Sayfa 1

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz NEDEN BİZ ARE OLUŞTURMA Cardano Öznel Bir Yaklaşım CHARLES HOSKINSON < Charles.Hoskinson@iohk.io> <C3A6 5E46 7B54 77DF 3C4C 9790 4D22 B3CA 5B32 FF66> 1. Giriş Motivasyon Sojourn's End Teminat Kanıtı Paranın Sosyal Unsurları Katmanlarda Tasarım - Cardano Yerleşim Katmanı Komut dosyası oluşturma Yan zincirler İmzalar Kullanıcı Tarafından Verilen Varlıklar (UIA'lar) Ölçeklenebilirlik Cardano Hesaplama Katmanı Yönetmelik Tüm bunların anlamı nedir? 2. Bilim ve Mühendislik Yineleme Sanatı Gerçekler ve Görüşler İşlevsel Günahlar Neden Haskell? Resmi Şartname ve Doğrulama Şeffaflık 3. Birlikte çalışabilirlik Büyük Miyopi NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 1 arasında 44

Sayfa 2

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Eski Cryptocurrency Birlikte Çalışabilirliği Daedalus Labirenti 4. Düzenleme Yanlış İkili Meta veriler Kimlik Doğrulama ve Uygunluk Pazar yeri DAO'ları 5. Sürdürülebilirlik 6. Sonuç 1. Giriş Motivasyon Cardano, 2015 yılında kripto para birimlerinin durumunu değiştirme çabası olarak başlayan bir projedir. tasarlanmış ve geliştirilmiştir. Belirli bir yenilikler dizisinin ötesindeki genel odak, bir kullanıcılarının ihtiyaçlarını daha iyi karşılayan daha dengeli ve sürdürülebilir ekosistem ve entegrasyon arayan diğer sistemler. Birçok açık kaynak projesinin ruhuna uygun olarak, Cardano kapsamlı bir yol haritası veya hatta yetkili bir teknik inceleme. Aksine bir tasarım koleksiyonunu kucakladı ilkeler, en iyi mühendislik uygulamaları ve keşif yolları. Bunlar aşağıdakileri içerir: ● Muhasebe ve hesaplamanın farklı katmanlara ayrılması ● Oldukça modüler işlevsel kodda temel bileşenlerin uygulanması ● Meslektaş incelemesinden geçmiş araştırmalarla rekabet eden küçük akademisyen ve geliştirici grupları ● InfoSec uzmanlarının erken kullanımı dahil olmak üzere disiplinler arası ekiplerin yoğun kullanımı ● Teknik incelemeler, uygulama ve yeni araştırma arasında hızlı yineleme gerekli inceleme sırasında keşfedilen doğru sorunlar ● Ağa zarar vermeden dağıtım sonrası sistemleri yükseltme becerisini geliştirme ● Gelecekteki çalışmalar için merkezi olmayan bir finansman mekanizmasının geliştirilmesi NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 2/44

3. Sayfa

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz ● Kripto para birimlerinin tasarımının üzerinde çalışabilmeleri için iyileştirilmesine ilişkin uzun vadeli bir bakış makul ve güvenli bir kullanıcı deneyimine sahip mobil cihazlar ● Paydaşları kripto para birimlerinin işlemlerine ve bakımına yaklaştırma ● Aynı defterde birden çok varlığı hesaba katma ihtiyacını kabul etme ● Soyutlama işlemleri, daha iyi uyum sağlamak için isteğe bağlı meta verileri içerecek şekilde eski sistemlerin ihtiyaçları ● Mantıklı özellikleri benimseyerek yaklaşık 1.000 altcoin'den bilgi edinin ● İnternet Mühendisliği Görev Gücü'nden esinlenen, standartlara dayalı bir süreci benimseyin: nihai protokol tasarımını kilitlemek için özel bir temel ● Ticaretin sosyal unsurlarını keşfedin ● Düzenleyicilerin ticaretle etkileşim kurması için sağlıklı bir orta yol bulun Bitcoin'den miras alınan bazı temel ilkelerden taviz vermek Bu yapılandırılmamış fikir dizisinden, Cardano üzerinde çalışan müdürler her ikisini de keşfetmeye başladı kripto para literatürü ve soyutlamalar için bir araç seti oluşturmak. Bu araştırmanın çıktısı IOHK kapsamlımakale kütüphanesiSayısız

anket bu son gibi sonuçları komut dosyası dil genel bakışı yanı sıra birAkıllı Sözleşmelerinin Ontoloji veScorex projesi. Dersler kripto para birimi endüstrisinin olağandışı ve bazen verimsiz büyüme. İlk olarak, TCP / IP gibi başarılı protokollerin aksine, tasarımında çok az katman vardır. kripto para birimleri. Etrafında tek bir fikir birliği fikrini koruma arzusu vardı. mantıklı olup olmadığına bakılmaksızın tek bir deftere kaydedilen gerçekler ve olaylar. Örneğin, Ethereum muazzam bir karmaşıklık yaratarak bir evrensel dünya bilgisayarı, ancakpotansiyel olarak sistemin zarar görmesine neden olan önemsiz endişelerden muzdariptir. bir değer deposu olarak faaliyet gösterme yeteneği. Herkesin programı birinci sınıf bir vatandaş olmalı mı? ekonomik değeri, bakım maliyeti veya düzenleyici sonuçları ne olursa olsun? İkincisi, genel kriptografik araştırmalardaki önceki sonuçlar için çok az takdir vardır. İçin örnek, Bitshares 'delege edilmiş Proof of Stake , kolayca ve güvenilir bir şekilde rastgele oluşturulmuş olabilir garantili çıktı teslimi ile bozuk para atmayı kullanan sayılar, 1980'ler (bkz Rabin ve Ben-Or tarafından seminal kağıt). Üçüncüsü, çoğu altcoin (aşağıdaki gibi birkaç önemli istisna dışındaTezos) hiç yapmadım gelecekteki güncellemeler için konaklama. Yumuşak veya sert çatalı başarılı bir şekilde itme yeteneği çok önemlidir herhangi bir kripto para biriminin uzun vadeli başarısına. Sonuç olarak, kurumsal kullanıcılar milyonlarca dolar değerinde kaynağı yol haritasının ve arkasındaki aktörlerin geçici, önemsiz veya radikalleştirildiği protokoller. Orada NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 3/44

4. sayfa

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz için bir vizyon etrafında sosyal fikir birliğinin oluşabileceği verimli bir süreç olması gerekir. temeldeki protokolü geliştirmek. Bu süreç son derece külfetli ise, parçalanma topluluğu parçalayabilir. Son olarak, para nihayetinde sosyal bir fenomendir. Anonimleştirme çabası ve Orta düzey merkezi aktörler, Bitcoin ve çağdaşları da ticari işlemlerde istikrarlı kimlikler, meta veriler ve itibar. Bu verileri eklemek merkezi çözümler aracılığıyla denetlenebilirliği, küresel kullanılabilirliği ve değişmezliği ortadan kaldırır - bu bir blockchain kullanmanın tüm amacıdır. SWIFT, FIX ve ACH'den oluşanlar gibi eski finansal sistemler, işlem meta verileri. Hesaplar arasında ne kadar değer taşındığını bilmek yeterli değildir, düzenleme genellikle ilgili aktörlerin atıfta bulunmasını, uyum bilgilerini, raporlamayı gerektirir. şüpheli etkinlik ve diğer kayıtlar ve eylemler. Bazı durumlarda meta veriler daha fazladır işlemden daha önemli. Bu nedenle, meta verilerin manipülasyonunun en az sahte para birimi veya işlem geçmişini yeniden yazma. Oyunculara yer yok bu alanları gönüllü olarak dahil etmek isteyenler ana akım benimsemeye ters etki yapıyor gibi görünüyor ve tüketicinin korunması. Sojourn's End Kripto para birimi uzayının ilkeli keşfimizin toplamı, iki koleksiyondur. protokoller. Sırasıyla, kanıtlanabilir şekilde güvenli bir Proof-of-Stake [1] [2] tabanlı kripto para birimi Cardano Yerleşim Katmanı (CSL) ve Cardano Hesaplama Katmanı adı verilen bir dizi protokol (CCL). Tasarım vurgumuz, kripto para birimlerinin sosyal yönlerini barındırmak, katmanlar halinde inşa etmektir. değer muhasebesini karmaşık hesaplamadan ayırarak ve çeşitli değişmez ilkeler kapsamında düzenleyiciler. Dahası, mantıklı olduğu yerde, 1deniyoruzakran değerlendirme yoluyla veteriner önerilen protokoller vekodu resme göre kontrol et özellikler. 1 Liste için Yönetmelik bölümüne bakın NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 4/44

5.Sayfa

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Teminat Kanıtı Bir kripto para birimi için hissenin kanıtını kullanmak,hararetle tartışılan tasarım seçimi, ancak çünkü güvenli oylama sağlamak için bir mekanizma ekler, daha fazla ölçeklendirme kapasitesine sahiptir ve daha fazlasına izin verir egzotik teşvik programları, onu benimsemeye karar verdik. Teminat kanıtı protokolümüzün adıOuroboros ve son derece Profesör Aggelos liderliğindeki beş akademik kurumdan yetenekli kriptograf ekibi 2Edinburgh Üniversitesi'nden Kiayias. Kanıtlanmış güvenli olmanın ötesinde getirdiği temel yenilik kullanaraktitiz kriptografik model , modüler ve esnek bir tasarımdır. işlevselliği geliştirmek için birçok protokolün bileşimi. Bu modülerlik, yetkilendirme, yan zincirler, abone olunabilen kontrol noktaları, Işık müşteriler için iyi bir veri yapıları, farklı formları rastgele numara düz ve farklı senkronizasyon varsayımları. Bir ağ geliştikçe, binlerce kişiden milyonlarca ve hatta milyarlarca kullanıcı, fikir birliği algoritmasının gereksinimleri de değişiklik. Bu nedenle, bu değişikliklere uyum sağlamak için yeterli esnekliğe sahip olmak hayati önem taşımaktadır ve dolayısıyla bir kripto para biriminin kalbini geleceğe hazırlayın. Paranın Sosyal Unsurları Kripto para birimleri, paranın sosyal bileşeninin en önemli örneğidir. Kısıtlarken yalnızca teknolojiye yönelik analiz, Bitcoin ile Litecoin arasında çok az fark vardır ve hatta Ethereum ve Ethereum Classic arasında daha az. Yine de hem Litecoin hem de Ethereum Classic büyük piyasa kapitalizasyonlarını ve sağlam, dinamik toplulukları ve kendi topluluklarını korumak sosyal görevler. Bir kripto para biriminin değerinin büyük bir kısmının kendi topluluğundan kaynaklandığı söylenebilir. para birimini kullanma şekli ve para biriminin gelişimine katılım düzeyi. İlerleme Dash gibi para birimleri, sistemleri doğrudan protokole entegre etti. neyin geliştirilmesi ve finanse edilmesi gerektiğine karar vermek için topluluklarını dahil edin. 2 Connecticut Üniversitesi, Atina Üniversitesi, Edinburgh Üniversitesi, Aarhus Üniversitesi, Tokyo Teknoloji Enstitüsü NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 5/44

Sayfa 6

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Kripto para birimlerinin geniş çeşitliliği, sosyal unsurları için de kanıt sağlar. Felsefe, para politikası ve hatta sadece çekirdek geliştiriciler arasındaki anlaşmazlıklar parçalanmaya ve çatallara yol açar. Yine de kripto para birimlerinden farklı olarak, fiat para birimleri süper güçler, bir döviz krizi veya krizi olmaksızın siyasi değişimlerden ve yerel anlaşmazlıklardan sağ çıkma eğilimindedir. toplu göç. Bu nedenle, eski sistemlerde eksik olan unsurlar var gibi görünüyor. kripto para birimi endüstrisi. Biz tartışıyoruz ve Cardano yol haritasına telkin ettik - Bir protokolün kullanıcıları, protokollerinin arkasındaki sosyal sözleşmeyi anlamak için teşviklere ihtiyaç duyar ve üretken bir şekilde değişiklik önerme özgürlüğüne sahip olun. Bu özgürlük herkese uzanır bir değer değişim sisteminin yönü, piyasaların nasıl düzenleneceğine karar vermekten hangisine projeler finanse edilmelidir. Yine de merkezi aktörler aracılığıyla aracılık edilemez ve iyi finanse edilen bir azınlık tarafından seçilebilecek bazı özel yetki. Cardano, CSL'nin üzerine inşa edilen bir bindirme protokolleri sistemi uygulayacaktır. kullanıcılarının ihtiyaçları. Birincisi, geliştirmeyi başlatmak için kitle satışının başarısı ne olursa olsun, fonlar eninde sonunda dağıtmak. Bu nedenle, Cardano, monoton olarak finanse edilen merkezi olmayan bir tröst içerecektir. 3enflasyon ve işlem ücretlerinin düşürülmesi. Herhangi bir kullanıcı, bir oy pusulası sistemi aracılığıyla güvenden fon talep etme hakkına sahip olmalıdır ve CSL paydaşları kimin yararlanıcı olacağı konusunda oy kullanır. Süreç üretken bir Hazine / güven sistemleri ile diğer kripto para birimlerinde görülen geri bildirim döngüsü,Dash gibi, tarafından Kimin finanse edilip edilmemesi gerektiği hakkında bir konuşma başlatmak. Finansman tartışmaları, kripto

para biriminin sosyal olan uzun ve kısa vadeli hedeflerin ilişkisini zorlar sözleşme, öncelikler ve belirli tekliflerle değer yaratma inancı. Bu konuşma topluluğun olasılıklara karşı inançlarını sürekli olarak değerlendirdiği ve tartıştığı anlamına gelir. yol haritaları. İkincisi, umudumuz, Cardano'nun sonunda resmi, blockchain tabanlı bir sistemi dahil edeceğidir. hem yumuşak hem de sert çatalları önerin ve oylayın. Blok boyutu tartışmasıyla Bitcoin, Ethereum ile DAO çatalı ve diğer birçok kripto para birimi uzun süredir ayakta kaldı ve sık vakalar, kod tabanının teknik ve ahlaki yönü üzerine çözülmemiş tartışmalar. Bu anlaşmazlıkların birçoğunun ve eyleme geçildiğinde ortaya çıkan topluluk, resmi süreçlerin eksikliğinin doğrudan bir sonucudur. değişimi tartışmak. 3 Bu aynı zamanda bir hazine sistemi olarak da bilinir NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 44 üzerinden 6

7. Sayfa

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Bitcoin kullanıcılarını Ayrılmış Tanık'ı benimsemeye ikna etmek için nereye gidilebilir? Nasıl olmalı Ethereum'un çekirdek geliştiricileri, DAO'yu kurtarmak için topluluk duyarlılığını ölçüyor mu? Eğer topluluk kırılmaları, kripto para birimi onarılamayacak kadar hasar görmüş mü? En kötü durumlarda, ahlaki eylem yetkisi, geliştiricilere sahip olan kişiye devredilebilir. altyapı ilişkileri ve para, büyük çoğunluğunun en iyi dilekleri değil topluluk. Ayrıca, topluluğun büyük bir kısmına erişilemezse veya süresi dolmuşsa kötü güdülere, o zaman kişi eylemlerinin meşru olup olmadığını nasıl gerçekten bilebilir? 4 Gibi Önerilen cryptocurrencies Tezos nerede incelemek için ilginç bir örnek teşkil kripto para protokolü, üç bölümden oluşan bir anayasa gibi ele alınır (İşlem, Konsensüs ve Ağ) anayasayı güncellemek için bir dizi resmi kural ve süreç ile. Hala Teşviklerle ve tam olarak nasıl modelleneceği ve değiştirileceği konusunda yapılacak çok iş var. resmi bir dile sahip bir kripto para birimi. Biçimsel yöntemlerin kullanımı,makine ile anlaşılabilir özellikler ve bir hazineyi birleştirme Bu mali teşvik süreci ilham almak için olası yollar olarak araştırılmaktadır. Sonuçta, şeffaf, sansürsüz bir şekilde bir protokol değişikliği önerme yeteneği Blockchain tabanlı oylama, daha zarif çözümler başaramasa bile süreci iyileştirmelidir. tasarlanacak. Katmanlar tasarlama - Cardano Uzlaşma Katmanı Harika protokoller ve diller tasarlarken, geleceğe değil, daha ziyade geçmiş. Tarih, kağıt üzerinde mükemmel olan harika fikirlerin hala bir şekilde hayatta kalamadı, örneğinAçık Sistemler Arabağlantı standartları. Tarih ayrıca TCP / IP'den JavaScript'e geçen mutlu kazalar sağlar. Tarihsel bir bakış açısıyla çıkarılan bazı ilkeler şunlardır: 1. Geleceği tahmin edemezsiniz, bu yüzden kıpır kıpır odada inşa edin 2. Karmaşıklık kağıt üzerinde iyidir, ancak basitlik genellikle kazanır 3. Çok fazla aşçı et suyunu bozar 4. Bir standart belirlendikten sonra, büyük olasılıkla geçerli olup olmadığına bakılmaksızın devam edecektir. standart altı 4 Bkz.rasyonel cehalet NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 44 üzerinden 7

8. Sayfa

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz 5. Bir irade varsa, kötü fikirler aslında oldukça iyi fikirlere dönüşebilir Cardano, sosyal yapısını kabul eden bir finansal sistemdir. Çok büyük bir ihtiyaç olacaktır. esneklik ve belirli bir kullanıcının işlemindeki keyfi karmaşıklığı ele alma yeteneği için. başarılı, muazzam hesaplama, depolama ve ağ kaynaklarına ihtiyaç olacak milyonlarca eşzamanlı işlemi barındırmak için. Yine de, zengin düğümlerden alabileceğimiz dijital, merkezi olmayan bir Robin Hood'umuz yok ve Vermek adil bir ağ oluşturmak için fakirler. İnsana güvenmek ağın daha büyük yararı için fedakarca fedakarlık yapma iyiliği. Bu nedenle, Cardano'nun tasarım, kaygıların ayrılması kavramını TCP / IP'den ödünç alır. Blok zincirler, nihayetinde, gerçekleri ve olayları garanti altına alan veri tabanlarıdır. zaman damgaları ve değişmezlik. Para bağlamında,

varlıkların sahipliğini sipariş ederler. programları depolayarak ve çalıştırarak karmaşık hesaplama ortogonal bir kavramdır. Alice'den Bob'a ne kadar değer kattığını bilmek mi yoksa dahil olmak mı istiyoruz? Anlamakta işlemin arkasındaki tüm hikaye ve ne kadar gönderileceğine karar vermek? Ethereum'un yaptığı gibi ikincisini seçmek inanılmaz derecede cazip çünkü daha esnek, ancak yukarıdaki tasarım ilkelerini ihlal ediyor. Hikayeyi anlamak, tek bir protokolün keyfi olayları anlayabilmeli, keyfi işlemleri yazabilmeli, tahkime izin vermeli dolandırıcılık vakaları ve hatta yeni bilgiler yapıldığında potansiyel olarak tersine işlemler mevcut. Daha sonra, her biri için hangi meta verilerin depolanacağına dair zor tasarım kararları vermek gerekir. Alice ve Bob'un işleminin arkasındaki hikayenin hangi unsurları önemlidir? Sonsuza kadar alakalı mı? Bazı verileri ne zaman çöpe atabiliriz? Bunu yapmak yasaları ihlal eder mi? içinde bazı ülkeler? Ayrıca, bazı hesaplamalar doğası gereği özeldir. Örneğin, ortalama hesaplanırken bir ofiste çalışanların maaşını, her bir kişinin ne kadarını sızdırmak istemeyiz? yapar. Peki ya her hesaplama herkes tarafından biliniyorsa? Ya bu reklamönyargı yürütme sonuca zarar verme emri? Bu nedenle, değer muhasebesinin, değerin neden değiştirildiğinin arkasındaki hikaye. Diğer bir deyişle, değerin hesaplamadan ayrılması. Bu ayrılık, Cardano'nun akıllı sözleşmeleri desteklemeyeceği anlamına gelmez. ayırmayı açık hale getirerek, tasarım, kullanım ve kullanımda önemli ölçüde daha fazla esnekliğe izin verir. akıllı sözleşmelerin gizliliği ve yürütülmesi. NEDEN BİZ Cardano inşa ediyoruz

Sayfa 9

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Değer defteri, Cardano Uzlaşma Katmanı (CSL) olarak adlandırılır. İçin yol haritasının aşağıdaki hedefleri vardır: 1. Biri değeri taşımak, diğeri geliştirmek için olmak üzere iki set betik dilini destekleyin yer paylaşımlı protokol desteği 2. KMZ yan zincirlerinin diğer defterlere bağlanması için destek sağlayın 53. Daha yüksek düzeyler için kuantuma dirençli imzalar dahil olmak üzere birden çok imza türünü destekleyin güvenlik 4. Birden çok kullanıcı tarafından verilen varlığı destekleyin 5. Gerçek ölçeklenebilirliğe ulaşın, yani daha fazla kullanıcı katıldıkça sistemin yetenekleri artırmak Komut dosyası oluşturma Komut dosyası dilinden başlayarak, bir defterdeki adresler arasındaki işlemler bazı çalıştırılacak ve geçerli olduğu kanıtlanacak bir komut dosyası biçimi. İdeal olarak, Havva'nın erişmek için Ne Alice'in parası, ne de kötü tasarlanmış bir senaryonun yanlışlıkla ölüye değer göndermesini istemez. fonları geri alınamaz hale getiren adres. Bitcoin gibi sistemler, son derece esnek olmayan ve acımasız bir betik dili sağlar. ısmarlama işlemleri programlamak ve okumak ve anlamak zordur. Solidity gibi dillerin programlanabilirliği olağanüstü miktarda karmaşıklık getirir sisteme dahil edilir ve yalnızca çok daha küçük aktörler için yararlıdır. Bu nedenle, yaratıcısının onuruna Simon adında yeni bir dil tasarlamayı seçtik. 6Simon Thompson ve ona ilham veren kavramların yaratıcısı Simon Peyton Jones. Simon, dayanmaktadır bir alana özgü dil oluşturma sözleşmeler: Mali bir macera mühendislik . Temel fikir, finansal işlemlerin genellikle bir koleksiyondan oluşmasıdır. temel unsurlar. Biri finansal periyodik tablolar tablosunu bir araya getirirse, o zaman 7Olmasa bile çoğunu kapsayacak, keyfi olarak büyük bir bileşik işlem kümesi için destek sağlamak tümü, genel programlanabilirlik gerektirmeyen yaygın işlem türleri. 5 Kiayias, Zindros ve Miller'dan bir makalede yakında geliyor 6 Spesifikasyonlar yaklaşan bir spesifikasyonda yayınlanacaktır.Tam dil, Shelley CSL sürümü 2017'nin 4. çeyreği için planlanıyor 7ACTUS ProjesiDerinlemesine bir ayrıntıya sahiptir NEDEN BİZ Cardano inşa ediyoruz

Sayfa 10

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Birincil avantaj, güvenlik ve uygulamanın son derece iyi anlaşılabilmesidir. şablonların doğruluğunu göstermek ve uygulama alanını tüketmek

için yazılabilir. oluşturulması gibi sorunlu işlem olaylarıhavadan yeni para dışarı veyaişlem uysallıkİkinci olarak, yumuşak çatallar yoluyla daha fazla eleman eklemek için uzatmalarda bırakılabilir. yeni işlevsellik gereklidir. Bununla birlikte, CSL'yi bindirme protokollerine, eski finansal sistemleri ve özel amaçlı sunucular. Böylece geliştirdik PlutusHem genel olarak amaçlı akıllı sözleşme dili ve ayrıca birlikte çalışabilirlik için özel amaçlı bir DSL. Plutus, Haskell'den gelen kavramlara dayanan, yazılı bir işlevsel dildir ve şu amaçlarla kullanılabilir: özel işlem komut dosyaları yazın. CSL için, gerekli karmaşık işlemler için kullanılacaktır. Yan zincir şemamız gibi bağlamamız gereken diğer katmanlar için destek ekleyin. Yan zincirler Yan zincirlerle ilgili olarak Cardano, Kiayias, Miller ve Zindros (KMZ yan zincirleri) önceki sonuçlara göreçalışma kanıtlarının kanıtlarıÖzel tasarım bu yazının kapsamı dışındadır; ancak konsept, güvenli ve fonların CSL'den herhangi bir Cardano Hesaplama Katmanına veya diğerine etkileşimli olmayan hareketi protokolü destekleyen blockchain. KMZ yan zincirleri, karmaşıklığı kapsüllemenin anahtarıdır. Yasal gerekliliklere sahip defterler, özel işlemler, sağlam betik dilleri ve diğer özel endişeler etkili bir şekilde siyahtır kutuları CSL'ye eklememize rağmen, CSL kullanıcısı muhasebe konusunda belirli garantiler ve hesaplama tamamlandıktan sonra fonları geri çağırın. İmzalar Değeri Alice'den Bob'a güvenli bir şekilde taşımak için, Alice'in Doğru fonları hareket ettirin. Bu görevi gerçekleştirmenin en doğrudan ve güvenilir yolu,halka açık anahtar imza şemasıFonların bir açık anahtara bağlandığı ve Alice'in bir ilişkili özel anahtar. Farklı güvenlik parametreleri ve varsayımlarına sahip yüzlerce olası şema vardır. Bazıları, aşağıdakilerle bağlantılı matematiksel problemlere güvenir:eliptik eğrilerDiğerleri ise egzotik kavramlarla bağlantılıkafesler. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 10/44

Sayfa 11

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Soyut hedef her zaman aynıdır. Çözülemedikçe çözülemeyecek zor bir problem vardır. birinin gizli bir bilgi parçası vardır. Bu bilgi parçasının sahibinin Olmak anahtar çiftinin sahibi ve kullanma yeteneğine sahip tek varlık olmalıdır O. Bir kripto para biriminin imza şeması seçerken karşılaştığı iki endişe grubu vardır. Birincisi, planın kendisinin uzun vadeli güvenlik dayanıklılığı vardır. Bazıları kriptografik 1970'lerde ve 1980'lerde kullanılan DES gibi şemalar kırıldı. planın ayakta kalması beklenmeli ve karar verilmelidir. İkincisi, tercih eden birçok işletme, hükümet ve diğer kurumlar var veya bazı durumlarda, belirli bir planın kullanılması zorunludur. Örneğin, NSA, Suite B protokol seti. Dan standartlar vardır ISOve hatta W3C kriptografi çalışma grupları. Bir kripto para birimi tek bir imza şeması seçerse, şemayı kabul etmek zorunda kalır. gelecekte bir noktada bozulabilir ve en az bir varlık yasal veya endüstri kısıtlamaları nedeniyle kripto para birimi. Yine de bir kripto para birimi, imza şeması, çünkü bu, her müşterinin her şemayı anlamasını ve doğrulamasını gerektirir. Cardano için eliptik eğri kriptografisini kullanmaya karar verdik.Ed25519 eğrisiİçinde Ayrıca, mevcut kütüphaneleri geliştirmek için destek ekleyerek karar verdik.HD cüzdanlar kullanmaDr Dmitry Khovratovich ve Jason Law'un Spesifikasyonu . 8 Bu, Cardano'nun gelecekte daha fazla imza planını destekleyeceğini söyledi. entegre etmekle ilgileniyorBLISS-B eklenti içinkuantum bilgisayara dirençli imzalarSistemimize. Ayrıca eklemekle ilgileniyoruzSECP256k1Eski ile birlikte çalışabilirliği geliştirmek için Bitcoin gibi kripto para birimleri. Cardano, daha fazla imza eklememizi sağlayacak özel uzantılarla tasarlandı bir soft fork aracılığıyla düzenler. Gerektiğinde ve içinde planlanan büyük güncellemeler sırasında eklenecekler. yol haritası. 9 Kullanıcı Tarafından Verilen Varlıklar (UIA'lar) Bitcoin'in tarihinin başlarında, protokoller, kullanıcıların bu tür varlıkları yayınlamasına olanak sağlamak için hızla geliştirildi. Aynı anda birden fazla para birimini izlemek için Bitcoin'in muhasebe sistemine bindirildi. 8 Bu,dokümantasyonCardano'nun HD Cüzdan Uygulaması için. Cardano'nun ilk Ed25519 HD Cüzdanlarını desteklemek için kripto para birimi 9 Bkz. Cardanoroadmap.com NEDEN

Sayfa 12

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Bu protokoller, Bitcoin protokolü tarafından yerel olarak desteklenmedi, ancak akıllı hackler. Bitcoin örneği gibi kaplayan yılında Renkli Coins veMastercoin (şimdi Omni denir) , hafif istemciler güvenilir sunuculara güvenmek zorunda kalıyor. Ayrıca işlem ücretlerinin hala ödenmesi gerekiyor bitcoins. Bu özellikler, işlem onayı için tek ardışık düzen ile birleştirildiğinde Çoklu varlık muhasebesi için Bitcoin yetersiz. Kullanarak Ethereum durumda ERC20 standardınıDaha fazla özellik zenginliği var. Ancak, işlem ücretleri hala eter gerektiriyor.Ayrıca, Ethereum ağı zorluk yaşıyor ölçeklemekverilen tüm ERC20 tokenlerinin ihtiyaçları. Temel sorun üç bölüme ayrılabilir: kaynaklar, teşvikler ve endişe. Kaynaklarla ilgili olarak, aynı deftere tamamen yeni bir para birimi eklemek, birinin sahip olduğu anlamına gelir. bant genişliği, mempool ve paylaşan iki bağımsız UTXO (harcanmamış işlem girdileri) seti blok alanı. Bu para birimlerinin işlemlerini yerleştirmekten sorumlu fikir birliği düğümleri bunu yapmak için bir teşvike ihtiyaç duyuyor. Bir kripto para biriminin her kullanıcısı bunu önemsemeyecek veya Hakkında belirli bir varlığın para birimi. Bu sorunlar göz önüne alındığında, çok varlıklı bir defterin birincil belirteci olarak faydaları muazzamdır. merkezi olmayan piyasa yapıcılığına izin veren bir köprü para birimi olarak etkili bir şekilde hizmet edebilir. Değer istikrarlı varlıklar gibi ek fayda sağlamak için amaçlı varlıklar ihraç edilebilir. Tetherveya MakerDAOBorç verme ve havale uygulamaları için yararlıdır. Zorluklar göz önüne alındığında, Cardano çoklu varlık muhasebesine pragmatik bir yaklaşım benimsemiştir. Aşamalar halinde inşa edilen ilk zorluk, Binlerce UIA'nın talepleri. Yani aşağıdaki ilerlemeler gereklidir: 1. Çok büyük bir verilerin izlenmesine izin vermek için özel amaçlı kimliği doğrulanmış veri yapıları UTXO durumu 2. Çok sayıda bekleyen işlemi tutmak için dağıtılmış bir mempool'a sahip olma yeteneği 3. Büyük bir küresel blok zincirine izin vermek için blok zinciri bölümleme ve kontrol noktaları 4. Farklı grupların dahil edilmesi için fikir birliği düğümlerini ödüllendiren bir teşvik şeması işlemler 5. Kullanıcıların hangi para birimlerini izlemek istediklerine karar vermelerine olanak tanıyan bir abonelik mekanizması 6. Güçlü güvenlik, UIA'ların yerel varlıkla benzer güvenlikten yararlanmasını garanti eder 7. UIA ve UIA arasındaki likiditeyi iyileştirmek için merkezi olmayan piyasa yapıcılığı için destek birincil belirteç NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 12 bölgesinin 44

Sayfa 13

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Doğrulanmış doğru veri yapısını bulmaya yönelik ilk çabalarımız, yeni bir türüLeo Reyzin, IOHK ve Waves tarafından ortaklaşa geliştirilen AVL + AğacıDaha fazla araştırma yapılması gerekiyor, ancak bu, Cardano'nun daha sonraki bir sürümüne dahil edilecek olan temel bir gelişmedir. Dağıtılmış bir mempool kullanılarak uygulanabilirStanford Üniversitesi'nin RAMCloud protokolü. Deneyler, Cardano'nun fikir birliği katmanına entegrasyonunu incelemek için 2017'nin 3. çeyreğinde başlayacak. Kalan konular birbiriyle bağlantılıdır ve devam eden araştırmalar kapsamındadır. Bekliyoruz - konu sonuçları araştırmak için - CSL Basho sırasında UIA'lar için Cardano'ya bir protokol eklemek 2018'de piyasaya sürüldü. Ölçeklenebilirlik Dağıtılmış sistemler, bir protokolü çalıştırmayı kabul eden bir dizi bilgisayardan (düğümlerden) oluşur veya ortak bir hedefe ulaşmak için protokoller paketi. Bu hedef, şu şekilde tanımlandığı gibi bir dosya paylaşmak olabilir: BitTorrent protokolü veya Folding @ Home kullanarak bir proteini katlama. En etkili protokoller, düğümler ağa katıldıkça kaynak kazanır. Barındıran bir dosya Örneğin, BitTorrent, eğer birçok eşdeğeri varsa, ortalama olarak çok daha hızlı indirilebilir. eşzamanlı olarak indiriyor. Akranlar kaynak

sağlarken hız artar ayrıca onları tüketiyor. Bu özellik, bir kişinin tipik olarak dağıtılmış bir sistem ölçekleri. Mevcut tüm kripto para birimlerinin tasarımındaki zorluk, aslında ölçeklenebilir olacak şekilde tasarlandı. Örneğin, blok zincirleri genellikle yalnızca ek bağlantılı bir listedir. bloklar. Bir blok zinciri protokolünün güvenliği ve kullanılabilirliği birçok düğüme bağlıdır blockchain verilerinin tam bir kopyasına sahip olmak. Bu nedenle, tek bir bayt veri kopyalanmalıdır N düğümler arasında. Ek düğümler ek kaynaklar sağlamaz. Bu sonuç, işlem işleme ve mesajların dedikoduları için aynıdır. sistem. Konsensüs sistemine daha fazla düğüm eklemek, ek işlem işleme gücü. Sadece aynı şeyi yapmak için daha fazla kaynak harcanması gerektiği anlamına gelir iş. Daha fazla ağ aktarımı, daha fazla düğümün aynı mesajları iletmek zorunda olduğu anlamına gelir. tüm ağ en güncel blok ile senkronizasyon halinde. Bu topoloji göz önüne alındığında, kripto para birimleri, mirasla aynı düzeyde küresel bir ağa ölçeklenemez finansal sistemler. Buna karşılık, eski altyapı ölçeklenebilirdir ve aşağıdakiler için büyük siparişlere sahiptir: daha fazla işlem ve depolama gücü. Belirli bir nokta eklemek, Bitcoin çok küçük bir ağdır ödeme emsallerine oranla, ancak mevcut yükünü yönetmekte zorlanıyor. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 13 bölgesinin 44

Sayfa 14

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Cardano için ölçeklenebilirlik hedeflerimiz, fikir birliği algoritmamız tarafından büyük ölçüde desteklenmektedir. Ouroboros daha fazla çalışabilen bir fikir birliği düğümleri yeterli çoğunluğunu seçmek için merkezi olmayan bir yola izin verir büyük şirketlerin ihtiyaçlarını karşılamak için son 20 yılda geliştirilen geleneksel protokoller Google ve Facebook gibi altyapı sağlayıcıları. 10 Örneğin, bir dönem için bir yeter sayının seçilmesi, bunu yapmak için güvenilir bir düğüm kümesine sahip olduğumuz anlamına gelir. defteri belirli bir süre boyunca koruyun. Aynı anda birden fazla yeter sayısı seçmek önemsizdir ve işlemlerin farklı çekirdek sayılarına bölünmesi. Ağ yayılımı ve ayrıca blok zincirini parçalamak için benzer teknikler uygulanabilir. kendisini benzersiz bölümlere ayırır. Mevcut yol haritamızda, ölçeklendirme yöntemleri uygulanacak Ouroboros 2018'de başlıyor ve 2019 ve 2020'de odak noktası olmaya devam ediyor. Cardano Hesaplama Katmanı Daha önce belirtildiği gibi, bir işlemin iki bileşeni vardır: gönderme mekanizması ve jeton akışını ve jetonların arkasındaki nedenlerin yanı sıra koşulları kaydedin. ikincisi isteğe bağlı olarak karmaşık olabilir ve terabaytlarca veriyi, çoklu imzaları ve özel Meydana gelen olaylar. İkincisi, tek bir imza değeri iten önemli ölçüde basit olabilir başka bir adrese. Değer akışının nedenlerini ve koşullarını modellemenin arkasındaki zorluk, En tahmin edilemez yollarla ilgili varlıklar için son derece kişiseldir. sözleşme hukuku, aktörlerin kendilerinin yapamayacağı daha da sorunlu bir tablo çiziyor hatta farkında olunişlem ticari gerçeklikle eşleşmiyorBiz buna genellikle "anlamsal boşluk" fenomeni. 11 Sonsuz bir karmaşıklık ve soyutlama katmanının peşinden koşan bir kripto para birimi neden inşa edilmeli? Doğası gereği Sisyphean ve pratikte naif görünüyor. Dahası, her soyutlama benimsendi. hem yasal hem de güvenlikle ilgili sonuçları vardır. Örneğin, evrensel olarak yasa dışı kabul edilen veya küçümsenen çok sayıda çevrimiçi etkinlik vardır. çocuk pornografisi kaçakçılığı veya devlet sırlarının satışı gibi. 10 Aynı sonuca ulaşmaya çalışan başka bağımsız araştırma protokolleri de vardır. elastico veBitcoin-NG 11 Loi Luu ve diğerleri bu boşluğu,Akıllı Sözleşmeleri Daha Akıllı Hale Getirme NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 14 bölgesinin 44

Sayfa 15

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz merkezi olmayan altyapı, biri şimdi bu faaliyetin gerçekleşmesi için bir kanal sağlıyor. Normal ticari işlemlerin sahip olduğu aynı sansür direnci. Yasal olarak belirsizdir. ağın fikir birliği düğümleri - daha fazla federe olma teşviki var Verimliliği artırma zamanı - barındırdıkları içerikten sorumlu tutulacak. Tor operatörlerin Savcılık ,İpek Yolu operatörünün acımasızca muamelesiVe genel olarak eksikliği protokol katılımcılarının yasal korumalarının ardındaki hukuki netlik belirsiz bir yol bırakmaktadır. Yeterince gelişmiş bir kripto para biriminin başka neler sağlayabileceğine dair hayal gücü eksikliği yok (görmek Gyges YüzüğüBir kripto para biriminin tüm kullanıcılarını onaylamaya veya en azından Web'in en kötü eylemlerini ve davranışlarını mümkün kılıyor mu? Ne yazık ki, bir kripto para birimi tasarımcısına fikir veren net cevaplar yok. bir pozisyon seçme ve onun değerini savunma hakkında daha fazla bilgi. Cardano'nun ve Bitcoin, endişeleri katmanlara ayırmayı seçmiş olmamızdır. Bitcoin ile, AnaçCardano ile Cardano Hesaplama Katmanı vardır. Daha önce detaylandırılan eylemleri mümkün kılacak karmaşık davranış türleri üzerinde çalışılamaz. CSL. Tam Turing dilinde yazılmış programları çalıştırma becerisine ihtiyaç duyarlar. hesaplamayı ölçmek için gaz ekonomisi biçimi. Ayrıca, işlemleri bloklarına dahil edin. Bu nedenle, bir işlevsellik kısıtlaması kullanıcıları makul şekilde koruyabilir. Şimdiye kadarki en köklü hükümetler, bir kripto para biriminin kullanımının veya bakımının bir yasadışı eylem. Bu nedenle, kullanıcıların büyük çoğunluğu, yetenek açısından dijital ödeme sistemiyle karşılaştırılabilir. Yeteneği genişletmek istendiğinde, iki olasılık vardır. Özel bir doğası gereği benzer düşünen bireyler topluluğu (örneğin, bir poker oyunu). Veya, Ethereum ile karşılaştırılabilir yeteneklere sahip bir defter tarafından etkinleştirilir. Her iki durumda da, olayları başka bir protokole devretmek. Özel, geçici bir olay durumunda, blok zinciri paradigmasından kaçınmak mantıklıdır. tamamen, ancak daha çok özel amaçlı MPC protokolleri kitaplığına yönelik çabaları sınırlandırır. benzer fikirlere sahip bir grup katılımcı tarafından istendiğinde çağrılabilir. özel bir ağda koordine edilir ve CSL'ye yalnızca güvenilir bir ilan tahtası ve bir gerektiğinde mesaj geçiş kanalı. Bu durumda temel kavrayış, rıza, sorumluluk kapsamı ve mahremiyet olduğudur. CSL kullanıcıların tanışması ve iletişim kurması için dijital bir ortak alan olarak kullanılıyor - tıpkı bir parkın yapacağı gibi Ev sahipliği yapmak özel etkinlik - ancak herhangi bir özel konaklama veya kolaylaştırma sağlamaz. Ayrıca, NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 15 bölgesinin 44

Sayfa 16

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz özel amaçlı MPC'nin kullanılması, gerek kalmadan düşük gecikmeli etkileşimi mümkün kılacaktır. blockchain bloat, böylece sistemin ölçeğini geliştirir. Cardano'nun bu kütüphaneye yönelik araştırma çabaları, Tokyo Tech laboratuvarımızda merkezileştirilmiştir. yurtdışındaki bilim adamlarından biraz yardım. Bir arkadaşımızın ardından kütüphaneye "Tartaglia" diyoruz. matematikçi ve Cardano'nun çağdaşı ve ilk yinelemenin mevcut olmasını bekliyor 2018'in 1. çeyreğinde. İkinci durumda, sanal makineli bir blok zincirine, bir dizi fikir birliğine ihtiyaç vardır. düğümler ve iki zincir arasında iletişimi sağlamak için bir mekanizma. Ethereum Sanal Makinesini titizlikle resmileştirme süreciK-çerçeve içinde 12Illinois Üniversitesi'nden bir ekiple ortaklık. Bu analizin sonucu, çoğaltılmış ve nihayetinde bir açık operasyonel anlamlara ve güçlü doğru garantilere sahip dağıtılmış sanal makine 13Spesifikasyondan uygulama. Başka bir deyişle, sanal makine aslında kodun söylediğini yapar en aza indirilmiş güvenlik riskleri ile ilgisi vardır. Ethereum tarafından önerilen gaz ekonomisi ve bunun nasıl olduğu hakkında hala çözülmemiş sorular var. gibi işle ilgiliJan Hoffmann ve diğerlerinin kaynağa duyarlı MLVe daha geniş çalışma hesaplama için kaynak tahmini. Dil düzeyini de merak ediyoruz sanal makinenin bağımsızlığı.Örneğin, Ethereum projesi, mevcut sanal makinelerinden Web Montajına geçiş için. Bir sonraki çaba, durum bilgisini ifade etmek için makul bir programlama dili geliştirmektir. merkezi

olmayan uygulamalar tarafından hizmet olarak adlandırılacak sözleşmeler. Bu görev için, eski akıllı sözleşme dilini destekleme yaklaşımını seçtiSağlamlıkDüşük için güvence uygulamaları ve adı verilen yeni bir dil geliştirmePlutusDaha yüksek güvence için resmi doğrulama gerektiren uygulamalar. Sağlamlık temelli gibi Zeppelin projesi, IOHK ayrıca bir Plutus kodu referans kitaplığı geliştirecek uygulama geliştiricilerin projelerinde kullanmaları için. Ayrıca özel bir araç seti geliştireceğiz. işinden esinlenen resmi doğrulama içinUCSD'nin Liquid Haskell projesi. Fikir birliği açısından Ouroboros, yeterince modüler bir şekilde tasarlandı. Akıllı sözleşme değerlendirmesi Bu nedenle, hem CSL hem de CCL aynı fikir birliği algoritmasını paylaşacaktır. 12 Profesör Grigore Rosu ve diğerleri tarafından icat edilen K, dilden bağımsız makinede çalıştırılabilir anlambilim. Çalışmamızdan önce, C, Java ve JavaScript 13 Farklı fikir birliği düğümlerinin farklı akıllı sözleşmeler yürüttüğü anlamına gelir. Ayrıca durum paylaşma olarak da bilinir. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 16 bölgesinin 44

Sayfa 17

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Aradaki fark, Ouroboros'un hem izinli hem de token dağıtımı yoluyla izinsiz defterler. Ada, CSL ile Asya'daki alıcılara jeton oluşturma etkinliğiyle dağıtıldı. İkincil bir pazarda nihayetinde yeniden satış yapacak. Bu, CSL'nin fikir birliği algoritmasının çeşitli ve giderek daha ademi merkeziyetçi bir dizi aktörler veya onların yetki verdiği CCL ile, delegeler tarafından tutulan özel amaçlı bir jeton oluşturmak mümkündür. o Düzenlenmiş varlıklar olabilen defter, böylece izinli bir defter yaratır. Bu yaklaşımın esnekliği, farklı CCL örneklerinin farklı işlemlerin değerlendirilmesiyle ilgili kurallar. Örneğin, kumar etkinlikleri kısıtlanabilir KYC / AML verileri yalnızca ilişkilendirilmemiş işlemleri kara listeye alarak mevcut olmadığı sürece. Nihai tasarım odağımız, güvenilendonanım güvenlik modülleri(HSM) protokolümüze Bunlar, bu yetenekleri ürüne tanıtmanın iki büyük avantajıdır. Birincisi, HSM'ler, güvenlik sunmadan performansta büyük artışlar sağlar. 14satıcıya güvenmenin ötesinde endişeler. İkincisi,Sızdırmaz Cam Kanıtı(SGP), HSM'ler, verilerin doğrulanabileceği ve daha sonra silinmeden imha edilebileceğine dair güvence sağlayabilir. kötü niyetli yabancılara kopyalandı veya sızdırıldı. İkinci noktaya odaklanıldığında, SGP'lerin uyumluluk üzerinde devrim niteliğinde bir etkisi olabilir. Normalde, bir tüketici kimlik doğrulamak için kişisel olarak tanımlanabilir bilgiler (PII) sağladığında kimlik veya katılma hakkını kanıtlamak, bu bilgiler güvenilir bir üçüncü tarafa verilir. kötü niyetle hareket etmemesi umudu. Bu etkinlik özünde merkezileştirilmiştir, veri sağlayıcı PII üzerindeki kontrolünü kaybeder ve ayrıca yargı yetkisine dayalı çeşitli düzenlemelere tabidir. Bir dizi güvenilir tasdik eden seçme ve ardından bir donanım yerleşim bölgesinde PII depolama yeteneği Yeterince yetenekli bir HSM'ye sahip herhangi bir aktörün, bir Aktör aktörün kimliğini doğrulayan kişi olmadan taklit edilemez bir şekilde. Örneğin, Bob dır-dir ABD vatandaşı değil. Alice, akredite bir yatırımcıdır. James, ABD vergi mükellefidir ve göndermeli X hesabına vergilendirilebilir kar. Cardano'nun HSM stratejisi, sonraki ikisinde özel protokolleri uygulamaya çalışmak olacaktır. yıllar kullanıyorIntel SGXve ARM Trustzone. Her iki modül de milyarlarca tüketiciye entegre edilmiştir dizüstü bilgisayarlardan cep telefonlarına ve tüketici tarafında ek çaba gerektirmeyen Her ikisi de yoğun bir şekilde incelenmiş, iyi tasarlanmış ve bazılarının yıllar süren yinelemelerine dayanmaktadır. nın-nin en büyük ve en iyi finanse edilen donanım güvenlik ekipleri. 14 Bkz.http://hackingdistributed.com/2016/12/22/scaling-bitcoin-with-secure-hardware/Cornell den Üniversite NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 17 bölgesinin 44

Sayfa 18

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Yönetmelik Tüm modern finansal sistemlerin sert gerçekliği, ölçeklendikçe bir ihtiyaç biriktirmeleridir. , veya en azından düzenleme arzusu. Bu sonuç genellikle tekrarlayan çöküşlerin sonucudur. bir pazardaki bazı aktörlerin veya aktörlerin ihmalinden dolayı. Örneğin, 1907 Knickerbocker Krizi, Federal Rezerv'in kurulmasıyla sonuçlandı. Son çare olarak 1913'teki sistem. Bir başka örnek de 1920'lerin aşırılıklarıdır. İçinde Amerika Birleşik Devletleri korkunç bir mali çöküşle sonuçlandı, Büyük Buhran. Bu çöküş 1934 yılında benzer bir oluşumun önlenmesi için Menkul Kıymetler Borsası Komisyonu'nun kurulmasını sağladı. olay veya en azından kötü aktörleri sorumlu tut. Düzenlemenin gerekliliği, kapsamı ve etkinliği makul bir şekilde tartışılabilir, ancak kimse inkar edemez varlığı ve büyük hükümetlerin uyguladığı gayret. Ancak, Dünya küreselleştikçe ve nakit dijital hale geldikçe, tüm düzenleyicilerin karşılaştığı zorluklar iki yönlüdür. Birincisi, bir koleksiyonla uğraşırken hangi düzenlemeler en üstün olmalıdır? Westfalyan egemenliğinin eskimiş kavramı, tek bir işlemin bir dakikadan kısa bir sürede üç düzine ülkeye dokunabilir. en jeopolitik etki? İkincisi, gizlilik teknolojisindeki gelişmeler, dijital bir silahlanma yarışı yarattı. bir işleme kimin katıldığını anlamak giderek daha zor hale gelirse, çok daha az kim belirli bir değer deposuna sahip? Milyonlarca doların olduğu bir dünyada Varlıklar gizlice tutulan 12 kelimelik bir anımsatıcıdan başka bir şey olmadan kontrol edilebilir, nasıl yaparsınız 15Etkili düzenleme uyguluyor mu? Tüm finansal sistemler gibi, Cardano protokolü de tasarımında ne olduğu konusunda bir görüşe sahip olmalıdır. adil ve makul. Bireysel haklar ve bir şirketin hakları arasında ayrım yapmayı seçtik. pazar yeri. Bireyler, fonlarına her zaman baskı veya sivil varlıkları olmaksızın tek erişime sahip olmalıdır. el koyma. Bu hak uygulanmalıdır çünkü tüm hükümetlere Venezuela'da görüldüğü gibi, yozlaşmış politikacıların kişisel kazançları için egemen güçlerini kötüye kullanmak ve Zimbabve Kripto para birimleri en düşük ortak paydaya göre tasarlanmalıdır. 15 Bkz BIP39 https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 18 bölgesinin 44

Sayfa 19

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz İkincisi, tarih asla değiştirilmemelidir. Blok zincirler bir değişmezlik vaadi sağlar. Tarihi geri alma veya resmi kaydı değiştirme gücünün tanıtılması çok fazla şey getirir belirli bir aktör veya aktörün yararına olmak için geçmişi değiştirme cazibesi. Üçüncüsü, değer akışı sınırsız olmalıdır. Sermaye kontrolleri ve diğer yapay duvarlar insan haklarını küçültmek. Bunları küresel ölçekte uygulama çabasının beyhudeliğinin dışında, 16en az gelişmiş ülkelerdeki birçok vatandaşın kendi yetki alanları dışında seyahat ettiği ekonomi yaşanabilir bir ücret bulmak, sermaye akışını kısıtlamak genellikle dünyadaki en yoksullara zarar verir . Belirtilen bu ilkeler, pazarlar bireylerden belirgin şekilde farklıdır. Cardano bireysel haklara inanır, ayrıca piyasaların açıkça ifade etme hakkına sahip olduğuna inanıyoruz. şartlar ve koşullar ve bir kişi bu pazarda iş yapmayı kabul ederse, o zaman tüm sistemin bütünlüğü için bu standartlara uyulmalıdır. Zorluk her zaman uygulamanın maliyeti ve uygulanabilirliği olmuştur. Küçük, çok yargılı işlemler, eski sistemlerde yüksek rücu güvencesi sağlamak için çok pahalıdır dolandırıcılık veya ticari bir anlaşmazlık durumunda. Banka havalesi Nijeryalı Prens, fonları geri almaya çalışmak genellikle çok pahalıdır. 17 Cardano için, üç düzeyde yenilik yapabileceğimizi düşünüyoruz. Birincisi, akıllı Sözleşmeler ticari ilişkilerin hüküm ve koşulları daha iyi kontrol edilebilir. dijitaldir ve yalnızca CSL'de ifade edilebilir, dolandırıcılık içermeyen ticaretin güçlü garantileri olabilir kazandı. İkincisi, HSM'lerin PII'nin sızdırılmadığı ancak henüz sızdırılmayan bir kimlik alanı sağlamak için kullanılması Eskiden kimlik doğrulama ve kimlik bilgileri aktörleri küresel bir itibar sistemi sağlamalı ve otomatikleştirilmiş çevrimiçi oyun oynama gibi çok daha düşük maliyetli düzenlenmiş faaliyetler vergi uyumu veya merkezi olmayan borsalar. Son olarak, Cardano yol haritasında modüler düzenlemenin oluşturulmasıdır DAOBu olabilir değişkenlik, tüketici eklemek için kullanıcı tarafından

yazılmış akıllı sözleşmelerle etkileşime girecek şekilde özelleştirildi koruma ve tahkim Bu projenin kapsamı daha sonraki bir makalede ana hatlarıyla açıklanacaktır. 16 sermaye akışına bir önlem bir örnek olarak, bkz Hawala Bankacılık Sistemi 17 BkzPeşin Ücret Dolandırıcılığı NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 19 bölgesinin 44

Sayfa 20

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Tüm bunların anlamı nedir? Cardano, yüzlerce parlak zihnin geri bildirimini içeren bir maraton projesidir. kripto para birimi endüstrisinin içinde ve dışında. Yorulmak bilmeyen yinelemeyi, meslektaş değerlendirmesi ve ortaya çıktığında büyük fikirlerin utanmazca çalınması. Kalan bölümlerin her biri, bir çekirdek olduğuna karar verdiğimiz odak noktasının belirli bir yönünü kapsamaktadır. projemizin bileşeni. Bazıları, genel olarak en iyiyi geliştirme arzusu nedeniyle seçildi uzay uygulamaları, diğerleri ise Cardano'nun evrimine özgüdür. Hiçbir proje her hedefi karşılayamaz veya her kullanıcıyı tatmin edemezken, umudumuz bir vizyon sağlamaktır. Kendiliğinden gelişen bir mali yığının, bunlardan yoksun yargı bölgeleri için nasıl görünmesi gerektiği. Nihai Kripto para birimlerinin gerçekliği, mevcut eski finansal sistemleri bozacakları değildir. Eski finansal sistemler her zaman değişimi özümseyebilir ve biçimlerini koruyabilir ve işlev. Aksine, mevcut olanı kurmanın çok pahalı olduğu yerlere bakılmalıdır. Birçoğunun günde birkaç doların altında bir gelirle yaşadığı bankacılık sistemi, istikrarlı bir kimliğe sahip değildir ve kredi bulmak imkansız. Bu yerlerde, bir ödeme sistemi, mülkiyet hakları, kimlik, kredi ve riski bir araya getirme gücü bir cep telefonunda çalışan tek bir uygulamaya koruma sadece yararlı değil, hayat değiştiriyor. Cardano'yu geliştirmemizin nedeni, teslim etme konusunda meşru bir şansımız olduğunu hissetmemizdir - veya en azından ilerleyen - gelişmekte olan dünya için bu vizyon. Başarısızlık durumunda bile, kripto para birimlerinin tasarlanma, gelişme ve finanse edilme şeklini değiştirebilirsek, o zaman büyük bir başarı var. 2. Bilim ve Mühendislik Yineleme Sanatı Kripto para birimleri, yazılım olarak uygulanan protokollerdir. Protokoller basitçe akıllıdır katılımcılar arasındaki konuşmalar.Yazılım, nihayetinde bazılarının verdiği verilerin manipülasyonudur. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 20 bölgesinin 44

Sayfa 21

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Ancak sağlam, güvenilir yazılımın yanı sıra kullanışlı, güvenli protokoller ve onların konuşmaları tamamen insandır. İyi bir yazılımın hesap verebilirliğe, açık iş gereksinimlerine, tekrarlanabilir süreçlere ihtiyacı vardır. kapsamlı testler ve yorulmak bilmeyen yineleme. İyi bir yazılımın aynı zamanda makul düzeyde yetenekli Yeterince etki alanına özgü bilgiye sahip geliştiriciler, tamamen çözmeye çalıştıkları sorunu çözmek. Yararlı ve güvenli protokollere gelince, özellikle kriptografi içeren ve dağıtılmış olanlar sistemler, daha akademik ve standartlara dayalı bir süreçte başlarlar. Akran değerlendirmesi, sonsuz Bir protokolün yararlı olmasını sağlamak için tartışmalar ve sağlam bir ödünleşme kavramı gereklidir. Bunlar tek başına yeterli değildir, protokollerin uygulanması ve gerçek yaşam kullanımıyla test edilmesi gerekir. Kripto para birimi endüstrisindeki benzersiz zorluk, ikisinin tamamen farklı olmasıdır. felsefeler düzgün bir Hegelci sentez olmadan birbirine karıştırılır. Tezimiz bir "hamle" dir. gençlik, açgözlülük ve tutku tarafından yönlendirilen başlangıç zihniyetidir. yavaş, metodik ve akademik odaklı yaklaşım alanımızın yeniliklerini, bol miktarda fon ve prestijin tadını çıkaran güzel bir niş haline getiriyoruz. Sonuç, birçok kripto para biriminin ya tamamen bir teknik incelemede belirtilmiş olmasıdır. CV ile ilgili veya aceleyle yazılmış bir kodla. Şu anki ilk on kripto para biriminden hiçbiri Tarafından 18Piyasa kapitalizasyonu, meslektaş incelemesine tabi tutulmuş bir protokole dayanmaktadır. Mevcut

on ilk kripto para birimleri resmi bir şartnameden uygulandı. 19 Yine de milyarlarca dolar değer söz konusu. Bir kez konuşlandırıldığında, bir kripto para birimi fazlasıyla değiştirilmesi zor. Bir kullanıcı güvenli bir sistem kullandığını nasıl anlar? Bir kullanıcı nasıl pazarlama iddialarının meşru olduğunu biliyor musunuz? Ya önerilen protokol asla başaramazsa iddialar? Bu sentez eksikliği ve sürece saygı eksikliği, IOHK'nın bunu yapmak istemesinin temel nedenlerinden biridir. Cardano'yu inşa et. Umudumuz, örnek teşkil edecek bir referans proje geliştirmekti. işleri daha etkili, mantıklı ve dürüst bir şekilde nasıl yapılır. Amaç, yazılım ve protokoller geliştirmenin tamamen yeni bir yolunu sunmak değil, daha ziyade harika yazılım ve protokollerin zaten var olduğunu ve koşulları taklit edebileceğimizi kabul edin bu onların yaratılmasına yol açtı. İkincisi, bu koşulları kamuya açık hale getirmek ve eğer tüm alanın yararı için taklit edilebilmeleri mümkündür. 18 Piyasa değerine göre kapsamlı bir liste için www.coinmarketcap.com adresine bakın. 19 Ethereum, Sarı Kağıt olarak bilinen yarı resmi bir spesifikasyona sahiptir; ancak, EVM semantiği tam olarak belirtilmemiştir ve protokolün tam olarak uygulanması için yeterli değildir. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 21 bölgesinin 44

Sayfa 22

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Gerçekler ve Görüşler Diğer endişe, gerçeklerin nerede bittiği ve fikrin başladığı yerdedir. Yüzlerce var programlama dilleri, düzinelerce geliştirme paradigması ve birden fazla felsefe proje Yönetimi. Akademik dünya, kendi iş kaygılarından ve pratikliğinden uzaklık. Cardano için ilk olarak evrensel olarak kabul edilebilecek bariz eksiklikleri yakalamaya çalıştık mühendislik açısından yararlı olmak. Örneğin, kriptografi ve dağıtılmış sistemlerin her ikisi de olağanüstü derecede ilgili konulardır.ne kadar saf ellere dair çok fazla örnek korkunç hatalar yapabilir. Bu nedenle, bu alanlardan içgörü gerektiren herhangi bir protokolün tanınmış bir uzman tarafından tasarlanacak ve diğer uzmanlar tarafından incelenmek üzere sunulacaktır. Ouroboros, bu alandaki ilk vaka çalışmamızdır. Bir kriptograf ekibi tarafından tasarlandı. geniş, çeşitli ve kamuya açık bir şekilde doğrulanabilir bir yayın geçmişi. Standarda göre inşa edilmiştir güvenlik varsayımları, rakip bir model ve kanıtlarla kriptografi süreci. Bunlar kanıtlar tarafından kontrol edildikonferanslara ve ayrıca bağımsız olarak bilgisayar tarafından sunulma 20Cambridge Üniversitesi'nden bir ekip tarafından Isabelle'de yazılmış kanıtlar. 21 Yine de bu çalışma tek başına yararlılık garantisi vermez - sadece sıkı bir güvenlik kontrolü modele bazı varsayımlar verildi. Yararlılık için, protokolün uygulanması ve test edilmesi gerekir. Geliştiricilerimiz her ikisinde de bunu yaptıHaskell ve ayrıca Pas. Bu çalışma daha fazla çabayı ortaya çıkardı yaratılmasına yol açan senkronizasyon modeline odaklanılması gerekiyorduOuroboros Praos. Bu yineleme sanatı, her adımda yeni derslere yol açan harika protokoller üreten şeydir. önceki adımın doğruluğunu yeniden doğrulama gereksinimi. Maliyetlidir, zaman alıcıdır ve 22zaman gerçekten sıkıcı olsa da, bir protokolün doğru bir şekilde tasarlandığından emin olmak gerekir. Protokoller - özellikle milyarlarca insan tarafından kullanılacak olanlar - kısa ömürlü ve hızlı değildir gelişen. Aksine, yıllarca ve on yıllarca takip edilmeleri amaçlanmıştır. Tamamen görünüyor dünyaya yeni bir finansal sistem yüklemeden önce hepimizin birlikte yaşaması gerektiği mantıklı Önümüzdeki 100 yıl için, tasarımcılarından biraz sıkıcılık ve titizlik talep etmek istiyoruz. IACR'nin Kaliforniya'daki Yıllık Kripto Konferansının 20 Kabul Edilmiş Kağıt Numarası 71 21 By Kawin WorrasangasilpaProfesör Lawrence Paulson gözetiminde 22 Alçakgönüllülük uğruna bir teğet takiben, kişiProfesör Halmos'un nasıl yapılacağı hakkındaki tartışması matematik ders kitabı yaz NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 22 bölgesinin 44

Sayfa 23

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz İşlevsel Günahlar Daha kararlı bir bölgeye, kullanılan araçlar, diller ve metodolojilere geçiş yazılım geliştirme, nesnel gerçeklikten çok dini takdirin ürünüdür. Kaynak kod, yazılı nesir gibidir. Herkesin neyin iyi olduğu ve ne olduğu hakkında bir fikri vardır bazen nasıl iletildiğinden daha az önemlidir. En az birinde yanlış olacağını kabul ederek bir taraf seçmenin günahını işlemeliyiz. Ancak, seçimimizin arkasında en azından büyük bir gerekçe külliyat var. Cardano'yu mümkün kılan protokoller Haskell'de uygulanıyor. Kullanıcı arayüzü bir çatal içinde kapsüllenmiştirDaedalus dediğimiz elektron . Biz seçtik mümkün olan yerlerde web mimari modelini kullanın ve veritabanımız için biranahtar / değer paradigmakullanarak RocksDB. Bileşen seviyesinden bakıldığında, bu soyutlama, bakımın çok daha basit, daha iyi olduğu anlamına gelir. teknoloji daha sonra çok az çabayla ikame edilebilir ve yığınımız kısmen Github ve Facebook'un geliştirme çabaları. Bir WebGUI kullanmak, React'ten yararlanmamızı ve araçları kullanarak ön uç özelliklerini geliştirmemizi sağlar yüz binlerce JavaScript geliştiricisi tarafından anlaşıldı. Bir web mimarisi kullanma bileşenlerin hizmet olarak değerlendirilebileceği ve güvenlik modelinin mantıklı olduğu anlamına gelir. Protokol geliştirme için Haskell'i seçmek en zor seçimdi. İşlevsel olarak bile dünya, bol seçenek var. Daha esnek ve saf olmayan tarafta, aşağıdaki gibi diller var: Clojure, Scala ve F #, Java'nın ve .Net'in muazzam kütüphanelerinden yararlanır. işlevsel programlamanın en iyi yönlerinden bazılarını korurken ekosistemler. Gibi daha akademik odaklı diller varAgda ve İdris bir kapanış var Doğruluğun güçlü bir şekilde doğrulanmasına izin verecek tekniklerle bağlantı. Yine de eksikler makul kütüphaneler ve alt düzey geliştirme deneyimine sahip. Cardano için seçim Ocaml ve Haskell'e geldi. Ocaml harika bir dildir harika bir topluluk, iyi araçlar, makul geliştirme deneyimi ve Coq aracılığıyla resmi doğrulama alanı Peki neden Haskell'i seçtik? 23 23 Bu noktaya ek olarak, IOHK'nın aslında Ocaml'da uygulanan bir projesi var:QeditasO sahte Bill White'dan miras aldık NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 23 bölgesinin 44

Sayfa 24

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Neden Haskell? Cardano'yu oluşturan protokoller dağıtılır, kriptografi ile paketlenir ve bir yüksek derecede hata toleransı. En iyi günlerde yine de olacakBizans aktörler, bozuk mesajlar ve hatalı istemciler istemeden ağda bir tür hasara neden olur. İlk olarak, araçları kolayca kullanabileceğimiz güçlü bir yazı sistemine sahip bir dil istedik. gibiQuickcheck ve bu şekilde daha ayrıntılı teknikler Arıtma türleri bir yaparken hata toleransı için makul beklenti. Bir Erlang stiliOTP modeli ikincisini karşılar Haskell ve Ocaml gibi diller ise ilkini tatmin eder. GirişiyleBulut HaskellHaskell, Erlang'ın birçok avantajını elde ederken kendini teslim ediyor. Ayrıca Haskell'in modülerliği ve biçimlendirilebilirliği, Cardano için Time Warp adlı daha hafif bir ısmarlama kitaplık kullanın. İkincisi, Haskell'in kütüphaneleri, kapsamlı çalışma sayesinde son birkaç yılda büyük ölçüde gelişti. gibi ticari kuruluşlarınGalois, FP tamamlayın ve İyi Yazılan. Sonuç olarak Haskell şunları yapabilir: üretim uygulamaları yazmak için kullanılabilir. 24 Üçüncü,PureScript'nin hızlı gelişimi, JavaScript dünyasına çok ihtiyaç duyulan bir köprüyü sağladı Clojurescript'in Clojure'a verdiği şeye benzer. PureScript'in özellikle önemli olmasını bekliyoruz Cardano'nun bir tarayıcıda çalışmasını sağlamak ve mobil cüzdanlar geliştirmek söz konusu olduğunda. Dördüncüsü, bağımlılık çözümü ile ilgili olarak, Haskell son birkaç yılda bir teknoloji uzmanları tarafından yönetilen önemli sosyal ve teknolojik çabaMichael Snoyman a yoluyla platform aradıistifBu hem kullanımı kolay hem de FP Complete tarafından iyi destekleniyor. Beşincisi, yeterli bağımlılık çözümünün ötesinde, yazılım yapılarımızın tekrarlanabilir. Başka bir deyişle, aynı

yapılandırma değerleri ve bağımlılık sürümleriyle tam olarak aynı yapı yapılarını üretmelidir. Yığın yoluyla, kullanıyoruzNixOps yeniden üretilebilirliği büyük bir başarıyla elde etmek. Son olarak, Haskell'de uzmanlaşan geliştiricilerin yetenek havuzu oldukça büyüktür - meslektaşları - ve akademik ve endüstri kimlik bilgilerinin doğru karışımı ile oldukça iyi eğitilmiş. Aynı zamanda bir yetkinlik filtresi görevi görür, çünkü tecrübeli Haskell geliştiricilerini, detaylı bilgisayar bilimi bilgisi. 24 Bryan O'Sullivan Haskell'ın endüstriyel kullanımı hakkında güzel bir konuşma sağlarburada. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 24 bölgesinin 44

Sayfa 25

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Resmi Şartname ve Doğrulama Kanıtlanabilir şekilde doğru bir güvenlik modeli kullanarak bir protokol geliştirmenin önemli bir gücü, garantili bir rakip güç limiti sağlar. protokole uyulur ve kanıtlar doğrudur, düşman güvenliği ihlal edemez mülk talep edildi. Daha derin düşünme, önceki iddiayı daha da önemli hale getirir. Düşmanlar keyfi olarak Sadece matematiksel bir model aracılığıyla yenildiklerini söylemek, olağanüstü ve tabii ki bu tamamen doğru değil. Gerçeklik, saf güvenlik ütopyasını engelleyen faktörleri ve koşulları ortaya çıkarır. mevcut davranışa göre doğru davranış. Uygulamalar yanlış olabilir. Donanım saldırıya neden olabilir daha önce değerlendirilmemiş vektörler. Güvenlik modeli yetersiz olabilir ve aşağıdakilere uymayabilir: gerçek hayat kullanımı. Bir değerlendirme için ne kadar spesifikasyon, titizlik ve kontrol talep edildiğine dair bir yargı çağrısına ihtiyaç vardır. protokol. Örneğin,SeL4 Mikro çekirdek projesiHer şeyin en iyi örneğidir belirsizliğe yönelik saldırı dışında, neredeyse 200.000 satır Isabelle kodunun doğrulanması 10.000 satır C kodu. Yine de bir işletim sistemi çekirdeği, bir düzgün bir şekilde uygulanmazsa ciddi güvenlik açığı. Tüm kriptografik yazılımlar aynı Herkül çabasını mı gerektirmeli? eşdeğer sonuçlar üreten güçlü bir yol mu? Ayrıca protokolün içinde çalıştığı ortam kötü şöhretli savunmasızsa, mükemmel bir şekilde uygulanır. Windows XP? Cardano için aşağıdaki uzlaşmayı seçtik: Birincisi, kriptografi ve dağıtılmış hesaplama alanları, ispatlar genellikle çok ince, uzun, karmaşık ve bazen oldukça teknik. Bu, insan odaklı denetimin sıkıcı ve hataya açık. Bu nedenle, her önemli kanıtın beyaz renkte sunulduğuna inanıyoruz. Çekirdek altyapıyı kapsayacak şekilde yazılmış kağıt makinede kontrol edilmelidir. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 25 bölgesinin 44

Sayfa 26

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz İkinci olarak, Haskell kodunu, teknik incelemelerimize doğru bir şekilde karşılık gelecek şekilde doğrulamak için, iki popüler seçenek arasında: SMT prova sağlayıcıları ile arayüz oluşturmaLiquidHaskell ve kullanma Isabelle / HOL. SMT (tatminkarlık modülo teorileri) çözücüler, işlevsellik bulma problemiyle ilgilenir. bir denklemi veya eşitsizliği karşılayan veya alternatif olarak bu tür parametreleri gösteren parametreler yok. Tartışıldığı gibiDe Moura ve Bjørner, SMT'nin kullanım durumları çeşitlidir, ancak anahtar önemli olan nokta, bu tekniklerin hem güçlü hem de hataları önemli ölçüde azaltabileceğidir ve anlamsal hatalar. Isabelle / HOLÖte yandan, daha etkileyici ve çeşitli bir araçtır ve her ikisi de uygulamayı belirtir ve doğrular. Isabelle, aşağıdakilerle çalışan genel bir teorem çözücüdür kümeleri ve diğer matematiksel nesneleri temsil edebilen yüksek dereceli mantık yapıları ispatlarda kullanılabilir. Isabelle'in kendisi, aşağıdakileri içeren problemlerle çalışmak için Z3 SMT prover ile entegre olur bu tür kısıtlamalar. Her iki yaklaşım da değer sağlıyor ve bu nedenle ikisini de aşamalı olarak kucaklamaya karar verdik. İnsanlara ait yazılı kanıtlar, doğruluğunu kontrol etmek ve dolayısıyla tatmin edici olmak için Isabelle'de kodlanacaktır. bizim makine kontrol gereksinimi. Ve kademeli olarak Liquid Haskell'i herkese eklemeyi planlıyoruz.

Cardano'nun 2017 ve 2018 boyunca uygulamasında üretim kodu. Son bir nokta olarak, resmi doğrulama, yalnızca doğrulandığı şartname kadar iyidir. Ve mevcut araç setleri. Haskell'i seçmenin başlıca nedenlerinden biri, Doğru pratiklik ve teori dengesi. Beyaz kitaplardan türetilen şartname, Haskell kodu ve ikisini birbirine bağlamak, bunu bir zorunluluk ile yapmaktan çok daha kolaydır. dil. Uygun bir spesifikasyonun yakalanması ve aynı zamanda güncellenmesi konusunda hala çok büyük zorluklar var. yükseltmeler, hata düzeltmeleri ve diğer endişeler gibi değişikliklerin ne zaman yapılması gerektiğinin belirtilmesi; ancak, bu gerçeklik hiçbir şekilde genel değeri azaltmaz. belaya kanıtlanabilir güvenlik üzerine bir temel oluşturmak, o zaman uygulama ne olmalıydı aslında kağıt üzerinde önerildi. Şeffaflık Bir kripto para birimi geliştirmenin bilimini ve mühendisliğini tartışırken son bir soru şudur: şeffaflık nasıl ele alınır. Tasarım kararları Boolean ve ruhani değildir. rüyalardaki geliştiriciler ve sonra aniden kanon olurlar. Deneyimden türetilirler, tartışma ve önceki hatalardan öğrenilen dersler. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 26 bölgesinin 44

Sayfa 27

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Buradaki zorluk, tamamen şeffaf bir geliştirme sürecinin tartışmayı etkileyebilmesidir. kanıta dayalı olmaktan çok teatral hale gelir. Egolar, bir topluluğu kazanma girişimleri ve korku Aptalca görünmek, konuşmaları kısır ve verimsiz olmaya zorlayabilir. Dahası, yabancılar, kendilerini zorlamak için sohbeti seçmeye çalışabilirler. tek ilgili konu haline gelmek için özel bir teğet.Herkesin kutsal bir ineği vardır. Öyleyse, şeffaf bir geliştirme sürecine olan ihtiyaç nasıl dengelenir? özgürlüğe ihtiyaç duyan bir dizi çekirdek geliştiriciye ilerlemeyi emanet eden topluluk korkusuz bir ifade mi? Cardano ile, yönlendirilmiş gözetim ile standartlara dayalı bir süreci benimsemeye karar verdik. Topluluğun bilim ve kodun iyi düşünülmüş, kontrol edilmiş ve iyi düşünülmüş olduğunu bilmesi gerekir. aslında geliştiricilerin yaptıklarını iddia ettikleri şeyleri çözüyorlar. Bu amaçla, meslektaş incelemeleri Bu amaç için özel olarak tasarlandığı için bilim bileşenini tamamen tatmin eder ve bize modern dünyayı verdi. Kod için bu konu biraz daha kararlı. Cardano için emanet etmeyi seçtik Cardano Vakfı, IOHK'nın çalışmalarının son denetçisi olarak görev yapacak. aşağıdaki görevlerle: 1. Kaliteyi kontrol etmek için Cardano Github'da bulunan kaynak kodunun düzenli olarak incelenmesi, test kapsamı, uygun yorumlar ve eksiksizlik 2. Tüm Cardano belgelerinin doğruluk ve kullanışlılık açısından gözden geçirilmesi 3. Bilim adamları tarafından üretilen protokollerin tam olarak uygulandığına dair iddiaların doğrulanması Bu görevi yerine getirmek için IOHK, Vakfa düzenli ve zamanında raporlar sunacak ve atar - gözden geçirmek için. Vakıf sırayla bir kalkınma gözetim raporu yayınlayacak En az üç ayda bir Cardano topluluğu. Bu ilk çaba, ademi merkeziyetçi bir projenin nasıl hesap verebilirlik sağlar. Güvenilir bir üçüncü tarafın geliştirme gözetimi, geliştiricilerin doğru yolda olduğundan emin olun, ancak proje her zaman teslim edecek. Bu nedenle, hazine CSL'ye entegre edildikten sonra Vakıf, resmi temelli alternatif müşteriler oluşturmak için ek geliştirme ekipleri IOHK ile ortak geliştirilen spesifikasyonlar.Geliştirme çeşitliliği harika bir teknik olmuştur. Ethereum projesi tarafından tek bir fikir kümesi etrafında oluşan bir monokültürden kaçınmak için kullanılır veya geliştiriciler. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 27 bölgesinin 44

Sayfa 28

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Spesifikasyonlar ile ilgili olarak, standartlardan elde edilecek çok sayıda bilgi vardır. tarafından takip edilen süreçWC3 veIETFSonuç olarak, Cardano'nun entegre ettiği her protokol akademik çalışmadan veya kaynak kodundan bağımsız bir şartname gerektirir. Bunun yerine, gibi uygun bir formatta olmakRFC. Cardano Vakfı'nın temel

ilkelerinden biri, özellikle aşağıdakiler için standartlar organı olarak hareket etmektir. Cardano protokolleri ve ilgili standartları güncellemek, eklemek veya değiştirmek için konuşmaları barındırmak için Cardano. IETF aracılığıyla internet (standartların bir ürünü), çekirdek protokoller kullanılacaksa, bu durumda özel bir kuruluşun aynı sonucu kolaylaştırabilir. Kapanış notu olarak, bu tartışmaları merkezi olmayan bir varlığa taşımayı keşfetmek ilginçtir. bir blok zincirinde barındırılır. Bu kavrama,merkezi olmayan özerk organizasyon(DAO) veön çalışmaIOHK, bu alanda bir referans DAO modeli geliştirecektir. Cardano ile arayüz oluşturan kuruluşlar istenirse kullanmak için ve Cardano Vakfı'nın ayrıcalığıdır bunu kendi standartlarına göre benimseyip benimsemeyeceğine karar vermek. 3. Birlikte çalışabilirlik Büyük Miyopi Finans ve daha geniş ticaret fikri nihayetinde bir insan çabasıdır. diller, amacı yakalamak için son derece hassas araçlar ve Kötü sonuçların yanı sıra binlerce yıllık yasa arayışı durumunda başvuruda bulunun ticarette eşitlik. Aslındaen eski yazı biçimleri ticari sözleşmelerdi. Yine de, mantığa aracılık etmesine bakılmaksızın insan unsurundan kaçınılamaz, korkunç güçlere emanet edilmiş hükümet nöbetçileri ya da makineler. kripto para birimlerinin miyopisi: Çoğunlukla insan gerçekliğinden ayrılmışlardır. İnsanlar hatalar yaparlar. İnsanlar fikirlerini değiştirirler. İnsanlar her zaman tam olarak anlamazlar. girmeyi kabul ettikleri iş ilişkileri İnsanlar yanıltılmakta ve dolandırılmaktadır. Benzersiz çözümler gerektiren koşullar, bireysel ve durum düzeyinde değişir. bu nokta, çoğu sözleşmedemücbir sebep hükümleri. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 28 bölgesinin 44

Sayfa 29

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Bununla birlikte, kripto para birimleri insan anlayışını, şefkatini ve yargısını ortaya çıkarmaya çalışır. dikkate alınmadan bir anayasaya mükemmel bir şekilde bağlı, umursamaz bir dijital yargıç karşılığında adalet veya sonuç için. İnsanların her zaman denediği ve yapmaya devam edeceği düşünülürse kuralları bencil amaçlarla değiştirin, aslında bozulamayacak bir sisteme sahip olmak ferahlatıcı . Ancak bir kullanıcının bu yeni sistemleri geleneksel finansal sistemlerle harmanlaması gerektiğinde ne olur? İnsan dünyasında yaşamaya ihtiyaç duyulduğunda ne olur? Örneğin, mülkiyet Tapu tescili gibi haklar tamamen fiziksel dünyada yaşar. görevli yargı yetkisinin bir miktar kabul edilmesini gerektirir. Başka bir nokta sağlamak için, bir altın külçesi kendi kendine hareket edemez. Dijital hakem komuta edebilir onun hareket, ancak insanlar olmadan onu uyum sağlamaya zorlayamaz. Bu nedenle dijital bir defter, gerçeklikten sapma. Bu nedenle, bir protokol tasarımcısının kendi içinde ne kadar insan gerçekliğine izin verilmesi gerektiğine karar vermesi gerekir. kripto para birimi. Daha fazla esneklik, mutlak olana daha az sadakat beklemelidir. daha fazla tüketici koruması, geri alma, geri ödeme sağlamak için daha fazla mekanizmanın var olması gerekir ve tarihin düzenlenmesi. Yönetmelikle ilgili bu bölüm ve sonraki bölüm, Cardano'nun konuya yönelik pragmatik yaklaşımını kapsar. birlikte çalışabilirlik açısından tartışılacak iki geniş grup vardır. Birincisi, birlikte çalışabilirlik eski finansal sistemler (kripto para birimi olmayan dünya). İkincisi, diğerleriyle birlikte çalışabilirlik kripto para birimleri. Eski Fintech, tek bir standart veya hatta ortak bir dilden oluşmaz. Muazzam var yaklaşımlardaki çeşitlilik, takas ve takasla sorumlu kuruluşlar, iş süreçler ve muhasebe, dönüşüm ve hareketle ilgili diğer alanlar değer. Sırf bir teknoloji daha üstün olduğu için geri kalanının ekosistem bir şekilde yenilgiyi ve yükseltmeyi kabul edecek. Örneğin, birçok kişi hala kullanıyor Windows XP , ilk sürümden 16 yıl sonra. Bu üzücü durum birisine eşdeğer 1984 yılında 2000 yılında piyasaya sürülen orijinal Macintosh'u kullanarak. Tüketici davranışı bir yana, işletmeler genellikle yükseltme döngülerinde daha yavaştır. Birçok bankalar hala Cobol'da yazılan arka uçları kullanıyor. Altyapının çalıştığı ve buluştuğu bilindiğinde iş gereksinimleri, genellikle yazılımı yükseltmek veya iyileştirmek için çok az teşvik vardır ve

uyumluluk veya güvenlik endişeleri dışında bir tüketicinin yararına olan protokoller. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 29 bölgesinin 44

Sayfa 30

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Cardano için, öncelikle eski bir köprünün neyi gerektireceğini belirlemeliyiz? Hangi sistemler, standartlar, varlıklar ve protokoller, makul bir kesinlik olmasını sağlamayı hedeflemeliyiz: birlikte çalışabilirlik? Bu köprüler federe veya ademi merkeziyetçi olabilir mi? Ya da borsalar gibi yapacaklar bilgisayar korsanları, kötü niyetli sahipler veya aşırı hevesli düzenleyiciler için merkezi başarısızlık noktaları haline geliyor mu? Ele alınması gereken üç endişe var. İlk olarak, bilginin temsili ve doğruluğuna olan inanç. İkincisi, değerin temsili ve bununla ilişkili mülkiyeti. Üçüncü, varlıkların temsili ve belirli bir kullanıcının bu türden toplam güven düzeyi ile birlikte varlıklar. Faydalı olabilmesi için, bilgi ve değerin eski finans dünyası ve Cardano. İtibar ve zemin oluşturmak için sonuçların belirlenmesi ve kaydedilmesi gerekir. başvuru için. Yine de, bu tür şeyler çoğunlukla ilgili aktörler için doğası gereği kapsamlıdır. Kodlamak için onları bir blok zincirinde küresel ve kalıcı hale getirecektir. Dahası, değer miras dünyasında her zaman serbestçe akamaz. Ambargolar, yaptırımlar, sermaye kontroller ve adli işlemler varlıkları dondurabilir. Birlikte çalışabilir olmak için kimse bir Değerin sızması için daima tahliye vanasını açın. Son olarak, kuruluşların markası ve itibarı, ticari faaliyetlerin temel taşlarından biridir. pazarlama kampanyalarına her yıl milyarlarca dolar harcanır. ve markaları onarın. Bir kişi veya kuruluş hakkında iftira niteliğinde, yanlış veya yanıltıcı iddialarda bulunulursa, O zaman yasal başvuru hakkına sahipler. Yine de blok zincirleri kalıcı olarak korumaya çalışıyor Tarih. Programlama dili seçimimiz gibi, Cardano'nun çözmesi için ideal bir çözüm yoktur. bu endişeler her zaman ve her yerde doğru bir şekilde. Bunun yerine, desteklenen görüşlere teslim olmalıyız. tekrar. Bilgi akışıyla ilgili olarak, bu akış güvenilir bir veri akışı olarak bilinir. Bir kaynağı var ve içerik. Kaynaklar, aldatmak veya sürdürmek için bazı güvenilirlik ve teşvik kavramına sahiptir. dürüstlük. İçerik keyfi olarak kodlanabilir. Protokol yığınımızdaki güvenilir donanımı desteklemeyi amaçladığımız için, Profesör Ari Juel ve diğerleri için destek eklemeyi keşfedin.Kasaba Crier ProtokolüVarsayarsak Güvenilir bir veri kaynakları kümesinin varlığı, Town Crier web'in güvenli bir şekilde kazınmasına izin verir akıllı sözleşmelerde ve diğer uygulamalarda kullanım için içerik. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 30 bölgesinin 44

Sayfa 31

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Emurgo, IOHK ve Cardano Vakfı tarafından kaynakların bir önyükleme listesi sağlanacaktır. bu liste, Cardano'dan türetilen mekaniği kullanan topluluk küratörlüğünde bir liste ile değiştirilecektir. hazine sistemi. Umudumuz, bir itibar sisteminin iyi veri akışları etrafında gerçekleşebilmesidir. böylelikle güvenilirliği ve doğruluğu kademeli olarak iyileştirmek için olumlu bir geri bildirim döngüsü oluşturur. Değerin temsili daha karmaşık bir konudur. Bilgiden farklı olarak - bir zamanlar doğruluk, dakiklik ve eksiksizlik kurulur, protokoller güvenilir ve güvenilir bir şekilde davranabilir. deterministik yol - değer daha hassastır. Değer, jetonlaştırıldıktan sonra benzersiz bir nesne gibi davranmalıdır. Bilgi kopyalanabilir ve etrafta dolaştırıldı, ancak bir şeyin sahipliğini temsil eden bir jeton (örneğin bir araç adı) olamaz klonlanmış ve iki farklı defterde işlem görmüştür. Bu eylem, sistemi. Tokenleştirilmiş değerle uğraşırken eski birlikte çalışabilirlikteki zorluk, bu güvendir Defterler arasında belirteçler aktıkça varsayımlar, güvenilirlik ve denetlenebilirlik değişir. Örneğin, Bob bir miktar Bitcoin'e sahip ve daha sonra bunları bir borsaya yatırıyor, ardından Bob şimdi Borsasının kendi defterinde Bitcoin'i temsil etmesi. MtGOX durumunda, defterleri gerçeğe uymamak, kullanıcıların her şeyi kaybetmesine neden olmaktır. Sorun,

eski sistemlerin içinde yaşayan jetonları tanıması ihtiyacı nedeniyle daha da karmaşık hale geliyor. bir kripto para birimi. Daha önce de belirtildiği gibi, işletmeler tarihsel olarak yükseltmeye dirençlidir yazılımları ve yeni protokolleri destekliyor. Bu durum net bir çözüm. Cardano için en iyi umudumuz, kullanıcılara zengin bir sarf malzemesi ekleme seçeneği sunmaktır. Meta verilerin yüzdesi işlemlerine devam edin ve ardından endüstri standartlarının devreye girmesini bekleyin. ile ilerleme kaydedildiInterledger çalışma grubuGibi çabalar R3CevVe uluslararası eski mali protokollerin güncellenmesi için talimatlar. Bununla birlikte, daha büyük zorluk, bir mirastan gönderilen değerin nicelendirilmesi ve nitelendirilmesidir. sistemi bir kripto para defterine aktarın. Örneğin, Bob bir banka sahibiyse ve bir dolar verirse desteklenmiş jeton, daha sonra jetonlarını bir deftere göndermek için her zaman bir köprü kurabilir. Cardano olarak kullanıcı tarafından verilen varlık. Cardano, sahipliği tam olarak takip eder ve ulaştığımız tüm özellikleri sağlarken Zaman damgası ve denetlenebilirlik gibi sevgi, hiçbir kripto para birimi Bob'u dürüst bir bankacı yapamaz. Her zaman kısmi bir rezerv bankası çalıştırma seçeneğine sahiptir, bunun için tüm gücünü desteklemeyecektir. Dolar NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 31 bölgesinin 44

Sayfa 32

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz jetonlar ile gerçek dolar. Bu dolandırıcılık, dolar olmadığı sürece bir kripto para birimi tarafından tespit edilemez. kendisi dijital bir defter tarafından hesaplanan bir belirteçti. 25 Son olarak, çevrimiçi varlıkların temsili, eski zamanlara kadar uzanan klasik bir ağ sorunudur. İnternet günleri. Üniversiteler, işletmeler, devlet daireleri ve herhangi bir keyfi kullanıcı bir noktada kimliklerini oluşturmaları gerekir. Bu amaçla, web'inki gibi pragmatik ancak merkezi çözümlerAçık Anahtar AltyapısıVe ICANN'in DNS sistemi uygulanmıştır. Verilen modern web zevk, bu çözümler hem ölçeklenebilir hem de pratiktir. Ancak daha ticari odaklı bir güvenilirlik, güvenilirlik ve belirlenmesi için gerekli diğer meta özellikler sorusu varlık ile iş yapmak isterse. EBay gibi çok taraflı pazar yeri sunucuları, bazılarını sağlamak için bir iş modeli oluşturdu. bu meta verilerin yanı sıra işlemleri tamamlamak için bir çerçeve. İçeriğin kalitesi, etkinlikler ve işletmeler genellikle yalnızca çevrimiçi derecelendirmelerden derinden etkilenir güvenilir kaynaklardan. 26 Bu noktanın Cardano ile ilgili kısmı, itibarın merkezileştirilmesi meselesidir. Cardano için hedeflerimiz, gelişmekte olan dünya için bir mali destek sağlamaktır. Bu çaba daha önce hiç tanışmadığı oyuncularla güven tesis edebilme yeteneğidir. Tek bir kuruluş veya bir varlıklar konsorsiyumu kimin iyi veya kötü olarak etiketlendiğini kontrol ediyorsa, Organik bir bütün olarak topluluktaki gerçek etkileşimlerden türetilen süreç, bu durumda bu varlıklar Algılanan herhangi bir günah için herhangi birini keyfi olarak kara listeye alın. Bu güç, bir proje olarak değerlerimize aykırıdır. ve bir kripto para birimi kullanmanın daha geniş anlamını ortadan kaldırır. Neyse ki, hazine sandıklarına oy verirken kullanılan aynı mekanizmalar, Güvenilir veri beslemeleri ve bir protokolün çatallanması, bir itibar alanı oluşturmak için yeniden kullanılabilir. Bir açık araştırma alanı ve umudumuz, merkezi olmayan bir araştırma için bir bindirme protokolü sağlamaktır. Daha temel unsurlar yerleştikten sonra 2018-2019'da güven ağının itibarını artırdı. Cryptocurrency Birlikte Çalışabilirliği 25 Sayısal defterler için ise,rezerv kanıtıAkıllıca bir tutmanın yolu olarak önerilmiştir cryptocurrency yalnızca dürüst bir şekilde değiş tokuş eder. 26 Bu oranlar, içeriğin oluşturulmasını bile etkiler. Nasıl olduğunu öğrenmek için bu ilgi öyküsüne bakın.Rotten Tomatoes film endüstrisini etkiledi. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 32 bölgesinin 44

Sayfa 33

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Eski dünyadan dağıtılmış dijital defterlere geçildiğinde, birlikte çalışabilirlik çok daha kolay hale geliyor. Her defterin bir ağ protokolü, iletişim standartları ve güvenlik varsayımları vardır. ilgili fikir birliği algoritması hakkında. Bunlar sırayla kolayca ölçülebilir. Yabancı ağa bağlanarak ve onun çevirisini yaparak bilgi hareketi tesis edilir. mesajlar. değerin Hareketi yoluyla yapılabilir bir röle sistemine, Atomik çapraz zincir ticaret ya da bir akıllı aracılığıyla yan zincirleri Şema. Merkezi bir operatör olmadığından, Varlıkların temsili, geliştiricilere, madencilere veya başka bir powerbroker. Cardano için Kiayias, Miller ve tarafından geliştirilen yeni bir yan zincir protokolü entegre ediyoruz. Zindros. İki zincir arasında değeri güvenli bir şekilde hareket ettirmek için etkileşimli olmayan bir yol sağlar. protokolü destekleyin. Bu mekanizma, değerin CSL ile bir CCL katmanı. Diğer kripto para birimleri için, Cardano'nun değeri ve kullanıcısı büyüdükçe federe köprüler oluşmalıdır. Cardano SL, bu büyümeyi hızlandırmaya yardımcı olmak için Plutus'un kısıtlı bir sürümünü destekler. birlikte çalışabilirlik komut dosyaları. Shelley ve CSL'nin sonraki sürümlerine yeni işlemler eklenecek özellikle bu ihtiyaçları karşılamak için. Daedalus Labirenti Birlikte çalışabilirlik konusundaki noktalar küresel bir perspektiften gelir. Özel protokoller, yeni işlem türleri, güvenilirliği değerlendiren sistemler ve bilgi akışının kapsamı, sadece tek bir bekçi veya kullanıcı. Aksine, bunlar olmadan herkes tarafından kolayca erişilebilir olmalıdır. sansür veya geçiş ücretleri. Yine de Cardano bir protokolü, işlemi veya uygulamayı desteklemediğinde ne olur? kullanıcı onsuz yaşayamaz mı? Sadece kapsam dışı mı kalmalıyız? Web de benzer bir endişeyle karşılaştı 1990'larda. İronik olarak, web, kripto para birimleriyle çoğaltılabilen iki farklı çözüm sunar. JavaScript'in tanıtımı, rastgele eklemek için herhangi bir web sitesine programlanabilirlik sağladı özellikleri. Tarayıcı eklentilerinin ve uzantılarının tanıtımı, aşağıdakiler için özel yetenekler ekledi: bunları yüklemeye istekli kullanıcılar. Her iki yaklaşım da bize tüm güvenliğinin yanı sıra modern ağı sağladı dehşet. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 33 bölgesinin 44

Sayfa 34

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Ethereum, kullanıcıların alt protokolleri Akıllı sözleşmeler olarak Ethereum blockchain. Cardano bu özelliği CCL aracılığıyla destekler paradigma. Peki özel uzantılar ne olacak? Açıklayıcı bir örnek, bir kripto para birimi tüccarı olabilir. Merkezi olmayan bir pazar yeri hayal edin, DM denilen, bir dizi farklı kripto para birimini destekleyen. Bir tüccar kendi DM'ye etki eden stratejiler. Parçalanmış bir ekosistemde, tüccarın her biri için düzinelerce müşteri kurması gerekecektir. kripto para birimi ve ardından koordine etmek için her müşteriyle konuşmak için özel bir yazılım yazın otomatik işlemler. Bir istemci güncellenirse, ısmarlama yazılımı bozabilir. Ayrıca, tüccar yazılımı satmak isterse ne olur? Çeşitli kripto para birimlerine arayüz olabilirse, uzantıların web modelinden esinlenilmiştir. bir web yığınına çekildiğinde, tüccarın görevi önemli ölçüde daha kolay hale gelir. Evrensel arayüz kurulabilir. Kurulum tek tıklamadır. Yazılım dağıtımı modellenebilir Chrome web mağazasından sonra. Cardano için, referansımızı kullanarak bu paradigmayı denemeye karar verdik. cüzdanın Electron'da ön ucu. Github tarafından sürdürülen açık kaynak kodlu bir projedir. Hem Düğüm hem de Chrome birlikte. Cardano'nun Electron yapısına Daedalus denir. İlk nesil Daedalus, beklenenlerin çoğunu destekleyen bir HD cüzdan görevi görecek. 27harcama parolaları gibi endüstri standartları olan muhasebe ve güvenlik özellikleri ve BIP39. Daha sonraki nesillerde Daedalus, bir mağazayla birlikte bir uygulama çerçevesi haline gelecektir. evrensel entegrasyon API'leri ve bir SDK. En önemli yenilikler, programcıların JavaScript'i kullanmasına izin veren geliştirme kolaylığıdır. Uygulamalarını oluşturmak için HTML5 ve CSS3 ve çapraz uygulamalar için birleşik bir köprü

iletişim. Kriptografi gibi karmaşık davranışlar, dağıtılmış bir ağı yönetme ve veritabanı mekaniği soyutlanabilir, böylece geliştiricinin yalnızca kullanıcıya odaklanmasına izin verilir deneyim ve uygulamalarının temel mantığı. Daedalus'un evrensel bir çerçeve olması amaçlandığından, yol haritası ve evrimi bir şekilde Cardano'dan bağımsız. 2017 boyunca birbirlerine sıkı sıkıya bağlılar, ancak daha sonra Cardano sadece Daedalus kullanıcısı için başka bir uygulama. Ayrıca son derece benzersiz özellikleri keşfetmeyi planlıyoruz yalnızca Intel SGX'te çalışan evrensel bir anahtar yönetimi hizmeti gibi. 27 Hangisi zaten mevcut?daedaluswallet.io NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 34 bölgesinin 44

Sayfa 35

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Sonuçta, protokol tasarımcıları olarak tüm ihtiyaçları destekleyemiyoruz. Umudumuz esnekliğin Daedalus'un CCL üzerinde çalışan durum bilgili akıllı sözleşmelerle birlikte sağlayacağı, tasarım kararlarımız tarafından dışarıda bırakılanlar. Ayrıca, daha iyi standartların ortaya çıkmasını umuyoruz. tüm kripto para birimlerini daha iyi birlikte çalışabilirlik ve güvenlikten yararlanmaya teşvik edin. 4. Düzenleme Yanlış İkili Düzenlemelerin çoğu zaman cıvıl cıvıl ve gizemli olabileceği gibi, biri mecazi olarak zarif bir sonuç çıkarabilir. yolsuzluğun ve adalet arayan savcılarının anlatı döngüsü. Ancak tüm araçlar gibi bunlar da kaba, eski veya basitçe kötüye kullanılmış olabilir. Kripto para birimleri insan durumunu veya anlatı döngüsünü değiştirmedi. en iyi niyetlere rağmen dolandırıcılık, kötü oyuncular ve korkunç sonuçlar olabilir. kripto para birimleri insan yargısını ortadan kaldırabilir, insan davranışını kaldıramaz. Bir kripto para birimi tasarımcısı, düzenleyiciye hangi araç setini sunacağı konusunda bir pozisyon almalıdır. Kötü olayları düzeltin. Kripto para birimlerinin karşılaştığı benzersiz zorluk, bunların bir ürünü olmalarıdır. düzenleyici ve parasal başarısızlık. 28 Kültürel olarak, kripto para birimlerinin çoğu, hükümetin eylemlerinin yozlaşmış, beceriksiz veya etkisizdir. Bu nedenle, çok az saygıları, sabırları veya özel bir arka kapıyı destekleme istekleri vardır. bir düzenleyici veya kanun adamı için yanlışları düzeltmek. Bu eylem tüm amaç için aforoz olacaktır. -Den kripto para birimleri. Öte yandan, değişim başarısızlıklarını ve tarihi olayları hesaba katarsak, Protokolün 3 Ocak 2009'da başlamasından bu yana Bitcoin kayboldu veya çalındı. 30 Haziran 2017'de kaybedilen veya çalınan değer 4 milyar doları biraz aşıyor. Ve bu rakam hesaba katmıyor dolandırıcılık ve kötü biçimlendirilmiş ICO'lar nedeniyle kaybolan Bitcoin ve diğer tokenler için. 28 gömülü olarak gerçeği Satoshi Bitcoin Genesis BlokThe Times'tan alınan şu başlık: Times 03 / Oca / 2009 Şansölye üzerinde eşiğine ait ikinci kurtarma için bankalar NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 35 bölgesinin 44

Sayfa 36

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Bir de mahremiyet meselesi var. Makro ölçekte değer, uzmanlaşmış kanallar aracılığıyla akıyor düzenlenmiş, meta veriler açısından zengin ve hukuki yaptırım, hükümetler tarafından aktif olarak izlenen ve uluslararası düzenleyicilerdir. Sızıntının sadece üzerinde meydana geldiği, iyi anlaşılmış bir oyundur. Dünya dijital paraya geçerken giderek azalan işlerin nakit tarafı. 29 Kripto para birimleri olmasaydı paradigma, giderek daha fazla tedavi eden bir dünya gibi görünecekti sosyal medya içeriği gibi finansal mahremiyet. Hiçbiri yoktur ve kimse vazgeçemez. Bu nedenle biz bariz bir ikilem yaratan bir ikilem var. Bir kripto para birimi tasarımcısı ilkelerden vazgeçebilir ve yerellerinin talep ettiği her şeye boyun eğebilir yargı yetkisi, kodlarına yerleştirir ve bu nedenle gizlilik ve bütünlüğünden ödün verir. Ya da daha ilkeli ama anarşist bir felsefe benimseyebilir, bu da kendisini güncel en iyi uygulamalar ve yasalar. Cardano için, bu anlatının hayal gücü eksikliğinden kaynaklanan yanlış bir ikilem olduğunu düşünüyoruz. . gerçek şu

ki, çoğu kullanıcı pazarlar için mevcut olan kurallar konusunda endişeli değil. bir veya daha fazla oyuncuya fayda sağlamak için kurallarda ani değişiklikler yapılmasından endişe duyuyorlar. kimin özel ayrıcalıklara sahip olduğu konusunda şeffaflık eksikliği hakkında. Bireysel ve piyasa hakları arasında ayrım yapmalıyız. Kripto para birimlerinin bir küresel erişim, hakların olabildiğince kullanıcı odaklı olması gerekir. Gizlilik makul olmalı ve bir bekçi değil, kullanıcının kontrolünde olmalıdır. Değer akışı Kısıtlamasız olmalıdır Değer, rıza olmaksızın ani elden çıkarılmamalıdır. Pazar perspektifinden bakıldığında, pazarın veri kullanımı konusunda şeffaf olması gerekir. fonlar kendi içinde ele alınacak ve herkesin aynı kurallara göre oynaması gerekecek. , Kullanıcı bir kez izin verdikten sonra fikrini aniden değiştiremez: rahatsızlık. Karşı tarafların da kesinliğe ihtiyacı vardır. Fakat soyuttan gerçek bir sisteme tam olarak nasıl geçilir? pratik ve yasal görünüm? Çözümümüzü üç kategoriye ayırdık: meta veriler, kimlik doğrulama ve uyumluluğun yanı sıra pazar DAO'ları. 29 Okuyucu, David Wolman'ın bir kopyasını almayı düşünmelidir.Paranın SonuKapsar. Nakit kaybına doğru uluslararası hareket. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 36 bölgesinin 44

Sayfa 37

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Meta veriler Bir şeyin eylemi, onu çevreleyen meta verilerden genellikle daha az ilgi çekici olabilir. Örneğin, Denver'dan Boulder'a gitmek bir eylemdir. Denver'dan Boulder'a arabayla gitmek bir eylemdir. Ferrari Ortalama 120 MPH'de 488 meta veridir. Kesinlikle bu, A Ortalama 30 MPH'de Toyota Prius. Finansal işlemler de farklı değil. Bunları çevreleyen bağlam olağanüstü ekonomistler, vergi otoriteleri, kolluk kuvvetleri, işletmeler ve diğer kuruluşlar için önemlidir. Ne yazık ki Mevcut fiat tabanlı sistemimizde, çoğu tüketici meta veriler açısından ne kadar zengin olduklarını asla işlemler veya kiminle paylaşıldığı. 30 Cardano için, kullanıcıların paylaşmaya ihtiyaç duyabileceğini veya yasal olarak gerekli olduğunu kabul ediyoruz Vergi daireleri gibi belirli aktörlerle yapılan işlem meta verileri. Ancak bu paylaşımın, kullanıcının rızasına bağlı olmak. Ayrıca, blockchain sistemlerinin sahtekarlığı, israfı ve dolandırıcılığı ortadan kaldırmak için muazzam bir güce sahip olduğuna inanıyoruz. denetlenebilirlik, zaman damgası ve değişmezlik sağlayarak kötüye kullanım. Bu nedenle, bazı meta veriler Cardano blok zincirine gönderildi. Zor kısım, blok zincirimizi önemli ölçüde kınamayan doğru bir denge bulmaktır. Bu endişeyi göz önünde bulundurarak, pragmatik bir yaklaşım seçtik. Birincisi, Daedalus önümüzdeki 12 ay boyunca etiketlenecek çok sayıda özelliği destekleyecek işlemler ve finansal etkinlik. Bu meta veriler, isteğe bağlı olarak dışa aktarılabilir ve paylaşılabilir: Kullanıcının gerekli gördüğü kişi.Ayrıca, veriler üç tarafça kullanılabilir. etki alanına özel amaçlar için uygulamalar (örneğin, vergi muhasebesi). İkinci olarak, karmalar ve hash'ler içerebilen özel adresler için destek eklemeyi araştırıyoruz. şifrelenmiş alanlar. Bu yapı, bir kullanıcının blok zincirimizdeki meta verileri, kamuya açıklıyor. Ancak verileri paylaşmak isterse, tüm verileri denetlenebilirlik, bir işlemin sahip olduğu değişmezlik ve zaman damgası garantisi. 30 Daha makro ölçekte, yazar Juan Zarate bu verilerin ABD Hazinesi Terörizmle savaş departmanıHazine Savaşı. küresel finans piyasalarının mevcut yapısı jeopolitik amaçlar için kullanılabilir. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 37 bölgesinin 44

Sayfa 38

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Bir öznitelik alanı içeren bir adres yapısını zaten konuşlandırdık. Şu anda hızlı cüzdan kurtarma için HD cüzdan ağaç yapısının şifrelenmiş bir kopyasını saklamak için kullanılır (bkz. HD Cüzdan dokümantasyonu) Daha sonraki sürümler bu yapıyı genelleştirecektir. Kimlik Doğrulama ve Uygunluk İşlemlerle yakından bağlantılı, işlem yapma hakkı konuları ve fon sahipliği. Örneğin, bir şey satın almak için yeterli fon varken (örneğin

alkol), satın alımında kısıtlamalar olabilir (yaş gereksinimleri). Fonların mülkiyeti ve menşei, genellikle müşteri düzenlemelerinizi bilmenizi sağlar. Banka veya döviz gibi bir para hizmeti işletmesi yeni bir müşteri için bir hesap açtığında, genellikle müşteri ve parasını nereden elde ettiği hakkında temel bilgileri toplamak gerekir itibaren. Teknolojik zorluk, yasal olarak gerekli olan bunu sunma sürecinde bilgileri, gönderen kullanıcının nasıl kullanılacağı, saklanacağı ve eğer hiç olmayacak imha edildi. Uygunluk bilgileri ticari olarak değerlidir. Kimlik hırsızlığı için çalınabilir veya düzenlemelerin izin verdiği yerlerde yeniden satılır. Cardano için olabildiğince yenilik yapmak istiyoruz.Protokollerin yazılım tarafında, Orada uyumluluk bilgisinin alıcısının bir Davranış kapsamı. Bununla birlikte, protokollerin donanım tarafında, güvenilir donanım kullanılarak, belirli politikaları uygulamak için Intel SGX ve diğer HSM'lerden yararlanın. Bu nedenle, kasaya izin vermek için bir paylaşım politikasının yanı sıra Sealed Glass Proofs kullanmayı araştırıyoruz. uygunluk bilgilerinin bir doğrulayıcıya iletilmesi, bu da daha sonra aşağıdakilere uymak zorunda kalır. politikalar altında aktarıldı. Hem tek tip standartların ortaya çıkabileceğine hem de ayrıca bu yöntemin, müşteri verilerinin kaybolmasını önleyerek doğrulayıcılar için riski azaltacağını hackerlar. Bu çabanın bir sonucu olarak, Cardano için önerdiğimiz katmanlı model, değeri hesaplama da bu yaklaşımdan yararlanabilir. Hesaplama katmanı düzenlenmiş varlıklar (örneğin borsalar veya kumarhaneler), daha sonra uyumluluk kontrolleri yapmaları ve potansiyel olarak kullanıcılara vergi politikasını uygulama. Kullanıcı, SGP'leri kullanarak kişisel olarak tanımlanabilir bilgilerle birlikte para gönderebilir. daha geniş internete sızacağı ya da fikir birliği düğümleri tarafından korunacağı endişesi NEDEN BİZ Cardano inşa ediyoruz

Sayfa 39

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Ayrıca, hesaplama katmanı tüm kullanıcıların işlem doğrulanmış ve yasaldır. Bu paradigma, düzenlemeye tabi kuruluşlar arasında müşteri taşınabilirliğine de olanak tanır. Borsalar, bu güvenli kanallar üzerinden müşteriler için bakiye ve hesapları anında aktarın ve ayrıca - Politikaların izin verdiği yerlerde - verileri düzenleyicilerle paylaşın. Bu teknolojinin ilk beta testinin 2018 ortalarında bir amaç 2018'in sonundaki Cardano entegrasyonuna doğru, araştırma sonuçlarının beklendiği 2019'un başlarına. Bu zaman çizelgesi ayrıca, üzerinde kod imzalanması için ARM ve Intel ile işbirliği yapma yeteneğini de varsayar. Koşmak onların donanımı. 31Pazar yeri DAO'ları Önceki iki bölüm, bilginin üretimini ve hareketini ele aldı. bazı harici sistemlerin varlığı. Eski birlikte çalışabilirliği sağlamak için bu özellikler her zaman gerekli olabilir, ancak blok zinciri tabanlı düzenlemelere değinmezler. Akıllı sözleşmeler, ilişkilerin mevcut olduğu tamamen yeni bir tür ticari sistem sağlar. deterministik, kendi kendini uygulayan ve belirsizlikten arındırılmış. Sırasıyla bunlar için kurallar oluşturmak için kullanılabilirler. tahkim, olaya dayalı geri ödemeler gibi keyfi olarak karmaşık yapıları içeren pazar yerleri, ve özel koşullar altında gerçeklerin açığa çıkarılması. Bu akıllı sözleşme zorlamalı yapılara Marketplace DAO'ları diyoruz. deftere yerleştirilecek özel protokol desteği veya değişkenlik. Aslında, bunlar tamamen birbirine bağlı akıllı sözleşmelerden oluşan bir koleksiyon kullanılarak oluşturulmuştur. Mimari konsept, esinlenerek ticari şablonlardan oluşan bir koleksiyon tasarlamaktır. sözleşme hukuku ve en iyi iş uygulamaları. Bu şablonlar, bir geliştiricinin Pazarda belirli standartları uygulamak için akıllı sözleşme. Örneğin, bir geliştiricinin toplu satış yapmak için CCL'de bir ERC20 jetonu düzenlemek istediğini varsayalım. . Bir Pazar yeri DAO, özellikle kalabalık satışlar ve hüküm ve koşulları için kurulabilir gönüllü veya yasal standartlar tarafından parametreleştirilmiş veya hatta zorunlu kılınmıştır. Geri ödeme gibi şeyler, Fonların yeniden tahsisi veya ödemenin dondurulması, geliştiricinin ERC20'sine devralınabilir sözleşme. 31 BkzIntel SGX Ticari Lisans Politikası NEDEN BİZ Cardano inşa ediyoruz

Sayfa 40

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Bu çaba, bir pazarın nasıl kontrol edilmesi gerektiğine dair makro bir tartışma yapmamızı sağlar. tüketicinin korunmasını sağlamak için. İkincisi, işlemlerin nasıl modelleneceğini tartışabiliriz. gibi belirli yargı alanlarında yasal korumayı ve hakları otomatik olarak sağlamanın yolu New Hampshire. Cardano Vakfı, IOHK ve diğer kuruluşlarla birlikte çalışan Cardano projesi, Akıllı sözleşme geliştiricilerinin kullanması için Marketplace DAO'larının referans kitaplığı. Umudumuz, sigorta ve düzenleyici piyasalar bu DAO'lar etrafında şekillenebilir ve sonuçlara göre kendi kendine gelişen. 5. Sürdürülebilirlik Kripto para birimi alanına dalmak, birçok kavramsal çelişkiye yol açar. Kripto para birimleri, değiştirilmesi zor olacak şekilde tasarlanmıştır, ancak tüm teknolojiler gibi, tasarım kusurlarını ve gelişmeleri ele almak için değişiklik. Blok zincirlerinin amacı merkezileştirme, ancak değişikliklere liderlik etmek veya kodu sürdürmek için güçlü aktörler gerektirir. Belki de en sinir bozucu deneyim, en çok göze çarpan açık eksiklikler olduğunda ortaya çıkar. Paydaşlar düzeltilmesi gerektiği konusunda hemfikirdir, ancak ileriye dönük yolda fikir birliği ortaya çıkamaz. Bitcoin'in blok boyutu tartışması artık iki yıldan fazla bir süredir aktif bir mesele. Günlük, toplamı birmilyar dolar beklemedeÇünkü ağ en yüksek kapasitede. Basit bir parametrenin değiştirilmesi - geçici çözümlerin varlığında bile - olamaz koordine edildiyse, o zaman işletmeler ve hükümetler milyarlarca bu sistemlerin üzerine altyapı inşa etmek için dolar mı? Bu konuda nasıl olabilir hesap veremeyen protokolleri entegre etmenin stratejik riski üzerine iş kumar rasyonel tasarım yükseltmeleri yapmak? Tarihe dönüp baktığımızda, internetin evrimi benzer bir model izlemiştir. geçiş gibi basit değişikliklerIPv4 ileIPv6'nın gerçekleştirilmesi onlarca yıl alıyor. Yine de bir blockchain teknolojisi ile internet arasındaki güçlü karşıtlık, farklı bir velayet tarzı. İnternet, DARPA'dan güçlü akademik çevrelerde büyüyen askeri bir projeydi. hükümet desteği ve iyi tanımlanmış bir dizi ilk koruyucu. İnternetin altında büyüdü kurumsal etkinin entrikaları olmadan ticari olmayan koşullar NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 40 bölgesinin 44

Sayfa 41

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz ağı tekelleştirmek. Aslında, e-ticaret,NSF AUP içinde yürürlükten kaldırılana kadar 1992 . İşletmeler interneti ticarileştirme lüksüne sahip olduklarında, zaten bir güçlü standartlar, ilkeler ve müjdeci taraftarlar. Bu gibi şirketleri durdurmadı AOL ve Microsoft'un oluşturmaya çalışmasındanduvar bahçeleri ve benzeri tescilli teknoloji oluşturma ActiveX. Gelen bu vakıf Google gibi yeni nesil aktörler durmadı bastırıyor kendi gündemleriMuazzam kullanıcı tabanları ve büyük harf kullanımları göz önüne alındığında. Tüccarlardan madencilere aktörler arayan kira sürüleri ile kripto para birimleri nihai 32ticari olarak motive edilmiş ekosistemler. Bu temel göz önüne alındığında, vesayetin evrimi kripto para birimleri, kişisel çıkar etrafında optimizasyonla sonuçlandı. Örneğin, doğrulamasız madencilik , bir madencinin kar marjı, ancak bu, madenciliğin tüm amacını ve faydasını tamamen göz ardı eder. Madencilik Merkezileşme, çoğunluğun kontrolünde sadece bir avuç aktörle gerçekleşti. Bitcoin'in hash gücü. İnternet gibi, kripto para birimlerinin de değişmesi için fikir birliği gerekir. Ama ne zaman bu kadar hızlı gücün bir avuç komisyoncuya merkezileştirilmesi gerçekleşir, değişim olmadığında ne olur onlara uygun mu? İnternetin aksine, çoğu kripto para biriminin önyüklemesi özgecil bir şekilde yapılmaz. ticari olmayan veya akademik araçlar. Başlangıçtan itibaren, bazı gruplar kazanç elde etmeye çalışır ve bu kazanımları sağlamaya yardımcı olmak için atanmış güç aracıları vardır. Merkezileştirme, her kripto para biriminin evriminde yüzleşmesi gereken bir gerçektir. Biz tam anlamıyla kaçamaz, ancak en azından kademeli ademi merkeziyetçilik etrafında tasarım yapmaya çalışmalı.

Cardano için, hangi faktörlerin merkezileştirmeyi desteklediğini ve protokolümüzün yavaş yavaş kamuoyuna açıklanmasını teşvik etmek için teknikler uygulanabilir web gibi altyapı. Tamamen ademi merkeziyetçiliğin hem imkansız hem de belki de ters etki Yine de bazı faktörler daha dengeli bir sistem üretmeye teşvik edilebilir. Birincisi, kitle satış fonlarının merkezi gözetimi çevik ve hızlı gelişime izin verirken protokolün ilk günlerinde, sonunda finansman çeşitlendirilmeli ve 32 Bkz.bağlantıBu terim hakkında daha fazla bilgi için NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 41 bölgesinin 44

Sayfa 42

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz kalkınmanın daha sistematik ve kasıtlı bir hızda emekliye ayrılması gerekiyor. Bu noktadan sonra, finansmanın kültürel, dilsel ve coğrafi önyargılardan kaçınması gerekir. İkincisi, topluluk sitenin altında yatan doğası hakkında daha fazla bilgi sahibi oldukça kripto para biriminin teknolojisi, yol haritasına ilişkin kararlar bir dizi çekirdek geliştiriciler veya vakıf. Teklif vermek için blockchain tabanlı bir yöntem olması gerekiyor, inceleme ve protokoldeki değişiklikleri yürürlüğe koyma. Üçüncüsü, Cardano SL blok zincirini korumanın arkasındaki teşvikler doğrudan uyumlu hale getirilmelidir. tüm kullanıcıların toplu istekleri ile. Bir grup uzman aktörün daha büyük topluluğun iradesinden bağımsız olan ortaya çıkar. İlk prensip olarak, bir hazine sistemini Cardano'ya entegre etmeyi seçtik. İçin ikinci olarak, Cardano İyileştirme Önerileri için resmi bir süreç uygulayacağız. CSL'nin kendisi tarafından koordine edilen sistem. Üçüncüsü için Ouroboros'un zarif bir çözüm. Yukarıdaki konularda daha fazla ayrıntı sağlanabilir, ancak bunlar kendi başlarına kapsamlıdır ve anket belgesinin kapsamı dışında. Mekanizma tasarımı en karmaşık olanlardan biridir ve Eksik teori ile birbirine bağlı akademik alanlar ve ayakta duracak sağlam kanonik model yok üzerinde. Bilime dayalı yaklaşımımızın daha ziyade,ikinci bölüm burada bize iyi hizmet ediyor. IOHK'dan Veritas ekibi, Lancaster Üniversitesi'nden bir grup araştırmacı ile ortaklaşa çalışmaktadır. yönüProfesör Bingsheng Zhang , Cardano'nun referans hazine modelini geliştirecek. İle 2018'deki entegrasyonun amacı, sonunda özel bir hakemli yayın bekliyoruz. 2017. Bir kripto para birimi protokolündeki değişikliklerin resmi açıklaması ve incelenmesi için bu konu şu şekildedir: en azından hem ontolojik kavramları hem de teşvik etmek için bir mekanizmayı gerektirdiği için anlaşıldı. geniş katılım. Belki bir tür temsili demokratik süreç ortaya çıkabilir veya daha rasyonel oylama sağlamak için sıvı geri bildirimin kullanılması. Bu yöndeki araştırmanın, IOHK'nın resmi katılımının çoğunu tüketmesini bekliyoruz. Cardano'nun gelişimi. Başlangıç noktası olarak, referans hazine ile birlikte konuşlanacağız. 33rızayı almak için birkaç mekanizma modelleyin. Kesin bir araştırma için daha fazla çalışma gereklidir. çözüm. 33 IOHK, 2020'nin sonuna kadar Cardano'yu inşa etmek için tutuldu NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 42 bölgesinin 44

Sayfa 43

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Son olarak, Ouroboros için teşvikleri iyileştirme çalışmaları,Profesör Elias Oxford Üniversitesi'nden Koutsoupias . Ouroboros'un kriptografik temellerinden sonra Tüm gerekli ölçeklenebilirlik çalışmaları, tahviller, cezalar ve egzotikler üzerine daha kapsamlı bir çalışma ile birlikte sağlamlaştırıldı teşvikler referans protokole eklenecektir. 6. Sonuç Bir kripto para birimi, protokollerinin, kaynak kodunun ve yardımcı programlarının toplamından daha fazlasıdır. nihayetinde bir İnsanlara ilham veren, onları mümkün kılan ve birbirine bağlayan sosyal sistem. Yarısı tarafından hayal kırıklığına uğramış Geçmiş protokollerin önlemleri, başarısızlıkları ve tutmayan vaatleri, daha iyi bir şey inşa etmek için yola

çıktık. Bu süreç ne basit ne de bitirebileceğine hiç inanmadık. Sosyal protokoller devam ediyor insanlar ve toplum değiştikçe sonsuza dek değişiyor. Yararlı olmak için gücü tuzağa düşürmek istiyoruz. nın-nin evrim ve Cardano'ya taşıyın. Evrim, tek bir el ya da büyük bir tasarım tarafından yönlendirilmez. Tesadüf esinli Cardano bu sürecin dijital düzenlemesi olmayı amaçlamaktadır. - bugünün piyasalarında ayakta kalabilecek kadar uygun ve gelişecek kadar uyarlanabilir Tanışmak geleceğin ihtiyaçları. Önceki bölümler, bu hedefe nasıl yaklaştığımıza dair kısa bir bakış sunuyor. bilişsel önyargıları tanımaya, tarihten öğrenmeye ve titizliği takip etmeye gayretle Hızlı gelişme ihtiyacını resmi yöntemlerle dengelemeye çalıştık. geleneksel olarak hızlı hareket edemez. Bu yolculuğa çıkmak olağanüstü bir ayrıcalık oldu. Son iki yılda, bizde var zaten kanıtlanmış güvenli bir risk kanıtı protokolü geliştirdi, küçük bir Haskell ordusu kurdu geliştirdiler ve Cardano'nun gelişimini birçok yetenekli bilim insanının endişesi haline getirdi. Laboratuvardan vahşi doğada konuşlandırılmış bir sisteme geçerken, Ağrıları ancak umudumuz, Cardano'nun geleceğinin tek bir insana benzeyen şekilde özetlenebilmesidir. Cardano, büyüklerinden öğrenen pragmatik bir hayalperest, iyi bir vatandaştır. onun ve her zaman faturalarını ödemenin bir yolunu bulur. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 43 bölgesinin 44

IOHK | 2017/06/28 | NEDEN BİZ Cardano inşa ediyoruz Geleceği bilemeyiz ama onu daha iyi hale getirmeye çalıştığımız için mutluyuz Herkes için bir tane. Okuduğunuz için teşekkürler. NEDEN BİZ Cardano inşa ediyoruz Creative Commons Attribution 4.0 Uluslararası Lisansı sayfa 44 bölgesinin 44