

Sayfa 1

Tether: Bitcoin blok zincirindeki Fiat para birimleri Özet . İtibari para birimi ile desteklenen bir dijital jeton, bireylere ve kuruluşlara tanıdık bir muhasebe birimi kullanırken sağlam ve merkezi olmayan değer alışverişi yöntemi. The blok zincirlerinin yeniliği, denetlenebilir ve kriptografik olarak güvenli bir küresel defterdir. Varlık destekli Token ihraç edenler ve diğer piyasa katılımcıları blockchain teknolojisinden faydalanabilir. tanıdık, daha az değişken para birimleri ve varlıklar ile işlem yapmak için gömülü fikir birliği sistemleri ile. İçinde Hesap verebilirliği sürdürmek ve döviz fiyatında istikrarı sağlamak için bir yöntem öneriyoruz. tethers adı verilen bir kripto para birimi belirteci arasında tek bir rezerv oranını korumak ve ilişkili realworld varlığı, fiat para birimi. Bu yöntem Bitcoin blok zincirini kullanır, Proof of Yedekler ve verilen jetonların tamamen desteklendiğini ve tamamen rezerve edildiğini kanıtlamak için diğer denetim yöntemleri zamanlar. 1

Sayfa 2

İçindekiler İçindekiler Giriş Teknoloji Yığını ve Süreçler Tether Teknoloji Yığını Fon Akışı Süreci Rezerv Kanıtı Süreci Uygulama Zayıf Yönleri Ana Uygulamalar Borsalar için Bireyler için Tüccarlar için Gelecek Yenilikler Multisig ve Akıllı Sözleşmeler Ödeme Gücü Yeniliklerinin Kanıtı Sonuç Ek Denetim Kusurları: Borsalar ve Cüzdanlar Mevcut Fiatpegging Sistemlerinin Sınırlamaları Piyasa Riski Örnekleri Hukuk ve Uyum Terimler Sözlüğü Referanslar 2

3. Sayfa

Giriş Dünyada insanların özgürce bir değer deposu olarak seçtikleri çok çeşitli varlıklar vardır. işlem ortamı veya bir yatırım. Bitcoin blok zincirinin daha iyi bir teknoloji olduğuna inanıyoruz bu varlıklar için işlem yapmak, depolamak ve muhasebeleştirmek. Çoğu tahmin, küresel serveti 250 civarında ölçüyor trilyon dolar [1] bunun büyük bir kısmı bankalar veya benzeri finans kurumları tarafından tutulmaktadır. Göç Bitcoin blok zincirindeki bu varlıklar, orantılı olarak büyük bir fırsatı temsil ediyor. Bitcoin, "güven yerine kriptografik kanıta dayalı bir elektronik ödeme sistemi, herhangi iki istekli tarafın güvenilir bir üçüncü tarafa ihtiyaç duymadan birbirleriyle doğrudan işlem yapmasına izin vermek parti." [2]. Bitcoin yeni bir dijital para birimi sınıfı, merkezi olmayan bir dijital para birimi veya kripto para birimi yarattı. 1 Kripto para birimlerinin başlıca avantajlarından bazıları şunlardır: düşük işlem maliyetleri, uluslararası sınırsız aktarılabilirlik ve dönüştürülebilirlik, güvene dayalı mülkiyet ve takas, sahte anonimlik, gerçek zamanlı şeffaflık ve eski bankacılık sistemi sorunlarından muafiyet [3]. Akım için ortak açıklamalar Kripto para birimlerinin sınırlı genel kullanımı şunları içerir: değişken fiyat dalgalanmaları, yetersiz kitle pazarı teknolojinin anlaşılması ve teknik bilgisi olmayan kullanıcılar için yetersiz kullanım kolaylığı. Varlığa dayalı kripto para birimleri fikri, başlangıçta Bitcoin topluluğunda popüler hale geldi. 20 Ocak 2012'de JR Willett tarafından yazılan Mastercoin teknik raporu [4]. Bugün bu fikirleri görmeye başlıyoruz BitAssets, Ripple, Omni, Nxt, NuShares / Bits ve diğerleri ile oluşturulmuştur. Biri hepsine dikkat etmelidir Bir itibari para olarak değer tutmanıza izin veren Bitcoin borsaları ve cüzdanları (Coinbase, Bitfinex ve Coinapult gibi) para zaten sağlamak benzer belirli kullanıcıları oynaklığı önlemek için bu hizmetin (ya da diğer özellikleri) fiat para birimi, altın veya başka bir varlık karşılığında satarak kripto para birimi. Dahası, hemen hemen her tür mevcut fiat değerini (veya diğer varlıkları) tutmanıza izin veren finansal kurumlar, ödeme sağlayıcıları vb. daha sonra benzer

bir hizmet sağlar. Bu teknik incelemede, fiat değerinin olduğu uygulamalara odaklanıyoruz açık kaynaklı, kriptografik olarak güvenli ve dağıtılmış kullanan bir yazılımla depolanır ve iletilir defter teknolojisi, yani gerçek bir kripto para birimi. Başarılı bir kripto para biriminin amacı güven gerekliliğini tamamen ortadan kaldırmak olsa da, her biri yukarıda belirtilen uygulamalar ya güvenilir bir üçüncü tarafa dayanır ya da başka tekniklere sahiptir, piyasa temelli veya süreç temelli dezavantajlar ve sınırlamalar. 3 1 tanımları için boyunca, bakınız Terimler Sözlüğü 2 Ancak Dr. Szabo'nun BitGold'u önerdiğinden beri tartışılıyor [5] 3 Burada, Ek'te özet: Mevcut Fiatpegging Sistemleri Sınırlamalar 3

4. sayfa

Çözümümüzde, fiatpegged kripto para birimleri "bağlar" olarak adlandırılır. Tüm bağlar başlangıçta 4Omni Katman protokolü aracılığıyla Bitcoin blok zinciri ve bu nedenle bir kripto para belirteci olarak var olurlar. Her bir bağlama birimi tedavüle çıkarılan teke oranla desteklenir (yani, bir Tether USDT, bir ABD dolarıdır) Hong Kong merkezli Tether Limited tarafından depozitoda tutulan karşılık gelen itibari para birimi. İpler olabilir Tether Limited'in hizmet şartlarına göre temel itibari para birimi için kullanılabilir / değiştirilebilir veya, eğer sahibi, Bitcoin'deki eşdeğer spot değeri tercih eder. Bir tether yayınlandıktan sonra aktarılabilir, tıpkı bitcoin veya diğer herhangi bir kripto para birimi gibi depolanır, harcanır, vb. Rezerv üzerindeki fiat para birimi, Bir cryptocurrency ve fiyatı özellikleri kalıcı olduğu tethered fiat para fiyatına. Uygulamamız, diğer fiatpegged kripto para birimlerine göre aşağıdaki avantajlara sahiptir: •İpler, daha az gelişmiş / test edilmiş bir "altcoin" blok zincirinden ziyade Bitcoin blok zincirinde bulunur. merkezi, özel veritabanları üzerinde çalışan kapalı kaynak yazılım içinde. •İpler tıpkı bitcoinler gibi kullanılabilir, yani p2p'de, sözde anonim, merkezi olmayan, kriptografik olarak güvenli ortam. •Tether'ler tüccarlar, borsalar ve cüzdanlarla Bitcoin veya herhangi biri kadar kolay bir şekilde entegre edilebilir. diğer kripto para birimleri entegre edilebilir. •İpler, Omni Katman protokolünün özelliklerini devralır ve şunları içerir: merkezi olmayan bir değişim; tarayıcı tabanlı, açık kaynaklı, cüzdan şifreleme; Bitcoin tabanlı şeffaflık, hesap verebilirlik, çok taraflı güvenlik ve raporlama işlevleri. •Tether Limited, Rezerv Kanıtı yürütmek için basit ama etkili bir yaklaşım kullanır. Rezerv varlıkların sorumlusu olarak karşı taraf riskimizi önemli ölçüde azaltır. •Tether ihracı veya geri alımı herhangi bir fiyatlandırma veya likidite kısıtlamasıyla karşılaşmayacaktır. Kullanıcılar satın alabilir veya satabilir istedikleri kadar, hızlı ve çok düşük ücretlerle. •Tethers, Black Swan olayları, likidite sıkışıklıkları vb. Gibi herhangi bir piyasa riskiyle karşı karşıya kalmayacaktır. 5rezervler, piyasa güçlerine dayanmak yerine bire bir oranında tutulur. •Tether'in teke bir destek uygulaması, teknik bilgisi olmayan kullanıcıların şu şekilde anlaması daha kolaydır: teminatlandırma tekniklerine veya türev stratejilerine karşı. Herhangi bir zamanda, rezervlerimizde tutulan fiat para birimi bakiyesi, dolaşımdaki ip sayısı. Bu basit yapılandırma, güvenilir bir Rezerv Kanıtı'nı en kolay şekilde destekler süreç; dolaşımdaki ipler arasındaki fiyat eşitliğini sürdürmek için temel olan bir süreç ve rezervlerde tutulan temel itibari para birimi. Bu yazıda, değişimi gösteren ve 64 Daha Bitcoin 2.0 protokolleri vb Ripple, NXT gibi, yakında gelecek 5 Bkz Ek bölüm: Piyasa Riski Örnekleri 6 bölümüne bakınız: Ödeyebilirlik Süreci kanıtı 4

5.Sayfa

cüzdan denetimleri (mevcut durumlarında) çok güvenilmezdir (yani, Proof of Solvency [6] yöntemlerindeki kusurlar) ve Bunun yerine söz konusu değişim ve cüzdan önermek outsource tethers aracılığıyla bize kullanıcı fonlarının gözetimine. Kullanıcılar Tether.to'dan

(web cüzdanımız) veya Bitfinex gibi desteklenen borsalardan tether satın alabilirler. Para yatırma ve çekme yöntemi olarak ipleri destekleyenler. Kullanıcılar ayrıca ipleri herhangi bir Ambisafe, Holy Transaction veya Omni Wallet gibi Omni Layer özellikli cüzdan. Diğer borsalar, cüzdanlar ve tüccarlar, tether'i geleneksel fiat için bir vekil olarak entegre etme konusunda bize ulaşmaya teşvik edilmektedir. Ödeme metodları. Tether Limited'in bir 7rezerv varlıkların merkezi sorumlusu (dolaşımda olsa da, merkezi olmayan dijital para birimi olarak mevcuttur). Ancak, bu uygulamanın gelecekteki yenilikleri inşa etmenin temelini oluşturduğuna inanıyoruz. bu zayıflıkları ortadan kaldırmak, yeni ürün ve hizmetler için sağlam bir platform oluşturmak ve büyümeyi desteklemek ve Bitcoin blok zincirinin uzun vadede faydası. Bu yeniliklerden bazıları şunları içerir: •Diğer kullanıcılar ve satıcılar dahil olmak üzere kullanıcılar ve diğer taraflar arasında mobil ödeme kolaylığı •Merkezi olmayan taraflar arasında anında veya anında itibari değer aktarımı (birden fazla borsalar) •Daha da iyileştirmek için akıllı sözleşmelerin ve çoklu imza yeteneklerinin kullanımına giriş genel güvenlik süreci, Rezerv Kanıtı ve yeni özellikleri etkinleştirin. Teknoloji Yığını ve Süreçler Dolaşıma giren her bir tether, eşdeğer miktarda bire bir oranında desteklenecektir. Hong Kong merkezli Tether Limited tarafından rezervlerde tutulan karşılık gelen fiat para birimi. Sorumlusu olarak destek varlığımız, bu varlıktan sorumlu, güvenilir bir üçüncü taraf olarak hareket ediyoruz. Bu risk, bir Hem fiat hem de kripto denetimlerinin karmaşıklığını toplu olarak azaltan basit uygulama bu denetimlerin güvenliğini, kanıtlanabilirliğini ve şeffaflığını artırırken. Tether Teknoloji Yığını Yığın 3 katmana ve en iyi şekilde bir diyagramla anlaşılan çok sayıda özelliğe sahiptir. 7 bölümüne bakınız: Uygulama zayıf yönleri 5

Sayfa 6

İşte her katmanın bir incelemesi. 1) İlk katman Bitcoin blok zinciridir. Tether işlem defteri Bitcoin'e gömülüdür Gömülü fikir birliği sistemi Omni aracılığıyla meta veri olarak blok zinciri. 2) İkinci katman Omni Layer protokolüdür. Omni, şunları yapabilen temel bir teknolojidir: a) Gömülü meta veriler olarak temsil edilen dijital belirteçleri verin (oluşturun) ve iptal edin (yok edin) Bitcoin blok zinciri; bu durumda, fiatpegged dijital belirteçler, bağlar. b) Bağlantıların dolaşımını Omnichest.info (Omni varlık kimliği # 31, örnek, TetherUSD'yi temsil eder) ve Omnicore API'sini temsil eder. c) Kullanıcıların bağlantılarını ve diğer varlıkları / jetonları bir: ben)p2p, sözde anonim, kriptografik olarak güvenli ortam. ii)açık kaynaklı, tarayıcı tabanlı, şifreli web cüzdan: Omni Cüzdan. iii)çoklu imzalı ve çevrimdışı soğuk hava depolarını destekleme sistemi 3) Üçüncü katman, iş birimimiz olan Tether Limited'dir ve temel olarak aşağıdakilerden sorumludur: a) İtibari mevduat kabul etmek ve karşılık gelen ipleri çıkarmak b) İtibari para çekme işlemlerinin gönderilmesi ve ilgili iplerin iptal edilmesi c) Dolaşımdaki tüm ipleri destekleyen fiat rezervlerinin muhafazası 6

7. Sayfa

d) Rezerv Kanıtı ve diğer denetim sonuçlarının kamuya bildirilmesi e) Mevcut Bitcoin / blockchain cüzdanları, borsaları ile entegrasyonları başlatmak ve yönetmek, ve tüccarlar f)Kullanıcıların göndermesine, almasına, depolamasına ve dönüştürmesine olanak tanıyan bir web cüzdan olan Tether.to'yu çalıştırma rahatça bağlar. Fon Akışı Süreci Bir ipin yaşam döngüsünde, en iyi şekilde bir diyagramla anlaşılan beş adım vardır. Adım 1 urgan Limited'in banka hesabına Kullanıcı mevduat fiat para birimi. 2. Adım urgan Sınırlı kullanıcının urgan hesabını oluşturur ve krediler. İpler dolaşıma girer. Miktarı kullanıcı tarafından yatırılan fiat para birimi = kullanıcıya verilen bağların miktarı (yani yatırılan 10.000 USD = 10.000 tetherUSD Veriliş). 7

8. Sayfa

Adım 3 Kullanıcılar tethers ile işlem. Kullanıcı ipleri bir p2p aracılığıyla aktarabilir, değiştirebilir ve depolayabilir 8açık kaynaklı, sözde anonim, Bitcoin tabanlı platform. Adım 4 fiat para birimine kurtuluş için Tether Limited ile kullanıcı mevduat tethers. Adım 5 urgan Sınırlı Bağları yok eder ve kullanıcının banka hesabına fiat para gönderir. Kullanıcılar, yukarıda belirtilen sürecin dışında bir değişim veya başka bir kişi aracılığıyla bağlar edinebilirler. bir Zamanlar bir ip dolaşıma girer, herhangi bir işletme veya birey arasında serbestçe işlem görebilir. Örneğin, kullanıcılar şunları yapabilir: Bitfinex'ten ipler satın alın, yakında daha fazla borsa da takip edecek. Fon Akışı diyagramında iletilecek ana kavram, Tether Limited'in ipleri dolaşıma sokabilir (yaratılabilir) veya dolaşımdan çıkarılabilir (yok edebilir). Bu Sistem ödeme gücünün korunduğu ana süreç. Rezerv Kanıtı Süreci Ödeme Gücü Kanıtı, Rezerv Kanıtı, Gerçek Zamanlı Şeffaflık ve diğer benzer ifadeler kripto para birimi endüstrisinde büyüyen ve yankılanan. Mevcut haliyle borsa ve cüzdan denetimleri çok güvenilmezdir. İflas çok sayıda meydana geldi Hack'ler, kötü yönetim ya da düpedüz dolandırıcılık yoluyla Bitcoin ekosistemindeki zamanlar. Kullanıcılar gayretli olmalı borsa seçimleri ve borsaları kullanımlarında dikkatli olmaları ile. O zaman bile, bilgili bir kullanıcı bunu yapamayacak riskleri tamamen ortadan kaldırmak için. Ayrıca, tüccarlar ve işletmeler gibi borsa kullanıcıları var. borsalarda her zaman önemsiz fiat bakiyeleri. Finans dilinde bu, "karşı taraf" olarak bilinir. üçüncü bir şahıs ile değer saklama riski. Mevcut haliyle takas ve cüzdan denetimlerinin çok güvenilir olmadığı sonucuna varmanın güvenli olduğuna inanıyoruz. Bu süreçler, kullanıcılara bir saklayıcı veya takasın çözücü olduğunu garanti etmez. Olmasına rağmen Merkle ağacı yaklaşımı [6] gibi değişim denetim süreçlerinin iyileştirilmesine büyük katkılar, büyük kusurlar hala aynı. 9 Tether'in Rezerv Kanıtı yapılandırması yenidir çünkü toplamın Dolaşımdaki iplerin sayısı (yükümlülükler) her zaman eşit miktarda fiat para birimi ile tam olarak desteklenir 8 bölümündeki Bağları kullanmanın bakınız faydaları: Temel Uygulamalar 9 Bkz bölümü: Denetim Kusurlar: Değişimleri ve Cüzdan 8

Sayfa 9

yedekte (varlıklar). Yapılandırmamızda, dolaşımdaki her tetherUSD, bizim rezervler (yani bire bir oran), bu da sistemdeki tüm bağların toplamı olduğunda sistemin tamamen ayrılmış olduğu anlamına gelir. mevcudiyeti (herhangi bir zamanda) rezervimizde tutulan USD bakiyesine tam olarak eşittir. Tethers yaşadığından beri Bitcoin blok zincirinde, bağlantıların herhangi bir zamanda kanıtlanabilirliği ve muhasebesi önemsizdir. Tersine, rezervlerimizde tutulan toplam USD tutarının banka tarafından yayınlanmasıyla kanıtlanır. uzmanlar tarafından düzenli aralıklarla denetime tabi tutulması ve geçirilmesi. Bu uygulamayı aşağıda daha ayrıntılı olarak bulun: •Tether Limited, Omni Layer protokolü aracılığıyla tüm bağları verir. Omni, Bitcoin üzerinde çalışıyor blok zinciri ve bu nedenle işlem geçmişi dahil olmak üzere tüm yayınlanan, kullanılan ve mevcut bağlar, Omnichest.info'da sağlanan araçlar aracılığıyla halka açık olarak denetlenebilir. ○TetherUSD için Omnichest.info varlık kimliği # 31'dir. ■İşte link: <http://omnichest.info/lookupsp.aspx?sp=31> ○Bu varlık kimliği altında verilen toplam ip sayısı TUSDissue olarak gösterilsin ○Bu varlık kimliği altında kullanılan toplam ip sayısı TUSDredeem olarak gösterilsin ○Herhangi bir zamanda dolaşımdaki toplam ip sayısı TUSD olarak gösterilsin ■TUSD = Doku TUSDredeem ■TUSD = "Toplam Mülk Jetonu" @ <http://omnichest.info/lookupsp.aspx?sp=31> •Tether Limited, itibari para birimini alacak ve kullanıcılara gönderecek bir banka hesabına sahiptir. ipleri doğrudan bizimle satın alın / kullanın. ○Bu hesaba yatırılan toplam tutarın DUSDdepo olarak gösterilmesine izin

verin ○Bu hesaptan çekilen toplam tutarın DUSDwithd olarak gösterilmesine izin verin ○Bu banka hesabının dolar bakiyesi DUSD olarak gösterilsin ■DUSD = DUSDdepo DUSDwithd ●Verilen her tether, eşdeğer miktarda para birimi ile desteklenecektir (bir tetherUSD eşittir bir dolar). Yukarıdaki kripto ve fiat muhasebe süreçlerini birleştirerek, Tether Sistemi için "Ödeme Gücü Denklemi". ○Ödeme Gücü Denklemi basitçe TUSD = DUSD'dir. ○Bitcoin blok zinciri tarafından halka açık olarak kaydedildiği şekliyle verilen veya kullanılan her tether, banka hesabından para yatırma veya para çekme işlemine karşılık gelir. ○TUSD'nin kanıtlanabilirliği, daha önce tartışıldığı gibi Bitcoin blok zincirine dayanır. ○DUSD'nin kanıtlanabilirliği birkaç sürece dayanacaktır: ■Banka hesabı bakiyesini web sitemizin Şeffaflık sayfasında yayınlıyoruz. ■Profesyonel denetçiler, temel bankamızı düzenli olarak doğrulayacak, imzalayacak ve yayınlayacaktır. denge ve finansal transfer tablosu. 9

Sayfa 10

Kullanıcılar bu bilgileri Şeffaflık Sayfamızdan görüntüleyebilecek ve aşağıdaki gibi görünecektir: Netlik sağlamak için, Tether Sisteminin Tether.to web cüzdanından farklı olduğunu kabul etmek isteriz. 10Rezerv Kanıtı Koşulları. Bu yazıda, çoğunlukla Tether Sistemi için Rezerv Kanıtı'na odaklanıyoruz; yani herhangi bir zamanda dolaşımdaki tüm ipler. Tether.to cüzdanı, tüketiciye dönük bir web cüzdanıdır ve kapalı kaynak kod ve merkezi sunucularda. Bu cüzdan için bir Rezerv Kanıtı yürütmek Tether Sistemi için özetlediklerimizden temelde farklı. Tether.to cüzdanı için PoR tabanlı bir şeffaflık çözümünün dağıtımını planlıyoruz. Biz buna inanıyoruz bugün var olan en gelişmiş PoR sistemi olacak. Belirtilen neredeyse tüm zorlukların üstesinden gelir bu konuyla ilgili ek bölümünde. Unutmayın, kullanıcılar özel bilgileri yöneterek her zaman bağlantılarını güvence altına alabilirler. 11anahtarlar kendileri veya Omni Cüzdan aracılığıyla. Uygulama Zayıf Yönleri Uygulamamızın hemen tamamen güvensiz bir kripto para birimi sistemi oluşturmadığını anlıyoruz. Temel olarak, kullanıcıların Tether Limited'e ve ilgili eski bankacılık kurumumuza güvenmesi gerektiğinden, rezerv varlıkların sorumlusu. Bununla birlikte, neredeyse tüm borsalar ve cüzdanlar (USD / fiat tuttuklarını varsayarak) aynı zayıflıklara tabidir. Bu hizmetlerin kullanıcıları zaten bu risklere tabidir. Burada bir yaklaşımımızdaki zayıflıkların özeti: ●İflas edebiliriz ●Bankamız iflas edebilir ●Bankamız fonları dondurabilir veya el koyabilir ●Yedek fonlarla kaçabiliriz 10 Bkz Terimleri Sözlüğü 11 Bkz Denetim Kusurlar: Değişimleri ve Cüzdan 10

Sayfa 11

●Tek bir başarısızlık noktasına kadar yakın zamanda merkezileştirilmiş risk Neredeyse tüm dijital para borsalarının ve cüzdanlarının (USD / fiat tuttuklarını varsayarak) halihazırda karşı karşıya olduğunu gözlemleyin. bu zorlukların çoğu. Bu nedenle, bu hizmetlerin kullanıcıları zaten bu risklere tabidir. Aşağıda biz Bu endişelerin her birinin nasıl ele alındığını açıklayın. Biz iflas olabilir Bu durumda, işletme varlığı urgan Sınırlı iflas ancak müşteri fonları gider güvenli olacak ve daha sonra tüm bağlar kullanılmaya devam edecek. Bitcoin'deki çoğu güvenlik ihlali işletmeler banka hesaplarından ziyade kripto para birimlerini hedeflediler. Bitcoin'de tüm bağlar olduğu için blok zinciri, kendi özel anahtarlarını güvence altına alarak doğrudan bireyler tarafından saklanabilir. İflas etmiş gidebiliriz Bankamız Bu eski finansal sistemin tüm kullanıcılar tarafından tüm karşılaştığı bir risktir değişim operatörleri. Tether Limited'in şu anda Cathay United Bank ve Hwatai Bank'ta hesapları var Tayvan, Tether'in iş modelinin kabul edilebilir olduğunun farkında ve emin. Ek Bu endişeyi daha da hafifletmek için diğer yetki alanlarında bankacılık ortakları kurulmaktadır. Bankamız dondurmak veya

fonlara el verebilir Bizim bankalar Bitcoin doğasının farkında ve vardır Bitcoin işletmelerinin kabulü. Ayrıca en büyük Bitcoin'lerden bazılarında bankacılık hizmetleri de sağlıyorlar küresel olarak değiş tokuş. Takip ettiğimiz KYC / AML süreçleri diğer dijital para birimi tarafından da kullanılmaktadır. Şu anda bankalandıkları borsalar. Bize tam uyumlu olduğumuza dair güvence verdiler. 12 Biz rezerv varlıkları alıp kaçmak olabilir kurumsal kiralama herkese açıktır yanı sıra iş 13 sahiplerin adları, yerleri ve itibarı. Hesabın mülkiyeti yasal olarak şirkete bağlıdır charter. Banka hesabına giren veya çıkan tüm transferler, ilgili izlere sahip olacak ve katı bir şekilde bağlanacaktır. İç politikalar. Başarısızlık tek noktaya riskin Recentralization Bu aşmak için bazı fikirler var ve yaparız bunları gelecek blog ve ürün güncellemelerinde paylaşıyor olacaksınız. Bu sorunu çözenin birçok yolu vardır. İçin şimdi, bu ilk uygulama bizi bu yenilikleri aşağıdaki versiyonlarda gerçekleştirmek için doğru yola sokuyor. Seçtiğimiz platformlardan yararlanarak, merkezileştirme riskini tek bir tekil sorumluluk: belirteçlerin oluşturulması ve kullanılması. Sistemin diğer tüm yönleri ademi merkezizetçi. 12 Bkz bölüm Yasal ve Uyumluluk daha fazla bilgi için 13 dipnot # 10 ile aynı 11

Sayfa 12

Ana Uygulamalar Bu bölümde, Bitcoin / blockchain genelindeki iplerin ana uygulamalarını özetleyecek ve tartışacağız. ekosistem ve küresel olarak diğer tüketiciler için. Yararlanıcıları üç kullanıcı grubuna ayırıyoruz: Borsalar, Bireyler ve Tüccarlar. Tüm gruplar için geçerli olan ana faydalar: •Diğer varlık sınıflarına bahsedilen Bitcoin'in özellikleri •Daha az değişken, tanıdık hesap birimi •Dünyanın varlıkları Bitcoin blok zincirine taşınır Borsalar için Borsa operatörleri, eski finansal sistemleri kullanarak fiat para yatırma ve çekme işlemlerini kabul etmenin farkındadır. karmaşık, riskli, yavaş ve pahalı olabilir. Bu sorunlardan bazıları şunları içerir: •Borsanız için doğru ödeme sağlayıcılarını belirleme ogeri dönüşü olmayan işlemler, dolandırıcılık koruması, en düşük ücretler vb. •Platformu API'si olmayan bankalarla entegre etmek •Uyum, güvenlik ve güven inşa etmek için bu bankalarla irtibat kurmak •Küçük değer transferleri için engelleyici maliyetler •Uluslararası banka havalelerinin gerçekleşmesi için 37 gün •Zayıf ve elverişsiz para birimi dönüştürme ücretleri Bağlayıcılar sunarak, bir değişim, kendilerini yukarıdaki komplikasyonlardan kurtarabilir ve ek kazanç sağlayabilir. aşağıdaki gibi faydalar: •Eski bir banka kullanmak yerine kripto para birimlerini para yatırma / çekme / depolama yöntemi olarak kabul edin veya ödeme sağlayıcı oKullanıcıların fiat'ı borsaya daha özgürce, hızlı ve ucuza girip çıkmasını sağlar •İtibari saklama riskini Tether Limited'e devredin, sadece kriptoları yönetin •Diğer bağlı itibari para birimlerini ticaret çiftleri olarak platforma kolayca ekleyin •Müşteri varlıklarını yalnızca kabul edilen kripto işlemlerle güvence altına alın oÇoklu imzalı güvenlik, soğuk ve sıcak cüzdanlar, HD cüzdanlar vb. 12

Sayfa 13

oTamamen kriptolu bir ortamda denetimleri daha kolay ve daha güvenli bir şekilde gerçekleştirin •Bitcoin ile takas olarak yapılabilecek her şey iplerle yapılabilir. Borsa kullanıcıları, bir borsada fiat para birimlerini tutmanın ne kadar riskli olabileceğini bilirler. Artan sayı ile iflas olayları oldukça tehlikeli olabilir. Daha önce de belirtildiği gibi, ipleri kullanmanın borsa kullanıcılarını borsalarda sürekli olarak fiat tutmaktan daha az karşı taraf riskine maruz bırakır. Bunlara ek olarak, Bir sonraki bölümde açıklanan ipleri tutmanın başka faydaları da var. Bireyler için Bugün dünyada pek çok bireysel Bitcoin kullanıcısı vardır. Kar elde etmek isteyen tüccarlardan günlük; Bitcoin'lerini güvenli bir şekilde saklamak isteyen uzun vadeli yatırımcılara; kaçınmak isteyen teknoloji tutkunu müşterilere kredi kartı ücretleri veya gizliliklerini korumak; dünyayı değiştirmek isteyen felsefi kullanıcılar; arayanlara

ödemeleri küresel olarak daha etkili bir şekilde havale etmek; finansal kaynaklara erişim arayan üçüncü dünya ülkelerindeki hizmetleri ilk kez; yeni teknolojiler yaratmak isteyen geliştiricilere; bulan herkese Bitcoin için birçok kullanım. Bu bireylerin her biri için, iplerin aşağıdakiler gibi benzer şekillerde faydalı olduğuna inanıyoruz: •Herhangi bir aracı / aracı olmadan sözde anonim olarak USD / fiat değerinde işlem yapın •Kişinin kendi özel anahtarlarını güvence altına alarak soğuk depo USD / fiat değeri •Borsalarda itibari para depolama riskinden kaçının, kriptofiat'ı borsalara kolayca girip çıkarın •İtibari değeri saklamak için bir fiat banka hesabı açmak zorunda kalmayın •Tether'i desteklemek için bitcoin ile çalışan uygulamaları kolayca geliştirin •Bitcoin ile bireysel olarak yapılabilecek her şey, tether ile de yapılabilir. Tüccarlar için Tüccarlar ödemelere değil işlerine odaklanmak isterler. Küresel, ucuz, her yerde bulunan eksikliği ödeme çözümleri, hem büyük hem de küçük tüm dünyadaki tüccarları rahatsız etmeye devam ediyor. Tüccarlar hak ediyor Daha. Tether'in onlara yardımcı olabileceği yöntemlerden bazıları şunlardır: •Malları Bitcoin yerine USD / fiat değerinde fiyatlandırın (hareketli dönüştürme oranları / satın alma pencereleri yok) •Bitcoin'den USD / fiat'a dönüştürme ve ilgili ücretler ve süreçlerden kaçının •Ters ibrazları önleyin, ücretleri azaltın ve daha fazla gizlilik elde edin •Fiat kripto özellikleri nedeniyle yeni hizmetler sağlayın ○Mikro nakliye, hediye kartları ve daha fazlası •Bir tüccar olarak Bitcoin ile yapılabilecek her şey, tether ile de yapılabilir. 13

Sayfa 14

Gelecek Yenilikler Multisig ve Akıllı Sözleşmeler Ödeme Gücü Yeniliklerinin Kanıtı Sonuç Tether, bugün var olan ilk Bitcoin tabanlı fiatpegged kripto para birimlerini oluşturuyor. Tether şuna dayanır: Bitcoin blok zinciri, var olan en güvenli ve en iyi test edilmiş blok zinciri ve halka açık defter. İpler piyasa güçlerinden, fiyatlandırmadan veya likiditeden tamamen bağımsız olarak tamamen teke oranlı olarak rezerve edilmiştir kısıtlamalar. Tether, basit ve güvenilir bir Rezerv Kanıtı uygulamasına sahiptir ve düzenli olarak profesyonel denetimler. Temel bankacılık ilişkilerimiz, uyumluluğumuz ve yasal yapımız güvenli bir rezerv varlıkların koruyucusu ve iplerin ihraççısı olmamız için vakıf. Ekibimiz şunlardan oluşmaktadır: Bitcoin ekosisteminden ve ötesinden deneyimli ve saygın girişimciler. Kripto para birimi alanındaki mevcut işletmelerle entegrasyonlar düzenlemeye odaklandık. İş borsalar, cüzdanlar, tüccarlar ve diğerleri gibi. Bitfinex, HolyTransaction ile zaten entegre olduk, Omni Cüzdan, Poloniex, CCEX ve daha fazlası gelecek. Daha fazlasını öğrenmek için lütfen bize ulaşın. Ek Denetim Kusurları: Borsalar ve Cüzdanlar İşte teknoloji tabanlı değişim ve cüzdan denetimlerinde bulunan mevcut kusurların bir özeti. 14 Merkle ağacı [6] yaklaşımında kullanıcılar, bakiyelerinin (kullanıcı sayfası) borsanın sorumluluk beyanına doğru şekilde dahil edilmiştir (borsanın Merkle hash'i) kullanıcı bakiyeleri veritabanı). Bu önerilen çözüm, yeterli sayıda kullanıcı hesaplarının ağaca dahil edilir ve hesaplarının dahil edilmediği bir durumda bu durum rapor edilir. Bir potansiyel risk, bir değişim veritabanı sahibinin, gerçek temsili olmayan bir hash üretebilmesidir. 14 Profesyonel bir denetçi tutmanın aksine 14

Sayfa 15

veri tabanı, eksik bir veri tabanını hash eder, bu da görünen yükümlülüklerini azaltacaktır. müşteriler, doğrulayıcı bir tarafa çözücü görünmelerini sağlar. İşte bir sahtekarlığın olduğu bazı senaryolar değişim hesapları hariç tutar ve: ○"Bitdust" Hesapları: Etkin olmayan veya düşük etkinliğe sahip hesaplar, bir ilgisiz kullanıcı tutarsızlıkları kontrol eder veya bildirir. Bazı durumlarda bu uzun kuyruk hesaplar, borsanın borçlarının önemli bir yüzdesini temsil edebilir. ○"Colluding Whales" Saldırısı: Büyük Bitcoin tüccarlarının önemli ölçüde çeşitli

borsalar ve hareketli pazarlar. Bu tür tüccarların sermayeye sahip olması gerekir emirleri hızlı bir şekilde yerine getirmek için en büyük borsalarda rezervler. Genellikle tüccarlar seçer "güvendikleri" alışverişler. Bu şekilde, bir hack veya likidite olması gerektiğinden emin olabilirler. sorun ortaya çıktığında, paralarını alma önceliğine sahipler. Bu durumda, borsa ve tüccar Balinaların hesap bakiyesini karma işlemine tabi tutulmadan önce veritabanından çıkarmak için işbirliği yapabilir. ○Anahtar Kiralama Saldırısı: Kötü niyetli bir takas, denetimi geçmek için özel anahtarları kiralayabilir. sahip olmadıkları bitcoinler. Bu, varlıklarını artırarak çözücü görünmelerini sağlayacaktır. bu fonların kendilerine ödünç verildiğine dair herhangi bir onay olmadan. Aynı şekilde, yapabilirlerdi Aynı şeyi yapmak için fiat para birimini "ödünç almak". ○Burada tartışılmayan daha fazla saldırı var. İstatistiksel Öneme Ulaşma (tamlığı bildirme): Bu üç saldırı vektörünün dışında bile, Yeterli sayıda kullanıcı doğrulamıyorsa, manipüle edilmiş veritabanı asla algılanamayabilir dengeler. Kullanıcıların% 100'ünün bakiyeleri doğrulamasını sağlama olasılığı, uygun olsa bile muhtemelen sıfırdır. Kullanıcıların bakiyelerini doğrulaması için teşvik yapısı. Bu nedenle, denetçilerin Örnekleme sıklığına, boyutuna ve örnekleme sıklığına dayalı olarak bir değişimin veritabanının geçerliliği hakkında açıklamalar yapın. diğer özellikler. Şu anda kullanıcılar, bir şeyler ters gittiğinde yasal yollarla tazminat alamaz. değişim. Örneğin, Mt.Gox işlemleri kapattığında, birçok kullanıcı bağımsız olarak hesap bakiyelerini (baskı ekranları, imzalı mesajları kendilerine vb.) kanun uygulayıcılarına bu borsanın IOU'larının gerçekte var olduğunu kesin olarak kanıtladı. Bu tür kullanıcılar o hash ağacının veya orijinal veritabanının bir kaydını bir şekilde yayınlamak için borsanın merhameti. Bu denetimlerin gerçekleştirileceği önerilen yapı, hala bazı ince ama önemli kusurlar. Özellikle, kurumun web sitesindeki veri raporlama (karma ağacı), aşağıdakilere hiçbir garanti vermez: 15

Sayfa 16

kullanıcılar, kötü niyetli bir değişim olarak farklı kullanıcı gruplarına farklı durumlar / dengeler yayınlayabilir veya durumu geriye dönük olarak değiştirin. Bu nedenle, bu verilerin güvenli bir yayın yoluyla yayınlanması esastır. kanal, örneğin Bitcoin blok zinciri. Gizlilik, otomatik / açık bir denetim sisteminin benimsenmesinin önündeki bir engeldir. Biraz ilerleme olurken daha iyi bir mahremiyet için yapılmıştır, henüz mükemmel bir çözüm yoktur. Dahası, doğru bir kullanıcı oluşturmak için doğrulanmış sorumluluk alanı, bu kullanıcıların borsa ve Bitcoin ile hesap bakiyelerini bildirmeleri gerekecek adresler. Teşvikten bağımsız olarak bazı kullanıcılar muhtemelen bu bilgiyi bildirmeyecektir, bu nedenle raporlama hedefini elde ederken kriptografik olarak güvenli gizlilik sağlamak çok önemlidir. Zaman Serisi: Merkle ağaç hash değeri, veritabanının tek bir zamanda tek bir anlık görüntüsüdür. Sahip olmamak veritabanının biraz sürekli zaman serileri, önemli saldırı vektörleri açar. Ek olarak, bir zaman bildirilen herhangi bir geçmişin bir araya getirilmesi için kullanıcı tarafından bildirilen bilgiler dizisi de gerekli olacaktır. dolandırıcılık olayları. Güvenilir Üçüncü Taraflar: Mevcut tüm değişim denetimleri bazı "saygın" güvenilir üçüncü taraflara dayanıyordu bir tür doğrulama yapmak için. Coinbase denetiminde [7], Kraken'daki Andreas Antonopoulos'du. denetim [8], o Stefan Thomas'dı. Kesinlikle güvenilir bir üçüncü tarafa güvenmemiz gerekiyorsa, o zaman bazı denetimler standartlar ve prosedürler bu zayıflıkların güçlendirilmesini sağlamalıdır. Mevcut Fiatpegging Sistemlerinin Sınırlamaları İşte mevcut fiatpegging sistemlerinin bazı yaygın dezavantajlarının ve sınırlamalarının bir listesi. ●Sistemler, özel, merkezi veritabanları üzerinde çalışan kapalı kaynaklı yazılımlara dayanmaktadır, temelde Paypal veya diğer mevcut perakende / kurumsal varlıklardan farklı değildir ticaret / transfer / depolama sistemi. ●Stres testi yapılmamış, geliştirilmiş altcoin blok zincirlerine dayanan

merkezi olmayan sistemler, veya Bitcoin gibi diğer blok zincirleri kadar yakından incelendi.
●Riskten korunma türev meta varlıklarına, verimli piyasa teorisine veya dayanak varlığın teminatlandırılması, burada likidite, devredilebilirlik, güvenlik ve diğer sorunlar var olabilir. 16

Sayfa 17

●Kripto, itibari para veya kendi iç işleri ile ilgili saklama kuruluşu için şeffaflık ve denetim eksikliği defterler (kapalı kaynak ve merkezi veritabanları ile aynı). ●Transfer olarak eski bankacılık sistemlerine ve güvenilir üçüncü taraflara (banka hesabı sahipleri) güvenme rezerv varlıklar için ödeme mekanizması. Piyasa Riski Örnekleri Teminatlandırma yönteminde, teminat olarak kullanılan varlığın fiyatının Desteklediği / sabitlediği varlığın fiyatına ters yönde hareket etmek. Bu, toplam değere neden olur teminatın ihraç edilen varlığın toplam değerinden daha az olması ve sistemi iflas ettirmesi. Bu risk, saklama görevlisinin bu olmadan önce pozisyonu kapatmasıyla hafifletilir; yani, teminat fiyatı sabit varlık fiyatına eşittir, ardından teminat tasfiye edilir (açık piyasada satılır) ve pozisyon kapalı. Liyakate sahip harika bir yaklaşım ve geleneksel bankacılıkta ve birçok likit piyasada kullanılır. finansal piyasalar. Ancak, küresel mali krizden de gördüğümüz gibi, bu tür olayların hızlanması "likidite sıkışıklığına" neden olur ve bu nedenle teminat hızlı bir şekilde tasfiye edilemez. ticaret yükümlülüklerini karşılamak için yeterli, daha sonra kayıplar yaratır. Kripto para piyasaları böyle olunca küçük ve uçucu, bu tür bir olay çok daha olasıdır. Ek olarak, genel yaklaşım diğerlerinden muzdariptir. teminat veren yeterli sayıda kullanıcı olması gerektiğinden, likidite ve fiyatlandırma kısıtlamaları ilk etapta var olmak için peggedassetlerin oluşturulması. Türev yaklaşımında, varlığın fiyatı çeşitli türevlerden birine girilerek sabitlenir. takas stratejileri, kapalı ve açık opsiyon stratejileri, çeşitli vadeli ve vadeli işlemler gibi stratejiler stratejiler. Her stratejinin kendi güçlü ve zayıf yönleri vardır ve bu tartışmalara katılmayacağız. burada. Özetlemek gerekirse, bu sabitleme süreçlerinin her biri benzer "piyasa riskine" sahiptir. yukarıda belirtilen teminatlandırma yöntemi olarak özellikler. İki yöntemin olduğu unutulmamalıdır. birbirini dışlamaz ve genellikle belirli bir ticaret, riskten korunma veya eski risk yönetimi işlevinde eşlenir sistem finans kurumları. Son olarak, yukarıdaki yaklaşımların bazı kombinasyonlarının güvenli olabileceğine inandığımızı anlayın, Varlıkları desteklemek / ilişkilendirmek için güvenilir ve genellikle risksiz süreç; ancak, bu noktada, bu, Likidite ve fiyat istikrarını sağlamak için almanın uygun olduğunu düşündüğümüz bir yön. Dahası, inanıyoruz ki bir rezerv temelli yaklaşım her zaman var olacak ve bu diğer yaklaşımları bir bütün olarak tamamlayacaktır. endüstri büyüyor. Teknolojideki gelişmeler devam ederken, mevcut tüm faydaları değerlendirip dahil edeceğiz % 100 geri alınabilirlik garantisini korurken. 17

Sayfa 18

Hukuk ve Uyum Tether Limited ("Tether"), Hong Kong Şirketleri uyarınca kurulmuş bir limited şirkettir Yönetmelik. Tümüyle Tether Holdings Limited'e aittir. BVI Ticari Şirketler Yasası, 2004. Tether, Mali Suçları Uygulama Ağında Para Hizmetleri İşletmesi olarak kayıtlıdır. ABD Hazine Bakanlığı (MSB Kayıt Numarası 31000058542968). Tether, bir ABD'deki Tether kullanıcılarına daha iyi hizmet verebilmek amacıyla bir ABD finans kurumu ile ilişki. Tether, RenRenBee Limited ("RenRenBee") ile bir ana-acente sözleşmesi imzalıyor. RenRenBee Hong Kong Gümrük ve Özel Tüketim Departmanı tarafından Para Hizmetleri Operatörü olarak lisans verilmiştir (Lisans No. 130901265). Anlaşma uyarınca, RenRenBee paranın aklanmasına karşı uyumluluk çalışması sağlayacaktır. ve Tether'in temsilcisi olarak müşteri durum tespiti prosedürleri. Bu ve diğer önlemlerle, Tether müşteri

durum tespiti, kayıt tutma ve ABD yasaları ve Hong Kong Para Aklamayla Mücadele ile tutarlı raporlama prosedürleri ve Terörle Mücadele Finansmanı (Finans Kuruluşları) Yönetmeliği. Tether Limited'in şu anda Tayvan'daki Cathay Bank ve Hwatai Bank'ta hesapları var ve her ikisi de Tether'in iş modelinin kabul edilebilir olduğunun bilincinde ve emin. Bu bankalar süreçlerimizden memnunlar ve ayrıca işimizin uygun şekilde çalıştığından da memnunlar. Tayvan açık deniz bankacılık düzenlemeleri ile, tüm bankalardan bunu kendi hesap açmadan önce kendi hukuk, uyumluluk ve merkez ofisi (ayrıca kendi isteğimiz üzerine). Bu bizim hedefimizdi en başından itibaren uyumlu bir operasyona sahip olmak ve maksimum düzeyde konforu sağlamak için burada bankacılık ortakları. Ek olarak, bu bankalar diğer Bitcoin tabanlı işletmelere sahiptir ve onlarla birlikte çalışmaktadır. 18

Sayfa 19

Terimler Sözlüğü Dijital para birimi: tanımladığı gibi http://en.wikipedia.org/wiki/Digital_currency Cryptocurrency veya merkezi olmayan dijital para birimi: opensource cryptocurrency her türlü, kriptografik olarak güvenlidir ve dağıtılmış bir defter kullanır. Görmek: <http://en.wikipedia.org/wiki/Cryptocurrency> Realworld para veya fiat para veya ulusal / egemen para birimi: Hangi cinsinden her türlü yukarıda tanımlandığı gibi kripto para birimleri değildir. Cryptocurrency sistemi: öncelikle varlığını sağlamak için oluşturulan yazılım ve süreçler koleksiyonu bir kripto para birimi. Eski mali sistemi: Bir cryptocurrency sistemi değil herhangi bir mali sistem. Utilitybacked dijital simge Dapps aka: bir değeri elde edilir dijital belirteci dağıtılmış sadece bir değer transfer sistemi olmaktan ziyade uygulamasının kullanışlılığı. Assetbacked / saptanmış cryptocurrency: kimin fiyatı realworld varlığa mihlan Herhangi cryptocurrency, yani, "fayda destekli" bir kripto para birimi değildir. Bağ (lar): tek bir birim (ya da birden fazla birim) fiatpegged cryptocurrency arasında Bariyer Limited tarafından verilen TetherUSD veya Illegal: cryptoUSD tek ünite urgan Limited tarafından yayınlanan Illegal: zaman içinde herhangi bir noktada dolaşımda Illegal kolektif miktarı. Bariyer Sistemi: topluca tüm süreci ve var olmaya Bağları sağlayan teknolojilere atıfta Karşılıklar ispatı: herhangi bir veren bir dijital simge dağıtılmış assetbacked bir süreç, kriptografik / matematiksel olarak, verilen tüm belirteçlerin tamamen ayrılmış ve desteklenmiş olduğunu kanıtlar dayanak varlık tarafından. 19

Sayfa 20

Referanslar [1]

<https://www.thefinancialist.com/wpcontent/uploads/2012/10/2012GlobalWealthReport.pdf> [2]

<https://bitcoin.org/bitcoin.pdf> [3]

http://www.deloitte.com/assets/DcomUnitedStates/Local%20Assets/Documents/FSI/us_fsi_BitcointheNewGoldRush_031814.pdf [4] <https://github.com/mastercoinMSC/spec> [5]

<http://unenumerated.blogspot.com/2005/12/bitgold.html> [6]

<https://iwillcox.me.uk/2014/provingbitcoinreserves> [7]

<http://antonopoulos.com/2014/02/25/coinbasereview/> [8]

<http://www.coindesk.com/krakensauditprovesholds100bitcoinsreserve/> 20