İçindekiler

VDex Tanıtım Belgesi v0.1.0

Volentix Labs Ekibi info@volentixlabs.com

19 Temmuz, 2018

satılabilir, belirli bir amaca uygun, kullanılabilir veya çalışır halde olduğu; (ii) bu tanıtım belgesinin içeriğinin hatasız olduğu; ve (iii) burada yer alan içeriklerin üçüncü taraf haklarını ihlal etmediği. Volentix Labs ve iştirakleri, olası zararlar hakkında bilgi sahibi olsa bile, bu tanıtım belgesine veya bu belgede yer alan içeriğe istinaden, bunlara atıfta bulunulmasından veya bunlara güvenmekten doğan herhangi bir zarardan sorumlu değildir. Hiçbir durumda Volentix veya bağlı kuruluşları, herhangi bir zarar, kayıp, yükümlülük, masraf veya hasar için herhangi bir kişiye, doğrudan veya dolaylı hukuki ve cezai sorumluluk sahibi olmayacaktır. Bu belgede yer alan herhangi bir içeriğin kullanımı, bunlara atıfta bulunulması veya bunlara güvenilmesi, bunlarla sınırlı olmamak üzere, herhangi bir iş kaybı, gelir, kar, veri, kullanım, şerefiye veya diğer maddi olmayan kayıplar yaşanması halleri de bu sorumsuzluk bildirimine dâhildir.

Özet

VDex, kullanıcı topluluğu dikkate alınarak geliştirilmiş merkezi olmayan bir takas borsasıdır. Bu eşler arası takas borsası, en yeni paradigmalar ve etkinliği kanıtlanmış güvenlik protokolleri, kullanım kolaylığı ve çok sayıda menkul kıymet desteği sunarak, tüm açık standartlara uymaktadır ve merkezi olmayan uygulamalar arasında uyumlu ve kesintisiz bir akış sağlar. Akıllı EOS.IO sözleşmelerinden oluşan bir koleksiyon sayesinde; güvenlik, anonimlik, ödeme hızı, likidite ve kar marjı için kullanımı kolay seçenekler içermektedir. Açık sipariş defterleri, diğer tüm merkezi olmayan borsalarla entegre şekilde çalışarak devasa bir "takas borsalarının borsası" oluşturmakta ve ona bağlı olan tüm borsaların likiditesi ile etkinliğini arttırmaktadır. VDex, aynı zamanda kullanıcıları için daha yüksek likiditeye erişim sağlayan bir DApps ağı olan Volentix ekosisteminin destekleyici bir sütunudur.

1 Giriş

VDex; hız, maliyet, anonimlik, güvenlik ve ölçeklenebilirlik için son derece özelleştirilebilir bir ortam sağlayan ve dağıtık ağ üzerinde çalışan bir takas borsasıdır. Üst düzey kullanıcılara seçme ve gelişme özgürlüğü sağlanırken, yeni kullanıcılar merkezi bir sistemde bulunan risklerden uzak, özgür bir deneyim elde ederler. Ürün, 2. nesil blok zinciri uygulamalarının en iyi yönlerini benimsemiş bir mimari üzerine kurulu olduğundan hızlı bir şekilde büyümeye açıktır. VDex'in geliştirilmesinde genel olarak 3. nesil blokzinciri teknolojileri ve merkezi olmayan EOS.IO işletim sistemi kullanılmış olup, tüm bunlar Volentix gereksinimlerini karşılamak için günümüzün en iyi protokolleri, paradigmaları ve modelleri ile birlikte başarılı bir şekilde entegre edilmiştir.

2 Metodoloji

Bu makaledeki tüm varsayımlar, EOS.IO'nun **cleos** komut satırı araçları kullanılarak tarafımızca geliştirilmiş olan özel EZEOS yazılımıyla prototipler oluşturularak doğrulanmıştır. Bu yazılıma şu adresten ulaşılabilir: https://github.com/Volentix/ezeos

3 Volentix

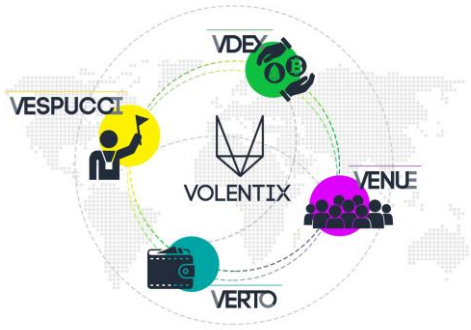
Volentix ekosistemi, birbirinin etkinliğini artıran DApp'lardan (dağıtık ağ üzerindeki programlardan) oluşur. Dört "destek sütunumuz", tüm Volentix ekosistemini destekleyen bir dizi DApp'tır ve her biri farklı bir ihtiyacı karşılar. VDex açısından, Volentix DApp'larının amacı, VDex kullanıcılarının sayısını artırmak ve böylelikle kullanıcıların faydalanabileceği likiditeyi artırmaktır.

- **Venue**
  Volentix topluluğunun büyümesine yardımcı olur
- **Verto**
  Kullanıcılarının menkul kıymetlerini VDex'i kullandıkları süre boyunca düzenli olarak yönetebilmesini sağlar
- **Vespucci**
  VDex üzerindeki jetonlara olan güveni artırır
- **VDex**
  Tüm kripto para birimleri arasında likidite akışı sağlar

3.1 Venue dinamik topluluk platformu

Venue, Volentix topluluğunun üyelerini bir araya getiren ve VTX'in dağıtımını kolaylaştıran ve Volentix projesine daha fazla farkındalık kazandıran bir platformdur.

Venue'nin ilk tekrar eden uygulaması, VTX'in dağıtımı için bir platform olmaktır. VTX ödülleri, topluluk oluşturma kampanyalarına katılarak, hata düzeltmeleri göndererek veya centilmenlik kampanyalarını tamamlayarak elde edilebilir. Bu web uygulamasında, kullanıcı katılımını gösteren skor tabloları ve canlı metrikler mevcuttur. İlk imza kampanyası 13 Temmuz 2018 tarihinde https://bitcointalk.org/ forumunda başlatılmıştır. Daha fazla bilgi için lütfen ***https://venue.volentix.io*** adresini ziyaret edin.



Resim 1:

3.2 Verto cüzdanı

Verto, VDex için geliştirilen bir çoklu para cüzdanıdır. Tüm Volentix platformlarının merkezi bileşenidir ve kullanıcıların kendi özel anahtarlarının sürekli ve güvenli bir şekilde muhafaza edilmesini sağlamak için gereklidir. Verto, takas işlemi yapan iki müşteri arasındaki durumu koruma altına almak için akıllı sözleşmelerden oluşan bir sistem kullanır. Bu bağlamda, en basit işlemler, atomik takaslar ile gerçekleştirilir.

3.3 Vespucci analitik motoru

Vespucci, hem takas edilebilir dijital menkul kıymetler hakkında analitik bilgi veren, hem de bu varlıkları karşılaştırmak için kullanılabilen grafik ve araçları sağlayan bir uygulamadır. Vespucci, kullanıcı güvenini artırarak ve daha fazla kullanıcıyı Volentix platformuna çekerek likiditeyi artırır. Vespucci, verilerini şu gibi kaynaklardan toplar: blokzinciri kaşifi siteleri, sohbet odaları, web siteleri, geçmişteki ticari kayıtlar, forum mesajları, plan analizleri, ticaret eğilimleri, geliştirici faaliyetleri, dijital varlık dağılımları, yönetim bilgileri, kullanım şart ve koşulları, geçmişteki blokzinciri adres bakiyeleri.

3.4 VDex

VDex, kullanıcıların kişisel ve kamusal anahtarlarının saklandığı Verto cüzdanı üzerinden kripto para birimi takas hizmetlerini sunar. Kripto varlıklarının takası, merkezi bir operatör tarafından jetonların geçici olarak muhafaza edilmesini gerektirmez. Bu nedenle, VDex, kullanıcıların sahip oldukları jetonların zilyetliğini kaybetmeden takas edilmelerine izin verir. Ayrıca, VDex, gerekli tüm işlemler tamamlanana kadar dijital jetonların sahiplerinin cüzdanında kalmasını sağlar. VDex, birçok farklı kripto para biriminin takasını desteklemektedir ve farklı pazar türlerine uyum sağlamak için birden çok likidite havuzuna ev sahipliği yapmaktadır. VDex, bu havuz ve ağlarda ticaret yapmayı mümkün kılan özgün ve merkezi olmayan bir sipariş

defteri sistemi, çoklu likidite havuzları ve kapsamlı güvenlik önlemleri ile ön plana çıkmayı başarır.

3.5 VTX

VTX, yukarıda izah edilen sütunlar arasında dolaşan ve onların iletişim kurmasını sağlayan para birimidir.

4 Mimari

4.0.1 Genel bilgi

Zincirler ve cüzdanlar arasında herhangi bir kripto para birimiyle işlem yapmak için, sözleşme ve betik bilgilerini içeren cüzdanlar gereklidir. Örneğin, Bob ve Alice arasındaki bir işlem, sağlanan bu sözleşmeler kullanılarak birbirlerinin hesabına para göndermeleri suretiyle gerçekleşir. Bu sözleşmelerle ilgili ayrıntılı bilgi, atomik takas belgelerinde bulunabilir. [15] Bu sözleşmelerin, zaman aşımı süresi içinde paylaşılan sırlar vasıtasıyla birbirlerine karşı garantileri vardır. Aksi halde, bir geri ödeme gerçekleşir. Belirli bir işlem için teminat temin etmenin çeşitli yolları veya bir ağın likiditesinin nasıl artırılabileceği, bu belgenin ilerleyen bölümlerinde açıklanacaktır.

4.0.2 İşletim sistemi

EOS.IO, merkezi olmayan uygulamaların oluşturulabileceği işletim sistemi benzeri bir çerçevedir. Bu yazılım; kümeler arasında hesaplar, kimlik doğrulama, veri tabanları, eşzamanlı olmayan iletişim ve zamanlama bilgilerini sağlar. Bileşenler ve protokoller zaten platformun içinde mevcuttur ve VDex gereksinimlerini karşılamak için sadece bir alt küme kullanılması yeterlidir. VDex, başlangıçta EOS.IO'nun hesap ve cüzdan oluşturma ve çalınan anahtarların kurtarılması gibi standart özelliklerden yararlanır, ancak ayrıca sözleşmeler ve sağlanan araçlar aracılığıyla merkezi olmayan takas borsalarının oluşturulması için gerekli protokolleri uygular. [10]

1. **Bağlamsız Eylemler**
   Ethereum tarafından önerilen ölçeklenebilirlik tekniklerinin çoğu (Sharding, Raiden, Plasma, State Kanalları) çok daha etkili, paralelleştirilebilir ve pratik hale gelirken, aynı zamanda bloklar arasındaki iletişimi hızlandırır ve sınırsız ölçeklenebilirlik sağlar. Bir Bağlamsız Eylem, yalnızca işlem verilerine bağlı olan, ancak blokzinciri durumuna bağlı olmayan hesaplamaları içerir. Örn: Paralel işlenen imza doğrulamaları

2. **İkili Sayı Sistemi/JSON çevrimi**

EOS sözleşmeleri, JSON'un okunabilirliği ile ikili sayı (binary) sisteminin verimliliğini birleştirir.

3. **Paralelleştirme ve optimizasyon**
   Kimlik doğrulamayı uygulamadan ayırmak, daha hızlı işlem süreleri sağlar ve bant genişliğini artırır. EOS.IO blokları, her 500 ms'de bir üretilir.

4. **Web Montajı (WMNT)**
   Web montajı (web assembly), hem yüksek performanslı web uygulamalarını mümkün kılar ve hem de her bir uygulamayı kendi sanal alanı içerisine hapseder. Bu, VDex'e ağ erişimi ve dosya sistemi ad alanı kısıtlamaları, zorlanmış kural tabanlı yürütme ve hangi süreçlerin ortaya çıktığı konusunda daha iyi bir kontrol sağlar.

5. **Rust/C++ sözleşmeleri**
   Bu belge hazırlandığı sırada, C ++, WMNT için en iyi araçlara ve yürütme hızlarına sahipti. C ++, örneğin Ethereum sözleşmeleri için kullanılan Solidity'den çok daha olgun bir dildir. Ayrıca, yıllar boyunca test edilmiş ve güvenilir işlevsellik sağlayan kütüphanelerin yanı sıra, daha iyi bir hata ayıklama desteğine de sahiptir. EOS kod tabanı da çok ağır şablon kullanımlarına sahiptir. Örneğin, C ++, birimlerin çalışma zamanı maliyetsiz doğrulamasını tanımlamak için şablonların ve operatörün aşırı yüklenmesinin kullanılmasına izin verir. Hafıza yönetimi, akıllı sözleşmelerin oluşturulmasını çok daha kolay hale getirir çünkü program her mesajın başında mevcut durumun temizlenmesi için yeniden başlar. Ayrıca, dinamik bellek tahsisini uygulamaya nadiren ihtiyaç duyulur. Web montajı çerçevesi, belleğe yanlış giden herhangi bir işlemi otomatik olarak reddeder. EOS.IO sözleşmeleri C ++ 14 kullandığından, dinamik bellek ayırma gerekliyse akıllı işaretçilere başvurabilir. PARSEC'in ilk uygulaması Rust'tır.[20]

6. **Şema tanımlanmış mesajlar ve veri tabanı**
   Hizmet sözleşmeleri, veri modellerinin uyumunu ve birlikte çalışabileceklerini garanti etmek için standartlaştırılmıştır. *Standartlaştırılmış Hizmet Sözleşmesi* tasarım ilkesi, hizmet sözleşmelerinin standart veri modellerine dayandığını savunur. Hizmetler arasında değiş tokuş edilen yaygın iş belgelerini bulmak için servis envanter planları üzerinde analiz yapılır. Bu iş belgeleri daha sonra standartlaştırılmış bir şekilde modellenir. Kanonik Şema modeli, veri modeli dönüştürme tasarımlarının uygulanmasına olan ihtiyacı azaltır. [9]

4.0.3 Sözleşmeler Arası İletişim

Veriler, zincirdeki verileri bir araya getiren bir işlem oluşturan bir kahin (oracle) yoluyla sözleşmeler arasında paylaşılır. "Bir kahin, blokzincirleri ve akıllı sözleşmeler bağlamında gerçek dünya olaylarını bulan ve doğrulayan ve bu bilgileri akıllı

sözleşmeler tarafından kullanılmak üzere blokzincirine gönderen bir ajandır." [3] Her düğümde bu verinin tıpatıp aynı bir kopyası vardır. Veri, bu nedenle akıllı bir sözleşme hesaplamasında güvenle kullanılabilir. Akıllı sözleşmeler veriyi blokzincirinden çekerken, kahinler onu blokzincirine gönderir. Verilerin çoğu, blok zincirinin durumunu izleyen ve yanıt olarak belirli eylemleri gerçekleştiren yoklama düğümcükleri (blokzinciri oturumu) aracılığıyla okunur.

4.0.4 Yan Zincirler

EOS.IO'da, jetonların atanması yan zincir oluşturan bir süreçtir. Yan zincirler, bir blokzincirindeki jeton ve diğer dijital varlıkların ayrı bir blokzincirinde güvenli bir şekilde kullanılmasına ve gerektiğinde orijinal blokzincirine geri taşınmasına izin veren mekanizmalardır. İşlemin verimliliğini artırmak için farklı görevlerin dağıtıldığı çoklu yan zincirler olabilir. Zincirler arası iletişim için, EOS.IO protokolü kanıtları değerlendirmek amacıyla zincirler arasında TCP benzeri bir iletişim kanalı oluşturur. Her bir parça (bir döngüdeki paralelleştirilebilir yürütme birimi) için, geçici bir paylaşımlı merkle kökü oluşturmak amacıyla bu eylem taahhütlerinden dengeli bir merkle ağacı oluşturulur. Bu, paralel hesaplama hızını artırmak için yapılır. Blok başlığı, bu dengeli merkle ağacının köküdür. Yapraklar ise, paylaşımlı merkle ağaçlarının kendi bağımsız kökleridir. [10]

4.0.5 Likidite

Bir jetonun global jeton ekonomisine etkin bir şekilde katılabilmesi için, alım satım hacminin, alıcılar ve satıcılar arasındaki eşleşmelerin istikrarlı bir "tesadüfen benzeşen talepler" [11] havuzunu oluşturtabilecek bir miktarı geçmesi gereklidir. Bir takas borsası içindeki bu güvenilirlik, likidite olarak bilinir. Fiyatını önemli ölçüde etkilemeksizin satın almak veya satmak mümkün ise, bir jetonun "likit halde" olduğu söylenebilir.

1. Loopring protokolünün, düğüm olarak işlev gören EOS.IO sözleşmelerinin kullanımı ile uygulanması.[25]
2. jetona istikrar getirmek için kullanılan Bancor algoritmasının uygulanması.[11]
3. VDex ağındaki Vespucci analizlerine göre, bu protokoller ve atomik takaslar (HTLC) arasında geçiş yapmak.

4.0.6 Tek şifreli ve zaman kilitli sözleşmeler (Atomik Takaslar)

Tek Şifreli ve Zaman Kilitli bir sözleşme (HTLC)[15], zaman aşımı süreleri olan işlemler içeren özel bir akıllı sözleşme çeşididir. Kullanıcılara işlemleri için değişken bir zaman kilidi oluşturabilme seçeneği sunulur. Seçilen süre ne kadar uzunsa, işlem masrafları da o denli az olacaktır.

4.1 Ağ Topolojisi

4.1.1 Düğümler

Düğümler, VDex ağının uç noktalarıdır. İşlevleri şunlardır:

1. Verto cüzdanı aracılığıyla, bir VDex portalı haline gelmek.
2. Sipariş defteri kayıtlarını diğerleri ile birleştirmek.
3. Sipariş defteri kayıtlarını düzeltmek.
4. Sipariş iptallerini yönetmek.
5. **Raft** protokolü için zaman aşımı sürelerini belirlemek
6. Tamamlanmış siparişler için sözleşmeleri başlatmak.

Düğümler, yaptıkları her işlem için bir ücrete hak kazanır. Ancak yeterli bakiyeye ve iyi bir sicile sahip olan kullanıcıların Verto cüzdanları bir düğüm görevi üstlenebilir.

4.1.2 Toplayıcılar

VDex toplayıcıları, simülatör ve güvenlik amacıyla kullanılan adanmış Volentix sunucularıdır. İşlevlerinden biri, sistemdeki anormallikleri algılamak için izinsiz giriş [16] analizi amacıyla kullanılmak üzere kayıtlar ile sipariş defteri verilerini düğümlerden toplamak ve sıralı dağıtılmış temsilciler haline getirmektir. Toplayıcılar, ayrıca meta zincir defterleri [4], blockchain kazıyıcıları ve Vespucci bileşenleri gibi diğer bileşenlere de ev sahipliği yapmaktadır.

4.1.3 Gecikme

EOS.IO blok onay süresi, düşük gecikmeye (0,5 saniye) sahiptir. [10] Bu gecikme, işlem gören para birimlerinin eşit derecede hızlı blokzincirlerinden çıkartılması durumunda sağlanabilir. Aksi takdirde, gerçekleşen işlem en yavaş blok zinciri kadar hızlıdır (örneğin, bir Bitcoin blokunu kazımak, bu yazının hazırlandığı sırada 9 dakikayı buluyordu). İşlem tamamlandıktan sonra, bir işlem makbuzu oluşturulur. Bir işlem tek şifresi (hash) almak, işlemin onaylandığı anlamına gelmez; Bu, sadece bir düğümün onu hatasız kabul ettiği anlamına gelir. Ancak elbette, diğer üreticilerin de onu kabul etmeleri son derece yüksek bir olasılıktır.

4.2 Sipariş Defteri

Bir sipariş defteri, bir dizi siparişten oluşur ve VDex, alıcıların ve satıcıların ilgilendiği şeyleri kaydetmek için bu defteri kullanır. Eşleştirme motorumuz, hangi siparişlerin yerine getirilebileceğini belirlemek için bu defteri kullanır. Sipariş defterleri, bu gereksinimi karşılamak için maliyet, güvenlik, hıza ve bu şartları yerine getirmek için sipariş defterinde hangi protokolün kullanılacağına göre ayarlanabilir. Örneğin, Loopring protokolü, diğer sipariş defterleri ile birlikte çalışabilmek için sipariş defterinin değiştirilmesine zaten izin

vermektedir. [25] Aynı durum; PARSEC, RAFT veya Bancor gibi her biri kendi özel avantajlarını sunan diğer kısıtlayıcı olmayan fakat etkili protokoller için de geçerlidir. Örneğin Loopring, ringfuffer (FIFO) veri yapısındaki alt-halkaları kontrol eden çok iyi bir ön-çalışma koruma kademesine sahiptir, Bancor formülü ise jetonların stabilize olduğundan emin olmak ya da likidite yaratmak için kullanılabilir. Öte yandan, PARSEC ya da RAFT, bu araştırmada henüz değinilmeyen basit ve verimli merkezi olmayan çözümler de sunmaktadır. Toplayıcılar üzerinde yer alan kahinlerin oluşturduğu model aracılığıyla ortaya çıkan kuralları kuralı baz alarak sipariş defteri uzlaşma yöntemlerini değiştirebilme yeteneği, VDex'in dengeli bir şekilde çalışmasını sağlamak için başka bir önlem yerine geçmektedir.

Yukarıdaki bilgiler ışığında, EOS.IO tarafından sağlanan konteynerlerin en iyi performansı sağladığını söylemek mümkündür. [17] Sipariş defteri morfolojisini birleştirmek için bu konteynerleri kullanmak en optimum sonuçları sağlar.

4.2.1 Örnek Veri Yapıları

1. Loopring FIFO ilk-giren-ilk-çıkar dairesel tamponu (protokol tarafından önerildiği gibi). Düğümler, sipariş defterlerini bir kullanıcının siparişini görüntüleyip eşleştirmek için herhangi bir şekilde tasarlayabilir. Limit emirlerinin sadece fiyata bağlı olarak belirlendiği bir OTC modeli takip edilir. [25]
2. EOS.IO kalıcı API. Sipariş defteri, aynı EOS.IO hesabında düğümler arasında paylaşılan güçlü çoklu-indeks konteynerinden faydalanır.

4.2.2 Zincir içindeki sipariş defteri

Zincir içindeki bir sipariş defteri, onu çözmek için seçilen cüzdan (düğüm) üzerinde bulunan tekliflerin bir kaydıdır. Her düğümün aynı hesaba abone olduğu kalıcı bir veri tabanında, diğer tüm düğümler (cüzdanlar) ile birlikte bulunur.

4.2.3 Zincir dışındaki sipariş defteri

Toplayıcılarda yer alan çevrimdışı sipariş defterleri, simülatör ve güvenlik amaçlı olarak kullanılır. İki defterin çözümü arasındaki sürede oluşturulan bu defter, kendi defterini oluşturmak için mümkün olduğunca çok sayıda düğümden kayıt toplar. Şu anda, düğümler zincir içindeki sipariş defterlerine yerleştirilmektedir ve her iki sipariş defteri de aynı olmalıdır.

4.2.4 Sipariş defteri çözümünün merkezi olmayan bir hale getirilmesi

Merkezi olmayan bir sistem oluşturmak için, düğümler Sipariş Defterini çözmek için sıraya girer. Çözüm düğümü, protokol tarafından belirlenmeli ve tüm düğümlerden

gelen tüm sipariş defteri girişleri, çözüm düğümleri için erişilebilir olmalıdır. RAFT [7] ve PARSEC [20] protokolleri zarif ve basit çözümler sunar. RAFT konseptinin uygulanması kolaydır ve PAXOS [16] zamanından beri kullanılmaktadır. PARSEC oldukça yeni ama daha etkilidir, yansıtılmış düz ağaçlı grafikleri kullanarak kayıtları kopyalama ihtiyacını ortadan kaldırır.

4.3 Sipariş çözümü

Sipariş defteri için bir FIFO konteyneri bulunması halinde, çözüm şu şekilde gerçekleşir:

1. Alt-halkaların kontrolü. Bu işlem, halka sırasının başlangıçtaki ile aynı olup olmadığını kontrol ederek güvenliği artırır.
2. Yük Dengeleme (Doluluk oranı/stok durumu)
3. Oran, kullanıcı tarafından belirlenen orijinal alış oranına eşit veya ondan daha azdır (Limit emirlerinin tanımlanması)
4. İşlem iptalleri
5. Siparişler, tamamlanan ve iptal edilen miktarların tarihine göre ölçeklendirilir

4.4 VTX

VTX, VDex takas borsasında kullanılan kripto para birimidir. Volentix sistemini destekleyen dört unsurun hepsinde de kullanılabilir:

1. VDex işlem masraflarını ödemek için.
2. VTX kullanıcılarına verilen oy hakkını kullanarak, ağa gönderilen tekliflerde oy kullanmak için.
3. Ağa teklif göndermek için.
4. Projenin inşasına, likiditeye veya teklif incelemelerine destekte bulunmak için.
5. VDex takas borsası üzerinde masrafların yeniden dağıtılması amaçlı kullanılacak bir jeton olmak için.
6. Kullanıcıları sipariş defteri çözümlerine katılmak amacıyla teşvik etmek için.
7. Fikir birliği ve Venue kampanyalarında kullanıcıları ödüllendirmek için.

4.4.1 Jeton yaratımı

EOS.IO çerçevesindeki **eosio.token** sözleşmesi, 1,3 milyar arz ile 2.1 milyar EOS.IO uyumlu jeton yaratmakta kullanılacaktır.

4.4.2 İlk Jeton teklifi

Dağıtım

1. **Kurucular**
   Projenin kavramlaştırma, planlama ve başlangıç sürecindeki ilk destekleyicileri.

2. **Öncül çalışmalar, çekirdek ekip**
   Yazılım mühendisleri, blokzinciri analistleri, hukuk uzmanları ve iş geliştirme uzmanlarından oluşur. Çekirdek ekibine ek olarak, Volentix, projeyle ilgili çeşitli alanlardan uzmanların oluşturduğu bir danışmanlar kuruluna sahiptir.

3. **Merkezi olmayan hazine**
   Topluluk projeleri, ticari faaliyetler ve projenin devam etmesi için gerekli olan maaşlardan oluşan kamuya açık fonlar. Yapılan her işlemin küçük bir yüzdesi, bu amaçlarla kullanılmak üzere hazineye geri döner.

4. **Devam eden geliştirme işlemleri**
   Çekirdek ekip için teşvikler. Bunlar, hedeflenen kilometre taşlarına ulaşıldıktan sonra proje boyunca verilen bonuslardır.

Tablo 1: Jeton dağıtımı

Yaratılan jetonların yüzdesi	fiyat	Zamankilidi
35% Gelecekteki Merkezi Olmayan Hazine		
5% İlk Finansman	0.000016-0.000020 BTC	
28% Dağıtım	0.000021 BTC+	
12% Kurucular		evet
10% İlk Çalışmalar, Takım ve Danışmanlar		evet
10% Devam Eden Geliştirme İçin Teşvik		

Topluluk satışı oylamasının gerekçeleri. Asıl satış öncesi VTX sahipleri, kurucuları ve çekirdek ekibi, Volentix topluluğunun bir topluluk satışına ihtiyaç duyup duymadığını anlamak için bir artırılmış oylama [6] gerçekleştirdi. Artırılmış oy sistemi, seçmenlerin topluluk satışı ile ilgili gerçekleri kabul ettiklerini kanıtlayan kolay bir test yapmasını gerektirir. Bu test şebekesinin hazırlanması sürecine katılan katılımcılar, topluluk satışları hakkındaki gerçeklerden bahseden yayınları derler ve ödül olarak VTX

kazanırlar. Sonuçta, tüm seçmenler konuyla ilgili aynı düzeyde bilgiye sahip olarak oy kullanma fırsatı elde ederler.

Çoklu imza hesapları. Toplanan fonlar, kurucuların sahip olduğu çok sayıda imzalı bir hesaba yatırılacak ve yalnızca üç kişiden en az ikisinin rızasıyla kullanılabilir olacaktır.

4.4.3 Masraf modeli

İşlem masrafları

1. İşlem masrafları herhangi bir para birimiyle ödenebilir.

2. İşlem masrafları, belirli hesaplara atanabilir

3. Geliştiriciler tarafından genel bakım masrafları için toplanan küçük bir ücret

Kilit süresi masrafı

Tek Şifreli ve Zaman Kilitli bir sözleşme (HTLC)[15], zaman aşımı süreleri olan işlemler içeren özel bir akıllı sözleşme çeşididir.

1. Kullanıcılar, fonlarını 24 saatliğine kilitleyebilir ve işlem ücreti ödemekten kurtulabilir

2. Kullanıcılar, fonlarını 24 saatten daha uzun bir süre için kilitleyebilir ve VTX jetonu kazanabilir

Sipariş defteri çözüm masrafları Bir cüzdan, bir düğüm haline gelebilir ve sipariş defteri çözümlerini yapmak karşılığında VTX jetonları kazanabilir

.

EOS.IO EOS.IO platform üzerinde takas işlemi yaparken aşağıdaki hususlar geçerlidir:

1. Bir sözleşme oluşturmanın belirli bir ücreti vardır, ancak kullanımı ücretsizdir.
2. Geliştiriciler, sözleşme oluşturmak için EOS.IO jetonları biriktirmelidir. Sözleşme yok edildikten sonra, ilgili jetonlar iade edilecektir.
3. DApp'lar, kaynaklarını sözleşmeler, bellek, işlemci ve bant genişliği için ayırmalıdır.
4. Kaynaklar için gerekli olan ödemeyi kimin yapacağına DApp karar verir.

5. Bir işlemdeki birden çok mesaj ve birden çok hesap, aynı iş parçacığına atanabilir.

Bütçe tahmini Henüz merkezi olmayan takas borsaları kabul görmediğinden ancak bu durum kısa bir süre içinde gerçekleşeceğinden, VTX'in değerinin 5 yıldan biraz daha uzun bir süre içinde talebe göre artış göstereceğini söylemek mümkündür.

4.5 Zincir içi iletişim

EOS.IO, zincir içi iletişim kanıtlarını zorlanmadan işleyebilecek şekilde tasarlanmıştır. IBC kanıtlarını işlemek ve geçerliliğini tesis etmek için yeterli kapasiteye sahip olmayan zincirler için, güvenilir bir kâhin/emanete indirgeme seçeneği vardır. EOS.IO tabanlı akıllı bir sözleşmeyle diğer para birimi işlemlerini doğrudan kontrol etmek için, emanetteki para birimini barındıran güvenilir bir çok imzalı cüzdan, kaynak zincirindeki IBC provizyonlarına dayanan transfer işleminin imzalanmasını/yayınlanmasını sağlamak için kullanılabilir.

4.6 Güvenlik modeli

4.6.1 Giriş

Bu bölümde yapılan varsayımlar, toplanan bilgilerdeki analizler vasıtasıyla elde edilmiştir. Tam güvenlik testi, devam eden prototip aşamasından sonra başlayacaktır.

VDex ortamıyla ilgili potansiyel güvenlik problemleri, aşağıdaki senaryoların benzerleri olarak kategorize edilebilir:

1. Saldırgan, bir işlem içinde zararlı bir kod çalıştırır
2. İşlemlerin sıralaması manipüle edilir
3. Bir blokun zaman mührü manipüle edilir

4.6.2 Yapılacak eylemler

1. Gelen veriyi filtrelemek
    (a) Blokzincirleri ve sipariş defteri çözümlerinden gelen veri.
    (b) Düğümlerden gelen veri
    (c) Cüzdandan gelen veri
    (d) Toplayıcılardan gelen veri
2. Giden veriyi filtrelemek
    (a) Sipariş iptali
    (b) Teslimat

4.6.3 Sözleşme güvenliği

1. Fonların büyük bir çoğunluğunu zaman-gecikmeli ve çok imzalı bir hesapta tutmak
2. Sıcak cüzdanlarda tüm para çekimlerini birden çok kez kontrol eden bağımsız işlem/sunuculara sahip olan çoklu imzalar kullanmak
3. Yalnızca MTB (müşteri tanımlama bilgileri) doğrulaması yapılmış hesaplara para çekilmesine izin veren ve hesapları beyaz listeye almak için çoklu imza gerektiren özel sözleşmeler yaratmak
4. Yalnızca MTB doğrulaması yapılmış hesaplardan gönderilen ve tanınan jetonları kabul eden özel bir sözleşme yaratmak
5. Tüm para çekimleri için 24 saat zorunlu bekleme süresi gerektiren özel bir sözleşme yaratmak
6. Tüm imzalama ve hatta otomatik para çekim işlemleri için bile donanım cüzdanları kullanılmasını gerektiren sözleşmeler yaratmak
7. Hatalı sözleşmeleri güncellemek için kesintisiz çalışan bir sistem geliştirmek
8. Bir sözleşmenin işlevselliğini duraklatma özelliği
9. Sözleşmede tanımlanmış bir faaliyeti erteleme özelliği

4.6.4 Denetim süreçleriyle zararlı yazılım tespiti

Sistem, toplayıcılar üzerinde bulunan yapay zekâ (AI) analizi yoluyla, bir işlem süresi içindeki zararlı yazılım ve yetkisiz uygulamaları tespit edebilmek için gerekli olan bilgiyi sağlar.

4.6.5 Rastgele çeşitlendirme

Seçim sürecinde RAFT protokolünü kullanarak, değişen zaman aşımı sürelerine sahip olan belirli bir rastgelelik elde edilir. Protokollerin değiştirilmesi, oldukça karmaşık bir süreçtir.

4.6.6 Çok faktörlü doğrulama

Birçok mevcut uygulamada olduğu gibi, bu tedbir oldukça etkilidir ve kullanıcılar tarafından büyük ölçüde benimsenmiştir.

4.6.7 Kayıtlar

Kontrol amaçlı olarak kayıtların incelenmesini sağlamak.

1. Raft.

2. Yapay zeka destekli anomali tespiti (Numenta).
3. Bazı jeton harici alımlarla ilgili adreslerin betik incelemeleri.

4.6.8 Biriktirme Kanıtı Olarak İşlem (BKOİ)

1. Referans veren bloku ilgilendirmeyen çatallarda bir işlemin tekrar edilmesini önler
2. Belirli bir kullanıcının ve biriktirdiklerinin yine belirli bir çatal üzerinde olduğunu doğrudan ağa bildirir.

4.6.9 Çoklu harcama

Çoklu harcama, sabit miktardaki jetonların birden çok işlem için kullanılmasına neden olan bir saldırı türüdür.

1. Birbiriyle çakışan iki işlemi hızlı bir şekilde ağa göndermek. Buna "yarış saldırısı" da denir.
2. Bir işlemi belirli bir blokta önceden kazımak ve bloku serbest bırakmadan önce aynı jetonları harcayarak o işlemi geçersiz hale getirmek. Buna *Finney* saldırısı adı verilir.
3. Her işlemi tersine çevirebilmek için ağdaki toplam işlem gücünün %51'ini control etmek ve bloklarda ortaya çıkan işlemler üzerinde tam kontrol sahibi olmak. Buna "51 saldırısı" denir. EOS.IO, Loopring veya Raft'a göre bunu yapmak imkansızdır. Bir blok üreticisi gereğinden fazla bir çalışma süresi talep ederse veya yeterince karlı değilse, o süreç kara listeye alınır.[25]

4.6.10 Ön koşucular

Birinin başka bir düğümün takas çözümünü kopyalamasını ve havuzdan bir sonraki işlemden önce çıkarmasını önlemek için, işlem başına daha yüksek bir ücret alınır.

Sipariş eşleştirmesi için herhangi bir protokolde ön çalışmada kullanılan ana şema, sipariş tablosudur: Bir ön koşucu, bekleyen bir sipariş defteri çözüm işleminden bir veya daha fazla emir çalabilir. Hem EOS.IO, hem de Loopring'in bu sorun için geliştirdiği çözümler vardır. Her iki durumda da anahtarlar, zincirdeki işlemin bir parçası değildir ve bu nedenle sipariş defteri çözüm düğümü dışındaki taraflarca bilinmemektedir. Düğümler, siparişleri nasıl yönettiklerini dikte eder. Her bir düğüm, sipariş defterlerinin çözümlenmesi için farklı bir teknik kullanır ve güvenliği teşvik etmek için başka bir rastlantısallık düzeyini tetikler.

4.6.11 Sahte kimlikler

Kötü niyetli ve/veya sahte kimlikli kullanıcılar, Loopring düğümlerine saldırmak için çok sayıda küçük sipariş gönderebilir. Bununla birlikte, bu siparişlerin çoğu, eşleştiğinde tatmin edici bir kazanç sağlamadığı için reddedilmektedir. Her halükarda, düğümler siparişleri nasıl yöneteceklerini dikte etmelidir.

4.6.12 Yetersiz Bakiye

Kötü niyetli kullanıcılar, değeri sıfır olmayan ancak ilgili adresinde sıfır bakiye olan siparişleri imzalayıp dağıtabilir. Düğümler, bazı siparişlerin gerçek bakiyesinin sıfır olduğunu görebilir ve bu sipariş durumlarını uygun şekilde günceller ve ardından bunları yok sayar. Düğümler, bir siparişin durumunu güncellemek için zaman harcamalıdır, ancak kara listeye alma ve ilgili siparişleri düşürme gibi yöntemlerle çabalarını en aza indirmeyi de seçebilir.

4.6.13 Zamanlama saldırısı

Zamanlama saldırıları, bir üçüncü taraf gözlemcinin, kriptografik algoritmaları yürütmek için harcanan süreyi kaydedip analiz ederek şifreli verilerin içeriğini çıkarabileceği bir kriptografik saldırı türüdür. Raft algoritmasında zaman aşımlarının rastgele olması, bu saldırıyı (örneğin) sipariş defteri seviyesinde engeller. Cüzdan ile ilgili olarak, eliptik eğri kriptografisinin dikkatli kullanımı, arka kapı (backdoor) girişlerini önleyebilir.

4.6.14 EOS.IO'nun diğer güvenlik özellikleri

1. Zincir içi paralelleştirme için kilitler veya karşılıklı dışlanan objeler (mutex) kullanılmaz
2. Tüm hesaplar, sadece kendi özel veri tabanlarında okuma/yazma yetkisine sahiptir

4.7 Zincir içi güvenlik

Yabancı bir zincire gönderilen işlemler, yabancı zincirdeki bazı tesislerin güvenilmez olmasını gerektirir. İki EOS.IO temelli zincir bulunması durumunda, yabancı blok zinciri, güvenilir olmayan kaynaklardan gelen blok başlıklarını ve gelen işlemleri kabul eden akıllı bir sözleşmeyi yönetir ve menşe zincirinden oldukları kanıtlanabilir olduğu takdirde gelen işlemlere güvenebilir. IBC kanıtlarını işlemek ve geçerliliğini tesis etmek için yeterli kapasiteye sahip olmayan zincirlerde, seçenekler güvenilir kâhinlere/emanet hesaplarına dönüşür.

4.8 Çoklu blokzinciri

Çoklu blokzinciri bilgileri; blokzinciri zaman çizelgeleri paralel sırada (durum değişimi sıklığına göre) ve anlaşılabilir bir veri yapısı halinde toplanarak elde edilebilir. Bu sayede, sistem çok zincirli yük dengeleyicilerini harekete geçirebilir; aktarım durumları akıllı sözleşmelerden veri çıktıları çekebilir ve yabancı bloklarda işlemlerin yürütülmesini tetikleyebilir. Göreli blok mesafesi, göreceli global durum ve zaman mührü olayları, işlemleri yerel zincirde gerçekleşmeden önce optimize etmek ve onaylamak için global bir deftere kaydedilir. Bu sistem, optimum likiditeyi seçmek için zincirler arasındaki blok üretim tesadüflerini belirlemek için kullanılabilir.[4]

4.9 Kullanıcı deneyimi

Simülatör Daha iyi ve güvenli bir kullanıcı deneyimi sağlamak için, VDex çeşitli senaryoların kullanılabileceği bir simülatöre sahiptir.

Şablonlar Standart işlemler için kullanımı kolay şablonlar tedarik edilmektedir.

Kapsamlı, özelleştirilebilir ve detaylı arayüz

1. Tüm pazarı ve fiyat dalgalanmalarını gösterir
2. Cüzdan bakiyesini ve önceki işlemleri gösterir.
3. Dâhili vergi hesaplayıcı ile ayrıntılı bir geçmiş bilgisi gösterir.
4. Gelişmiş özellikler devreye alınıp devreden çıkartılabilir.

4.10 Gerçek merkeziyetsizlik

Merkeziyetsizleştirme, planlama ve karar alma süreçlerinin merkezi bir yer veya gruba bağlı olmaması anlamına gelir.

EOS.IO, merkezi olmayan uygulamalar için ücretsiz, açık kaynaklı ve ölçeklendirilebilir bir altyapıdır. Demokratik delegasyona sahip bir pay kanıtı (DPoS) konsensüsünü kullanarak, adil ve şeffaf bir blok yapımcı (BP) seçim sürecini sağlamaya çalışır. İnsan etkileşimlerinin öngörülemezliği ve hedeflenen amacın karmaşıklığı, pragmatik olarak ilk aşamalarda küçük bir miktar merkezileşmenin gerekebileceğini gösterir. Ancak zamanla merkezileşmeye olan ihtiyacı azaltacak kriterlerin uygulanması gereklidir. Her hâlükârda, bu takas borsası, merkeziyetsizliği teşvik etmek için çeşitli mekanizmalara sahiptir. Örneğin, sipariş defterleri çözümünde düğümleri seçmek için kullanılan sistem ortak bir merkezi saat veya (DPoS) kullanmaz, ancak bir seçimdeki (RAFT) liderlerin belirlenmesi için rastgele zaman aşımlarına ya da PARSEC protokolünde olduğu gibi grafik teorisini (DAG) kullanmaya dayanır.

4.11 Sistem kurtarma

Defterin en son sürümünün her zaman ortaya konulduğundan emin olunduğu sürece, RAFT ve PARSEC protokolleri, düğüm hatası durumunda sistem kurtarma işlemleri için sağlam bir Zemin sağlar. IBC durumunda yerel bloklarla ticaret için güvenlik önlemleri de sağlanmaktadır. Zincirin tanımlanmaması durumunda, bir sonraki bloğa kadar beklemek veya kısa süreli bir zaman kilidi oluşturmak için yerel kuralların uygulanması da mümkündür.

4.12 Ölçeklenebilir ve modüler mimari

İnovasyon potansiyelini güvence altına almak için, sistemin bileşenleri tarafından önerilen ilkeler, kavramlar ve paradigmalar, teknolojilerin ayrışmasından yana olmalıdır. Ayrık ve merkezi olmayan sistemler oluşturmak ve sürdürmek çok karmaşık olduğundan, farklı stratejiler kullanmak gereklidir:

4.12.1 Problem ayrışması

Problem çözme stratejisi şu şekilde uygulanır: Bir problemi alt problemler haline getirme, alt problemlerin her birini çözme ve daha sonra alt problem çözümlerinden orijinal problemin çözümünü oluşturma.

4.12.2 Etki alanını küçültme

Dinamik programlama ve şablon kullanımı; karmaşıklık ve hata ayıklama sorunları nedeniyle zordur. Yerleştirme koşulları normal programların yürütülmesi için önemsiz gibi görünebilir. Bu modellere ve ilk tasarımdaki detaylara özen gösterilmesi, bileşenlerin kolayca değiştirilmesini veya eklenmesini sağlarken, verimliliği de en üst seviyeye çıkaracaktır. Kazanılan paranın CPU, bant genişliği ve RAM'a bağlı olduğu dikkate alındığında, bu durum daha da fazla önem kazanır.

5 Katkılar

Volentix için herkese açık yazılım deposu şu adreste bulunabilir: https://github.com/Volentix. Bu depoya yapılan tüm katkılar ve öneriler gözden geçirilecek ve entegre edilecektir.

6 Risk

VDex üzerindeki işlem sayısının ne kadar olacağını tahmin etmesi zor olsa da, merkezi olmayan borsalara olan artan ilgi bağlamında, daha fazla işlem daha fazla risk doğuracaktır. Merkezi sağlayıcılar için para işlemleri risklerini yönetmek, her daim zorlu bir süreç olmuştur. Bir ağın güvenini kazanmak, uzun ve zahmetli bir süreçtir.

Merkezi olmayan borsaların da farklı bir şekilde evrimleşmesi beklenmemelidir. Ancak onlar, merkezi olan takas borsalarından farklı olarak, oluşan problemleri çözmek ve takas miktarını arttırmak için hızla katkıda bulunan açık kaynak geliştirici topluluğunun desteğine sahip olabilirler.

7 Teşekkür

Bu belge hakkındaki yorumları için Ulusal ve Kapodistrian Atina Üniversitesi Bilişim ve Telekomünikasyon Bölümü'nden Profesör Yiannis Emiris'e teşekkür ederiz.

8 Sonuç

Verimliliğini korurken sadelikleriyle öne çıkan yapılar, kavramlar ve protokoller; mikro servisler oluşturulduğunda dikkatli şekilde ilerleyen işlevsellik beklentileri ile bileşenlerin kolayca eklenebileceği veya değiştirilebileceği kapasitede bir sistem kuran modüler bir tasarımın uygulanmasını sağlar. Bu belgede değinilen bazı varsayımlar hala doğrulanmaya devam etse de, VDex mimarisinin yönü, değişen teknolojik ekosisteme uyum ve tepki verebilen oldukça esnek ve modüler bir MVP kullanılarak belirlenmiştir. Bunun için EOS.IO işletim sistemi, Loopring, Bancor, RAFT ve PARSEC protokolleri kullanılmıştır.

Kaynakça

Referanslar

[1] Aelf, *A multi-chain parallel computing blockchain framework*, (2018).

[2] ARK, *A platform for consumer adoption*, (2018). [3] blockchainhub.net, *blockchain-oracles*, (2017). [4] BlockColliderTeam, *Block collider white paper*, (2018).

[5] V. Buterin, *Ethereum: a next generation smart contract and decentralized application platform*, (2013).

[6] S. Cormier, *A machine based societal model for curbing citizen cynicism*, (2017).

[7] J. O. Diego Ongaro, *In search of an understandable consensus algorithm*, (2018).

[8] M. Duncan, Quale, *Halo platform*, (2018).

[9] T. Earl, *Soa principles of service design*, (2016).

[10] EOS.IO, *Eos.io technical white paper v2*, (2018).

[11] G. B. Eyal Hertzog, Guy Benartzi, *Bancor protocol: Continuous liquidity for cryptographic tokens through their smart contracts*, (2018).

[12] S. D. K. M. T. S. H. Garcia-Molina, *The eigentrust algorithm for reputation management in p2p networks*, (2018).

[13] M. R. Garrick Hileman, *Global cryptocurrency benchmarking study*, (2017).

[14] Komodo, *An advanced blockchain technology, focused on freedom*, (2018).

[15] K. Kurokawa, *Atomic cross chain transfer, an overview*, (2015).

[16] L. Lamport, *The part time parliament*, (1998). [17] D. Larimer, *eosio.boot telegram chat*, (2018).

[18] Q. Liquid, *Providing liquidity to the non-liquid crypto economy*, (2018).

[19] S. R. M.P.M-S, Aniket Kate Matteo Maffei, *Concurrency and privacy with payment-channel networks*, (2017).

[20] F. H. Q. M. S. S. Pierre Chevalier, Bart lomiej KamiÂťnski, *Protocol for asynchronous, reliable, secure and efficient consensus (parsec)*, (2018).

[21] SingularityNET, *A decentralized, open market and inter-network for ais*, (2018).

[22] M. M. Timo Hanke ve D. Williams, *Dfinity technology overview series consensus system*, (2018).

[23] A. B. Will Warren, *0x: An open protocol for decentralized exchange on the ethereum blockchain*, (2017).

[24] G. Wood, *Ethereum: A secure decentralised generalised transaction ledger.ethereum project yellow paper*, (2014).

[25] F. Zhou, Wang, *Loopring: A decentralized token exchange protocol*, (2018).

[9] [3] [10] [5] [24] [13] [25] [23] [19] [11] [12] [14] [2] [8] [18] [21] [22] [7] [1] [4] [6]