Sayfa 1

Uniswap v2 Çekirdeği
Hayden Adams
hayden@uniswap.org
Noah Zinsmeister
noah@uniswap.org
Dan Robinson
dan@paradigm.xyz
Mart 2020
Öz
Bu teknik rapor, Uniswap'in arkasındaki bazı tasarım kararlarını açıklıyor
v2 temel sözleşmeleri. İsteğe bağlı çiftler de dahil olmak üzere sözleşmelerin yeni özelliklerini kapsar
ERC20'ler arasında, diğer sözleşmelerin
Belirli bir aralıktaki zaman ağırlıklı ortalama fiyat, tüccarların
varlıkları almak ve bunları işlemde daha sonra ödemeden önce başka bir yerde kullanmak,
ve gelecekte açılabilecek bir protokol ücreti. Ayrıca sözleşmeleri yeniden tasarlar
saldırı yüzeylerini azaltmak için. Bu teknik inceleme, Uniswap v2'lerin mekaniklerini açıklar.
Likidite sağlayıcılarının fonlarını depolayan çift sözleşmesi dahil "ana" sözleşmeler - ve
çift sözleşmeleri somutlaştırmak için kullanılan fabrika sözleşmesi.
1. Giriş
Uniswap v1, Ethereum blok zincirinde akıllı sözleşmelerin zincir üzerinde bir sistemidir.
"sabit ürün formülüne" dayalı otomatik bir likidite protokolünden bahsetmek [1]. Her biri
Uniswap v1 çifti, iki varlığın havuzlanmış rezervlerini depolar ve bu ikisi için likidite sağlar
varlıklar, rezervlerin ürününün azaltamayacağı değişmezi muhafaza etmek. Tüccarlar
likidite sağlayıcılarına giden işlemlerde 30 baz puanlık bir ücret ödersiniz. Sözleşmeler
yükseltilemez.
Uniswap v2, aynı formüle dayalı yeni bir uygulamadır ve birkaç yeni
arzu edilen özellikler. En önemlisi, keyfi ERC20 / ERC20'nin oluşturulmasını sağlar
yalnızca ERC20 ve ETH arasındaki çiftleri desteklemek yerine çiftler. Aynı zamanda sert bir
Başlangıçta iki varlığın göreceli fiyatını biriktiren ened fiyat oracle'ı
her blok. Bu, Ethereum'daki diğer sözleşmelerin zaman ağırlıklı ortalamayı tahmin etmesini sağlar.
keyfi aralıklarla iki varlık için fiyat. Son olarak, kullanıcıların
varlıkları serbestçe alabilir ve zincirin başka bir yerinde kullanabilir, yalnızca ücretini ödeyerek (veya
iade ederek)
bu varlıklar işlemin sonunda.
Sözleşme genel olarak yükseltilebilir olmasa da, şu özelliklere sahip özel bir anahtar vardır:
Fabrika sözleşmesindeki bir değişkeni zincir üzerinde 5 temel puanlık bir ücreti etkinleştirmek için
güncelleme yeteneği
esnaf üzerinde. Bu ücret başlangıçta kapatılacak, ancak gelecekte daha sonra açılabilir.
Hangi likidite sağlayıcıları her işlemde 30 baz yerine 25 baz puan kazanacak
puan.
Bölüm 3'te tartışıldığı gibi Uniswap v2, Uniswap v1 ile ilgili bazı küçük sorunları da düzeltir.
uygulamayı yeniden tasarlamak, Uniswap'in saldırı yüzeyini azaltmak ve
"çekirdek" sözleşmedeki mantığı en aza indirerek sistem daha kolay yükseltilebilir.
likidite sağlayıcılarının fonlarını tutar.

Sayfa 2

Bu makale, bu temel sözleşmenin işleyişini ve fabrika sözleşmesini açıklamaktadır.
bu sözleşmeleri somutlaştırmak için kullanılır. Aslında Uniswap v2'yi kullanmak,
takas veya depozito tutarını hesaplayan bir "yönlendirici" sözleşmesi aracılığıyla çift sözleşmesi ve
çift sözleşmesine fon aktarır.
2 Yeni özellik
2.1 ERC-20 çifti

Uniswap v1, ETH'yi köprü para birimi olarak kullandı. Her çift, ETH'yi bir
varlıklar. Bu, yönlendirmeyi daha basit hale getirir - ABC ile XYZ arasındaki her ticaret,
ETH / ABC çifti ve ETH / XYZ çifti - ve likiditenin parçalanmasını azaltır.
Ancak bu kural, likidite sağlayıcılarına önemli maliyetler getirir. Tüm likidite sağlayıcıları
ETH'ye maruz kalırlar ve diğerlerinin fiyatlarındaki değişikliklere bağlı olarak kalıcı zarara uğrarlar.
ETH'ye göre varlıklar. İki varlık ABC ve XYZ ilişkilendirildiğinde - örneğin,
her ikisi de USD stablecoin'tir — bir Uniswap çifti ABC / XYZ'deki likidite sağlayıcıları
genellikle ABC / ETH veya XYZ / ETH çiftlerinden daha az kalıcı kayba maruz kalır.
ETH'yi zorunlu bir köprü para birimi olarak kullanmak, tüccarlar için de maliyetler getirir. Tüccarlar
var
doğrudan bir ABC / XYZ çiftine kıyasla iki kat daha fazla ücret ödemek zorunda kalırsa
iki kez kayma.
Uniswap v2, likidite sağlayıcılarının herhangi iki ERC-20 için çift sözleşmeler oluşturmasına izin
verir.
Keyfi ERC-20'ler arasındaki çiftlerin çoğalması bunu biraz daha zor hale getirebilir.
belirli bir çiftle ticaret yapmak için en iyi yolu bulmak için, ancak yönlendirme daha yüksek bir
katmanda yapılabilir
(zincir dışı veya zincir üstü yönlendirici veya toplayıcı aracılığıyla).
2.2 Fiyat oracle
Uniswap tarafından t zamanında teklif edilen marjinal fiyat (ücretler dahil değildir) hesaplanabilir
a varlığının yedeklerinin, b varlığının yedeklerine bölünmesiyle.
p t =
r a
t
r b
t
(1)
Arbitrajcılar, bu fiyat yanlışsa (yeterli bir tutarda) Uniswap ile ticaret yapacaklardır.
ücreti telafi etmek için), Uniswap tarafından sunulan fiyat, göreceli piyasa fiyatını izleme
eğilimindedir.
Varlıkların, Angeris ve ark. [2] tarafından gösterildiği gibi . Bu, yaklaşık olarak kullanılabileceği
anlamına gelir
fiyat oracle.
Bununla birlikte, Uniswap v1'in zincir üzerinde fiyat kahini olarak kullanılması güvenli değildir,
çünkü
manipüle etmesi kolay. Başka bir sözleşmenin ödeme yapmak için mevcut ETH-DAI fiyatını
kullandığını varsayalım
bir türev. Ölçülen fiyatı değiştirmek isteyen bir saldırgan, ETH'yi
ETH-DAI çifti, türev sözleşmesinde uzlaşmayı tetikler (bu,
şişirilmiş fiyat üzerinden) ve ardından ETH'yi tekrar gerçek fiyata takas etmek için parite
satabilirsiniz.1
Bu, atomik bir işlem olarak veya siparişi kontrol eden bir madenci tarafından bile yapılabilir.
bir blok içindeki işlemlerin oranı.
Uniswap v2, fiyatı ölçüp kaydederek bu oracle işlevselliğini geliştirir
her bloğun ilk işleminden önce (veya eşdeğer olarak, önceki işlemin son işleminden sonra)
1 Uniswap v1'i bir oracle olarak kullanmanın bir sözleşmeyi bu tür
bir saldırı, bkz. [3] .

---

blok). Bu fiyatın manipüle edilmesi blok sırasındaki fiyatlardan daha zordur. Saldırgan
bir bloğun sonunda fiyatı değiştirmeye çalışan bir işlem gönderir, bazıları
diğer arbitrajcılar, hemen geri alım satım yapmak için başka bir işlem gönderebilir
daha sonra aynı blokta. Bir madenci (ya da bir saldırganın tamamını doldurmak için yeterli gazı
kullanan bir saldırgan)

blok) fiyatı bir bloğun sonunda manipüle edebilir, ancak bir sonraki bloğu benimsemedikleri sürece ayrıca, takası geri alma konusunda tahkimde belirli bir avantaja sahip olmayabilirler.
Özellikle Uniswap v2, kümülatif toplamı takip ederek bu fiyatı biriktirir
Birisinin sözleşmeyle etkileşime girdiği her bloğun başındaki fiyatlar. Her biri
fiyat, içinde bulunduğu son bloktan bu yana geçen süreye göre ağırlıklandırılır.
blok zaman damgasına göre güncellenir.[2] Bu, herhangi bir akümülatör değerinin herhangi bir
verilen süre (güncellendikten sonra), her saniyedeki spot fiyatın toplamı olmalıdır.
sözleşmenin tarihi.

$$a_t = \sum_{i=1}^{t} p_i \quad (2)$$

T 1 ile t 2 arasındaki zaman ağırlıklı ortalama fiyatı tahmin etmek için , harici bir arayan
akümülatörün değerini t 1 ve sonra tekrar t 2'de kontrol edin , ilk değeri çıkarın
ikincisini seçin ve geçen saniye sayısına bölün. (Sözleşmenin kendisinin
bu akümülatör için geçmiş değerleri saklamayın — arayan kişinin sözleşmeyi şuradan araması gerekir:
bu değeri okumak ve saklamak için dönemin başlangıcı.)

$$p_{t1,t2} = \sum_{i=t1}^{t2} p_i = \sum_{i=1}^{t2} p_i - \sum_{i=1}^{t1} p_i = \frac{t_2 - t_1}{t_2 - t_1} = \frac{a_{t2} - a_{t1}}{t_2 - t_1} \quad (3)$$

Oracle kullanıcıları bu dönemin ne zaman başlayıp biteceğini seçebilirler. Daha uzun seçmek
dönem, bir saldırganın TWAP'yi manipüle etmesini daha pahalı hale getirir, ancak
daha az güncel bir fiyata.
Bir komplikasyon: A varlığının fiyatını B varlığı açısından mı ölçmeliyiz, yoksa
A varlığı açısından B varlığının fiyatı? A'nın B cinsinden spot fiyatı her zaman
A cinsinden B'nin spot fiyatının tersi, B varlığı açısından A varlığının ortalama fiyatı
belirli bir süre boyunca B varlığının ortalama fiyatının karşılığına eşit değildir.
varlık şartları A[3] Örneğin, USD / ETH fiyatı 1. blokta 100 ve 2. blokta 300 ise,
ortalama USD / ETH fiyatı 200 USD / ETH olacaktır, ancak ortalama ETH / USD fiyatı
1/150 ETH / USD olacaktır. Sözleşme, iki varlıktan hangisinin kullanıcıların
hesap birimi olarak kullanmak isteyen Uniswap v2, her iki fiyatı da takip eder.
Diğer bir komplikasyon da, birisinin varlıkları çift kontrole göndermesinin mümkün olmasıdır.
yol - ve böylece bakiyelerini ve marjinal fiyatı değiştirmeden - onunla etkileşime girmeden ve
böylece bir oracle güncellemesini tetiklemeden. Sözleşme sadece kendi bakiyesini kontrol ettiyse
ve mevcut fiyata göre oracle'ı güncellediğinde, bir saldırgan kehaneti manipüle edebilir
ilk kez aramadan hemen önce sözleşmeye bir varlık göndererek
blok. Son işlem, zaman damgası X saniye önce olan bir blokta ise, sözleşme
hiç kimse olmasa bile, yeni fiyatı biriktirmeden önce X ile yanlışlıkla çarpabilir
2 Madencilerin blok zaman damgasını belirleme özgürlüğü olduğundan, oracle kullanıcıları şunu bilmelidir:
bu değerler tam olarak gerçek dünya zamanlarına karşılık gelmeyebilir.

3 A varlığının belirli bir süre boyunca B varlığı açısından aritmetik ortalama fiyatı, karşılıklı
A varlığı açısından B varlığının harmonik ortalama fiyatının o dönem için. Sözleşme ölçüldüyse
geometrik ortalama fiyat, o zaman fiyatlar birbirinin karşılığı olacaktır. Bununla birlikte, geometrik
ortalama
TWAP daha az kullanılır ve Ethereum'da hesaplanması zordur.
3

---

4. sayfa

bu fiyata ticaret yapma fırsatı buldu. Bunu önlemek için, temel sözleşme önbelleğe alınır
her etkileşimden sonra rezervlerini tutar ve oracle'ı,
cari yedekler yerine önbelleğe alınmış yedekler. Kahini korumaya ek olarak
manipülasyon, bu değişiklik, aşağıdaki bölümde açıklanan sözleşme yeniden mimarisini etkinleştirir
3.2.
2.2.1 Kesinlik
Solidity, tamsayı olmayan sayısal veri türleri için birinci sınıf desteğe sahip olmadığından,
Uniswap v2 fiyatları kodlamak ve değiştirmek için basit bir ikili sabit nokta formatı kullanır.
Spesifik olarak, belirli bir andaki fiyatlar UQ112.112 sayıları olarak saklanır, yani 112
kesirli kesinlik bitleri ondalık noktanın her iki yanında işaretsiz olarak belirtilir.
Bu sayıların bir aralığı [0, 2 112
- 1]
4 ve 1 hassasiyet
2 112 .
UQ112.112 formatı pragmatik bir nedenle seçilmiştir - çünkü bu rakamlar
bir uint224 içinde depolanabilir, bu 256 bitlik bir depolama yuvasının 32 bitini boş bırakır. Ayrıca şu da olur
her biri bir uint112'de depolanan rezervler ayrıca (paketlenmiş) 256 bitlik bir depolama yuvasında 32 biti serbest bırakır.
Bu boş alanlar, yukarıda açıklanan biriktirme işlemi için kullanılır. Özellikle,
rezervler, en az bir işlemle en son bloğun zaman damgasıyla birlikte saklanır,
32 bite sığması için 2 32 ile modifiye edilmiştir . Ek olarak, verilen herhangi bir fiyat olmasına rağmen
momentin (bir UQ112.112 numarası olarak saklanır) 224 bit'e sığması garanti edilir, birikim
Bu fiyatın bir aralığı üzerinden değil. İçin depolama yuvalarının ucundaki ekstra 32 bit
A / B ve B / A'nın birikmiş fiyatı, tekrarlanan işlemlerden kaynaklanan taşma bitlerini depolamak için kullanılır
fiyatların özeti. Bu tasarım, fiyat oracle'ının yalnızca üç tane daha eklediği anlamına gelir.
Her bloktaki ilk ticarete SSTORE işlemleri (yaklaşık 15.000 gaz cari maliyet).
Birincil dezavantajı, 32 bitin zaman damgası değerlerini depolamak için yeterli olmamasıdır.
makul ölçüde asla taşmayacaktır. Aslında, Unix zaman damgasının bir uint32'yi aştığı tarih
02/07/2106. Bu sistemin bu tarihten sonra düzgün çalışmasını sağlamak için,
ve 2 32'nin her katı
- Bundan 1 saniye sonra oracle'lar fiyatları kontrol etmek için yeterlidir
aralık başına en az bir kez (yaklaşık 136 yıl). Bunun nedeni, temel yöntem
birikimi (ve zaman damgasının modellenmesi), aslında taşmaya karşı güvenlidir, yani
oracle'ların kullanımda olduğu göz önüne alındığında, taşma aralıkları uygun şekilde açıklanabilir.
deltaları hesaplamak için uygun (basit) taşma aritmetiği.
2.3 Flaş Değişimleri
Uniswap v1'de, XYZ ile ABC satın alan bir kullanıcının XYZ'yi sözleşmeye göndermesi gerekir
ABC'yi almadan önce. Bu, kullanıcının ABC'ye ihtiyaç duyması durumunda sakıncalıdır.
ödeme yaptıkları XYZ'yi elde etmek için satın alıyorlar. Örneğin, kullanıcı
bir fiyatı arbitraj yapmak için başka bir sözleşmede XYZ'yi satın almak için bu ABC'yi kullanıyor olmak
Uniswap'ten farklı olabilir veya Maker veya Compound'da bir pozisyonu çözüyor olabilirler.
Uniswap'i geri ödemek için teminatın satılması.
Uniswap v2, bir kullanıcının ödeme yapmadan önce bir varlığı alıp kullanmasına izin veren yeni bir özellik ekler

bunun için, ödemeyi aynı atomik işlem içinde yaptıkları sürece. Takas
işlevi, aktarım arasında isteğe bağlı kullanıcı tanımlı bir geri arama sözleşmesine çağrı yapar
kullanıcı tarafından talep edilen jetonları dışarı çıkarın ve değişmezi zorlayın. Geri arama olduğunda
tamamlandığında, sözleşme yeni bakiyeleri kontrol eder ve değişmezin karşılandığını onaylar
4 teorik üst 2'nin bağlanmış 112
- (
1
2 112) içinde UQ112.112 numaraları gibi, bu ortamda geçerli değildir
Uniswap her zaman iki uint112 oranından üretilir. Gibi en büyük oranı 2 112
−1
1
= 2 112
- 1.
4

5.Sayfa

(ödenen tutarlardaki ücretleri ayarladıktan sonra). Sözleşme yeterli değilse
fonlar, tüm işlemi geri alır.
Bir kullanıcı, Uniswap havuzunu tamamlamak yerine aynı jetonu kullanarak da geri ödeyebilir.
takas. Bu, herhangi birinin depolanan varlıklardan herhangi birini flash-ödünç almasına izin vermekle
etkili bir şekilde aynıdır.
bir Uniswap havuzu (Uniswap'in alım satım ücretleriyle aynı% 0,30 ücret karşılığında).5
2.4 Protokol ücreti
Uniswap v2, açılıp kapatılabilen% 0,05'lik bir protokol ücreti içerir. Açılırsa,
bu ücret, fabrika sözleşmesinde belirtilen bir ücret adresine gönderilecektir.
Başlangıçta, ücretTo belirlenmez ve herhangi bir ücret alınmaz. Önceden belirlenmiş bir adres
(ücretToSetter) şunları yapabilir:
Uniswap v2 fabrika sözleşmesinde setFeeTo işlevini çağırın, ücreti farklı bir değere ayarlayın
değer. FeeToSetter ayrıca, FeeToSetter adresini değiştirmek için setFeeToSetter'ı da çağırabilir.
kendisi.
FeeTo adresi belirlenirse, protokol 5 baz puanlık bir ücret talep etmeye başlayacaktır;
1 olarak alınır
Likidite sağlayıcıları tarafından kazanılan 30 baz puanlık ücretten 6 kesinti. Yani, tüccarlar
tüm işlemlerde% 0,30'luk bir ücret ödemeye devam edin; Bu ücretin% 83,3'ü (işlem gören miktarın%
0,25'i)
likidite sağlayıcılarına gidecek ve bu ücretin% 16,6'sı (işlem gören miktarın% 0,05'i)
the FeeTo adresi.
Bu% 0,05'lik ücretin ticaret sırasında tahsil edilmesi, ek bir gaz maliyetine neden olur.
her ticaret. Bunu önlemek için birikmiş ücretler yalnızca likidite yatırıldığında toplanır
veya geri çekilmiş. Sözleşme, birikmiş ücretleri hesaplar ve yeni likidite jetonlarını verir
herhangi bir jeton basılmadan veya yakılmadan hemen önce ücret yararlanıcısına.
Toplanan toplam ücretler, / k (yani / x · y) cinsinden büyüme ölçülerek hesaplanabilir.
son zamandan beri ücretler toplandı.6 Bu formül size şu tarihler arasında birikmiş ücretleri verir:
t 1 ve t, 2 t havuzda likidite yüzdesi olarak 2 :
f 1,2 = 1 -
/ k 1
/ k 2
(4)
Ücreti t önce etkinleştirilmişse 1 , feeTo adresi yakalamak gerekir 1
6 ücret
t 1 ile t 2 arasında birikmiştir . Bu nedenle, yeni likidite tokenlerini
f φ · temsil feeTo adresi 1,2 φ olan havuzun 1
6 .
Yani, aşağıdaki ilişkiyi sağlamak için s m'yi seçmek istiyoruz , burada s 1 toplam
t 1 zamanında tedavüldeki hisse senedi miktarı :

s m
s m + s 1 = φ · f 1,2
(5)
1 - √k 1'in değiştirilmesi dahil olmak üzere bazı manipülasyonlardan sonra
√k 2
f 1,2 için ve s m için çözerken , biz
bunu şu şekilde yeniden yazabilir:
s m =
/ k 2 -
/ k 1
(1
φ - 1) ·
/ k 2 + / k 1 · s 1
(6)
Φ 1'e ayarlanıyor
6 bize şu formülü verir:
5 Uniswap girdi tutarları üzerinden ücret aldığından, çekilen miktara göre ücret gerçekte
biraz daha yüksek:
1
1−0,003 - 1 =
3
997 ≈% 0,3009203.
6 Basılmış veya yakılmış likidite jetonlarını hesaba katmayan bu değişmezi kullanabiliriz,
çünkü her likidite yatırıldığında veya çekildiğinde ücretlerin toplandığını biliyoruz.
5

Sayfa 6

s m =
/ k 2 -
/ k 1
5 ·
/ k 2 + / k 1 · s 1
(7)
İlk yatırıcının bir çifte 100 DAI ve 1 ETH koyduğunu ve 10 hisse aldığını varsayalım.
Bir süre sonra (bu çifte başka bir emanetçi katılmadan),
çiftin 96 DAI ve 1.5 ETH'ye sahip olduğu bir zamanda geri çekmek için. Bu değerleri takmak
Yukarıdaki formül bize şunu verir:
s m =
/1.5
· 96 -
/ 1
· 100
5 ·
/1.5
· 96 +
/ 1
· 100
· 10 ≈ 0,0286
(8)
2.5 Havuz hisseleri için meta işlemler
Uniswap v2 çiftleri tarafından basılan havuz paylaşımları, meta işlemleri yerel olarak destekler. Bu şu anlama gelir
kullanıcılar bir imza ile havuz paylaşımlarının devrine izin verebilir7bir zincirden ziyade
adreslerinden işlem. Bu imzayı kullanıcı adına herkes tarafından gönderebilir:
izin işlevini çağırmak, gaz ücretlerini ödemek ve muhtemelen

aynı işlem.
3 Diğer değişiklikler
3.1 Sağlamlık
Uniswap v1, Python benzeri bir akıllı sözleşme dili olan Vyper'da uygulanmaktadır. Uniswap v2 bazı yetenekler gerektirdiğinden, daha yaygın olarak kullanılan Solidity'de uygulanmaktadır. Henüz Vyper'da mevcut değil (standart olmayanların dönüş değerlerini yorumlama yeteneği gibi) ERC-20 belirteçlerinin yanı sıra, satır içi montaj yoluyla chainid gibi yeni işlem kodlarına erişim) geliştirildiği zaman.
3.2 Sözleşmenin yeniden yapılandırılması
Uniswap v2 için bir tasarım önceliği, yüzey alanını ve karmaşıklığını en aza indirmektir. çekirdek çifti sözleşmesi - likidite sağlayıcılarının varlıklarını saklayan sözleşme. Bunda herhangi bir hata var
Milyonlarca dolarlık likidite çalınabilir veya dondurulabileceği için kontrat felaket olabilir.
Bu temel sözleşmenin güvenliğini değerlendirirken en önemli soru şudur:
likidite sağlayıcılarını varlıklarının çalınmasına veya kilitlenmesine karşı koruyup
korumadığı. Herhangi bir özellik
bu, tüccarları destekleme veya koruma amaçlıdır - izin vermenin temel işlevi dışında
havuzdaki bir varlık bir başkasıyla takas edilecek - bir "yönlendirici" sözleşmesiyle ele alınabilir. Aslında, takas işlevselliğinin bir kısmı bile yönlendirici sözleşmesine çekilebilir.
Yukarıda belirtildiği gibi, Uniswap v2 her bir varlığın son kaydedilen bakiyesini saklar (
oracle mekanizmasının belirli bir manipülatif istismarını önlemek). Yeni mimari
Uniswap v1 sözleşmesini daha da basitleştirmek için bundan yararlanır.
Uniswap v2'de satıcı, takası çağırmadan önce varlığı ana sözleşmeye gönderir
işlevi. Ardından, sözleşme, varlığın ne kadarını aldığını, karşılaştırarak ölçer.
son kaydedilen bakiye mevcut bakiyesine. Bu, temel sözleşmenin agnostik olduğu anlamına gelir
7 İmzalı mesaj, EIP-712 standardına uygundur, meta işlemler için kullanılanla aynıdır.
CHAI ve DAI gibi belirteçler.

---

7. Sayfa

tüccarın varlığı transfer etme şekline. TransferFrom yerine, bir
ERC-20'lerin transferini yetkilendirmek için meta işlem veya gelecekteki herhangi bir mekanizma.
3.2.1 Ücret için düzenleme
Uniswap v1'in alım satım ücreti, sözleşmeye ödenen tutar düşülerek uygulanır.
Sabit çarpım değişmezini zorlamadan önce% 0.3. Sözleşme zımni olarak
aşağıdaki formül:
(x 1 - 0,003 · x inç)) · y 1 > = x 0 · y 0
(9)
Flaş swap ile Uniswap v2 tanıtır olasılığı, x in ve y olarak kudreti hem
sıfırdan farklı olmalıdır (bir kullanıcı çifti aynı varlığı kullanarak geri ödemek istediğinde,
takas). Ücretleri doğru bir şekilde uygularken bu tür durumları ele almak için sözleşme,
aşağıdaki değişmezi uygulayın:8
(x 1 - 0,003 · x inç) · (y 1 - 0,003 · y inç)> = x 0 · y 0
(10)
Zincir üzerindeki bu hesaplamayı basitleştirmek için, eşitsizliğin her bir tarafını şununla çarpabiliriz:
1.000.000:
(1000 ax 1 - 3 · X olarak) · (1000 * y 1 - 3 · y de)> = 1000000 ax 0 * y 0
(11)
3.2.2 sync () ve skim ()
Çift sözleşmesini güncelleyebilen ısmarlama belirteç uygulamalarına karşı koruma sağlamak için ve toplam arzı 2 112'den fazla olabilen tokenleri daha zarif bir şekilde yönetmek için ,
Uniswap v2'nin iki kurtarma işlevi vardır: sync () ve skim ().
sync (), eşzamansız olarak bir belirtecin olması durumunda bir kurtarma mekanizması olarak işlev görür.

bir çiftin dengesini söndürür. Bu durumda, alım satımlar optimumun altında oranlar alacaktır ve eğer hayır ise
Likidite sağlayıcısı durumu düzeltmeye istekli, parite sıkışmış durumda. sync () ayarlamak için var sözleşmenin yedeklerinin mevcut bakiyelere göre biraz zarif bir iyileşme sağlaması
bu durumdan.
skim (), bir çifte yeterli token gönderilmesi durumunda bir kurtarma mekanizması olarak işlev görür. rezervler için iki uint112 depolama yuvasını aşın, aksi takdirde alım satımların
başarısız. skim (), bir kullanıcının mevcut bakiye arasındaki farkı çekmesine izin verir.
çift ve 2112
- Arayan kişiye 1, eğer bu fark 0'dan büyükse.
3.3 Standart olmayan ve olağandışı belirteçleri kullanma
ERC-20 standardı, transfer () ve transferFrom () 'un bir boolean girişi döndürmesini gerektirir. aramanın başarılı veya başarısız olduğunu belirten [4]. Bunlardan birinin veya her ikisinin uygulamaları
Tether (USDT) ve Binance Coin gibi popüler olanlar dahil olmak üzere bazı belirteçler üzerinde işlevler
(BNB) - bunun yerine dönüş değeri yoktur. Uniswap v1, eksik dönüş değerini yorumlar
yanlış olarak tanımlanan bu işlevler, yani transferin
başarılı değil - ve işlemi geri döndürerek transfer girişiminin başarısız olmasına neden olur.
8 , yeni mimari ile bu Not x de kullanıcı tarafından sağlanan değildir; bunun yerine şu şekilde hesaplanır:
geri aramadan sonra sözleşmenin bakiyesini ölçmek, x 1 ve ondan çıkararak (x 0 - x out). Bu mantık Sözleşmeye çağrılmadan önce gönderilen varlıklar ile sözleşmeye gönderilen varlıklar arasında ayrım yapılmaması
geri arama sırasında. y in , y 0 , y 1 ve y çıkışı temel alınarak aynı şekilde hesaplanır .

---

8. Sayfa

Uniswap v2, standart olmayan uygulamaları farklı şekilde ele alır. Özellikle, eğer bir transfer () telefon etmek9'un dönüş değeri yoktur, Uniswap v2 bunu başarısızlıktan çok başarı olarak yorumlar. Bu
değişiklik, standarda uyan herhangi bir ERC-20 jetonunu etkilememelidir (çünkü
belirteçler, transfer () her zaman bir dönüş değerine sahiptir).
Uniswap v1 ayrıca transfer () ve transferFrom () çağrılarının
Uniswap çifti sözleşmesine bir evresel çağrıyı tetikler. Bu varsayım, belirli kişilerce ihlal edilmektedir. ERC-20 jetonları, ERC-777'nin "kancalarını" [5] destekleyenler dahil . Bunu tam olarak desteklemek için
belirteçler, Uniswap v2, tüm kamusal duruma yeniden girişi doğrudan engelleyen bir "kilit" içerir. değişen işlevler. Bu aynı zamanda kullanıcı tarafından belirtilen geri aramadan yeniden girişe karşı koruma sağlar
Bölüm 2.3'te açıklandığı gibi bir flash takasında .
3.4 Likidite belirteci arzının başlatılması
Yeni bir likidite sağlayıcısı tokenleri mevcut bir Uniswap çiftine yatırdığında, numara basılan likidite tokenleri, mevcut token miktarına göre hesaplanır:

$$s_{\text{NANELİ}} = \frac{x_{\text{yatırıldı}}}{x_{\text{başlangıç}}} \cdot s_{\text{başlangıç}} \quad (12)$$

Peki ya ilk emanetçi onlarsa? Bu durumda, x başlangıcı 0'dır, dolayısıyla bu formül çalışmıyor.
Uniswap v1, ilk hisse arzını yatırılan ETH miktarına eşit olacak şekilde ayarlar (wei). Bu biraz makul bir değerdi, çünkü ilk likidite yatırıldıysa
Doğru fiyata, 1 likidite havuzu payı (ETH gibi 18 ondalık bir belirteçtir)
yaklaşık 2 ETH değerinde olacaktır.
Ancak bu, bir likidite havuzu payının değerinin orana bağlı olduğu anlamına geliyordu.

likiditenin başlangıçta yatırıldığı, özellikle de oradan beri oldukça keyfi olan
bu oranın gerçek fiyatı yansıttığının garantisi yoktu. Ek olarak, Uniswap v2 şunları destekler:
keyfi çiftler olduğu için pek çok çift ETH'yi içermeyecektir.
Bunun yerine, Uniswap v2 başlangıçta mints, miktarların geometrik ortalamasına eşit paylaşır
yatırıldı:
s basılan = / x bırakılmış * y tevdi
(13)
Bu formül, herhangi bir zamanda bir likidite havuzu payının değerinin esasen
başlangıçta likiditenin yatırıldığı orandan bağımsızdır. Örneğin, varsayalım
1 ABC'nin fiyatının şu anda 100 XYZ olduğunu. İlk depozito 2 ABC ve
200 XYZ (1: 100 oranında), mudiye / 2 · 200 = 20 hisse almış olur. Şunlar
hisseler artık 2 ABC ve 200 XYZ değerinde ve birikmiş ücretler olmalıdır.
İlk depozito 2 ABC ve 800 XYZ (1: 400 oranında) olsaydı, yatıran
/ 2 · 800 = 40 havuz payı alacaktı.10
Yukarıdaki formül, bir likidite havuzu payının asla değerinin altında olmayacağını garanti eder.
o havuzdaki rezervlerin geometrik ortalaması. Ancak değeri için mümkündür
9 Yukarıda Bölüm 3.2'de açıklandığı gibi , Uniswap v2 çekirdeği transferFrom () kullanmaz.
10 Bu aynı zamanda yuvarlama hatalarının olasılığını da azaltır, çünkü hisse miktarındaki bit sayısı
yedeklerdeki X varlığı miktarındaki bit sayısının yaklaşık ortalaması ve
rezervlerdeki Y varlığı miktarındaki bit sayısı:
günlük 2 √x
· Y =
günlük 2 x + günlük 2 y
2
(14)

Sayfa 9

ya alım satım ücretlerini biriktirerek ya da
Likidite havuzuna “bağışlar”. Teorik olarak bu, değerin
Minimum likidite havuzu hisselerinin (1e-18 havuz hisseleri) oranı o kadar değerlidir ki
küçük likidite sağlayıcılarının herhangi bir likidite sağlaması imkansız hale gelir.
Bunu azaltmak için Uniswap v2, ilk 1e-15 (0.000000000000001) havuz paylaşımını yakar.
sıfıra gönderilerek (minimum havuz payı miktarının 1000 katı)
madenci yerine adres. Bu, neredeyse tüm belirteçler için ihmal edilebilir bir maliyet olmalıdır
çift.11 Ancak yukarıdaki saldırının maliyetini önemli ölçüde artırır. Yükseltmek için
Bir likidite havuzu payının değeri 100 $ ise, saldırganın 100.000 $ bağış yapması gerekir.
havuz, kalıcı olarak likidite olarak kilitlenecek.

3.5 ETH'yi Sarma

Ethereum'un yerel varlığı ETH ile işlem yapmak için arayüz,
ERC-20 belirteçleri ile etkileşim için standart arayüz. Sonuç olarak, diğer birçok protokol
Ethereum ETH'yi desteklemiyor, bunun yerine kanonik bir "sarılmış ETH" belirteci kullanıyor, WETH
[6] .
Uniswap v1 bir istisnadır. Her Uniswap v1 çifti, tek bir varlık olarak ETH'yi içerdiğinden,
ETH'yi doğrudan ele almak mantıklıydı, bu da biraz daha gaz verimli.
Uniswap v2, rastgele ERC-20 çiftlerini desteklediğinden, artık
paketlenmemiş ETH'yi destekler. Bu tür bir desteğin eklenmesi, çekirdek kod tabanının boyutunu iki
katına çıkarır.
ve ETH ve WETH çiftleri arasında likidite bölünmesi riski12. Yerel ETH ihtiyaçları
Uniswap v2'de işlem görmeden önce WETH'e sarılacaktır.

3.6 Deterministik çift adresleri

Uniswap v1'de olduğu gibi, tüm Uniswap v2 çifti sözleşmeleri tek bir fabrika tarafından somutlaştırılır
sözleşme. Uniswap v1'de, bu çift sözleşmeler CREATE işlem kodu kullanılarak oluşturuldu,
Bu, böyle bir sözleşmenin adresinin, söz konusu çiftin hangi sırayla
yaratıldı. Uniswap v2, bir çift oluşturmak için Ethereum'un yeni CREATE2 işlem kodunu [8] kullanır

belirleyici bir adresle sözleşme. Bu, bir çiftin hesaplanmasının mümkün olduğu anlamına gelir.
zincir durumuna bakmaya gerek kalmadan zincir dışı adres (varsa).
3.7 Maksimum belirteç bakiyesi
Oracle mekanizmasını verimli bir şekilde uygulamak için Uniswap v2 yalnızca rezervi destekler
2'ye kadar bakiyeleri 112
- 1. Bu sayı, 18 ondalık basamaklı jetonları destekleyecek kadar yüksektir
1 katrilyonun üzerinde toplam tedarik ile.
Her iki rezerv dengesi 2 üzeri go yoksa 112
- 1, takas işlevine yapılan herhangi bir çağrı başlayacaktır
başarısız olabilir (_update () işlevindeki bir denetim nedeniyle). Bu durumdan kurtulmak için herhangi bir kullanıcı
fazla varlıkları likidite havuzundan çıkarmak için skim () işlevini çağırabilir.
11 Teorik olarak, bu yanmanın göz ardı edilemeyebileceği bazı durumlar vardır, örneğin yüksek değerli
sıfır ondalık belirteçler. Bununla birlikte, bu çiftler yine de Uniswap için uygun değildir, çünkü yuvarlama hataları
ticareti olanaksız kılmak.
12 Bu yazı itibariyle, Uniswap v1'deki en yüksek likidite çiftlerinden biri ETH ve WETH arasındaki çifttir.
[7] .

Sayfa 10

Referanslar
[1] Hayden Adams. 2018. URl : https://hackmd.io/@477aQ9OrQTCbVR3fq1Qzxg/HJ9jLsfTz ? tür = görünüm.
[2] Guillermo Angeris ve ark. Uniswap piyasalarının analizi. 2019. arXiv : 1911.03380 [q-fin.TR].
[3] samczsun. Eğlenmek ve kâr sağlamak için yetersiz teminatlı krediler almak. Eylül 2019. URl: https: / / samczsun. com / alma - yetersiz teminatlı - krediler - eğlence için - ve - kar amaçlı /.
[4] Fabian Vogelsteller ve Vitalik Buterin. Kasım 2015. URl : https: //eips.ethereum. org / EIPS / eip-20.
[5] Jordi Baylina Jacques Dafflon ve Thomas Shababi. EIP 777: ERC777 Token Standardı. Kasım 2017. URl : https://eips.ethereum.org/EIPS/eip-777.
[6] Radar. WTF WETH mi? URl: https://weth.io/.
[7] Uniswap.info. Sarılmış Eter (WETH). URl : https://uniswap.info/token/0xc02aaa39b223fe8d0a0e5c4f27ead9083c756
[8] Vitalik Buterin. EIP 1014: Sıska CREATE2. Nisan 2018. URl : https: //eips.ethereum . org / EIPS / eip-1014.
4 Sorumluluk Reddi
Bu kağıt yalnızca genel bilgi amaçlıdır. Yatırım teşkil etmez
herhangi bir yatırımı satın almak veya satmak için tavsiye veya tavsiye veya talep ve
herhangi bir yatırım kararı vermenin esasının değerlendirilmesinde kullanılabilir. Olmamalı
muhasebe, hukuk veya vergi danışmanlığı veya yatırım tavsiyeleri için güvenilebilir. Bu
makale yazarların güncel görüşlerini yansıtır ve Paradigm veya onun adına yapılmamıştır.
bağlı kuruluşlardır ve Paradigm'ın, bağlı kuruluşlarının veya bireylerin görüşlerini yansıtması gerekmez
Paradigma ile ilişkili. Burada yansıtılan görüşler,
güncellenmiş.