Sayfa 1

Sarılmış Jetonlar

Herhangi bir varlığı belirtmek için çok kurumsal bir çerçeve

Teknik Rapor v0.2
24 Ocak 2019

Kyber Ağı
BitGo Inc
Cumhuriyet Protokolü

Sayfa 2

Öz

ERC20'nin popülaritesinin artmasıyla, Ethereum ekosistemindeki dijital tokenler ortaya çıktı. önemli bir varlık sınıfı olarak. Bu tokenlar, blok zincirlerinin tüm avantajlarına sahiptir ve Ethereum, toplam coin sayısında, sahiplerinde, darphanesinde, hızlı bir şekilde şeffaflık sunmalıdır. onay süreleri, işlem ayrıntıları ve akıllı sözleşme yürütme. Ethereum'daki Jetonlar blok zinciri birkaç farklı işleve hizmet edebilir; bu makale özellikle varlığa odaklanacak desteklenen veya paketlenmiş belirteçler. Bu tokenlerin fiyatları, varlık desteğinin fiyatını yansıtır bunlar ve dolayısıyla "sabit madeni paralar" olarak da adlandırılabilirler. Varlık destekli belirteçler genellikle yapılır iki farklı şekilde:

● **algoritmik** - Bu Ethereum yere birkaç jeton ardından bir mekanizmadır talep ve arz, fiyatını korumak için akıllı sözleşmelerle kontrol edilir. itibari para birimine uygun belirteç. Bunun bazı örnekleri Dai, Basis, Carbon ve NuBits

● **Merkezi** - Varlık rezervlerinin kanıtı yayınlayan bir organizasyon ile saklanır. Tether, True USD, USDC (USD), Digix (altın), Globcoin (bir fiat karışımı) para birimleri) ve AAA rezervi (devlet tahvilleri)

Sarılmış belirteçler, merkezi modeli takip eder, ancak tamamen tek bir kuruma güvenmek yerine, ağda farklı roller üstlenen bir kurumlar konsorsiyumuna güvenirler. Bu Teknik inceleme, zorlukları ele alarak varlık destekli belirteçleri yayınlamak için bir çerçeve önerir ölçeklenebilirlik, güven, düzenleme ve yönetişim ile. Başlatacağımız ilk sarılmış jeton bir Bitcoin (BTC) tarafından desteklenen ve uygun şekilde "Sarılmış BTC" olarak adlandırılan ERC20 jetonu (WBTC). Merkezi çözümlerden (USD) farklı olarak, WBTC tamamen hesaba katılacak ve BTC zincirinde yayınlanan rezervler.

WBTC'yi kullanmak için ek ikincil hizmet / ödeme jetonu ve transfer gerekmez blockchain ücretleri dışındaki ücretler. WBTC, basit bir federe yönetişim modeli kullanır ve kullanılabilirliği artırmak için.

---

3. Sayfa

Kullanım Durumları

Tokenizasyon

Varlıkları belirtme eylemi şunları yapabilir:

● İşlemlerin hızını artırın

Ethereum blokları her ~ 15 saniyede bir oluşturulur ve

5 dakikadan daha kısa bir sürede bir işlemin geri alınamaz olduğuna dair güven. Bu hız
Bitcoin, altın gibi diğer birçok varlığa kıyasla yerel olarak işlem yapmaktan daha hızlı,
ve fiat para birimleri
● Aracıların sayısını azaltın
Bir blok zincirindeki varlıkların en önemli avantajlarından biri, işlem yapabilme yetenekleridir.
aracılar olmadan. Bu, merkezi olmayan atomik takaslar yoluyla yapılabilir.
değişim protokolleri ve yıldırım / raiden tarzı kanallar.
● Güvenliği geliştirin
Tokenizasyon, kullanıcıların varlığın özel anahtarları üzerinde tam kontrole sahip olmasını
sağlar. Kullanıcılar
anahtar tutmak istemiyorum, karşı taraf riskini borsalardan diğerine taşıyarak azaltabilir.
güvenlik odaklı bir emanetçi.
● Kullanılabilirlik
ERC20 standardı çok sayıda kurum ve ürün tarafından benimsenmiştir.
Bu, kullanıcılara çeşitli borsalar, cüzdanlar ve Dapps sağlar.
tokenize edilmiş varlıklarını idare etmek. Ayrıca jetonları hızlı bir şekilde 7/24 taşıma yeteneğine de sahipler.
● Şeffaflığı İyileştirin
Toplam token sayısı, token oluşturma işlemleri, token kaldırma işlemleri,
token sahiplerinin sayısı ve transfer kuralları genel bir blok gezgininde görülebilir
kimse tarafından. Bu şeffaflık seviyesi genellikle fiat gibi varlıklar için mevcut değildir.
para birimleri, emtialar ve hisse senedi.

Merkezi olmayan borsalarda ve dapp'larda likidite

Bugün merkezi borsalarda ERC20 ticaretinin çoğu ETH ile değil BTC ile yapılmaktadır.
Merkezi olmayan borsaların çoğu yalnızca ETH / Token sunar, BTC / Token alım satımlarını sunmaz. Sarılmış
token'lar bu açığı kapatabilir ve merkezi olmayan borsalarda daha fazla likidite sağlayabilir. Ek olarak,
diğer merkezi olmayan uygulamalar / protokoller (fonlar, kredi ödemeleri gibi) da yararlanacaktır.
Bir BTC belirtecinin getirebileceği daha fazla likiditeye erişime sahip olmak. WBTC,
Bitcoin için akıllı sözleşmelerin oluşturulması.

Fiat jetonlarının faydaları

İtibari para birimleriyle desteklenen jetonlar, yatırımcılara paralarını bir
fiyat dalgalanmaları hakkında endişelenmenize gerek kalmadan kripto para birimi. Bu özellikle şunlar için kullanışlıdır:
doğrudan bir yolu olmayan hem merkezi hem de merkezi olmayan borsalarda tüccarlar
fiat para birimlerini transfer etmek. Fiat para birimi destekli belirteçler, aynı zamanda

---

kripto para birimi geleneksel finansın yerini alabilir. Özellikle e-ticarette her ikisi tarafından da kullanılabilir.
alıcı ve satıcı, dönüştürme oranları veya vergiler konusunda endişelenmenize gerek kalmadan (alıcılar gereklidir
ABD'de satın alma sırasında hesaplanan sermaye kazancı vergisini ödemek için).

Kripto para birimleri arasında birlikte çalışabilirlik

Bugün kripto para birimlerinin sayısında bir artış gördükçe, her biri bazılarına odaklanıyor
parasal mübadele yönü. Bu türden bazı yönler, işlem hacmi, gizlilik,
ucuz işlem ücretleri, akıllı sözleşme yeteneği ve düğümlerin / madencilerin ademi merkeziyetçiliği.
sarılmış çerçeve, diğer herhangi bir kripto para birimini temsil etmeyi kolaylaştıracaktır.
Bitcoin, Ethereum'da ve böylece Ethereum'un tüm yetenekleriyle geliştirin
blok zinciri. Böyle bir kullanım durumu, ilk madeni para tekliflerinin (ICO'lar) doğrudan finanse edilebilmesidir.
ve paketlenmiş Bitcoin jetonlarının depozitolarında para iadesi. Gelecekte, merkezi borsalar
ve kripto para birimlerini kabul eden diğer kurumların birden fazla
kripto para düğümleri ve bunun yerine sadece Ethereum'da gelişebilir.

Politikaları uygulamanın zincir yollarında
Tokenizasyon, aynı zamanda zincir üzerinde politikaları uygulamak için bir yol sağlar. Zincir politika uygulaması hakkında
kuralları daha şeffaf hale getirir ve bunları uygulamak için tek bir tarafa güvenmez. Dayalı
Varlığın türü, varlık transferi veya ticareti ile ilgili kuralları uygulama ihtiyacı olabilir. Menkul Kıymetler
örneğin, beyaz listeye alma, bekletme süreleri ve kimlik yönetimi gerektirir.

Ortak sorunlar

Ölçeklenebilirlik
Ocak 2018 itibariyle, Ethereum'un ana ağındaki maksimum pratik gaz limiti,
Blok başına 8.000.000 gaz[1] . Bu sınır hem donanıma hem de yazılıma bağlıdır. Varken
birkaç ölçeklenebilirlik çözümü önerildi, çoğu önemli geliştirici artışı gerektiriyor (durum kanalları),
veya pratik kullanım için çok erken geliştirme aşamasındadır (plazma, parçalama). Bu bir problemdir
Dapps ve ağ kullanıcıları, çünkü çekişme dönemlerinde gaz fiyatları fırlıyor
(sıcak ICO'lar, CryptoKitties). Bu yılın başlarında Temmuz ayında, işlemler Çin borsasından kaynaklandı
Fcoin her zaman yüksek işlem ücretlerine neden oldu[2] .

Güven
Varlık destekli belirteçler genellikle varlığı elinde bulunduran kurum (lar) a duyulan güveni içerir. Bu gider
operasyonlarda güven ihtiyacını en aza indirmeye çalışan kripto para birimlerine karşı.
Burada cevaplanması gereken bazı temel sorular şunlardır:

- Varlık sahibi, mevcut yasal çerçevede varlığı elinde tutma yetkisine sahip mi?
- Sorumlu, keyfi miktarda jeton oluşturabilir mi?
- Saklama memuru, gözetim altındaki varlığa sahip olduğunu nasıl kanıtlar?

Yönetmelik
Varlığa dayalı belirteçlerin saklayıcılarının, varlığı elinde bulundurmaları için lisanslanması gerekir. Bu lisans,
saklama görevlisinin varlığına ve coğrafi yargı yetkisine göre değişiklik gösterir. Muhafızlar ayrıca
1: 1 destek eksikliğinin tüm sistemi baltalayacağı düşünüldüğünde rezervleri düzenli olarak kanıtlayın.
KYC ve AML kısıtlamaları, varlık destekli belirteçlerle uğraşan kullanıcılar için de geçerlidir. Bunlar
belirteçlerin satın alınması, kullanılması veya aktarılması sırasında kısıtlamaların uygulanması gerekir.

Yönetim
Sistemde birden fazla paydaş olduğunda, bunun nasıl yapılacağıyla ilgili bir yönetişim sorunu vardır.
jetonda yapılan değişiklikleri işlemek için. Varlık destekli tokenlerin çoğu, tamamen
jetonu yöneten kurallarda / akıllı sözleşmede değişiklik yapmak için varlık saklama. Genellikle içinde
ICO'lar söz konusu olduğunda, jetonu veren kuruluş protokol değişiklikleri üzerinde tam kontrole sahiptir. Oldu
kullanıcıların sahip olduğu merkezi olmayan otonom ilk madeni para teklifleri (DAICO'lar) gibi bazı durumlar
haklarını oylama, ancak bir seçmen sayısının azlığı sorunuyla karşı karşıya [3].

Uygulama ve Teknoloji

Anahtar Roller
- Sorumlu - Varlığı elinde tutan kurum veya taraf. WBTC söz konusu olduğunda, bu
BitGo tarafından oynanacak[4]. Muhafızlar, jeton basmak için anahtarları tutarlar.
- Satıcı - Paketlenmiş jetonların basılacağı ve yakılacağı kurum veya taraf

itibaren. Satıcılar, paketlenmiş jetonun dağıtımında önemli bir rol oynar. Bu durumuda

---

Sayfa 6

WBTC, bu Kyber tarafından başlangıçta oynanacak [5] ve Cumhuriyet Protokolü[6]. Her tüccar yeni sarılmış jetonların basımını ve sarılmış jetonların yakılmasını başlatmak için bir anahtar tutar.
● Kullanıcı - Sarılmış jetonun sahipleri. Kullanıcılar aktarım için sarılmış jetonları kullanabilir ve Ethereum ekosistemindeki diğer ERC20 belirteçleri gibi işlem yapın.
● WBTC DAO üyesi - Sözleşme değişiklikleri ve saklama görevlilerinin eklenmesi / kaldırılması ve tüccarlar, çoklu imzalı bir sözleşme ile kontrol edilecektir. Anahtarların sahipleri çoklu imza sözleşmesi WBTC DAO'nun bir parçası olarak kurumlar tarafından yapılacaktır.

Muhafızlar, tüccarlarla paketlenmiş jetonlar için varlıkları değiştirir. Bu iki aracılığıyla yapılır farklı işlem türleri; darphane (sarılmış jeton oluşturma) ve yakma (azaltma sarılmış jeton temini). Bu işlemler halka açık olacak ve görüntüleyebilecek bir blok gezgini aracılığıyla herkes. İlk değişimden sonra, tüccarlar bir tampon tutmayı hedefliyor kullanıcılarla değiş tokuş edebilmeleri için paketlenmiş belirteçler. İki aşamalı basım süreci Para basma ve yazma gibi, kullanıcıların jetonları alması için geçen süreyi azaltmaya yardımcı olur daha fazla zaman alan süreçler.

Saklama cüzdanı kurulumu

Muhafızların tüm tüccarlar için havuzlanmış bir cüzdana sahip olması bekleniyor. Cüzdan kullanacak saklama görevlisi tarafından kontrol edilen tüm anahtarlarla çoklu imza. Cüzdan yalnızca şu adrese gönderebilir:
zincirdeki beyaz listeye eklenmiş satıcı adresi. Tüm basım ve yazma işlemleri bekleniyor bakıcıya teslim edildikten sonra 48 saat içinde yapılmalıdır. Birden fazla olması durumunda saklama görevlileri, tek bir cüzdanın, bekleyen tüm paketlenmiş olanları geri almak için yeterli parası olmayabilir.
belirteçler.

Darphane

Darphane, yeni sarılmış belirteçler oluşturma sürecini ifade eder. Sarılmış olarak darphane çerçeve bir bakıcı tarafından yapılmalıdır, ancak bir tüccar tarafından "başlatılması" gerekir. Bu Darphanenin kullanıcıyı kapsamadığına dikkat etmek önemlidir. Yapılan bir dizi işlemdir tüccar ve bekçi arasında.

---

7. Sayfa

WBTC için basım olaylarının sırası

● Satıcı, saklama görevlisine X WBTC'yi
Ethereum zincirindeki satıcının adresi.
● Satıcı, saklama görevlisine X BTC gönderir.
● Saklama kuruluşu, BTC işleminin 6 onayını bekler
● Sorumlu, Ethereum zincirinde X yeni WBTC jetonu basmak için bir işlem oluşturur

---

8. Sayfa

Kullanıcıların WBTC jetonları alması için olay dizisi

● Kullanıcı, bir satıcıdan paketlenmiş jeton talep eder
● Satıcı gerekli AML, KYC prosedürlerini uygular ve kimliği alır
kullanıcıdan bilgi
● Kullanıcı ve satıcı biratomik takas ya sahip güvenilir alışverişi kullanmak
Bitcoin alan satıcı ve WBTC alan kullanıcı

Yanan

Yazma, WBTC tokenleri için BTC'yi kullanma eylemini ifade eder. Yalnızca satıcı adresleri

sarılmış jetonları yak. Bunu yapmak için, 'yakma' işlevi ile yapılan sözleşmede
Ethereum zincirinde yakılacak token miktarı. Bunu yaparak tutar düşülür
tüccarın WBTC bakiyesinden (zincirde) ve WBTC arzı azalır.

'

WBTC jetonlarını yakmak için olay dizisi
● Satıcı, X WBTC jetonlarını yakarak bir yazma işlemi oluşturur
● Sorumlu, ETH işleminin 25 blok onayını bekler
● Sorumlu, tüccarın Bitcoin adresine X BTC'yi serbest bırakır
● Sorumlu, yanma talebini tamamlandı olarak işaretleyen bir ethereum işlemi gerçekleştirir

---

Sayfa 9

Kullanıcıların Bitcoin alması için olay dizisi
● Kullanıcı, bir tüccardan jetonların kullanılmasını ister
● Satıcı gerekli AML, KYC prosedürlerini uygular ve kimliği alır
kullanıcıdan bilgi
● kullanıcı ve bir tüccar, bir yerine atom takas, ya da güvenli bir şekilde değiştirilmesine kullanımı burada
kullanıcı Bitcoin alır ve tüccar WBTC jetonları alır
Zincirde aktarım kısıtlamaları
Jetona bağlı olarak, jetonların aktarımı için kısıtlamalar olabilir. WBTC için,
transferlerde herhangi bir kısıtlama olmayacaktır.
Yönetim
Sarılmış belirteç sözleşmesi, imzaların
üye eklemek / çıkarmak için DAO üyelerinden gereklidir. Tüm emanetçiler ve tüccarlar
DAO üyesi olacak, ancak diğer kurumlar da sahip olmadan üye olarak dahil edilebilirler.
bir emanetçi veya tüccar rolü. Sözleşmede "M of N" imza imzası kullanılacaktır
burada M, multisig sözleşmesinde gerekli imza sayısıdır ve N, toplam sayıdır
üye sayısı. M ve N'nin değerleri, içinde kalan üyeler arasında karşılıklı olarak kararlaştırılacaktır.
zihin güvenliği ve üye ekleme / çıkarma kolaylığı.
Sarılı jetonlar için yan zincir
Başlangıçta, WBTC Ethereum ana ağ zincirinde başlatılacak. Ana ağ zinciri kolayca
bir değişim ağı, blok kaşifleri, cüzdanlar ve diğerleri olduğu için erişilebilir ve kullanılabilir
Üzerine Dapps. Tokenizasyonun en önemli avantajlarından biri, ucuz işlem maliyetidir. Fakat
Ethereum'un popülaritesini artırmak ve Dapp oluşturma artışını, paketlenmiş işlem maliyetlerini artırmak
jetonlar, ana zincirde bunu yapmanın ucuz olmadığı noktaya yükselebilir.
sarmalanmış çerçevede birden fazla kurumun işbirliği, bir
işlem verimini artırmak için pratik ölçeklenebilir çözüm.

Sayfa 10

Bu, mevcut yazılım (kullanarak, bir sabitleştirilmiş yan zincir kullanımı yoluyla yapılabilir eşlik-köprü)
DAO üyeleri arasında çalışır. Zincir, kendi yetki ağı kanıtı üzerinde çalışacak[7] ile
Aura fikir birliği algoritması[8]. Bloklar tahmin edilebilir şekilde her 4 saniyede bir ve
performans tarzı. Şu anda, zaten böyle bir zincir (Kovan testnet) var ve
Mart 2017'den beri operasyon. Sarılmış jetonlar, ana ve yan zincir arasına sabitlenecek
mainnet ve yan zincir üzerindeki 2-yönlü bir çoklu sig cüzdan oluşturarak. Yan zincirler sağlamak
Ethereum'da çok ihtiyaç duyulan ölçeklenebilirlik. Bir yan zincirin ticaret için bazı faydaları ve
sarılmış belirteçlerin aktarılması:

● Minimum geliştirme maliyetiyle ölçeklendirme (aynı EVM)

● Özel, artırılmış işlem hacmi - ayrı donanımda ayrı blok zinciri ve
potansiyel otorite kanıtı (PoA) avantajları (daha hızlı bloklar)
● Mevcut istemcilerde ve cüzdanlarda desteklenmesi kolay
● Zincir diğer "gürültülü komşulardan" arındırılmıştır
● Minimum işlem maliyeti (spam'ı önlemek için)

Doğrulayıcılar (blok oluşturucular) sarmalanmış ortaklardan ve diğer güvenilir taraflardan seçilecektir.
Coğrafi olarak dağılmış olacak ve birkaç farklı ikametgah / hükümeti temsil edecek.
Doğrulayıcılar ayrıca ana ve yan zincir arasındaki 2 yollu sabitlemeyi de koruyacaktır. Değeri sabitlemek için
her iki zincirdeki sarılmış belirteçlerin arasında, çok imzalı bir sözleşme
ana ağ ve yan zincir.

● Ethereum mainnet'ten Ethereum yan zincirine göndermek için:
○ Ana ağ adresinden federe ana ağ çoklu imza adresine gönderin
■ Miktarı aranırken göndermeniz tavsiye edilir.
Multi-sig adresinde "sendToSidechain" yöntemi,
yan zincirdeki hedef adresi argüman
■ Bir yöntem olmadan gönderilirse, yan zincirdeki hedef adres
kaynak adresle aynı olduğu varsayıldı
○ Göndermeyi kaydetmek için ana ağda bir olay oluşturulur.
○ Federe imzalayanlar, tokenleri ana ağda "kilitler"
○ Bir "onay döneminden" sonra, yan zincirdeki multisig yetkilileri,
ana ağdaki gönderme olayı ve miktarı hedefe ödeyin
yan zincirdeki adres, daha az işlem ücreti
● ETH yan zincirinden ETH ana ağına göndermek için:
○ Özdeş (simetrik)

WBTC, yan zincirdeki ilk varlık olacak ve bu bileşenlerin bir kombinasyonunu kullanacak
bir ekosistem oluşturmak için birlikte çalışmak:

● Düğüm Yazılımı ve Yapılandırması
● Explorer'ı Engelle
● Cüzdan Sağlayıcıları

Sayfa 11

● Doğrulayıcıları Engelle
● Çoklu imza Yetkilileri

Teşvik

İşlemler, çalışan bloğu kapsayacak şekilde 1 Gwei'nin minimum başlangıç gaz fiyatı üzerinden ücretlendirilecektir.
doğrulayıcılar ve yan zincirde spam'ı önlemek için. Doğrulayıcılar, zincir dışında da teşvik edilebilir
her Dapp için veya blok ödülleri var. Ether dağıtımının / yönetiminin ayrıntıları
yan zincir hala belirlenecek.

Atomik Takas

WBTC değişimi yapmak için tüccarlar ve kullanıcılar arasında atomik swaplar kullanılabilir ve
BTC. Kullanıcı WBTC veya BTC'yi daha hızlı almak isterse, güvenilir bir yöntem
tüccarlar aracılığıyla da değişim yapılabilir.

KYC tamamlandığında, kullanıcıların BTC'yi WBTC ile atomik olarak takas etme adımları
tüccar:
● Kullanıcı bir sır üretir ve bunun karma değeri satıcıya zincir dışı sağlanır. Kullanıcı
ve satıcı ayrıca alma adresleri (ETH
ve BTC)

● Kullanıcı, satıcının hesabını kullanarak bir Bitcoin HTLC (Karma Süreli Kilitleme Sözleşmesi) oluşturur.
Bitcoin adresi, kullanıcının geri ödeme adresi, gizli hash ve son kullanma süresi. Bu alışkın kullanıcının X BTC ile finanse edeceği bir P2SH adresi oluşturun
● 6 onaydan sonra satıcı, Ethereum üzerinde bir HTLC sözleşmesi oluşturacaktır.
kullanıcının Ethereum adresi, satıcının iade adresi, gizli hash ve son kullanma tarihi
zaman. Satıcı daha sonra X WBTC'yi atomik takas sözleşmesine aktarır.
● Kullanıcı, X WBTC'yi atomik takas sözleşmesinden
kullanıcının Ethereum adresi
● Satıcı, Bitcoin fonlarını P2SH adresinden taşımak için sırrı kullanır
● Kullanıcı sona erme süresi içinde WBTC'yi talep etmezse, işlem
gider ve kullanıcı BTC'yi geri talep edebilir

Burada dikkat edilmesi gereken bazı önemli noktalar:
● Atomik takas sözleşmesini uygulamak ve ona WBTC göndermek için işlem var
ilgili ücretler. Bu nedenle, kullanıcının bir atomik takas ücreti ödemesi gerekir.
takas.
● Atomik takaslar zaman alır ve hem BTC hem de ETH zincirinde birden fazla işlem yapar.
kullanıcı, BTC'nin aktarıldığı güvenilir bir takas yapma seçeneğine sahip olabilir.
satıcı adresi ve bitcoin ağındaki 6 onaydan sonra satıcı gönderir
Kullanıcıya WBTC. Bu, tüccara güveni içerir, ancak daha hızlı ve daha ucuzdur.

Sayfa 12

WBTC ve Atomik Takas

Atomik takaslar, yalnızca bir işlem yapmak isteyen kullanıcılar için WBTC olmadan gerçekleştirilebilir.
BTC-ETH ticareti. Bir mekanizma aracılığıyla özetlenen merkezi olmayan bir borsada yapılabilir.
Komodo platform tarafından [9] . Ancak, WBTC'nin bir
DAPP'ler ve ekosistem için gerekli olan ETH zincirinde BTC'nin temsili
etkileşimde olmak. Atomik takasları WBTC ile karşılaştırırken göz önünde bulundurulması gereken birkaç başka değiş tokuş:

● Atomik değiş tokuşu yapan kişi tarafından fiyat keşfinin yapılmasını gerektirirler. Sarılmış Token fiyat keşfi yalnızca merkezi olmayan bir şekilde işlem yaparken yapılmalıdır.
WBTC'yi elde ettikten sonra değişim.
● Mevcut cüzdanlar tarafından desteklenecek atomik takas teknolojisi gerektirir ve
merkezi olmayan borsalar. Sarılmış BTC, herhangi bir ERC20'de kullanım için mevcut olacaktır
desteklenen cüzdan.
● Gerçekten yavaşlar çünkü her işlem, birden fazla onay kadar yavaş ilerliyor
ETH zinciri ve ardından Bitcoin zinciri (WBTC'nin tersine,
para basma / tokenleştirme yavaştır ancak oluşturulduktan sonra ETH zincirinde kolayca takas edilebilir)
● Merkezi olmayan bir borsada atomik bir takas yapmak, ayrı bir para yatırma ve
atomik takas ücreti de. Bu, kullanıcılar para birimlerini her takas etmek istediğinde sakıncalıdır.

Ücretler

Kullanıcılar arasındaki WBTC transferlerinin ağ ücretlerinden başka bir maliyeti olmayacaktır. Üç vardır
ağdaki farklı tarafların ücret kazanabileceği yollar:
● Saklama ücretleri: Bu, bir tüccarın darphane veya nane
sarılmış jetonları yakar.
● Satıcı ücretleri: Bu, kullanıcının paketlenmiş jetonları takas ettiği satıcı tarafından alınır.
varlık için ile.
● Yan zincir işlem ücretleri: Bu ücret, ağırlıklı olarak
Yan zincir. Bu, yan zincirdeki düğümleri çalıştıran tüm kurumlar arasında eşit olarak paylaşılır.

Yasal Bağlama

Muhafızlar ve tüccarlar arasındaki sözleşme
Jeton basma ve yazma işlemi kullanıcıyı içermez ve güvenilenler arasındadır.
kurumlar. Satıcıların, kullanıcının kimlik bilgilerini güvenli bir şekilde saklaması gerekir.
Saklama görevlilerinin, gözaltına alınan varlıkların ayrıntılarını üç ayda bir yayınlamaları ve
zamanında basım / yakma görevleri. Bu kriterlerin karşılanmaması, kaldırılmaya neden olabilir
ağdan.

Sayfa 13

Ağda birden fazla bekçinin olabileceği unutulmamalıdır, ancak bu,
ağdaki riski artırmanın maliyeti. Velayetin paylaşıldığı bir model
Gelecekte multi-sig cüzdanın anahtarlarını tutan farklı kurumlar da mümkündür. Rağmen
operasyonel olarak, basım / yazma / denetim daha fazla koordinasyon ve zaman
gerektirecektir. Güvenlik
Muhafızlardan herhangi birinin ihlali, güven kaybına neden olur ve kitlesel
para çekme. Bir tüccar ile güvenlik ihlali, tüm bekleyen belirteçler kadar çok daha az ciddidir
yine de saklama görevlileri tarafından yedeklenecek, ancak bunun yerine KYC / AML kullanıcı
verilerinin kaybolmasına neden olabilir.

Güven modeli

Varlıklar çalınabilir ya da
bire bir desteği onurlandırmayabilirler. Bununla birlikte, sarmalanmış çerçeve şunları
amaçlamaktadır:
bu güveni birkaç şekilde en aza indirin:

● Üç aylık denetimler, tamamının paketlendiğini doğrulamak için harici üçüncü taraflarca
yürütülecektir.
basılan jetonlar, tüm saklama görevlileri arasında depolanan eşit miktarda varlığa sahiptir. Durumda
WBTC, rezervlerin kanıtı adreslerden imzalar yayınlayarak gösterilebilir.
hangi bitcoin saklanır.
● Saklama sorumluları kendi başlarına jeton basamazlar, bunun yerine
bunu yapmak için bir tüccarın başlatılması. Bu nedenle, yeni tokenlerin oluşturulması her ikisini de
içerir
bakıcı ve tüccar.
● Kullanıcının, bir satıcı grubu aracılığıyla bakıcıyla etkileşime girmesi engellenmiştir
kurumlar. Bireysel bir tüccarın güvenilmesi gerekmez, bunun yerine
tüccarların birlikte olması gerekir.
● İlgili kurumların mevcut güvenilirliği, dahil olan tüm kurumlar için tehlikededir
çerçeve ile.

Şeffaflık

Sarılmış jetonun işleyişinde tam şeffaflık olacaktır. Tüm önemli ayrıntılar
ağ, bazıları aşağıdaki gibi bir gösterge tablosuna yansıtılacaktır:

● Ağda farklı roller üstlenen kurumların adları ve ayrıntıları
● Darphane ve yakma emirlerinin durumu (beklemede, işleniyor, iptal edildi, tamamlandı)
● Saklama görevlileri tarafından depolanan toplam BTC miktarı
● Ağdaki toplam WBTC miktarı (BTC ile aynı veya biraz daha düşük olacaktır
saklanmış)
● Saklama görevlisinin anahtarlara sahip olduğunu kanıtlayan işlemler şeklinde üç aylık denetimler
Bitcoin'e
● Tüccar ve Muhafızlar ethereum adresleri
● Satıcı tarafından kontrol edilen, her satıcıyla ilişkili Bitcoin adresi
● Açık kaynak belirteç sözleşme koduna / bir blok gezgininde konuşlandırılmış sözleşmeye
bağlantılar

Sayfa 14

Kontrol panelinin nasıl görünebileceğine bir örnek:

Sonuç

Sarılmış belirteçler aracılığıyla, varlıkları değiştirilebilir hale getirmek için bir çözüm öneriyoruz ve Ethereum zincirinde temsil edilebilir. Küresel likidite, artan kısmi sahiplik, akıllı sözleşme programlanabilirliği ve işlem ücretlerinde azalma, jetonlaştırma. WBTC, Dapps'ın Bitcoin'e kolay erişimini sağlayan bu tür ilk belirteç olacak. Herşey işlemler, sözleşmeler ve denetimler şeffaflığı korumak ve ağa güven. Çerçeve, aynı zamanda, kripto para birimi alanı, varlığın karşılaştığı ortak sorunları aşmak için farklı roller üstlenebilir desteklenen belirteçler.

Sayfa 15

Sözlük

Sorumlu - Varlığı tutan kurum veya taraf. WBTC durumunda bu, BitGo tarafından oynanır. Muhafizlar, jeton basmak için anahtarları tutarlar.

Tüccar - Paketlenmiş jetonların basılacağı ve yakılacağı kurum veya taraf. Satıcılar, paketlenmiş jetonun dağıtımında önemli bir rol oynar. WBTC söz konusu olduğunda, bu başlangıçta Kyber ve Cumhuriyet Protokolü ile oynanacak. Her satıcının onaylamak için bir anahtarı vardır yeni paketlenmiş jetonların basılması ve sarılmış jetonların yakılması.

Kullanıcı - Sarılmış jetonun sahipleri. Kullanıcılar, sarılmış belirteçleri kullanarak aktarabilir ve Ethereum ekosistemindeki diğer ERC20 belirteçleri gibi işlem yapın.

KYC (Müşterinizi tanıyın) - FINCEN ve OFAC'a göre Gerekli Yönergeler kurumlar, müşterilerin OFAC'a tabi olmadıklarını teyit etmek için bilgi aramalıdır. yaptırımlar, herhangi bir Banka Gizlilik Yasası kuralını ihlal eden veya potansiyel olarak parayla ilgili olanlar aklama faaliyetleri.

AML (Kara para aklamayı önleme) - Düzenleyici makamlar tarafından uygulanan kurallar ve düzenlemeler (ABD'deki Hazine Bakanlığı dahil) yasadışı fon kaynaklarını hedef almak ve bunlarla mücadele etmek için aklanabilir.

WBTC (Sarılmış Bitcoin) - Ethereum üzerinde Bitcoin tarafından 1: 1 desteklenen bir ERC20 jetonu.

Referanslar

[1] - https://etherscan.io/chart/gaslimit
[2] - https://www.coindesk.com/ethereums-growing-gas-crisis-and-whats-being-done-to-stop-it/
[3] - https://cointelegraph.com/explained/what-is-a-daico-explained
[4] - https://www.bitgo.com
[5] - https: // https: //kyber.network
[6] - https://republicprotocol.com
[7] - https://paritytech.github.io/wiki/Proof-of-Authority-Chains
[8] - https://wiki.parity.io/Aura
[9] - https://komodoplatform.com/atomic-swaps/