
koymak.
B.1) Toll API: Bugün mevcut olan çoğu API herkese açıktır
herkes tarafından aranabilir veya başka bir kişi tarafından güvence altına alınmıştır.
kullanıcı adı-şifre-düzeni veya benzersiz erişim belirteçleri. Ödemek-
ment kanalları, yeni bir API türüne izin verir.
API'ye yapılan her çağrı, muhtemelen her HTTP isteği için ödeme yapar.
Bir API'ye erişmek için ödeme yapmak DDoS sorunlarını çözer ve
her zaman kullanılabilen yüksek kaliteli API'ler oluşturmak daha kolaydır.
Ödeme gerektiren API yanıtları,
henüz imkansız olan işletmelerin yaratılması ve
ademi merkeziyetçiliğin ortaya çıkmasında önemli bir rol oynar.
ekonomi. Bilgi sahiplerinin
aksi takdirde özel verileri kamuya açık hale getirin.
B.2) Sigortalı kitle fonlaması: Sigortalı uygulayabiliriz
baskın güvence sözleşmelerini kullanarak kitle fonlaması [ihtiyaç duyulan kaynak] .
Bunlar, para toplamak için kullanılan akıllı sözleşmelerdir.
yeni bir köprü, okul veya pazar gibi kamu malı.
Hakim güvence sözleşmeleri, geleneksel güvence sözleşmelerinden farklıdır.
Kickstarter gibi surance sözleşmeleri,
katılmak için baskın strateji. Mal finanse edilmezse,
tüm katılımcılar aeon artı faizlerini geri alırlar, bu yüzden onlar
teminat almadan likiditesini düşürmeye karşı sigortalı
iyi. Bir oracle kullanarak, sağlayıcının
mal veya hizmet yalnızca mal veya hizmetin
aslında sağlanmıştır.
B.3) Çapraz zincir atomik takas: Çapraz zincir atomik
swaplar, bitcoin [14] için güven gerektirmeyen aeon değişimine izin verir ,
[15]. Bunlar bir hashlock kullanılarak uygulanabilir.
her iki blok zincirindeki işlemler aynı değerde.
B.4) Kararlı değer varlıkları ve portföy replikasyonu: Biz
kalan sentetik varlıkları programlamak için akıllı sözleşmeleri kullanabilir
bir gerçek dünya varlığıyla neredeyse aynı fiyat. Örneğin,
altınla aynı fiyatta kalan bir varlık yapabiliriz.
Sentetik türevler eşit ve zıt çiftler halinde oluşturulur.
Bir kullanıcının altınla hareket eden bir varlığa sahip olması için farklı bir
Kullanıcının altına ters yönde hareket eden bir varlığa sahip olması gerekecektir.
Örneğin, Alice, Bob ile bir sözleşme yapabilir, böylece
Alice'in 1 gram altını var. Sözleşmedeki paranın dışında,
bir gram altın değerinde aeon Alice'e gidecek ve
Artık para Bob'a gider. Sözleşmenin sona ermesi var
altın fiyatının ölçülecek olduğu tarih ve fonlar

buna göre Alice ve Bob'a dağıtılır.
B.5) Etkinlik sözleşmeleri: Etkinlik sözleşmeleri, bir olay
olur ve bir olay olmadığında ödeme yapmaz, çünkü
kehanet başına göre. İçlerinde ilginç olmalarının dışında-
kendileri, bunlar birkaç farklı uygulama tarafından kullanılabilir:
a) Sigortalar: Uygulama için etkinlik sözleşmelerini kullanabiliriz.
ment sigortaları. Örneğin, pahalı müzik etkinliği biletleri
hava kötü giderse değersiz hale gelebilir. Ancak, eğer
oracle buna karar verirse konsere giden kişi para alır
olay günü yağmur yağdı, yatırım olabilir
duygusal olarak bir bulmayı göze alabilsin diye korunmuş
yeterli alternatif. Biraz daha ciddiyim, çiftçiler
genellikle yağmurun toplam sayısıyla ilgilenir
mevsim. Onları ekinlerinin solmasına karşı sigortalayabiliriz
kuruluk.
b) Bilgi uçurma: Etkinlik sözleşmeleri de kullanılabilir
hassas bilgileri açıklamayı teşvik etmek. Örneğin,
olaya bahse girebiliriz "Bunu gösteren bilgi
A Şirketi yasadışı böcek ilacı kullandı.
24 Ocak 2017'den önce ". Buna erişimi olan herhangi bir kişi
bilgi, etkinliğin ilk bahse girmesi için teşvik edilecektir.
olacak ve sonra onu serbest bırakacak.
B.6) Tahmin piyasaları: Bir tahmin piyasası,
kullanıcıların gelecekteki bir olayın gerçekleşip gerçekleşmeyeceğine bahse girmesine izin
vermek. Nereden
Gelecekteki olasılığı tahmin edebileceğimiz bahislerin fiyatı [3] ,
[8], [16]. Bunları ölçmenin en doğru yoludur.
belirli bir fiyata gelecek [cit. gerekir] . Olay gerçekleştiğinde,
Pazar kehanet kullanılarak çözülür.
Bölüm II-D'de belirtildiği gibi , örneğin tahmini
yazılım için hangi güncellemelerin yapılacağını tahmin etmek için piyasalar
yararlı ve zararlı olacak. Onları da kullanabiliriz
bir seçimde gerçekte ne kadar adayın olacağını tahmin etmek
başarabilmek için yalanlar ve temelsiz sözler olabilir
daha kolay tespit edildi.
Şekil 5. Çok boyutlu tahmin pazarı.
a) Çok boyutlu tahmin pazarları: Çok boyutlu
tional tahmin piyasaları, korelasyonu tahmin etmemize izin verir
gelecekteki olası olaylar arasında. Örneğin, biri
Alice lider seçilirse patateslerin fiyatının
düşecek ve Bob kazanırsa fiyat yükselecek.
Google'ın sonraki 3 için A planını kullanması halinde öğrenilebilir.
aylar, muhtemelen daha fazla para kazanacağını ve eğer öyleyse
B planını kullanırsa, muhtemelen daha az kazanacaktır. Veya şek. 5 , biz
Alice başkan seçilirse, bir
patates fiyatının yüksek olma olasılığı oldukça düşüktür.
B.7) Tek fiyattan toplu alım satım yapılan piyasa: Orada
soymak isteyen saldırganlar için mevcut iki yaklaşımdır
aeon bir pazardan. Piyasadan faydalanabilirler
zaman içinde bölünmek veya bundan faydalanabilirler
uzayda bölünmüş.
• Pazar uzaya bölünmüşse, saldırgan
arbitraj. Aynı anda her iki piyasada da ticaret yapıyor
aynı anda kets böylece riski ortadan kalkar ve bir

kar.
• Pazar zamana göre bölünmüşse, saldırgan cephede-
piyasayı yönetiyor. Gelen işlemleri okur
piyasa ve hemen alış ve satış emirleri oluşturur
önce ve sonra.
Şekil 6. Siyah çizgi talep eğrisidir, kırmızı çizgi ise arzdır
eğri. Kırmızı renkteki satışlar, kırmızı renkteki satışlarla aynı büyüklüktedir. Dikey
satır, piyasa yapıcının seçtiği fiyattır. Satın almak isteyen herkes
Bu fiyattan daha yüksek fiyat ticareti yapıldı, herkes daha düşük bir fiyata satmaya istekli
bu fiyattan işlem görüyor.
Pazarları uzayda birleştirmek için herkes kullanmalıdır
aynı piyasa yapıcı. Pazarları zamanında birleştirmek için şuna ihtiyacımız var:
işlemlerin toplu olarak, tek fiyat üzerinden yapılması. Market
yapıcı, karar verdiği fiyatı her kişiye taahhüt etmelidir,
ve eğer herhangi biri, aşağıdakilerden çelişkili taahhütler bulabilirse
piyasa yapıcıysa, tüm müşterilerinin aşağıdakileri yapabilmesi gerekir:
tüm kanallarını boşaltın. Piyasa yapıcı bir taahhütte bulunursa
uygun fiyat, o zaman aynı hacimdeki alıcılarla eşleşecek ve
satıcılar birlikte, incir . 6 gösteri. Aksi takdirde, o sona erecek
şek. 7 , bu nedenle büyük bir risk alıyor.
Şekil 7. Siyah, kırmızıdan çok daha büyük. Piyasa yapıcı satıyor
satın aldığından çok daha fazla hisse, dolayısıyla çok fazla risk alıyor.
IV. I EKLEME
Anahtar kavramların çoğu zaten kavram kanıtı uygulamasına sahiptir.
Erlang'daki sözler. Bu, blok zincirinin kendisini içerir,
sözleşme dili ve sanal makine, oracle ve yönetişim
mekanizmalar ve konsensüsün eski bir versiyonu
mekanizma. Erlang / OTP kullandık çünkü bunu yapıyor
içindeki birçok isteğe yanıt verebilecek kod yazması kolay
paraleldir ve çökmez. En yüksek seviyeye sahip sunucular
Dünyadaki zaman Erlang'a dayanmaktadır. İçin kullanıldı
30 yıldır endüstriyel uygulamalar,
güvenilir ve istikrarlı ürün.
A.Sanal makine ve sözleşme dili
Sanal makine yığın tabanlıdır ve Forth'a benzer
ve Bitcoin'in kodlama dili, ancak
ikincisi, oldukça zengindir. VM bunun yerine işlevleri destekler
gotos, anlambilimini analiz etmeyi nispeten basit hale getiriyor.
VM'nin işlem kodlarının bir listesi Github'ımızda bulunabilir3.
Ek olarak, daha yüksek düzeyde bir Forth benzeri dil vardır.
Chalang adlı guage için bayt kodu derleyen
VM. Makroları ve değişken adlarını destekler, ancak
yığın tabanlı yürütme modeli [17]. Chalang kodu örnekleri
Github'ımızda da bulunabilir4.
B. Web entegrasyonu yoluyla benimseme
Web, en popüler uygulama platformudur. Biz
JS gibi kullanımı kolay web geliştirme araçları sağlayacaktır.
Æternity'nin temel özellikleri için kitaplıklar ve JSON-API'ler
blok zinciri.
C. Açık kaynak modülleri
Özel blockchain con için kolayca yeniden kullanılabilmesi için
sortium ve diğer kullanım durumları, yazılım
Konsensüs modülü gibi MIT lisanslı modüller,

özel ihtiyaçlara uyarlanabilir.
D. Kullanılabilirlik ve UX tasarımı
Sürtünmesiz insan etkileşimi, büyük bir odak noktası olacak
geliştirme çabaları. Daha spesifik olarak, emin olacağız
kimliği, anahtarları ve işlemleri kimin kontrol ettiği açıkça
kuruldu. Ayrıca, web ağ geçitleri aracılığıyla kolay erişim sunmak,
gelecekteki gelişimin merkezi bir odak noktası olmak. Katılan kullanıcılar
Tahmin piyasalarında Tinder benzeri bir yöntemle (sola / sağa kaydırın)
mobil arayüz ve kolayca kullanılabilen basit web cüzdanları
bir iframe aracılığıyla bir web sitesine entegre edilmiş yeni olacak
norm.
V. D ISCUSSION
Nasıl mimarlık yapılacağına dair bir açıklama yaptık
temelde daha verimli bir değer transfer sistemi. The
tarif edilen sistem aslında bunu yapabilen küresel bir oracle makinesidir.
küresel ölçekte karar verme hizmetleri sağlamak için kullanılabilir.
Özellikle, III . Bölümde önerilen tüm uygulamalar ,
kolayca ve verimli bir şekilde doğanın üzerine inşa edilebilir.
3https://github.com/aeternity/chalang/blob/
master / opcodes.md
4https://github.com/aeternity/chalang/tree/
ana / örnekler

Sayfa 9

Bununla birlikte, yaklaşımımızın her iki temel sınırlaması vardır
ve iyileştirme yolları. Bunlar burada tartışılmaktadır.
A. Sınırlamalar ve ödünleşmeler
Bizler değiş tokuşların yapıldığına inansak da,
ortaya çıkan performans göz önüne alındığında mimari makul
diğer alanlarda artış, *Æ*ternity her şeyi kapsayan bir çözüm değildir
merkezi olmayan uygulamalar için. Daha çok şu şekilde görülmelidir
mevcut teknolojiler için sinerjik bir tamamlayıcı. Var
dikkat edilmesi gereken birkaç uyarı.
A.1) Zincir üzerinde durum: Birçok avantaja sahip olmasına rağmen,
Ternity'nin programlanabilir durumunun olmaması, onu,
özel bir durumun denetim altında olmasını gerektiren uygulamalar
sensus. Örneğin, bu, genellikle oldukları gibi DAO'ları içerir.
tasarlanmış, özel ad sistemleri ve alt para birimleri
dayanak varlığın değerine bağlı değildir.
A.2) Ücretsiz seçenek sorunu: Alice ve Bob'un bir
kanal ve Alice bir sözleşme imzalarsa, esasen Bob'a
ona gönderdiğinde ücretsiz bir seçenek: Bob,
sözleşmeyi istediğiniz zaman imzalayın ve iade edin (yani etkinleştirin)
gelecek. Genellikle amaçlanan bu değildir. Bundan kaçınmak için
sorun, kanal sözleşmeleri ile hemen etkinleştirilmez
tam tutar. Zamana veya mekana bölünmüşlerdir. Her ikisi de
katılımcılar sözleşmeye küçük aralıklarla kaydolurdu
böylece hiçbir kullanıcı hiçbir zaman geniş bir ücretsiz seçenek sunmaz.
diğer.
Örneğin, taraflar 100 aeon bahis yapmak isterse, o zaman
1000 adımda kaydolabilirler ve her biri
0,1 aeon ile bahis. Bu yaklaşık 1000 mesaj gerektirir
geçmek, her yönde 500, çünkü bu yeterince ucuz
sözleşme asla blok zincirine gönderilmez. Bir başkası gibi

Örneğin, bir finansal varlık yapmak istendiğinde
100 gün sürerse, biri 2400 adımda kaydolabilir
her saat. Bu, yaklaşık 2400 mesajın geçmesini gerektirir.
Her yönde 1200.
A.3) Likidite kaybı ve durum kanalı topolojileri: Ne zaman
hashlock'ları kullanarak kanal oluşturma,
Bölüm II-B.1 , herhangi bir aracı en az iki kez kilitlemek zorundadır
onlar aracılığıyla iletilecek kadar aeon. İçin
örneğin, Alice ve Carol, Bob aracılığıyla işlem yapmak isterse,
Bob, Alice ile etkileşimde Carol gibi davranacak ve yardımcısı-
tersi.
Bu Bob için pahalı olduğu için, büyük olasılıkla
tazminat olarak bir ücret kazanın. Alice ve Carol bunu beklerse
birbirleri arasında birçok ticaret yapmak, bundan kaçınabilirler
yeni bir kanal oluşturarak ve aktif olanı güvenmeden hareket ettirerek
bir hashlock kullanarak yeni kanalla sözleşme yapar.
Yine de, fazladan bir kanalı açık tutmak kişinin
likidite olumsuz, aracılardan geçmesi bekleniyor
birçok durumda, özellikle de
taraflar gelecekte çok fazla ticaret yapmayı beklemiyor. Böylece, bir
belirli zengin kullanıcıların para kazandığı kanal topolojisi
işlemleri diğer kullanıcılar arasında güvenle iletmek,
ortaya çıkması bekleniyor.
Unutulmamalıdır ki, bu tek bir
başarısızlık noktası, çünkü bu işlemlere güvenmediğimiz için
herhangi bir şey olan vericiler. Daha önce bir verici çevrimdışı olursa
bir hashlock'un sırrı ortaya çıktı, işlem
geçmez. Daha sonra çevrimdışı olursa, tek
olası "olumsuz" etki, vericinin
aeon olduğunu iddia etmek.
B. Gelecekteki çalışma
Mevcut durumu iyileştirmenin birkaç olası yolu vardır.
mimari.
B.1) İşlevsel sözleşme dili: Makul bir gelecek
yön, yüksek seviyeli dilleri denemek olacaktır.
işlevsel paradigmaya daha yakından bağlı. Tut-
Örtük bir yığının izini sürmek genellikle hataya meyillidir ve
muhtemelen üst düzey, geliştiriciye dönük bir dil için uygun değildir
guage. Bu, programlar olduğu için oldukça kolay olmalıdır.
zaten saf fonksiyonlar (modulo bazı ortam değişkenleri),
ve hem geliştirme hem de biçimselliği büyük ölçüde basitleştirecektir.
sözleşmelerin doğrulanması. Bu yapılırsa, o da yapabilir
yeni ile sıkı bir şekilde birleştirilecek sanal makineyi revize etme duygusu
derlemeyi hataya daha az eğilimli ve daha az
geliştiricilere olan güvene bağlı. İdeal olarak, çeviri
yüzey dilinden sanal makine koduna kadar basitçe
pragmatik olmasına rağmen hakemli araştırmanın transkripsiyonu
taviz verilmesi gerekecek.
B.2) Çok partili kanallar: Şu anda, tüm kanallar
Staj iki tarafla sınırlıdır. Çok partili seçim
nels, hashlocking yoluyla fiilen elde edilebilir, bu,
pahalı ol. Bu nedenle, olasılığı araştırmayı planlıyoruz
m-of-n ile n partili kanallar için destek eklemenin
yerleşim mekanizması.
G KAYIP

Blockchain Benimle dağıtılmış, kurcalamaya dayanıklı bir veritabanı
erişim. Veritabanı, büyüyen bir listeyle tanımlanır.
karma bağlantılı bloklar ve eklemek için herhangi bir kural olabilir
onları.
Aeon Bir aeon, bir hesap birimini ve bir erişimi temsil eder
doğu blok zincirine doğru. Devredilebilir.
İşlem Bir kullanıcıdan blok zincirine gönderilen bir mesaj.
Bu, kullanıcıların para birimlerini kullanarak
blok zinciri.
Durum Kanalı Kaydedilen iki kullanıcı arasındaki bir ilişki
blok zincirinde. Kullanıcıların tekrar geri göndermesini sağlar
ve ileriye doğru ve aralarında güvensiz akıllı sözleşmeler yaratmak için
blok zinciri tarafından uygulanan ve yerleşen bunları.
Hash Bir hash, her boyutta bir ikiliyi girdi olarak alır. O verir
sabit boyutlu bir çıktı. Aynı girdi her zaman hash değerine sahiptir.
aynı çıktı. Bir çıktı verildiğinde, hesaplanamaz
girdi.
Hashlocking Kanal çiftlerini bu şekilde bağlarız.
2 kişiden fazlasını içeren akıllı sözleşmeler yapın.
Bir sır, hash değeri ile belirtilir. Sır olduğu zaman
aynı anda birden fazla kanalı güncelleyebilir
zaman.
Yönetişim İyi tanımlanmış bir karar verme süreci
blok zincirinin gelecekteki protokol (ler) i.
9

Sayfa 10

Oracle Blockchain hakkındaki gerçekleri anlatan bir mekanizma
yaşadığımız dünya. Oracles'ı kullanarak kullanıcılar,
Blockchain sistemi dışındaki olayların sonucu.
Değer Sahibi Bir aeon veya bir finansal
sistemdeki türev.
Doğrulayıcı Doğrulayıcı,
fikir birliği mekanizması. Ternity durumunda, her
değer sahibi katılabilir.
TEŞEKKÜRLER
Vlad, Matt, Paul, Dirk, Martin, Alistair, Devon sayesinde
ve prova okuması için Ben. Bunlar ve diğerleri sayesinde
insanlar anlayışlı tartışmalar için.
R EFERANSLAR
[1] S. Nakamoto, "Bitcoin: Bir eşler arası elektronik nakit
system, ”2008. [Çevrimiçi]. Mevcut : https: / /
bitcoin.org/bitcoin.pdf.
[2] V. Buterin, "Ethereum: Yeni nesil akıllı kontrol
tract ve merkezi olmayan uygulama platformu, ”2014.
[İnternet üzerinden]. Kullanılabilir : https: / / github. com.tr /
ethereum / wiki / wiki / White-Paper.
[3] P. Sztorc, "Pazar ampirizmi" [Çevrimiçi]. Mevcut:
http://bitcoinhivemind.com/papers/1_
Amaç.pdf.
[4] M. Liston ve M. Köppelmann, "Ora'ya bir ziyaret
cle, ”2016. [Çevrimiçi]. Mevcut : https: // blog.
gnosis.pm.
[5] C. Detrio, "Akıllı sözleşmeler için akıllı pazarlar" 2015.
[İnternet üzerinden]. Mevcut : http://cdetr.io/smart-

pazarlar /.
[6] Namecoin wiki, 2016. [Çevrimiçi]. Mevcut : https:
//wiki.namecoin.org/index.php?title=
Hoşgeldiniz.
[7] P. Snow, B. Deery, J. Lu, ve diğerleri, "Factom: Business
üzerinde değişmez denetim izleri ile güvence altına alınan süreçler
blockchain, ”2014. [Çevrimiçi]. Mevcut: http: / /
bravenewcoin.com/assets/Whitepapers/
Factom-Whitepaper.pdf.
[8] J. Peterson ve J. Krug, "Augur: Merkezi olmayan bir,
tahmin pazarları için açık kaynak platformu, ”2014.
[İnternet üzerinden]. Mevcut : http: / / bravenewcoin.
com.tr / assets / Whitepapers / Augur - A -
Merkezi Olmayan - Açık - Kaynak - Platform -
için-Tahmin-Markets.pdf.
[9] A. Swartz, "Üçgenin karesini almak: Güvenli, merkezi olmayan-
izlenmiş, insan tarafından okunabilir isimler, ”2011. [Çevrimiçi]. Mevcut-
mümkün: http: / / www. aaronsw. com / weblog /
squarezooko.
[10] T. Hvitved, "Resmi Diller Araştırması
Biçimsel Diller ve Analizde Sözleşmeler, "
Sözleşmeye Dayalı Yazılım, 2010, s. 29–32. [Açık-
hat]. Mevcut : http: / / www. diku.
dk / hjemmesider / ansatte / hvitved /
yayınlar / hvitved10flacosb.pdf.
[11] RC Merkle, "Açık anahtarlı şifreleme protokolleri-
tems, ”IEEE Güvenlik ve Gizlilik Sempozyumu'nda,
1980.
[12] V. Buterin, "Teminat kanıtı: Nasıl öğrendim
zayıf öznelliği seviyorum, ”2014. [Çevrimiçi]. Mevcut:
https://blog.ethereum.org/2014/11/
25 / kanıt - kazık - öğrendi - aşk - zayıf -
öznellik /.
[13] "Schema.org şemaları," 2016. [Çevrimiçi]. Mevcut:
http://schema.org/docs/schemas.html.
[14] “Atomik zincirler arası ticaret,” 2016. [Çevrimiçi]. Mevcut-
mümkün: https: / / tr. bitcoin. it / wiki /
Atomic% 5C_cross-chain% 5C_trading.
[15] "Interledger," 2016. [Çevrimiçi]. Mevcut : https: //
interledger.org/.
[16] KJ Arrow, R. Forsythe, M. Gorham ve diğerleri, "The
tahmin piyasalarının vaadi, ”Science, 320 2008.
[İnternet üzerinden]. Mevcut : http://mason.gmu.edu/
˜rhanson / PromisePredMkt.pdf.
[17] Z. Hess, "Chalang," 2016. [Çevrimiçi]. Mevcut:
https://github.com/aeternity/chalang.