Sayfa 1

devir 5b

Sağlanabilir pTokens

DeFi ekosistemi için Sağlanabilir, taşınabilir ve sabitlenmiş bir çözüm.

pTokens.io
info@ptokens.io

Sayfa 2

Öz

Bu belge, DeFi DApp'lerin güvenli,
birden fazla finansal sistemin geliştirilmesini kolaylaştıran, tamamen denetlenebilir çapraz zincir tokenleri
merkezi olmayan türevler gibi araçlar.

pTokens.io
info@ptokens.io

---

3. Sayfa

İçindekiler

pTokens.io
info@ptokens.io

Giriş

Açık Finans olarak da bilinen Merkezi Olmayan Finans (DeFi), geniş bir kategoriyi temsil eder.
açık, merkezi olmayan ağlarda geliştirilmekte olan finansal uygulamalar. Amaç,
Kripto para birimlerine özgü, yeniden yaratan ve
eski finansal sistemi iyileştirir. Merkezi olmayan, öncelikle DeFi çözümleri
likiditeye erişmeniz gerekiyor. Kripto para birimi alanında, bu likidite genellikle ince bir şekilde yayılır
birlikte çalışamayan birden fazla blok zinciri ağında.

Şu anda, mevcut DeFi DApp'lerin büyük çoğunluğu aşağıdakilere dayalı çözümlerden oluşmaktadır:
Ethereum ağında yürütülen akıllı sözleşmeler. Bu akıllı sözleşmeler yalnızca
yerel Ethereum token Ether'i veya protokolün üzerine inşa edilen tokenları tüketmek için
ERC-20 standardı ve benzerleri.

Bu nedenle, merkezi olmayan finansmanın likidite açısından potansiyeli aşağıdakilerden biri ile sınırlıdır:
Ethereum ekosistemindeki Ether (ETH) ve Ethereum yerel tokenlerinden Bitcoin'e (BTC)
Bitcoin ekosistemi içinde, EOS ekosistemindeki EOS ve EOS yerel belirteçlerine ve
her bir blok zinciri protokolü için benzer şekilde. Zincirler arası birlikte çalışabilirlik bir anahtardır
Bu sınırlamanın üstesinden gelmek için öğe.

Terimler Sözlüğü

Sağlanabilir pTokens

Sağlanabilir pTokenler, kanıtlanabilir, taşınabilir ve sabitlenmiş bir belirteci tanımlar. Sağlanabilir bir pToken
yerel olmayan bir kripto para birimine bire bir sabitlenmiş bir belirteçtir.

pTokens teknolojisi ile idare edilir. Örneğin, Ethereum'daki bir pToken bir Ethereum'dur
ERC-20 jetonu, bire bir Ethereum tabanlı olmayan bir kripto para birimine sabitlendi.
Bu yazıda gösterim amacıyla, kullanılan ana blok zinciri Ethereum ve
kullanılan Ethereum dışı kripto para birimi EOS olacaktır.
Ortaya çıkan pToken, basitlik açısından ETH üzerinde pEOS olarak adlandırılır.
Ana bilgisayar blok zinciri açık olduğunda pEOS.

Yerel blok zinciri

Yerel blok zinciri, bir kripto para biriminin veya
belirteç tutturulmuştur.

EOS

PTokens karşı taraf varlığına örnek olarak kullanılan yerel olmayan kripto para birimi
bu belge boyunca. EOS, yerel olarak yetkilendirilmiş bir teminat kanıtı kripto para birimidir.
jetonlu EOS, şu anda EOSIO dışındaki ağlarda kullanılamaz.

Bu belgede örnek olarak EOS kullanılırken, aynı mantık ve süreç diğerleri için de geçerlidir.
blockchain ağları ve varlıkları.

Ana bilgisayar blok zinciri

Ana bilgisayar blok zinciri, yerel olmayanları barındıran hedef blok zinciri veya ağdır.
kripto para birimi veya belirteç.

Ethereum

Bu süreçte pTokenisation mekanizmasına örnek olarak kullanılan ana bilgisayar blok zinciri
belge. Ethereum, akıllı sözleşme özelliğine sahip, iş kanıtı merkezi olmayan bir ağdır.
işlevsellikler.
Bu belge örnek olarak Ethereum kullanırken, aynı mantık ve süreç aşağıdakiler için de geçerlidir:
diğer blockchain ağları ve varlıkları.

Peg-in işlemi

Sabitleme süreci, yerel olmayan bir kripto para biriminin
ana bilgisayar blok zinciri ile uyumlu başka bir dijital formata dönüştürülür ve
sonuç olarak böyle bir ana bilgisayar blok zincirine taşındı.
PTokens durumunda, peg-in işlemi otomatikleştirilir ve Trusted içinde gerçekleştirilir.
Yürütme Ortamları.

Peg-out işlemi

Peg-out süreci, tokenize edilmiş bir varlığın içinden geçtiği ters tokenizasyon sürecidir.
kullanılır ve orijinal biçimine geri döner.
PTokens durumunda, peg-out işlemi otomatikleştirilir ve Trusted içinde gerçekleştirilir.
Yürütme Ortamları.

Güvenilir Yürütme Ortamı (TEE)

Güvenilir Yürütme Ortamı, sistemden yalıtılmış bir hesaplama ortamıdır.
belirli bir cihazda çalışan ana işletim sistemi. Bu tür bir izolasyon, her ikisi aracılığıyla elde edilir
yazılım ve donanım tarafından uygulanan mekanizmalar.
Genel olarak, bir TEE, minimal bir arayüz ortaya çıkaran küçük ayak izli bir işletim sistemi çalıştırır.
cihazda çalışan ana işletim sistemine. Bu daha küçük ayak izi,
TEE'nin potansiyel saldırı yüzeyleri. Bu nedenle, TEE'ler uygulamaları aşağıdakilerle çalıştırabilir:
yüksek güvenlik
Gereksinimler,
böyle
gibi
kriptografik
anahtar yönetimi,
biyometrik kimlik doğrulama, güvenli ödeme işleme ve DRM. TEE örnekleri:
Akıllı telefonlarda yaygın olarak kullanılan ARM Trustzone tabanlı Güvenli Öğeler ve daha fazlası
yakın zamanda Intel Software Guard Extensions (SGX) Enclaves'i piyasaya sürdü.

Sayfa 6

Yerleşim bölgesi

Buradaki örtüşme, güvenilir bir yürütme ortamını tanımlamak için kullanılır.

Uzaktan Onay

Uzaktan doğrulama, bir cihazın donanım ve yazılımlarının kimliğini doğruladığı bir yöntemdir.
uzak bir ana bilgisayara yapılandırma. Uzaktan doğrulamanın amacı, harici bir partiyi
etkinleştirmektir.
cihaz üzerinde çalışan platformun bütünlüğüne güven sağlamak için.
Uzaktan doğrulama, genellikle cihazın imzalı bir belge oluşturmasını sağlayarak uygulanır.
bu, sistemin durumunu kanıtlar. İmzalama genellikle bir karma özet üzerinden gerçekleştirilir
kanıtlanacak kaynak kodun. İmza, özel bir onaylama anahtarı tarafından yapılır.
Üretimi sırasında cihaza gömülü ve üçüncü tarafın hangi anahtarın üzerinde
platformda çalışan uygulamanın kontrolü yoktur.
Bu onaylama anahtarı, cihazın üreticisi tarafından bilinir ve bu nedenle
bütünlük belgesini imzalayın ve platformun durumunu ve üzerinde çalışan kodu
tasdik talebini başlatan taraf.

Blockchain Oracle Mimarisi

Blok zincirlerinin gerektirdiği içsel determinizm nedeniyle, onların
harici veri kaynakları ile arayüz. Bu tür bir arayüze izin vermek için, bir blockchain-oracle
Ebedi veri kaynağına erişmek için gerekliyse, veri kaynağı tarafından tanınan bir formatta paketleyin.
blok zincirini kullanın ve bu verileri bir işlem biçiminde zincire koyun, böylece
dış veri belirleyici.
Yukarıdakileri gerçekleştirmek için bir blockchain-oracle 2015'ten beri Ethereum ağına hizmet veriyor
Oraclize LTD şeklinde, şimdi Provable Things LTD. 2015'ten beri Provable Things née
Oraclize, hizmetlerini sayısız veri kaynağından veri getirmeyi içerecek şekilde genişletti.
Ethereum dışındaki blok zincirleri için ve kriptografik olarak oracle'ları uygulamak
çeşitli TEE'lerin kullanımıyla veri getirme süreçlerini güçlendirir ve merkezden uzaklaştırır.
Güvenilir yürütme içinde çalışan bu aynı blockchain oracle hizmetini sağlayarak
Ortamlar, Provable Things geliştirebildi ve bir ademi merkeziyetçilik seviyesine ulaştı
kullanıcıların beklentileri ile uyumlu.
PTokens kullanım durumu için TEE, aşağıdakine benzer bir blockchain-oracle olarak düşünülebilir.
veri için hedefi yine Ethereum blok zinciri olan, ancak
Bu verilerin kaynağı, temel varlığın blok zincirindeki bir hesabın bakiyesidir.

7. Sayfa

Çok Taraflı Hesaplama

Çok Taraflı Hesaplama (MPC), dağıtılmayı sağlayan genel bir kriptografik ilkeldir.
tarafların kendi özel girdilerini ifşa etmeden keyfi bir işlevselliği ortaklaşa hesaplamaları
ve çıktılar.
MPC'nin temel bir özelliği, hesaplamanın belirli bir güvenliği koruma becerisidir.
bazı taraflar protokole gizlice girip kötü niyetle saldırsa bile.
Kriptografinin güvenlik ve bütünlüğü sağladığı geleneksel kriptografik görevlerden farklı olarak
iletişim veya depolama, düşmanın sistemin dışında bir varlık olduğunu varsayarak
katılımcılar (gönderen ve alıcıya kulak misafiri olan), bu modeldeki kriptografi
katılımcıların mahremiyetini birbirinden korur.
PTokens MPC bağlamında, dağıtılmış imzalamayı etkinleştirmek için kullanılır (bir eşik yoluyla
ağ doğrulayıcıları arasında peg-in ve peg-out işlemlerinin imza şeması).

pTokens ağı

PTokens ağı, pTokens sisteminin temelindeki merkezi olmayan altyapıdır.

Ağ, çok taraflı olarak ortaklaşa çalışan aktörlerin, doğrulayıcıların çalışma alanıdır.
gerçekleştirmek için gerekli anahtar çiftlerini oluşturmak ve yönetmek için enklavlar aracılığıyla
hesaplama
varlıkların çapraz zincir hareketi.

Doğrulayıcı

Doğrulayıcı, pTokens ağı içinde bir veya daha fazla yerleşim bölgesi işleten bir aktördür.
bir veya daha fazla TEE özellikli cihaz. PTokens ağının her bir doğrulayıcısı koordinatları ve
çok partili hesaplamalar yapmak için ağın diğer doğrulayıcıları ile işbirliği yapar.

Çok imzalı Cüzdan

Yetkilendirmek için birden fazla özel anahtardan imzalar gerektiren bir kripto para birimi cüzdanı
işlemler.

DApp'ler

Arka uç mantığı bir akıllı sözleşme veya başka bir tarafından desteklenen Merkezi Olmayan bir
Uygulama
bir blok zincirinde komut dosyası oluşturma tekniği.

---

8. Sayfa

DeFi DApps

Çeşitli kullanımları kapsayan çok yönlü merkezi olmayan finans uygulamaları için şemsiye terim
merkezi olmayan borsalar ("DEX'ler"), borç verme ve borçlanma, türevler gibi durumlar,
marj ticareti ve tahmin piyasaları.

DeFi Yaklaşımları

WBTC - Federe Bir Yaklaşım

WBTC, Bitcoin'i ERC20 formatına standart hale getirerek Bitcoin için akıllı sözleşmeler oluşturur. Bu
Bitcoin, Ethereum'un akıllı sözleşmelerinin sağladığı daha büyük mantıktan yararlanmasını sağlar,
madeni paranın yeteneklerini basit transferlerin ötesine genişletmek. Bire bir pegging
BTC'den WBTC'ye, özel anahtarları yöneten federe bir aktör grubu tarafından garanti edilir
WBTC neslinin giriş noktası olarak kullanılan bitcoin çoklu imzalı cüzdanın arkasında.
Yazma sırasında tek sorumlu ortak BitGo'dur.

Yetki Kanıtı Ağı (POA)

Bir POA Ağı hem özel hem de açık, genel, izinli bir blok zinciri olabilir. Ulaşmak için
küresel devlet üzerinde fikir birliği, bir Yetki Kanıtı fikir birliği algoritması kullanır.
kimliği bir menfaat biçimi olarak kullanır. Bir grup doğrulayıcı ("yetkililer"),
blok zinciri ve işlemlerini ve bloklarını doğrulayın.

Provable pTokens Yaklaşımı

Provable pTokens yaklaşımı, çapraz zincir hareketini merkezden uzaklaştırmaktır.
Birlikte mümkün kılan güvenilir hesaplama ve çok partili hesaplama yoluyla kripto para birimleri
güvenli
çapraz zincir
işlem imzalama
yetenekler
arasında
iki
geleneksel olarak
birlikte çalışmayan blok zincirleri. Bu şekilde iki farklı kripto para birimi olabilir
güvensiz ve merkezi olmayan bir şekilde tutulan bire bir çivileriyle değiş tokuş edildi,
likiditenin zincirler arasında sorunsuzca akmasına izin verir.

PTokens Mimarisi

Sayfa 9

Bu yazıda gösterim amacıyla, kullanılan yerel blok zinciri EOS ve
kullanılan ana blok zinciri Ethereum olacaktır. Bunun için Ethereum ve EOS protokollerinin seçimi
Her iki ağın da belirteçli varlıkları destekleme kapasitesi verildiğinde örnek alınmıştır,
çift yönlü çapraz zincir bağlantısının mümkün kılınması. Bu örnek EOS'u gösterir
Ethereum blok zincirinde taşınması için tokenizasyon süreci. Aynı süreç
Ether (ETH) ve Ethereum tabanlı tokenlar için ters yönde uygulanmalıdır.
EOS'a taşındı.
EOS-Ethereum kullanım durumu için sunulan mantık ve süreçler, herhangi bir
varlık ve herhangi bir blok zinciri.

Genel Bakış

Bu yazıda açıklanan pEOS pToken, aşağıdaki altyapı parçalarını gerektirir:
1. Bir EOS tam düğümü.
2. Bir Ethereum tam düğümü.
3. TEE'lerin içinde çalışan enklavları güvenli hale getirin.
4. Özel alanları birlikte oluşturmak ve yönetmek için işbirliği yapan bir onaylayıcılar ağı
peg-in / out işlemi için anahtarlar.
Her iki tam düğüm de, blokların kaynağı olarak mahal bölgesine iletilmek üzere gereklidir.
istenen pToken çiftini oluşturan zincirlerin durumuyla senkronize olmasını sağlayın.
Harici taraflar da bu senkronizasyona yardımcı olmak için mahalleye bloklar gönderebilir.
merkezi olmayan moda.
Enklav, her ikisi için de özel anahtarların karşılık geldiği güvenli sanal alanı temsil eder.
Blok zincirleri oluşturulabilir, depolanabilir ve her iki fonun da işlem imzalaması için kullanılabilir.
ve pTokens'ı yakar. Enklavın kendi güvenli ortamında yürüttüğü diğer mantık,
gelen blokları ve işlemlerini doğrulamak için kullanılır, yalnızca geçerli işlemlerin yapılmasını sağlar
her iki zincirden de eşit ve zıt işlemsel muadillerinin imzalanmasına neden olabilir
yerleşim bölgesi tarafından.

Sağlanabilir pTokens Yolculuğu

Jetondan pToken'e (bu örnekte EOS'tan pEOS'a) yolculuk,
aşağıdaki şekilde:
1) Kullanıcı, EOS pTokens para yatırma akıllı sözleşmesine EOS yatırır.
bir EOS işleminde gerekli olan "not" alanında istenen hedef ETH adresi.
2) Önceki işlemin gerçekleştiği blok enklav'a sunulur,
tüm işlemleri ve eylemleri ile birlikte.
3) Enclave, EOS blok başlığını tüm işlemlerle birlikte doğrular.

---

4) Doğrulandıktan sonra, enklavlar EOS'a gönderilen pToken işlemini bulur
akıllı sözleşme yapın ve EOS miktarını ve hedef ETH adresini ayrıştırın.
5) 4. Adımdaki verileri kullanarak enklavlar, MINT'e eşit miktarda bir işlem hazırlar.
ETH akıllı sözleşmesinde pEOS belirteçlerinin sayısı.
6) Enklavlar, işlemi müştereken imzalamak için çok taraflı bir hesaplama gerçekleştirir.
türetilmiş ETH özel anahtarı.
7) Enklavlar işlemi yayınlar.
8) İşlem, Ethereum blok zincirine yayınlanır.
9) İşlem çıkarıldıktan sonra, yeni basılan pEOS jetonları artık
Adım 1'de kullanıcı tarafından sağlanan hedef ETH adresi).
PEOS'tan EOS'a sohbet yolculuğu şu şekilde gerçekleşir:
1) Kullanıcı, ETH akıllı sözleşmesinde "yazma" işlevini çağırır. Fonksiyon iki alır
parametreler; yakılacak pEOS miktarı ve istenen değeri temsil eden bir "dize"
hedef EOS adresi.
…
2) ila 8) arasındaki adımlar, ETH'den bahseden yukarıdakiyle aynıdır
EOS ile değiştirildi

…
9) İşlem onaylandıktan sonra
EOS blok zincirinde, EOS
smart-Contract, EOS depozitosundan istenen miktarda EOS aktarır
Adım 1'de kullanıcı tarafından sağlanan hedef EOS adresine adres)
Bu örnek için Ethereum ve EOS protokollerinin seçimi,
çift yönlü çapraz zincir bağlantısı. Şimdiye kadarki süreç izlenirken
EOS'tan pEOS'a yolculuk, ters yönde bir köprü de mümkündür
her iki ağın da belirteçli varlıkları destekleme yeteneği sayesinde.
Ters yolculuk (bu örnekte ETH'den pETH-on-EOS'a) Ethereum'u
ana blok zinciri olarak yerel blok zinciri ve EOS ve aşağıda yer almaktadır
tavır:

Sayfa 11

1) Kullanıcı, ETH pTokens para yatırma akıllı sözleşmesine ETH yatırır,
istedikleri hedef EOS adresini sağlamak.
2) Önceki işlemin gerçekleştiği blok,
tüm işlemleri ve eylemleri ile birlikte enklav.
3) Enklavlar, tüm işlemlerle birlikte ETH blok başlığını doğrular.
4) Doğrulandıktan sonra, enklavlar ETH'ye gönderilen pTokens işlemini bulur
smart-contract ve ETH miktarını ve hedef EOS adresini ayrıştırır.
5) 4. Adımdaki verileri kullanarak enklavlar, MINT'e bir işlem hazırlar.
EOS akıllı sözleşmesindeki pETH jetonlarının miktarı.
6) Enklavlar, işlemi EOS özel anahtarı ile ortaklaşa imzalar, yani
böyle bir özel anahtarı hesaplayan bir dizi doğrulayıcının ortak çabasının sonucu
her bir aktörün katıldığı bir Çok Taraflı Hesaplama tekniğini takip ederek
ortak imzalama, enklavlar içinde mühürlenmiş özel bir anahtardan yararlanır.
7) Enklavlar işlemi yayınlar.
8) İşlem, EOS blok zincirine yayınlanır.
9) İşlem çıkarıldıktan sonra, yeni basılan pETH tokenleri artık
Adım 1'de kullanıcı tarafından sağlanan hedef EOS adresi).
Bu yazıda gösterim amacıyla, kullanılan iki protokol,
Ethereum ve EOS. Bununla birlikte, sistem, olanak sağlayan esnek özellikler sunar.
çeşitli türlerin belirtilmesi için uygulanacak benzer bir işlem
kripto para birimleri ve belirteçler.
Uygulama ayrıntıları
EOS ve ETH anahtar çiftinin oluşturulması
Enklavlar secp256k1 eliptik eğri kriptografik ilkelleri uygular (her ikisi tarafından da kullanılır)
EOS ve ETH protokolleri) asimetrik anahtar çiftleri oluşturmak için doğrudan
güvenli enklav TEE'lerin şifrelenmiş belleği. Oluşturulduktan sonra, her anahtar normal olarak
Güvenilir Yürütme Ortamı (örneğin, SGX) sözlüğünde "mühürlenmiş",

---

Sayfa 12

veriler, imalat tarafından donanıma eklenen özel anahtar kullanılarak şifrelenir,
diske kaydedilmeden önce. Yalnızca verileri mühürleyen mahfaza şifresini çözebilir. Bu verir
özel anahtarların güvenliğine ilişkin güçlü garantiler.
İkinci süreç, her bir mahfaza, her biri için kullanılabilen anahtar çiftlerine güvenli erişim sağlar.
etkileşim kurduğu zincirler, adım 6) 'da gerekli işlemleri birlikte imzalamasına izin verir.
yukarıdaki yolculuk.
Her TEE mahfazasında oluşturulduktan ve mühürlendikten sonra, bu tür anahtar çiftleri,

toplu olarak bir ana anahtar çifti üretin, bu anahtar çiftinin her bir anahtarından türetilir.
Çok Taraflı hesaplamaya katılan aktörler. MPC ilkel, katılımcıların
birbirlerinden mahremiyet sağlarken, dağıtılmış enklav operatörlerinin ortaklaşa hesaplamasını sağlar
Çapraz zincir hareketini gerçekleştirmek için gereken işlemleri imzalayacak anahtar çiftleri
varlıklar.
Enklavlar sistem için ekstra bir kalkan görevi görerek sistemi ekonomik ve pratik hale getirir.
kötü niyetli bir doğrulayıcının ağa saldırması sakıncalıdır. Birden fazla TEE varsayılması
teknikler, anahtar çiftlerini korumak için bir güvenlik duvarı olarak benimsenmiştir.
düşman tarafından başarılı bir şekilde gerçekleştirildiğinde, bunun birden fazla katmanını atlaması
gerekirdi.
koruma manevrası keşfedilmemiş güvenlik açıklarını kontrollü bir şekilde farklı
ilgili Güvenilir Yürütme Ortamlarının korumaları ve eşzamanlı olarak çoğaltma
çok partili hesaplamaya katılan her yerleşim birimi operatörü için böyle bir hack.

Gönderimi Engelle

Enklavların saldırı yüzeylerini azaltmak için ağ bağlantısı yoktur.
Bunun yerine, birlikte çalıştığı zincirlerin her biri için bloklar enklavın içine itilir. Kimse
bir blok gönderebilir. Enclave, blok başlığını ve işlem girişlerini doğrular
bir bloğun kabul edilip edilmeyeceğini düşünmeden önce. Blok bu doğrulama adımını geçtiyse
ve enklavın beklediği bir sonraki blok, blok enklav tarafından kabul edilecek ve
işlemleri ayrıştırıldı. PToken'larla ilgili herhangi bir işlem bulunursa, imza adımları
üstlenilecek. Enklav, bir bloğun nereden geldiği konusunda agnostiktir ve
sadece bir bloğu kabul ederken kriptografik geçerlilik.

Blok Doğrulaması

Gelen ETH blokları, ilk önce bunları içindeki zincir başına serileştirerek enklav tarafından doğrulanır.
Sorunun formatı daha sonra bu sonucu karma haline getirip, sonuçta yer alan blok karması ile
karşılaştırarak
blok başlığı.
Gelen EOS blokları, ilişkili imza için genel anahtarın kurtarılmasıyla doğrulanır.
blok başlığı ile ve bilinen EOS blok doğrulayıcıları listesiyle karşılaştırarak.

İşlem Doğrulama

Enklavın işlemlerle ilgili ayrıntıları bilmesi için imzalamak için imzalaması gerekir.
pEOS nane veya EOS jetonlarını taşıyın, ilgili bir blok içeren bir bloğun tüm işlemleri
işlemlerin söz konusu blokla aynı anda sunulması gerekir. Şunlar
işlemler daha sonra serileştirilir ve kökü keşfetmek için bir merkle ağacına eklenir.
ağacın karması. Bu kök karması daha sonra beklenen işlem kök karması ile karşılaştırılabilir
zaten doğrulanmış blok başlığında yer alır.

Ölçeklenebilirlik

TEE enklavları tarafından sunulan güçlü güvenlik garantileri,
akıllı sözleşmeler, Provable pTokens altyapısının herhangi bir sayıda çalıştırılmasına izin verir
tamamen ayrı TEE özellikli donanım üzerine yerleştirilmiştir. Buna izin vermek için yeni yerleşim
bölgeleri
çevrimiçine getirilir ve kaynak kodlarının geçerliliği başlamadan önce uzaktan doğrulanması
pToken kodunu çalıştırma.

Güvenlik

Uzaktan doğrulama ve açık kaynak kodlu TEE yerleşim birimlerinin doğal güvenliği
kod, ilgilenen tarafların çalışan enklav örneklerini bağımsız olarak denetlemesine olanak tanır. Alenen
Mevcut kod, enklavın üstlenebileceği ve gerçekleştiremeyeceği her süreci açıklığa kavuşturur,
uzaktan doğrulama, açık kaynak kodunun gerçekte var olan şey olduğunu doğrularken
enklavda idam edildi. Bu nedenle, enklav yazarları bile kötü niyetli veya
kapalı özel anahtar güvenliğini tehlikeye atabilecek gizli giriş noktaları
enklav kodunun açık kaynaklı doğası.

Koruma için bir güvenlik duvarı olarak birden fazla Güvenilir Yürütme Ortamı tekniği benimsenmiştir.
anahtar çiftleri, her biri farklı olan ve birden çok katmandan oluşan bir kalkan görevi görür.
diğerlerini tamamlayıcı. Bir saldırının düşman tarafından başarıyla gerçekleştirilmesi için (
kötü niyetli doğrulayıcı veya harici bir saldırgan), bunun birden çok katmanı atlaması gerekir.
koruma manevrası keşfedilmemiş güvenlik açıklarını kontrollü bir şekilde farklı
tüm ilgili Güvenilir Yürütme Ortamlarının korumaları. TEE teknolojisi şu şekilde hareket eder:
sistem için ekstra bir kalkan, onu ekonomik ve pratik olarak bir
sistemin güvenliğini tehlikeye atmak için düşman.
Ek olarak, böyle bir saldırının her yerleşim birimi operatörü için çoğaltılması gerekir.
işlem (ler) i imzalamak için kullanılan anahtar çiftleri olarak çok partili hesaplamaya katılmak
Yukarıdaki yolculuğun 6. Adımında şart koşulduğu üzere, her birinin içinde mühürlenmiş tek anahtar çiftleri değildir.
enclave, daha ziyade bunların bir kombinasyonundan türetilen anahtar çiftleri.
Çok Taraflı Hesaplamanın kullanılması, enklav operatörlerinin işbirliği yapmasını ve gerçekleştirmesini sağlar
hepsi bağımsız olarak harici olarak doğrulandıktan sonra varlıkların zincirler arası hareketi
blok zincirlerinin koşulları.

Sayfa 14

PTokens için uygulamalar

Tamamen denetlenebilir çoklu blok zinciri finansal işlemlerin güvenliğini sağlayın

Blok zinciri ekosistemi büyüyor ve farklı ağlar arasındaki parçalanma
operatörler ve kullanıcılar için artan bir sorun. Şu anda, arasındaki değişim noktaları
kripto para varlıkları genellikle takas ve ticaret platformlarıdır.
Bu platformlar şunları sunar:
kullanıcılar için mükemmel erişilebilirlik, ancak denetlenebilirlikten yoksundur,
birlikte çalışabilirlik ve ademi merkeziyetçilik; her değişim platformunun farklı bir güven modeli vardır,
ancak çoğu kapalı kaynaktır ve bir emanetçi yönetişim modeli kullanır.
Bunun yerine uygulanabilir pTokenler, tasarım gereği tamamen denetlenebilir ve saklama güven modeli
operatörden uzağa bir TEE'ye geçti. Sağlanabilir pTokens ile blockchain parçalanması
artık sorun olmayacak çünkü pTokens denetlenebilir, güvenli ve
çoklu blok zinciri finansal işlemleri için merkezi olmayan değişim noktası.

ETH DeFi DApp'leri için harici likiditeyi artırın

Daha önce belirtildiği gibi, DeFi ekosistemi iki şeye şiddetle ihtiyaç duyuyor; artan likidite,
ve Fintech bürokrasisini büyütmek ve aşmak için birlikte çalışabilirlik. Ayrılmak yerine
Geçici olarak uygulamak için DApp geliştiricilerine kadar birlikte çalışabilirlik, Sağlanabilir
pTokens, DApp üzerinde daha fazla çalışmaya gerek kalmadan bu birlikte çalışabilirliği sağlayacaktır.
geliştiriciler bölümü.
Nitekim, pEOS belirteci durumunda, her Ethereum DApp EOS için erişilebilir hale gelir.
sahipleri ve tersi. Daha fazla pToken entegrasyonuyla Provable, DApp'ı artırmayı hedefliyor
birçok blok zinciri arasında büyüklük sırasına göre birlikte çalışabilirlik, herkes için likiditeyi artırıyor
katılan zincirler. Bu, DApp operatörleri için zaman veya çaba harcamayı gerektirmez ve
DApp kullanıcıları için hala sorunsuz bir DeFi deneyimini koruyor. pToken sahipleri kendi
güvenlikle ilgilenmelerine gerek kalmadan zincirler arası para birimleri ve
zincirler arası pimleme işlemleri.

Sayfa 15

Sonuç

Bu yazıda, güvenli ve merkezi olmayan güvenlik için ölçeklenebilir ve merkezi olmayan bir çözüm sunduk.
tamamen denetlenebilir çoklu blok zinciri finansal işlemleri. Mimari, güvenilen
bilgi işlem teknolojileri ve güvenli, kurcalamaya karşı korumalı olarak çalışmak için kod yürütme kanıtı
kaynağı yayınlanan ve üçüncü taraf denetlenebilir ortamlar. Bu ekstra olarak hareket eder
çok partili hesaplamaları çalıştıran doğrulayıcılar ağı üzerinde koruma kalkanı
pToken'ların ilgili temel varlıklarına sabitlenmesini garanti ederek sistemi yapar
merkezi olmayan ve güvenli.

Bu yazıda tanıtım amaçlı olarak, kullanılan yerel blok zinciri EOS ve ana bilgisayardır
kullanılan blockchain Ethereum'dur. Bu örnek için Ethereum ve EOS protokollerinin seçimi
her iki ağın da belirteçli varlıkları destekleme yeteneği verilmiş ve
iki yönlü çapraz zincir bağlantısı sergilemek mümkündür. Bu örnek EOS'u açıklar
Ethereum blok zincirine taşınması için tokenizasyon süreci ve süreç
Ether (ETH) ve Ethereum tabanlı tokenlerin EOS üzerinde hareket ettirilmesi için ters yön.
Ethereum-EOS kullanım durumu için sunulan mantık ve süreçler, herhangi bir
varlık ve herhangi bir blok zinciri.

pTokens.io
info@ptokens.io