İÇİNDEKİLER

<ÖZNEL BİR YAKLAŞIM>

CHARLES HOSKINSON

<Charles.Hoskinson@iohk.io>

<C3A6 5E46 7B54 77DF 3C4C 9790 4D22 B3CA 5B32 FF66>

1.GİRİŞ

1.1. Motivasyon

2015 yılında başlayan Cardano, kripto para birimlerinin tasarlanma ve geliştirilme şeklini değiştirmeyi amaçlayan bir projedir. Getireceği yeniliklerden ayrı asıl amacı kullanıcıların ve sisteme uyum sağlamak isteyen diğer sistemlerin ihtiyaçlarını daha iyi karşılayan, dengeli ve sürdürülebilir bir ekosistem yaratmaktır.

Cardano da açık kaynaklı bir proje olarak kapsamlı bir yol haritası veya otoriter bir beyaz kağıtla başlamadı. Bunun yerine aşağıda verilen tasarım ilkeleri, sağlam mühendislik uygulamaları ve keşif yollarını benimsedi:

●Muhasebe ve hesaplama katmanlarının ayrılması,
● Temel bileşenlerinin son derece değiştirilebilir ve fonksiyonel bir kodla uygulanması,
● Akademisyenler ve geliştiricilerden oluşan grupların hakemli araştırmalarla çekişmesini sağlanması,
● Bilgi güvenliği uzmanlarının projeye erken dahil edilip disiplinlerarası ekiplerin yoğun olarak kullanımı,
●İncelemeler sonucunda keşfedilen sorunları düzeltmek için teknik incelemelerin ve uygulamaların hayata geçirilmesi; yeni araştırmalar arasında hızlı yineleme sağlanması,
●Güncellemelerin ağı yok etmeden uygulanmasının sağlanması,
● Gelecekteki çalışmalar için merkezi olmayan bir finansman mekanizmasının geliştirilmesi,
● Makul ve güvenli bir kullanıcı deneyimi ile mobil cihazlarda çalışabilmeleri için kripto para birimlerinin tasarımını iyileştirmeye yönelik uzun vadeli bir görüşün geliştirilmesi,
●Kullanıcıların kripto para birimlerinin fonksiyonlarına ve işlemlerine yaklaştırılması,
● Aynı defterde birden fazla varlığı hesaba katma zorunluluğunun göz önünde bulundurulması,
●Eski sistemlerin ihtiyaçlarına daha iyi uyum sağlamak için isteğe bağlı meta verileri içerecek şekilde soyutlama işlemlerinin olması,
●Sayıları neredeyse 1000'e varan altcoinlerin mantıklı özelliklerinden ders alınması,

● Protokol tasarımının son halini belirlemek için sadece buna özel olarak kullanılan ve Internet Engineering Task Force'dan ilham alan, standartlara dayalı bir süreci benimseyen bir vakfın kurulması,
● Ticaretin sosyal unsurlarının keşfedilmesi,
● Bitcoin'den devralınan temel ilkelerden ödün vermeden piyasa düzenleyicilerinin ticaretle etkileşime girmesi için sağlıklı bir orta yolun bulunmasıdır.

Cardano yukarıdaki fikirlerden yola çıkarak hem kripto para birimi literatürünü keşfetmeye hem de karşılaşılabilecek problemler için fikirler oluşturmaya başladı. Bu araştırmaların sonuçları ise İOHK'un kapsamlı makale kitaplığı, bunun gibi script diline genel bakışlara dair çok sayıda anket sonucu, Akıllı Sözleşmelerin Ontolojisi ve Scorex projesi gibi çok sayıda araştırma kağıdıdır. Araştırmalardan çıkan sonuçlar aynı zamanda kripto para birimleri endüstrisinin sıradışı ve hatta zaman zaman verimsiz büyümesinin değerinin bilinmesini sağladı.

Birincisi, kripto para birimlerinin tasarımında TCP/IP gibi başarılı protokollerin aksine çok az katman vardır. Mantıklı olup olmadığına bakılmaksızın, tek bir defterde kaydedilen gerçekler ve olaylar etrafında tek bir fikir birliği kavramını koruma arzusu olmuştur.

Örneğin Ethereum evrensel bir hesaplama bilgisayarı olmaya çalışırken muazzam bir karmaşıklığa maruz kalıyor ve potansiyel olarak sistemin değer depolama işlevini yok edecek basit problemlerden muzdarip. Herkesin programı ekonomik değeri, bakım maliyeti veya devletlerin düzenleyici organlarının tepkileri gözetilmeksizin birinci sınıf vatandaş muamelesi görmeli midir?

İkincisi, güncel kriptografik araştırmalar, kendilerinden önce yapılan araştırmaların değerini bilmez. Örneğin, 1980'lerde Bitshares'in Delegated proof of stake yöntemi teknik olarak garantili sonuç vererek kolaylıkla ve güvenilir bir şekilde rastgele sayı üretebiliyordu. (bkz. Rabin ve Ben-Or'un çığır açan makalesi).

Üçüncüsü, Tezos gibi birkaç önemli istisna dışında çoğu altcoin gelecekteki güncellemeler için var olan zincirde herhangi esneklik payı bırakmaz. Herhangi bir kripto para biriminin uzun vadede başarılı için soft ve hard forku başarılı bir şekilde uygulayabilme yeteneği çok önemli bir faktördür.

Kurumsal kullanıcılar, yol haritasının ve yol haritasının arkasındaki kişilerin geçici, önemsiz veya radikalleşmiş olduğu protokollere milyonlarca dolar değerinde kaynak ayıramazlar. Protokolün gelişimi için, bir vizyon etrafında fikir birliğinin olduğu verimli bir süreç olması gerekir. Bu süreç aşırı derecede külfetli ise oluşabilecek fikir ayrılıkları kripto para etrafındaki topluluğu parçalayabilir.

Para en nihayetinde sosyal bir olgudur. Bitcoin ve çağdaşları ticareti anonimleştirme ve aracıların ortadan kaldırılması amacıyla ticari işlemlerde istikrarlı kimlikler, meta veriler ve itibar ihtiyacını da ortadan kaldırdı. Bu verileri merkezi çözümler aracılığıyla eklemek ise bir blok zinciri kullanmanın ana nedeni olan denetlenebilirliği, küresel kullanılabilirliği ve değişmezliği ortadan kaldırır.

SWIFT, FIX ve ACH gibi eski finansal sistemler işlemlerinde meta veriler açısından zengindir. Bu sistemlerde hesaplar arasında ne kadar değerin taşındığını bilmek yeterli değildir. Hukuksal düzenlemeler gereği genellikle ilgili aktörlerin belgelendirilmesi, kanunlara uyum bilgilerinin düzenlenmesi, şüpheli faaliyetlerin rapor edilmesini ve diğer kayıt ve eylemler gerekir. Hatta bazı durumlarda bu meta veriler işlemlerin kendisinden daha önemlidir.

Bu nedenle meta verilerde yapılabilecek manipülasyonun, sahte para birimi kullanımı veya işlem geçmişinin manipülasyonu kadar zararlı sonuçlarının olabileceği sonucunu çıkarmak mümkündür. Bu alanları kendi isteğiyle doldurmak isteyen aktörler için ise hiçbir düzenleme yapmamak, protokolün benimsenme sürecine ve tüketici korunmasına zarar verir.

1.2. Misafirliğin Sonu

Kripto para birimi alanına yönelik araştırmamızın sonucu iki protokol koleksiyonudur. Bunlar sırasıyla, Cardano Settlement Layer (Anlaşma Katmanı) (CSL) ve Cardano Calculation Layer (Hesaplama Katmanı) (CCL) olarak adlandırılan, kanıtlanabilir şekilde güvenli bir proof of stake (Hisse ispatı) [1][2] tabanlı kripto para birimidir.

Tasarımımızda vurgumuz, kripto para birimlerinin sosyal yönlerini barındırmak, değer muhasebesini karmaşık hesaplamalardan ayırarak katmanlar halinde oluşturmak ve birkaç değişmez ilkeye[1] bağlı kalarak piyasa düzenleyicilerin ihtiyaçlarını ele almaktır.

Ayrıca makul olduğu durumlarda, hakemli bilimsel araştırmalar yoluyla önerilen protokolleri incelemeye ve kodlarımızı resmi spesifikasyonlara göre kontrol etmeye çalışıyoruz.

1.3. Proof of Stake (Hisse İspatı)

Proof of stake'in bir kripto para birimi için kullanması tartışmalı bir tasarım tercihidir, ancak güvenli oylama için bir mekanizma sağlaması, daha fazla ölçeklendirme kapasitesine sahip olması ve farklı teşvik yöntemlerine izin vermesi nedeniyle bu yöntemi benimsemeye karar verdik.

Cardanoda kullanılan protokolümüz Ouroboros, Edinburgh Üniversitesi'nden Profesör Aggelos Kiayias tarafından yönetilen ve beş akademik kurumdan[1] oluşan son derece yetenekli bir kriptograf ekip tarafından tasarlanmıştır. Getirdiği temel yenilik, titiz bir kriptografik model kullanarak güvenliği kanıtlı olmasından öte, işlevselliği artırmak için birçok protokolün birleştirilmesine izin veren modüler ve esnek bir tasarımdır.

Bu modülerlik; delegasyon, yan zincirler, abone olunabilir kontrol noktaları, hafif istemciler için daha iyi veri yapıları, farklı rasgele sayı oluşturma biçimlerine ve senkronizasyon türleri gibi özelliklere izin vermesidir. Bir ağ binlerce, milyonlarca ve hatta milyarlarca kullanıcıya sahip olmaya doğru evrildikçe konsensüs algoritmasının gereksinimleri de değişecektir. Bir kripto para biriminin temelinin geleceğe hazır olması için yeterli esnekliğe sahip olması, o para birimi için hayati önem taşımaktadır.

[1] Liste için Yönetmelik bölümüne bakınız.
[2] Connecticut Üniversitesi, Atina Üniversitesi, Edinburgh Üniversitesi, Aarhus Üniversitesi, Tokyo Teknoloji Enstitüsü.

1.4. Paranın Sosyal Unsurları

Paranın sosyal bileşenlerinin en iyi örnekleri kripto para birimleridir. Eğer yalnızca teknolojiye odaklanırsak Bitcoin ve Litecoin arasında çok az fark vardır; Ethereum ile Ethereum Classic arasında daha da az fark vardır. Yine de hem Litecoin hem de Ethereum Classic, piyasa büyüklükleri, sağlam ve dinamik toplulukları ile üstlendikleri sosyal görevlerini sürdürüyor.

Bir kripto para biriminin değerinin büyük bir bölümünü sahip olduğu topluluğun para birimini kullanma biçiminden ve para biriminin evrimine katılım düzeyinden türediği iddia edilebilir. Dash gibi para birimleri topluluklarını kriptonun gelişimi ve önceliklerin belirlenmesi ve finanse edilmesi sürecine dahil etmek için bazı sistemleri doğrudan protokole entegre etti.

Kripto para birimlerinin çeşitliliği aynı zamanda sosyal unsurlarının varlığına da kanıt sağlar. Kriptografik para birimlerinde uygulanan felsefe, para politikası hatta çekirdek geliştiriciler arasındaki anlaşmazlıklar bile toplulukta parçalanmalara ve forklara yol açabilir. Devletlerin fiat para birimleri ise kripto para birimlerinden farklı olarak siyasi değişimler ve yerel anlaşmazlıklardan bir para birimi krizi veya toplu göçler olmadan kurtulma eğilimindedir.

Bu bilgiden yola çıkarak devletlerin paralarındaki sosyal unsurların kripto para birimlerinde eksik olduğu iddia edilebilir. Kullanıcıların protokollerin arkasındaki sosyal sözleşmeyi anlamak için teşviklere ihtiyaç duyduklarını biliyoruz ve isteklerini üretken bir şekilde önerme özgürlüğüne sahip olduklarını savunuyoruz. Bu ilkemizi baştan beri Cardano'nun yol haritasına dahil ettik. Bu özgürlük piyasaların nasıl düzenleneceğinden hangi projelerin finanse edileceğine kadar değerin el değiştiği her yöne uzanıyor. Cardano sağladığı bütün bu özgürlüklere rağmen merkezi aktörler tarafından aracılık edilemez veya zengin bir azınlık tarafından atanacak yetkilere ihtiyaç duymaz.

Cardano kullanıcılarının ihtiyaçlarını karşılamak için CSL'nin üzerine kurulmuş bir katmanlama protokolleri sistemi uygulayacak.

İlk olarak, geliştirmeye para toplamak için halka arzda toplanan sermaye ne kadar büyük olursa olsun o fonlar zaman içinde eriyecektir. Bu nedenle Cardano belirli aralıklarla düşecek.

enflasyon oranına ve işlem ücretlerinden finanse edilen merkezi olmayan bir vakfa sahip olacak[1].

Her kullanıcı sistemden oylama ile fon talep edebilmeli ve fondan kimin yararlanacağı hususundaki oylamalara katılabilmelidir. Dash gibi hazine/vakıf sistemlerine sahip diğer kripto para birimlerinde görülen bu süreç, üretken bir geri bildirim döngüsü yaratır ve kimin finanse edilip edilmemesi gerektiği hakkında üretken tartışmalar başlatır.

Fonun dağıtımıyla ilgili tartışmalar, uzun ve kısa vadeli hedefler, kripto para biriminin sosyal sözleşmesi, projenin öncelikleri ve sunulacak tekliflerle değer yaratma inancı arasındaki ilişkinin kurulmasına destek olur. Yapılacak görüşmeler aynı zamanda topluluğun olası yol haritalarını sürekli olarak değerlendirdiği ve tartıştığı anlamına da gelir.

İkincisi, temennimiz Cardano'nun hem yumuşak hemde sert forkları önermek ve oylamak için resmi ve blok zinciri tabanlı bir sistem içermesidir. Blok boyutu tartışmasıyla Bitcoin, DAO çatalıyla Ethereum, ve birçok kripto para birimi kod tabanını teknik ve ahlaki yönü üzerinde uzun süredir ve çoğu durumda çözümlenmemiş argümanlara dayatır.

Topluluğun parçalanmasına neden olabilecek anlaşmazlıkların birçoğunun altındaki nedenin değişimi tartışmak için resmi süreçlerin eksikliği olabileceği tartışılabilir, ve tartışılmalıdır.

Biri Bitcoin kullanıcılarına Segregated Witness'ı tanıtmak için nereye gidebilir? Ethereum'un çekirdek geliştiricileri DAO'yu kurtarmak için topluluklarının görüşlerini nasıl öğrenecekti? Topluluğun parçalanması kripto para birimine onarılamayacak zararlar verir mi?

Bu konu için en kötü durumlarda harekete geçme otoritesi topluluğa değil, geliştiricilere, altyapı ilişkilerine veya paraya sahip olan kişilere devredilebilir. Ek olarak, topluluğun büyük bir kısmı kötü teşvikler[2] nedeniyle konularla ilgilenmiyorsa veya bağlantısı kesilmiş ise uygulanan eylemlerin meşru olup olmadığını nasıl bilebiliriz?

[1] Aynı zamanda hazine sistemi olarak da bilinir.
[2] Bkz: Rational İgnorance (Mantıklı Cahillik)

Tezos gibi bir kripto para birimlerinin anayasasını güncellemek için bir dizi resmi kural ve süreç uyguladığı ve anayasasını üç bölümde (İşlem, Konsensüs ve Ağ) ele alındığını bilmek bize bu konuda ilginç bir model sunar. Fakat bunlara rağmen teşviklerle ve bir kripto para biriminin kod olarak tam olarak nasıl modellenip değiştirileceği konusunda yapılacak çok iş var.

İlham almak için olası çözüm yolları olarak mali teşvikler için resmi yöntemlerin kullanımı, makine tarafından anlaşılabilir spesifikasyonlar ve bir hazinenin bu süreçlerle birleştirilmesi araştırılmaktadır. Bu konuda daha uygun çözümler tasarlanmasa bile, şeffaf ve sansürsüz bir şekilde blok zinciri tabanlı oylama ile bir protokol değişikliği önerme yetisi iyileştirmelidir.

1.5. Katmanlı Tasarım – Cardano Anlaşma Katmanı (CSL)

Kaliteli protokoller ve diller tasarlarken geleceğe değil, geçmişe bakılmalıdır. Tarih bize Açık Sistemler Bağlantısı (OSI) standartları gibi, kağıt üzerinde mükemmel ancak pratikte başarısız olan mükemmel fikirlerden örnekler sunar. Tarih, bize aynı zamanda TCP/IP ve JavaScript gibi mutlu kazalardan da örnekler verir.

Tarihsel bir bakış açısıyla düşünürsek, çıkarılabilecek bazı ilkeler şunlardır:

1. Geleceği tahmin edemezsiniz, esneklik payı tanıyın,
2. Karmaşıklık kağıt üzerinde güzeldir,ama genellikle basitlik kazanır,
3. Nerede çokluk orada karmaşıklık,
4. Bir standart benimsendikten sonra verimliliğine fazla bakılmaz, gelişimi muhtemelen yavaşlayacaktır,
5. Eğer ortada irade varsa kötü fikirler de iyi fikirlere dönüşebilir.

Cardano sosyal doğasını kabul eden finansal bir sistemdir. İleriki zamanlarda kullanıcıların işlemlerinde, esnekliğe ve karmaşıklığı ele alma becerisine büyük ihtiyaç duyulacaktır. Cardano başarılı olur ise milyonlarca eşzamanlı işlemi barındırmak için muazzam hesaplama, depolama ve ağ kaynaklarına ihtiyaç duyacaktır.

Adil bir ağ olmak için zengin node'lardan alıp fakirlere verecek dijital, merkezi olmayan bir Robin Hood'umuz yok. Ağın iyiliği için fedakarlık yapacak insanların hayır işleme duygusuna güvenme lüksümüz de yok. Bu nedenle Cardano'nun tasarımı endişelerin ayrılması kavramını TCP/IP'den ödünç alır.

Temelinde blok zincirleri, zaman damgaları ve değişmezlik hakkında garantiler vererek gerçekleri ve olayları sıraya dizen bir veri tabanlarıdır. Para bağlamında ise varlıkların sahipliklerini sıraya dizen bir veri tabanıdır. Programları depolayarak ve yürüterek karmaşık hesaplamaları eklemek ise ortogonal (dikey) bir kavramdır. Alice'ten Bob'a ne kadar değer gittiğini bilmek mi istiyoruz, yoksa işlemin arkasındaki tüm nedenleri anlamaya ve ne kadar göndereceğimize dair karar sürecine dahil olmak mı istiyoruz?

Ethereum daha esnek olduğu için ikinci seçeneği seçmiştir. Bu seçenek inanılmaz derecede caziptir, ancak böyle yaparak yukarıda belirtilen tasarım ilkelerini de ihlal etmiş oluyor. İşlemin nedenini anlamak, protokolün rastgele olayları anlayabilmesi, keyfi işlemler yazabilmesi, dolandırıcılık durumlarında tahkime izin verilebilmesi, hatta yeni bilgiler kullanıma sunulduğunda potansiyel olarak işlemleri tersine çevirebilmesi anlamına da gelir.

Bu durumda ise her işlem için hangi meta verilerin depolanacağı konusunda zor tasarım kararları vermek gerekir. Alice ve Bob'un alışverişinin arkasındaki nedenin hangi unsurları işlemle alakalı? Bu unsurlar sonsuza kadar işlemle alakalı mı kalacaklar? Bazı verileri ne zaman sistemden atabiliriz? Bunu yapmak bazı ülkelerde yasaları ihlal ediyor mu?

Ayrıca, bazı hesaplamalar doğası gereği özeldir. Örneğin, bir ofisteki çalışanların ortalama maaşını hesaplarken herhangi bir kişinin ne kadar kazandığını sızdırılması mutlaka istenmedik bir durumdur. Ama ya hesaplamalar herkes tarafından biliniyorsa? Ya bu bilgilerin halka açıklığı sonuca zarar verecek şekilde yürütmeyi önyargılı hale getirirse?

Bu nedenle değer muhasebesi ile değerin taşınmasındaki nedenin ayrı tutulmasına karar verdik. Başka bir deyişle değeri muhabesinden ayrı tutmayı seçtik. Bu ayrım Cardano'nun akıllı sözleşmeleri desteklemeyeceği anlamına gelmiyor; aksine, ayrımı bariz hale getirmek akıllı sözleşmelerin tasarımında, kullanımında, mahremiyetinde ve yürütülmesinde daha fazla esneklik sağlar.

Cardano'nun değer defterine Cardano Settlement Layer (Cardano Anlaşma Katmanı) (CSL) denir.

Amacı bir değerin muhasebesi olduğu için yol haritamız bu katmanla ilgili aşağıdaki hedefleri güder:

1. Biri değeri taşımak, diğeri katmanlama protokolünü geliştirmek üzere iki script dili grubunu desteklemek,
2. KMZ[1] yan zincirlerinin diğer defterlere bağlanması için destek sağlamak,
3. Yüksek güvenlik için kuantum dirençli imzalar dahil olmak üzere birden çok imza türünü desteklemek,
4. Birden çok kullanıcı tarafından tanımlanan varlıkları desteklemek ve
5. Gerçek ölçeklenebilirliği başarmak, yani daha fazla kullanıcı sisteme katıldıkça sistemin yeteneklerinin artmasıdır.

1.6. Script (Programlama Dili) Yazımı

Bir defterdeki adresler arasındaki işlemlerin yürütülmesi ve geçerliliğinin kanıtlanması için bir tür script (programlama dili) gerekir. İdeal olarak kişi, Eve'in Alice'in parasına erişmesini veya kötü tasarlanmış bir sözleşmenin değeri yanlışlıkla ölü bir adrese değer göndermesini ve fonları geri alınamaz hale getirmesini istemez.

Bitcoin gibi sistemler, despotik ve aşırı derecede katı bir script diline sahiptir; yapılan işlemleri anlamak ve okumak zordur. Solidity gibi dillerin genel programlanabilirliği ise sisteme olağanüstü bir karmaşıklık getirir ve getirdiği fayda geliştiricilerin azınlığına faydalıdır.

Bu nedenle yaratıcısı Simon Thompson ve ona ilham veren kavramların yaratıcısı Simon Peyton Jones'un onuruna Simon[2] adında yeni bir dil tasarlamayı seçtik. Simon "Composing contracts: an adventure in financial engineering" üzerine kurulu domain-spesific bir dildir.

Ana fikri finansal işlemlerin genellikle bir dizi temel unsurdan oluşmasıdır[3]. Eğer finans konusunda bir periyodik element tablosunu olsa idi, genel programlanabilirlik gerektirmeden ortak işlem türlerinin çoğunu kapsayacak büyük bir işlem kümesi için destek sağlanabilirdi.

[1] Bkz: Kiayias, Zindros ve Miller'dan Etkileşimli Olmayan Proof-of-Work Kanıtları.
[2] Özellikleri yaklaşan bir spesifikasyonda yayınlanacak. Dilin tamamı 2017'nin 4. çeyreği için planlanan Shelley CSL sürümünde desteklenecektir.
[3] Bkz: ACTUS Projesi

Birincil avantajı güvenliğin ve yürütmenin son derece iyi anlaşılabilmesidir. Şablonların doğruluğunu göstermek, havadan yeni para yaratma veya işlem esnekliği gibi sorunlu işlemlerin yürütme alanınından temizlenmesi için kanıtlar yazılabilir. İkinci avantajı ise sisteme yeni işlevsellik eklenmek istendiğinde yumuşak fork yoluyla daha fazla öğe eklemek için önceden bırakılmış uzantılar kullanılabilmesidir.

Bununla birlikte CSL'ı katmanlama protokollerine, eski finansal sistemlere ve özel amaçlı sunuculara bağlama ihtiyacı her zaman olacaktır. Bunu başarmak için ise hem genel amaçlı bir akıllı sözleşme dili olan hem de diğer sistemlerle uyumluluğu sağlamak için özel amaçlı bir DSL olarak Plutus'u geliştirdik.

Plutus, özel script yazmak için kullanılabilen, Haskell'in kavramlarına dayanan yazılı bir işlevsel dildir.

1.7. Yan Zincirler

Cardano yan zincirlerle ilgili olarak proof of work (iş ispatından) elde edilen sonuçlara dayalı olarak Kiayias, Miller ve Zindros (KMZ yan zincirleri) tarafından geliştirilen yeni bir protokolü destekleyecektir. Tasarımı bu makalenin kapsamı dışındadır; ancak konsept olarak sermayenin CSL'den herhangi bir Cardano Hesaplama Katmanına veya protokolü destekleyen diğer blok zincirlerine güvenli ve etkileşimli olmayan hareketini ele alır.

KMZ yan zincirleri, karmaşıklığa set çekmekteki anahtardır. Piyasa düzenleyicilerinin gereksinimlere, özel işlemlere, sağlam script dillerine ve diğer kaygılara sahip defterler, CSL için kara kutulardır. CSL kullanıcısı buna rağmen hesaplama tamamlandıktan sonra muhasebe ve fonları geri çekme yeteneği ile ilgili belirli garantiler elde edecektir.

1.8. İmzalamalar

Bir değeri Alice'ten Bob'a güvenli bir şekilde taşımak için Alice'in sermayeyi taşıma hakkına sahip olduğunu kanıtlaması gerekir. Bu görevi gerçekleştirmenin en doğrudan ve güvenilir yolu, fonların açık bir anahtara bağlı olduğu ve ona bağlı olarak Alice'in de bir özel anahtarı kontrol ettiği bir ortak anahtar imza şeması kullanmaktır.

Farklı güvenlik parametreleri ve varsayımlara sahip yüzlerce olası şema vardır. Bazıları eliptik eğrilere bağlı matematiksel problemlere dayanırken, diğerleri lattice (kafes) gibi egzotik kavramlara bağlı olarak çalışır.

Ana amaç ise her zaman aynıdır. Gizli bir bilgiye sahip olmadıkça çözülemeyecek zor bir problem vardır ve bu bilgiye sahip kişinin anahtar çiftinin sahibi olduğu ve onu kullanma yeteneğine sahip tek varlık olduğu varsayılır.

Bir kripto para birimi imza şemasını seçerken iki problemle karşılaşır. İlki uzun vadeli güvenliğin dayanıklılığıdır. DES gibi 1970'lerde ve 1980'lerde kullanılan bazı şifreleme yöntemleri işlevselliklerini yitirmiştir. Buna bağlı olarak kullanılan yöntemin hayatta kalma süresi hesaba katılmalıdır.

İkincisi, belirli bir yöntemin kullanımını tercih eden veya bazı durumlarda zorunda olan birçok işletme, hükümet ve diğer kurum vardır. Örneğin, NSA (Amerikan Ulusal Güvenlik Ajansı), Suite B protokol setini kullanır. Kriptografi konusunda ISO, hatta W3C çalışma gruplarının standartları var.

Bir kripto para birimi tek bir imza yöntemini seçmesiyle, yöntemin gelecekte işlevselliğini yitirebileceğini, yasal veya sektör kısıtlamaları nedeniyle bazı işletmelerin kripto para birimini kullanamayacağını da kabul etmiş olur.

Cardano için, özellikle Ed25519 eğrisi olmak üzere eliptik eğri kriptografisini kullanmaya karar verdik. Ayrıca Dr. Dmitry Khovratovich ve Jason Law'ın Spesifikasyonunu[1] kullanarak HD cüzdanlar için destek ekleyerek mevcut kütüphaneleri geliştirmeye karar verdik.

Cardano soft forklar aracılığıyla gelecekte daha fazla imza yöntemini destekleyecek. Özellikle kuantum bilgisayarlara dirençli imzaları sistemimize entegre etmek ile ilgileniyoruz.

[1] Bu belge Cardano'nun HD Cüzdan Uygulamasını açıklar. Cardano'nun Ed25519 HD Cüzdanlarını destekleyen ilk kripto para birimi olduğuna inanıyoruz.

Cardano, yumuşak forklar ile daha fazla imza yöntemini eklememizi sağlayacak özel uzantılarla tasarlanmıştır. Gerektiğinde ve yol haritasında[1] planlanan büyük güncellemeler sırasında eklenecektir.

1.9. Kullanıcılar Tarafından Yaratılan Varlıklar (User Issued Assets(I.U.A.s))

Bitcoin'de başlarda kullanıcıların aynı anda birden fazla para birimini takip etmesi zordu. Bunun için Bitcoin'in muhasebe sistemindeki varlıkları yayınlabilen protokoller hızla geliştirildi. Bitcoin bu katmanları doğal olarak desteklemiyordu; protokoller zekice yöntemlerle bu engelleri aştılar..

Colored Coins ve Mastercoin (Omni) gibi Bitcoin katmanları için hafif istemciler güvenilir sunuculara dayanıyordu ve işlem ücretlerinin bitcoin olarak ödenmesi gerekiyordu. İşlem onayları tek hatta birleştirilen bu özellikler Bitcoin'i çoklu varlık muhasebesi için yetersiz hale getirir.

ERC20 standardını kullanan Ethereumda ise özellik çeşitliliği vardır. Ancak işlem ücretleri için hala ethere ihtiyaç duyar. Ayrıca Ethereum, ağı verilen tüm ERC20 tokenlerının ihtiyaçlarına göre ölçeklendirilmede zorluk yaşıyor.

Temelde bu sorun üç bölüme ayrılabilir: kaynaklar, teşvikler ve endişeler. Kaynaklarla ilgili olarak aynı deftere tamamen yeni bir para birimi eklemesi, eklenen birimin bant genişliğini, bellek havuzu ve blok alanını paylaşan iki bağımsız UTXO (harcanmamış işlem girişi) setine sahip olması anlamına da gelir. Bu para birimlerinin işlemlerini zincire yerleştirmekten sorumlu olan node'lar teşvike ihtiyaç duyar. Fakat bir kripto para biriminin her kullanıcısı her varlığın para birimini umursamaz, ve umursamamalıdır da.

Bu sorunlar göz önüne alındığında çok varlıklı bir defterin birincil önceliğini merkeziyetsiz piyasa yapımına izin veren bir köprü para birimi olarak alması çok daha verimlidir. Tether veya MakerDAO gibi borç verme ve havale uygulamalarına ek fayda sağlamak için özel amaçlı varlıklar ihraç edilebilir.

[1] Bkz: Cardanoroadmap.com

Cardano bu konuda çok varlıklı muhasebeye pragmatik bir yaklaşım benimsemiştir. Amacı aşamalar halinde inşa edilip binlerce UIA'nın taleplerini desteklemek için aşağıda belirtilen gerekli altyapıyı sağlamaktır:

1. Büyük sayıda UTXO durumunun izlenmesine olanak sağlamak için özel amaçlı kimlik doğrulaması yapılmış veri yapılarının sağlanması,
2. Çok sayıda işlemi sıraya almak için dağıtılmış bir bellek havuzuna sahip olma yeteneğinin sağlanması,
3. Küresel bir blok zinciri için blok zincirinin bölünebilmesinin ve kontrol mekanizmalarının tasarlanması,
4. Farklı işlem gruplarını dahil etmek için node'ları ödüllendiren bir teşvik sisteminin tasarlanması,
5. Kullanıcıların hangi para birimlerini izlemek istediklerine karar vermelerini sağlayan bir abonelik mekanizmasının oluşturulması,
6. UIA'ların yerel varlıkla benzer güvenlikten yararlandığını garanti eden güçlü güvenlik mekanizmalarının tasarlanması ve
7. UIA ile ana token arasındaki likiditeyi iyileştirmek için merkeziyetsiz piyasa yapımına destek vermektir.

Cardanoda kullanılacak kimliği doğrulanmış veri yapısını bulmaya yönelik ön çabalarımız Leo Reyzin, IOHK ve Waves tarafından ortaklaşa geliştirilen yeni bir AVL+ Ağacı türüyle sonuçlandı. Daha fazla araştırma tabiki gerekli, ancak bu Cardano'nun sonraki bir sürümüne dahil edilecek temel bir gelişmedir.

Bu konuda Stanford Üniversitesi'nin RAMCloud protokolü kullanılarak dağıtılmış bir bellek havuzu uygulanabilir. Cardano'nun anlaşma katmanına entegrasyonunu incelemek için 2017'nin 3. çeyreğinde deneyler başlayacak.

Kalan konular birbiriyle bağlantılı ve devam eden araştırmalar kapsamındadır. Araştırma sonuçlarına bağlı olarak, 2018'de Basho'nun CSL sürümü sırasında UIA'lar için Cardano'ya bir protokol eklemeyi ümit ediyoruz.

1.10. Ölçeklenebilirlik

Dağıtılmış sistemler ortak bir amacı gerçekleştirmek için bir protokol veya protokoller paketini çalıştıran bir dizi bilgisayardan (node'dan (düğümden)) oluşur. Protokol veya protokol paketlerinin amacı ise BitTorrent protokolü gibi bir dosyayı paylaşmak veya Folding@Home kullanarak bir proteini katlamak olabilir.

Etkili protokoller, node'lar ağa katıldıkça kaynak kazanır. Örneğin, BitTorrentte bulunan bir dosya aynı anda birçok eş tarafından tohumlanıyorsa çok daha hızlı indirilebilir. Hız, eşler kaynakları sağlarken aynı zamanda tükettiği için artar. Dağıtılmış bir sistemin ölçeği belirtilirken genellikle bu özellik kastedilir.

Tüm mevcut kripto para birimlerinin tasarımındaki zorluk aslında ölçeklenebilir bir şekilde tasarlanmamalarıdır. Blok zincirleri genellikle birbirleriyle bağlantılı blokların bir listesidir. Bir blok zincirinde güvenlik ve kullanılabilirlik kavramları ise blok zinciri verilerinin tam kopyasına sahip olan çok sayıda node'a dayanır. Bu nedenle her bir bayt veri, node sayısı (N kadar) kadar çoğaltılmalıdır. Ek node'lar bu durumda ek kaynak sağlamaz.

Sistem genelinde işlemlerin yapılması ve mesajların dağılımı için de bu durum geçerlidir. Konsensüs sistemine daha fazla node eklemek sisteme ek işlem gücü sağlamaz; aynı işi yapmak için daha fazla kaynak harcanması anlamına gelir. Daha fazla relay (ağ geçidi) ise tüm ağı en güncel blokla senkronize tutmak için daha fazla node'un aynı mesajları iletmesi gerektiği anlamına gelir.

Bu ağ yapısı göz önüne alındığında kripto para birimleri klasik küresel finansal sistemler gibi ölçeklenemez. Eski altyapı ise ölçeklenebilir; hatta ölçeklenmek için daha fazla işlem ve depolama gücüne sahiptir. Bitcoin ise klasik yapıdaki akranlarına kıyasla çok küçük bir ağdır ve belirli bir bloğu ekleyebilmek ve mevcut yükünü yönetmekte zorluk çeker.

Konsensus algoritmalarımız, Cardano için ölçeklenebilirlik hedeflerimizi büyük ölçüde destekliyor. Ouroboros, Google ve Facebook gibi büyük altyapı sağlayıcılarının ihtiyaçlarını karşılamak için[1] son 20 yılda geliştirilmiş ve geleneksel protokolleri de çalıştırabilen bir konsensüs node'udur.

[1] Bağımsız olarak aynı amaçta ilerleyen Elastico ve Bitcoin-NG gibi başka protokoller de vardır.

1.11. Cardano Computation Layer (Cardano Hesaplama Katmanı) (CCL):

Daha önce de belirtildiği gibi bir işlemin iki bileşeni vardır: tokenların akışını gönderme ve kaydetme mekanizması ile tokenlerin hareket etmesinin arkasındaki nedenler ve koşullar. İkinci bileşen terabaytlarca veriyi, çoklu imzalamaları ve meydana gelen özel olayları içerebilecek kadar karmaşık, veya değeri başka bir adrese iten tek bir imza kadar basit de olabilir.

Değer akışının nedenlerini ve koşullarını modellemenin arkasındaki zorluk ise bu verilerin işlemi yapan taraflarca öngörülemeyecek derecede kişisel olmasıdır. Sözleşme hukukundan alınan dersler bize ticari açıdan kullanıcıların ne yaptıklarının farkında bile olamayacağı gibi daha da sorunlu bir tablo çiziyor. Buna "semantic gap (anlamsal boşluk)" denir[1].

Neden bu kadar karmaşık ve soyutluğa sahip bir kripto para birimi oluşturmak isteyesiniz? Böyle bir uğraş hem nafile, hem de pratikte naif görünüyor. Ayrıca her soyutlamanın hem yasal hem de güvenlik açısından sonuçları da vardır.

Örneğin, çocuk pornografisi paylaşımı veya devlet sırlarının satışı gibi evrensel olarak yasa dışı kabul edilen ve toplumca yüz kızartıcı olarak nitelendirilebilecek çok sayıda çevrimiçi etkinlik vardır. Güçlü bir merkeziyetsiz sistemin devreye sokulması, bu faaliyetin normal ticari işlemlerin sahip olduğu sansür direnciyle gerçekleşmesi için bir kanal sağlanması anlamına da gelir. Merkeziyetsizleşmeye teşvik edilen konsensüs nodelarının barındırdıkları içeriklerden sorumlu tutulup tutulamayacağı yasal olarak belirsizdir.

Bu konuda Tor operatörlerinin yargılanması, İpek Yolu tüccarının acımasızca muamelesi ve protokol katılımcılarının yasal korumalarındaki belirsizlik, bu konuda netlik sağlamıyor. Gelişmiş bir kripto para biriminin başka neleri mümkün kılınacağı bilinemez (bkz. Ring of Gyges). Bir kripto para biriminin tüm kullanıcılarından İnternetin en kötü eylemlerini ve davranışlarını onay vermeye zorlanması mantıklı mıdır?

[1] Loi Luu et al. Akıllı Sözleşmeleri Daha Akıllı Yapmak makalesinde bu boşluğu araştırıyor.

Ne yazık ki bu konuda bir kripto para tasarımcısına öngörü sağlayan net örnekler de yoktur. Bu konu daha çok bir pozisyon almak ve onu savunmakla ilgilidir. Bu konuda hem Cardano hem de Bitcoin'in avantajı, endişeleri katmanlara ayırmasıdır. Bitcoin'de Rootstock; Cardano da ise Cardano Hesaplama Katmanı (CCL) vardır.

Değinilen eylemleri mümkün kılacak karmaşık davranış türleri, CSL üzerinde çalıştırılamaz. CSL, Turing dilinde yazılmış programları çalıştırma becerisine, hesaplamayı ölçmek için ise bir tür gaz ekonomisine ve işlemleri bloklarına dahil etmeye istekli konsensus nodelarına ihtiyaç duyar.

CSL'de bazı özelliklerin kısıtlaması kullanıcıları makul ölçüde koruyabilir. Şimdiye kadar hükümetlerin birçoğu kripto para birimlerinin kullanımının veya sahip olmanın yasadışı bir eylem olduğuna karar vermedi. Bu nedenle kullanıcılar bir dijital ödeme sistemi kabiliyetinde bir dijital defteri tutma konusunda rahat olabilirler.

Zincirin yetenekleri genişletilmek istediğinde ise iki olasılık vardır: ya bir poker oyunu gibi fikir birliğine sahip bireylerden oluşan, ve doğası gereği geçici olan bir grup tarafından; ya da Ethereum'a benzer yeteneklere sahip bir defter tarafından etkinleştirilir. Her iki durumda da, bunları başka bir protokole taşımayı seçtik.

Özel ve geçici bir olay söz konusu olduğunda blok zincirlerinden kaçınmak mantıklıdır. Bunun yerine aynı fikirdeki bir grup katılımcıdan, istendiğinde çalıştırılabilen özel amaçlı MPC (güvenli çok partili hesaplama) protokolleri kitaplığına yönelik çabaları kısıtlamak mantıklıdır. Hesaplamalar ve faaliyetler özel bir ağda koordine edilir. CSL bu durumda yalnızca güvenilir bir bülten tahtası ve gerektiğinde bir mesaj iletme kanalı olarak kullanılır.

Buradaki ana fikir izin ve sorumluluğun ve mahremiyetin korunmasıdır. Bir parkın bir etkinliğe ev sahipliği yapması gibi, CSL de burada kullanıcıların buluşması ve iletişim kurması için dijital bir ortak alan olarak kullanılmaktadır. Ancak CSL ancak bir konaklama sağlamaz veya etkinliğin icrasını kolaylaştırmaz. Ayrıca özel amaçlı MPC'lerin kullanılması blok zinciri şişirmeden düşük gecikmeli etkileşimi sağlayacak ve sistemin ölçeğini geliştirecektir.

Cardano'nun bu kütüphaneye yönelik araştırmaları yurt dışındaki bilim adamlarının da yardımlarıyla Tokyo Tech laboratuvarımızda yürütülmektedir. Kütüphaneye hem çağdaş hem de dost sayılabilecek bir matematikçiye ithafen kütüphaneye "Tartaglia" adlandırıyoruz. Tartaglia'nın ilk versiyonlarının 2018'in ilk çeyreğinde sunulmasını bekliyoruz.

İkinci durumda ise sanal bir makineye, bir grup konsensüs noduna ve iki zincir arasında iletişimi sağlamak için bir mekanizmaya sahip bir blok zincirine ihtiyaç vardır. Illinois Üniversitesi'nden bir ekiple ortaklaşa K-framework[1] kullanarak Ethereum Sanal Makinesinin üzerinde titizlikle çalışmaya başladık.

Analizin sonucu, işlevsel semantiklere ve tanımlamalara uygun bir cihazın üretimi hatta dağıtımı konusunda en uygun bilgileri sağlayacaktır. Başka bir deyişle VM (sanal makine) kodun söylediklerini güvenlik risklerini[2] minimuma indirgeyerek uygulanacaktır.

Ethereum tarafından önerilen gaz ekonomisi ile Jan Hoffmann et. al.'in kaynak bilinçli ML'si için kaynak tahmininin hesaplanması gibi çalışmalarla nasıl ilişkili olduğuyla ilgili hala cevaplanmamış sorular bulunmaktadır.

Sanal makinenin dil bağımsızlığı düzeyini de merak ediyoruz. Örneğin, Ethereum projesi mevcut VM'lerinden Web Assembly'ye geçme arzusunu dile getirdi.

[1] Profesör Grigore Rosu et. al.
K, dilden bağımsız makine çalıştırılabilir anlambilimi için evrensel bir çerçevedir. Bizim çalışmamızdan önce C, Java ve JavaScript'i modellemek için kullanılıyordu.
[2] Farklı konsensüs düğümlerinin farklı akıllı sözleşmeler çalıştırdığı anlamına gelir. State sharding olarak da bilinir.

Bir sonraki amacımız merkezi olmayan uygulamalar tarafından hizmet olarak adlandırılacak durum bildiren sözleşmeleri yazmaya uygun bir programlama dili geliştirmektir. Bunun için hem düşük güvenceli uygulamalarda eski bir akıllı sözleşme dili Solidity'yi desteklemeyi, hem de resmi doğrulama gerektiren daha yüksek güvence uygulamaları için Plutus adlı yeni bir dil geliştirmeyi seçtik.

Solidity tabanlı Zeppelin projesi gibi, IOHK da uygulama geliştiricilerin projelerinde kullanmaları için bir Plutus kodu referans kitaplığı geliştirecek. Ayrıca UCSD'nin Liquid Haskell projesindeki çalışmalardan esinlenerek resmi doğrulama için özel bir araç seti geliştireceğiz.

Konsensüs açısından Ouroboros, akıllı sözleşmelerin gelecekteki hallerini de destekler şekilde yeterince modüler bir yapıda tasarlandı. Bu nedenle, hem CSL hem de CCL aynı konsensus algoritmasını paylaşacaktır. Ouroboros'un farkı, token dağıtımıyla hem halka açık hem de halka kapalı defterlere izin verebilmesidir.

ADA bir token oluşturma etkinliğinde CSL üzerinden Asya'daki alıcılarına dağıtıldı. Bu, CSL'nin konsensüs algoritmasının çeşitli ve giderek daha merkeziyetsiz bir grup kullanıcı veya onların atadıkları taraflarca kontrol edildiği anlamına da gelir. CCL ile yasalara tabi varlıklar ve temsilcilerince tutulmak üzere bu defterde özel amaçlı tokenler oluşturarak halka kapalı defterler oluşturmak mümkündür.

CCL örneklerinin bu yaklaşımda esnekliği, işlemin değerlendirilmesine ilişkin farklı kurallarla gerçekleşmesine izin vermesidir. Örneğin, KYC/AML verileri ile ilişkilendirilmemiş işlemlerin kara listeye alınmadığı sürece kumar faaliyetleri kısıtlanabilir.

Tasarımımızda son odak noktamız protokol yığınımıza güvenilir donanımsal güvenlik modülleri (HSM) eklemektir. Bu modüller iki büyük avantaj sağlar. İlki HSM'ler, satıcıya güvenmenin ötesinde, endişelere yer vermeden performansta büyük artışlar[1] sağlar. İkincisi, Mühürlü Cam Kanıtların (SGP) kullanımıyla HSM'ler verilerin kopyalanmadan ve kötü niyetli kişilere sızdırılmadan doğrulanmasını, ve ardından imha edilmesini garanti edebilir.

[1] Bkz: Cornell Üniversitesi'nden Scaling Bitcoin with Secure Hardware.

İkinci noktada SGP'lerin kanuna uyum konusunda devrim niteliğinde bir etkisi olabilir. Normalde bir tüketici kimliğini doğrulamak veya katılma hakkını kanıtlamak için kişisel olarak tanımlanabilir bilgilerini (Personally Identifiable Information) (PII) sağladığında, bu bilgilerin kötü niyetli kullanılamayacağı umuduyla sunar. Bu faaliyet özünde merkezileştirilmiştir, sunulduktan sonra veri sağlayıcı kendi bilgileri üzerindeki kontrolünü kaybeder, ve bölgelerin çeşitli düzenlemelerine tabidir.

Bir grup güvenilir doğrulayıcı seçme ve bir donanımda PII'ları depolama yeteneği, yeterince gelişmiş bir HSM'ye sahip herhangi bir kullanıcının, doğrulayıcının kimliğini bilmeksizin başka bir kullanıcı hakkındaki gerçekleri taklit edilemez bir şekilde doğrulayabileceği anlamına gelir. Örneğin, Ali ABD vatandaşı değil. Ayşe, onaylanmış bir yatırımcıdır. Veli bir ABD vergi mükellefidir ve vergiye tabi kârlarını X hesabına göndermesi gerekmektedir.

Cardano'nun HSM'deki stratejisi önümüzdeki iki yıl boyunca Intel SGX ve ARM Trustzone kullanarak özel protokoller geliştirmeye çalışmak olacak. Her iki modül de dizüstü bilgisayarlardan cep telefonlarına kadar milyarlarca tüketici cihazında zaten yerleşiktir. Tüketici tarafında kullanımı ek bir çaba gerektirmez. Her ikisi de büyük ve iyi finanse edilmiş donanım güvenlik ekiplerince yoğun bir şekilde incelenmiş ve iyi tasarlanmıştır.

1.12. Yasal Düzenlemeler

Büyük ölçeklerde tüm modern finansal sistemlerin acı gerçeği, düzenlemelere bir ihtiyaç veya arzu duymasıdır. Bunun altında ise genellikle piyasalarda bazı aktörlerin veya grubun ihmali nedeniyle tekrarlayan çöküşler yatar.

Örneğin Federal Rezerv Sisteminin oluşturulması 1907'deki Knickerbocker Krizinin sonucudur. Bir başka örnek ise 1920'lerde ABD'de korkunç bir mali çöküş ve mali çöküşle Büyük Buhran ile sonuçlanan aşırılıklardır. Bu çöküş, benzer bir olayı önlemesi ya da en azından kötü aktörlerin yargılanması için 1934'te Menkul Kıymetler Borsası Komisyonunun (S.E.C.) kurulmasına neden oldu.

Düzenlemelerin gerekliliği, kapsamı ve etkinliği tartışılabilir, ancak bu konuda varlıkları ve hükümetlerin gayretleri inkar edilemez. Ancak bu noktada düzenleyicilerin küreselleşen dünyada ve dijitalleşen nakitte karşılaştığı iki zorluk vardır.

İlk zorluk yargı yetkileri ile ilgilenirken, hangi düzenlemelerin daha üstün olacağıdır. Tek bir işlemin etkisi bir dakikadan kısa sürede üç düzine ülkeye dokunabildiğinde, her ülkenin kendi sınırları içinde kendi hukukunu uygulayabilme ilkesi yok olur. Bu konuda yetki, en fazla jeopolitik etkiye sahip olan ülkede mi olmalıdır?

İkincisi, gizlilik teknolojisindeki gelişmeler değere kimin sahip olduğu bir yana, bir işleme kimin katıldığını bilmenin bile giderek zorlaşacağı bir dijital silahlanma yarışı başlattı. Milyonlarca dolarlık varlığın 12 gizli kelimeyle[1] kontrol edilebildiği bir dünyada hukuksal bir düzenlemeyi nasıl uygularsınız?

Cardano da tüm finansal sistemler gibi tasarımında neyin adil ve makul olduğuna dair bir görüşe sahip olmalıdır. Bunun için bireysel haklar ile piyasa hakları arasında ayrım yapmayı seçtik.

Bireyler, zorlama veya varlıklarına el konulma korkusu olmaksızın sermayelerine her zaman erişme hakkına sahip olmalıdır. Bu hak mutlaka uygulanmalıdır. Örneğin Venezuela ve Zimbabve ülkelerinde de görüldüğü gibi, yozlaşmış politikacılarca hükümet güçlerinin şahşi çıkarları için kötüye kullanmamaları konusunda güvenilemez. Kripto para birimleri en düşük ortak paydaya göre tasarlanmalıdır.

İkincisi, tarih değiştirilememelidir. Blok zincirleri bu konuda değişmezliği garantiler. Tarihi geri alma veya resmi kayıtları değiştirme yetkisi birçok aktör ve gruba çok çekici gelir.

Üçüncüsü, değer akışının kısıtlanmaması gerekir. Sermaye kontrolleri ve diğer yapay engeller insan haklarını arka plana atar. Sermaye kontrollerinin nafileliği[2] bir yana; az gelişmiş ülkelerdeki birçok insanın geçimini sağlamak için yurt dışına çıktığı küresel bir ekonomide sermaye kontrolleri, genellikle dünyanın en yoksul insanlarına zarar verir.

Piyasalar için ise bu prensipler bireylerden belirgin bir şekilde farklıdır. Cardano tasarımcıları olarak bireysel haklara inanırken aynı zamanda piyasaların şartlarını ve koşullarını açıkça belirtme hakkına da sahip olduğuna inanıyoruz. Bir kişi bu pazarda iş yapmayı kabul ederse tüm sistemin bütünlüğü için bu standartlara uyulması gerektiğine inanıyoruz.

[1] Bkz: BIP39
[2] Sermaye akışına karşı bir önlem örneği olarak, bkz. Hawala Bankacılık Sistemi.

Bu konuda asıl zorluk ise yaptırımın maliyeti ve uygulanabilirliği olmuştur. Küçük uluslararası işlemler eski sistemlerde dolandırıcılık veya ticari bir anlaşmazlık bakımından güvence sağlamak için çok pahalıdır. Örneğin biri Nijeryalı bir prense parasını gönderdiğinde[1] (ön ödeme dolandırıcılığına uğradığında) parasını geri almaya çalışması genellikle çok pahalıdır.

Cardano için bu konuyla ilgili üç düzeyde yenilik yapabileceğimizi düşünüyoruz. İlk olarak, akıllı sözleşmelerin kullanılmasıyla ticari ilişkilerin hüküm ve koşulları daha iyi kontrol edilebilir. Tüm varlıklar dijital ise ve CSL'de ifade edilebiliyorsa, dolandırıcılık içermeyen ticaret için güçlü garantiler elde edilebilir.

İkincisi HSM'ler, kişisel verileri sızdırılmadan, sadece kimlik doğrulamak için kullanılabilen küresel bir itibar sistemi sağlar. Bu sistemler düzenlemelere tabi merkeziyetsiz borsa ve otomatik vergi uyumluluklu çevrimiçi oyunlar gibi faaliyetlerin çok daha düşük maliyetle yürütülmesine izin verirler.

Son olarak Cardano'nun yol haritasında değişkenlik, tüketici koruması ve tahkim imkanı için kullanıcı tarafından yazılan akıllı sözleşmelerle etkileşime girecek şekilde özelleştirilebilen, modüler bir sistem olan DAO'ların oluşturulması yer alıyor. Bu projenin kapsamı daha sonraki bir makalede özetlenecektir.

1.13. Bütün Bunların Asıl Amacı Nedir?

Cardano projesi kripto para birimi endüstrisinin içindeki ve dışındaki yüzlerce parlak insanlanın geri bildirimlerini içeren bir maraton oldu. Yorulmadan yinelemeyi, hakemli araştırmaların aktif kullanımını ve ortaya çıkan büyük fikirlerin umarsızca araklanmasını kapsar.

Kalan bölümlerin her biri, projemizin temel bir bileşeni olduğuna karar verdiğimiz belirli yönlerini kapsamaktadır. Bu yönlerden bazıları alanın genel olarak en iyi uygulamalarını iyileştirme amacında iken, diğerleri Cardano'nun evrimine özgüdür.

Hiçbir proje her hedefi kapsayamaz veya her kullanıcıyı tatmin edemez. Fakat, kendi kendine gelişen bir finansal yığının, bunlardan yoksun bölgeler için nasıl sağlanabileceğine dair bir vizyon sağlamayı umut ediyoruz. Kripto para birimlerinin asıl amacı mevcut finansal sistemleri bozmak değildir. Eski finansal sistemler, her zaman değişimi özümseyerek biçimlerini ve işlevlerini sürdürme yetisine sahiptir.

[1]Bkz: Ön ödeme dolandırıcılığı

Bunun yerine klasik bankacılık sistemi kurmanın çok pahalı olduğu, bir çok insanın günde birkaç dolardan az bir gelir elde ettiği, stabil bir kimliğe sahip olmanın ve kredi bulmanın imkansız olduğu yerlere odaklanılmalıdır.

Bu yerlerde bir ödeme sistemini, mülkiyet haklarını, kimliği, krediyi ve risk korumasını cep telefonunda çalışan tek bir uygulamada birleştirilmesi sadece faydalı olmakla kalmaz, insanların yaşamlarını da kökten değiştirir.

Cardano'yu inşa etmemizin nedeni gelişmekte olan dünya ülkeleri için bu vizyonu gerçekleştirme veya en azından ilerletme konusunda bir şansımız olduğunu hissetmemizdir.

Kripto para birimlerinin tasarlanma, geliştirilme ve finanse edilme şeklini değiştirebilirsek, o zaman büyük bir başarı elde etmiş oluruz.

2. BİLİM VE MÜHENDİSLİK

2.1. Yineleme Sanatı

Kripto para birimleri yazılım olarak uygulanan protokollerdir. Protokoller ise katılımcılar arasındaki akıllı konuşmalardır. Yazılım ise belirli bir amaç taşıyan verilerin manipülasyonudur. Dolayısıyla sağlam ve güvenilir yazılım ile kullanışlı ve güvenli protokoller arasındaki karşılıklı etkileşim tamamen beşeridir.

İyi yazılım; hesap verebilirlik, net iş gereksinimleri, tekrarlanabilir süreçler, kapsamlı testler ve yorulmadan yineleme gerektirir. İyi yazılım aynı zamanda çözmeye çalıştığı sorunu tam olarak çözebilecek şekilde tasarlanması için alanında yeterli bilgiye sahip yetenekli geliştiricilere de ihtiyaç duyar.

Özellikle kriptografi ve dağıtılmış sistemler içeren yararlı ve güvenli protokollerin geliştirilmesi, daha akademik ve standart odaklı bir süreçte ilerler. Bir protokolün yararlı olduğundan emin olmak için bilimsel hakemli araştırmalar, konu hakkında yapılacak görüşmeler ve kar/zarar hesabının yapılması gerekir; fakat bunlar tek başına yeterli değildir. Protokollerin gerçek yaşamda uygulanması ve test edilmesi de gerekir.

Kripto para endüstrisine özgün zorluk ise tamamen farklı iki felsefenin sentezi olmadan bir araya getirilmesidir. Tez; gençlik, açgözlülük ve tutku tarafından yönlendirilen "hızlı hareket et ve bir şeyleri kır" zihniyetidir. Antitez ise, alanımızın yeniliklerini bol miktarda sermaye ve prestije sahip güzel bir niş içinde sağlamlaştırma arzusuyla motive edilen yavaş, metodik ve akademik odaklı bir yaklaşımdır.

Birçok kripto para birimi ya tamamen bir CV'lik bir beyaz kağıt ya da aceleyle yazılmış bir koddur. Piyasa değerine göre mevcut ilk on[1] kripto para biriminin hiçbiri hakemli bilimsel araştırmalar içeren bir protokole sahip değildir. Mevcut en iyi on kripto paranın hiçbiri resmi bir spesifikasyona[2] sahip değildir.

Bütün bunlara rağmen kripto para piyasasında milyarlarca dolar söz konusu. Bir kez uygulanmaya konulduktan sonra bir kripto para biriminde değişiklik yapmak ise son derece zordur. Peki kullanıcı sistemin güvenli olduğunu nasıl anlar? Kullanıcı pazarlanan özelliklerin meşruluğunu nasıl teyit eder? Peki ya protokol söz verdiği yenilikleri getiremez ise?

Bu sentez eksikliği ve sürece saygı, IOHK'un Cardano'yu inşa etmek istemesinin başlıca nedenlerindendir. Umudumuz, işlerin daha etkin, aklı başında ve dürüst bir şekilde nasıl yapılacağına örnek teşkil edecek bir referans proje geliştirmektir.

2.2. Gerçekler ve Görüşler

Başka bir endişe kaynağı ise gerçeklerin nerede bittiği ve fikirlerin nerede başladığıdır. Yüzlerce programlama dili, onlarca geliştirme anlayışı ve proje yönetimi konusunda birden fazla felsefe vardır. Akademik dünya ise ticari kaygılardan ve pratiklikten uzak olmanın getirdiği zorluklardan muzdariptir.

Cardano için ilk önce mühendislik açısından yararlı olduğu genel olarak kabul edilebilecek eksiklikleri gidermeye çalıştık. Örneğin kriptografi ve dağıtılmış sistemler naif ellerin nasıl korkunç hatalar yapabileceğine dair çok fazla olağanüstü örnek taşıyan konulardır. Bu alanlarda içgörü çıkarmak isteyen bir protokolün, tanınmış bir uzmanca tasarlanması ve diğer uzmanlarca incelenmek üzere sunulması gerekir.

[1] Piyasa değerine göre kapsamlı bir liste için coinmarketcap.com'a bakın.
[2] Ethereum, Sarı Kağıt olarak bilinen yarı resmi bir özelliğe sahip olmakla birlikte EVM semantiği tam olarak belirtilmemiştir ve protokolün tam olarak uygulanması için yeterli değildir.

Ouroboros bu alandaki ilk vaka çalışmamızdır. Geniş, çeşitli ve doğrulanabilir bir yayın geçmişine sahip bir kriptografi ekibi tarafından tasarlanmıştır. Rakip modeller göz önünde bulundurularak, güvenlik varsayımları ve kanıtlarıyla bilimsel bir kriptografi geliştirme sürecine göre inşa edilmiştir. Bu kanıtlar bağımsız olarak Cambridge Üniversitesi'ndeki bir ekip tarafından Isabelle'de yazılan bilgisayarda kontrol edilmiş[1] ve konferanslara sunulmuştur.[2]

Yine de tek başına bu çalışma yararlı olduğuna dair garanti vermez. Yalnızca bazı varsayımlar için güvenlik modelini titiz bir şekilde kontrol eder. Yararlılığın asıl testi için protokolün uygulanması ve test edilmesi gerekir. Geliştiricilerimiz bunu hem Haskell'de hem de Rust'ta yaptı. Bu çalışma, Ouroboros Praos'un yaratılmasına yol açan senkronizasyon modeline odaklanmak için daha fazla çaba gösterilmesi gerektiğini ortaya koydu.

Yeni derslerin alınmasına ve atılmış önceki adımların[3] doğruluğunun teyit edilmesine yol açan, ve büyük protokoller üreten asıl şey, işte bu yineleme sanatıdır. Maliyetli, zaman alıcı ve bazen gerçekten sıkıcı olsa da, bir protokolün doğru şekilde tasarlanmış olmasından ancak bu şekilde emin olunabilir.

Özellikle ilerde milyarlarca insan tarafından kullanılmayı hedefleyen protokoller kısa ömürlü değildir ve hızla gelişmektedirler. Varlıklarını yıllarca, on yıllarca korumayı devam etmeleri amaçlanmıştır. Önümüzdeki 100 yıl boyunca birlikte kullanacağımız yeni bir finansal sistem dünyaya yüklenmeden önce, bu protokollerin tasarımcılarından biraz can sıkıntısı ve titizlik talep etmek bu durumda tamamen mantıklı görünüyor.

2.3. Fonksiyonel Günahlar

Daha tartışmalı bir konu ise yazılım geliştirmede kullanılan araçların, dillerin ve metodolojilerin nesnel gerçekliklerden ziyade dini bir takdirmiş gibi kabul edilmesidir. Kaynak kodu yazılı nesir gibidir. Herkesin neyin iyi olduğuna dair bir fikri vardır, ve bazen neyin iletildiği nasıl iletildiğinden daha az önemlidir.

En az bir kişinin gözünde yanlış olacağını kabul ederek taraf seçme günahını işlemek zorundayız. Ancak, en azından seçimimizin arkasında geniş bir gerekçelendirme var.

[1] Profesör Lawrence Paulson gözetiminde Kawin Worrasangasilpa tarafından.
[2] IACR'nın California'daki Yıllık Kripto Konferansında kabul edilen 71 Numaralı Makalesi.
[3] Konudan sapıyoruz ama Profesör Halmo'nun matematik ders kitabının nasıl yazılacağı konusundaki tartışmasını izlemeniz lazım.

Cardano'yu mümkün kılan protokoller Haskell'de yazılıyor. Kullanıcı arayüzü, Daedalus olarak adlandırdığımız bir Elektron forkuyla yapılmıştır. Mümkün olduğunda web mimari modelini kullanmayı ve veritabanımız için RocksDB kullanan bir anahtar-değer anlayışını seçtik.

Bileşen düzeyinde bu soyutlama, bakımının çok daha basit olduğun, ileride daha az çabayla teknolojisinin değiştirilebileceğini ve temelimizin kısmen de olsa Github ve Facebook'un geliştirme çabalarına bağlı olduğu anlamlarına da gelir.

WebGul kullanmak, React'ten yararlanmamıza ve yüz binlerce JavaScript geliştiricisi tarafından anlaşılan araçları kullanarak ön yüz özellikleri geliştirmemize olanak tanır. Web mimarisi kullanmak, bileşenlerin hizmetler olarak ele alınabildiği ve güvenlik modelinin mantıklı olduğu anlamına da gelir.

Protokol geliştirme için Haskell'i kullanmak ise en zor seçimdi. İşlevsel diller dünyasında bol bol seçenek var. Esnek fakat saf olmayan diller tarafında Clojure, Scala ve F# gibi işlevsel programlamanın en iyi yönlerinden bazılarını koruyan, muazzam Java kitaplıklarından ve .Net ekosistemlerinden yararlanan diller vardır.

Agda ve İdris gibi kod doğruluğunun güçlü bir şekilde doğrulanmasına izin verecek tekniklere sahip, daha akademik yönelimli diller de vardır; ancak bu diller makul kütüphanelerin yoksunluğundan ve ortalamanın altında bir geliştirme deneyiminden muzdariptir.

Cardano için seçim Ocaml ve Haskell'e düştü. Ocaml, harika bir topluluğa, iyi araçlara, makul geliştirme deneyimine ve Coq[1] aracılığıyla resmi doğrulamalar için büyük bir mirasa sahip harika bir dildir. Peki biz neden Haskell'i seçtik?

[1] Bu noktaya ek olarak, IOHK'nın aslında Ocami'de uygulanan ve takma adlı Bill White'dan miras aldığımız Qeditas adlı bir projesi var.

2.4. Neden Haskell?

Cardano'yu oluşturan protokoller merkeziyetsizlik, kriptografi ile paketlenme ve yüksek derecede hata toleransı gerektirir. En iyi durumlarda bile Bizans aktörleri (iletişim problemleri), hatalı biçimlendirilmiş mesajlar ve istemeden ağda hasar verebilecek hatalı istemciler olacaktır.

Haskell'in seçiminde ilk olarak Quickcheck gibi araçları ve Arıtma Türleri (Refinement Types) gibi, daha ayrıntılı teknikleri kolayca kullanabileceğimiz ve makul bir hata toleransına sahip olduğuna inandığımız güçlü bir tür sistemine sahip dil istedik. Erlang stili bir OTP modeli ikinci kriteri tatmin ederken, Haskell ve Ocaml gibi diller ise birinci kriteri tatmin eder.

Cloud Haskell'in piyasaya sürülmesiyle Haskell, Erlang'ın birçok avantajını kendi avantajlarından taviz vermeden elde etti. Ayrıca Haskell'in kompozisyonu ve modüler yapısı Cardano için Time Warp adlı daha hafif, Cardanoya has bir kitaplık kullanmamıza izin verdi.

İkincisi Galois, FP Complete ve Well-Typed gibi ticari kuruluşların kapsamlı çalışmaları sayesinde Haskell'in kütüphaneleri son birkaç yılda büyük ölçüde gelişti. Böylelikle Haskell üretim odaklı uygulamalarının yazımı için kullanılabilir[1].

Üçüncü olarak PureScript'in hızlı gelişimi Clojurescript'in Clojure'a sağladığına benzer şekilde JavaScript dünyasına çok ihtiyaç duyulan bir köprü sağlamıştır. Cardano'nun bir tarayıcıda çalışmasını sağlamak ve mobil cüzdanlar geliştirmek söz konusu olduğunda PureScript'in özellikle önemli olacağını umuyoruz.

Dördüncü olarak bağımlılık çözümü ile ilgili olarak Haskell son birkaç yılda Michael Snoyman gibi teknoloji uzmanları tarafından, hem kullanımı kolay hem de FP Complete tarafından desteklenen stackage adlı bir platform aracılığıyla önemli bir sosyal ve teknolojik çabanın da keyfini çıkardı.

Beşinci olarak bağımsızlığın ötesinde, yazılım yapılarımızın tekrarlanabilir olmasını hedefliyoruz. Başka bir deyişle, aynı yapılandırma değerleri ve bağımlılık sürümleriyle, tam olarak aynı sonuçları üretmelidir. Stackage yoluyla büyük oranda tekrarlanabilir sonuçlar elde etmek için NixOps kullanıyoruz.

[1] Bryan O'Sullivan burada Haskell'in endüstriyel kullanımı hakkında güzel bir konuşma yapıyor.

Son olarak, emsallerine kıyasla Haskell'de uzmanlaşmış geliştiricilerin yetenek havuzu oldukça geniştir. Geliştiriciler akademik ve endüstri referansları ile oldukça iyi eğitilmişlerdir. Ayrıca, bilgisayar bilimi hakkında ayrıntılı bilgiye sahip olmayan Haskell geliştiricileri nadir olduğu için dil, yeterlilik filtresi görevi de görür.

2.5. Resmi Spesifikasyon ve Doğrulama

Kanıtlanabilir olarak doğru bir güvenlik modeli kullanarak bir protokol geliştirmenin önemli bir avantajı, saldırgan kişilerin gücüne sınır olmasıdır. Protokole uyulduğu ve deliller doğru olduğu sürece, saldırganın iddia edilen güvenlik özelliklerini ihlal edemeyeceği bir sözleşme elde edilir.

Konuyu daha derin düşünmek önceki iddiayı daha da önemli hale getirir. Saldırgan kişiler nispeten zeki ve yetenekli olabilir. Sadece matematiksel bir modelle mağlup olduklarını iddia etmek olağanüstü olurdu; fakat bu görüş tamamen doğru değildir.

Gerçek hayat, mükemmel güvenlik ve doğru davranışlar ütopyasının var olmasını engelleyen faktörleri ve koşulları ortaya çıkarır. Uygulamalar yanlış olabilir, donanım daha önce dikkate alınmamış saldırı vektörlerini sunabilir, güvenlik modelleri yetersiz ve/veya gerçek hayattaki kullanıma uygun olmayabilir.

Bir protokol için ne kadar spesifikasyon, titizlik ve kontrolün istendiği konusunda bir görüş birliğine ihtiyaç vardır. Örneğin, SeL4 Microkernel projesi, 10.000 satırdan daha az C kodunu doğrulamak için yaklaşık 200.000 satır Isabelle kodu gerektiren, belirsizliğe yönelik topyekün bir saldırının başlıca örneğidir. Yine de bir kernel (işletim sistemi çekirdeği), düzgün uygulanmadığı takdirde ciddi bir güvenlik açığı olabilecek kritik bir altyapıdır.

Tüm kriptografik yazılımlar aynı çabayı mı gerektirmeli? Ya da eşdeğer sonuçlar üreten fakat daha az efor isteyen bir yol seçebilir mi? Ayrıca, çalıştığı ortam Windows XP'de olduğu gibi herkesin farkında olduğu savunmasızsa, protokolün mükemmel bir şekilde uygulanıp uygulanmadığının bir önemi var mıdır?

Cardano için aşağıdaki orta yolu seçtik. Birincisi, kriptografi ve dağıtılmış hesaplama alanlarının karmaşık doğası gereği ispatlar çok ince, uzun, karmaşık ve bazen oldukça teknik olma eğilimindedir. Bu durum insan güdümünde yürütülen kontrolün sıkıcı ve hataya açık olabileceği anlamına gelir. Bu nedenle, temel altyapıyı kapsayacak şekilde yazılmış bir teknik incelemede sunulan her önemli kanıtın makine tarafından kontrol edilmesi gerektiğine inanıyoruz.

İkinci olarak, Haskell kodunun teknik incelemelerimizde doğrulamak için, iki popüler seçenek arasından seçim yapabiliriz: LiquidHaskell aracılığıyla SMT kanıtlayıcılarla arayüz oluşturmak ya da Isabelle/HOL kullanmak.

SMT (memnuniyet modülü teorileri) çözücüleri, bir denklemi veya eşitsizliği sağlayan fonksiyonel parametrelerini bulma veya bu tür parametrelerin mevcut olmadığını gösterme problemiyle ilgilenir. De Moura ve Bjørner tarafından da gösterildiği gibi, SMT'nin kullanım durumları çeşitlidir ancak kilit noktası bu tekniklerin hem güçlü olması hem de bugları ve anlamsal hataları önemli ölçüde azaltabilmesidir.

Öte yandan Isabelle/HOL, uygulamayı hem belirtmek hem de doğrulamak için kullanılabilecek daha anlamlı ve çeşitlilik içeren bir araçtır. Isabelle, ispatlamada kullanılacak kümeleri ve diğer matematiksel nesneleri temsil edebilen, üst düzey mantık yapıları ile çalışan genel bir teorem çözücüdür. Isabelle, bu tür kısıtlamaları içeren problemlerle çalışmak için Z3 SMT kanıtlayıcı ile çalışır.

Her iki yaklaşım da değerlidir. Bu nedenle her ikisini de aşamalı olarak benimsemeye karar verdik. İnsan kaynaklı kanıtlar doğruluğunu kontrol etmek için Isabelle'de kodlanacak ve böylece makine kontrol gereksinimimizi karşılayacak. 2017 ve 2018 boyunca Cardano'nun uygulamasındaki tüm üretim kodlarına Liquid Haskell'i kademeli olarak eklemeyi planlıyoruz.

Son bir nokta olarak resmi doğrulama, bir insanın doğruladığı spesifikasyon ve mevcut araç setleri kadar iyi çalışır. Haskell'i seçmenin başlıca nedenlerinden biri de pratiklik ve teori arasında doğru dengeyi sağlamasıdır. Teknik incelemelerden çıkan spesifikasyon Haskell koduna çok benziyor. Dolayısıyla bu ikisini birbirine bağlamak Haskell'i zorunlu bir dil tutarak yapınca çok daha kolay.

Uygun spesifikasyonu yakalamak, yükseltmelerin, hata düzeltmelerinin ve diğer endişelerle ilgili değişikliklerin yapılması gerektiğinde spesifikasyonları güncellemek konusunda hala çok büyük zorluklar var; ancak bu gerçek hiçbir şekilde bu konuya verilen değeri azaltmaz. Kanıtlanabilir güvenlik üzerine bir temel oluşturmakta sıkıntı çekilecek ise uygulama aslında kağıt üzerinde önerilen şey olmalıdır.

2.6. Şeffaflık

Bilim ve mühendisliği bir kripto para biriminin gelişimi açısından tartışılacak son konusu şeffaflığın nasıl ele alınacağıdır. Tasarımda verilen kararlar geliştiricilere rüyalarında gelen, sonra aniden resmiyet kazanan siyah/beyaz veya ruhani şeyler değildir. Tasarımda verilen kararlar, önceki başarısızlıklardan öğrenilen deneyimlerden, konu hakkında tartışmalardan ve derslerden türetilir.

Buradaki asıl zorluk tamamen şeffaf bir geliştirme sürecinin, konu hakkındaki tartışmaları kanıta dayalı olmaktan ziyade drama haline çekebilmesidir. Yüksek egolu bireyler, topluluğu kendi tarafına çekme niyeti ve aptal gibi görünme korkusu, konuşmaları kısır ve verimsiz olmaya zorlayabilir.

Ayrıca, yeni gelen katılımcılar kendi özel isteklerini konuşulacak tek konu olmaya zorlamak amacıyla konuşmayı kendi aralarında seçmeye çalışabilirler. Herkesin kendince istediği şeyler olabilir.

Peki bu durumda topluluk tarafından bir grup çekirdek geliştiriciye emanet edilmiş şeffaflık ile korkmadan kendini ifade edebilme özgürlüğü arasında ilerlemeyi sağlamak için nasıl bir denge kurulabilir?

Cardanoda yönlendirmeli gözetimle belirli standartlara uyacak bir süreci benimsemeye karar verdik. Topluluğun, bilimin ve kodun iyi düşünüldüğünü, kontrol edildiğini ve geliştiricilerin çözdüğünü iddia ettiği şeyleri gerçekten çözdüğünü bilmesi gerekir. Konu hakkında yapılan bilimsel hakemli araştırmaların özellikle bu amaçla tasarlanmış olması ve bilimin gerekliliklerini tam olarak karşılaması gerekir.

Kodlama konusu şeffahlık açısından da hararetli bir konudur. Cardano için, Cardano vakfını IOHK'un icraatlarının aşağıda verilen koşulları gözetmek hususunda nihai otorite olarak atadık:

1. Cardano Github kodlarının kalite kontrol, test kapsamlıkları, yorumlamalar ve bütünlük açısından düzenli olarak gözden geçirilmesi,
2. Tüm Cardano belgelerinin doğruluk ve fayda açısından değerlendirilmesi ve
3. Bilim adamları tarafından üretilen protokollerin tam olarak uygulandığının tasdik edilmesidir.

Yukarıda verilen kriterlerin sağlanması için IOHK Cardano Vakfına ve vakıf tarafından atanmış kişilere, gözden geçirilmek üzere güncel ve düzenli olarak rapor sunacaktır. İncelemeler sonucunda Cardano vakfı da en az üç ayda bir olmak üzere Cardano topluluğu için geliştirme gözetim raporu yayınlayacaktır.

Burada asıl amaç ise merkezi olmayan bir projede hesap verebilirliği nasıl sağlanabileceği hakkında daha geniş bir tartışma başlatmaktır. Güvenilir bir üçüncül şahıslar tarafından yapılan geliştirme gözetimi geliştiricilerin doğru yolda olmasını sağlamak için güçlü bir araç olsa da, her zaman projenin başarılı olacağını garantilemez.

Bunun için ise hazine CSL'ye entegre edildikten sonra Vakıf başka geliştirme ekiplerinin, Vakıf ve IOHK'un ortaklaşa geliştirdiği koşullara dayanan alternatif istemcileri oluşturması için teşvik edecektir. Ethereum projesi tarafından kullanılan geliştirmede çeşitlilik, tek bir fikir veya tek bir geliştirici takımı etrafında oluşabilecek monokültürden kaçınmak için harika bir tekniktir.

Spesifikasyonlarla ilgili ise, WC3 ve IETF tarafından uygulanan standartlar süreci ilham almak için zengin bir bilgi kaynağıdır. Aslında Cardano'nun entegre ettiği her protokol akademik çalışmalardan veya kaynak kodundan bağımsız olarak RFC'ye (konu uzmanları tarafından yorumlanma talebine) uygun bir formatta olması gerekir.

Cardano Vakfının temel görevlerinden birisi de özellikle Cardanoda uygulanacak protokollerde standartların uygulanmasını sağlayan organ olarak hareket etmektir. Aynı zamanda ilgili standartları güncellemek, eklemek veya değiştirmek için yapılacak görüşmelere ev sahipliği yapmaktır.

Eğer belirli standartların ürünü olan internet IETF aracılığıyla hangi çekirdek protokollerin kullanılacağı konusunda fikir birliğine varılabiliyor ise, özel bir kuruluşun da protokollerinde fikir birliğine sahip olacağını varsaymak mantıklıdır.

Son olarak bu tartışmaları blok zincirinde barındırılan ve merkezi olmayan bir varlığa taşıma fikri ilginçtir. Buna merkezi olmayan otonom organizasyon (DAO) denir ve bu alanda ön çalışmalar yapılmaktadır. IOHK eğer Cardano ile iş yapan kuruluşlarca talep edilirse Cardano için referans DAO modeli geliştirecek. Bunu, protokolün standartları kapsamında benimseyip benimsememeye karar vermek ise Cardano Vakfı'na kalacaktır.

3. ESKİ SİSTEMLERLE UYUMLULUK (Interoperability)

3.1. Büyük Miyopi

Özünde finans, ve daha geniş kapsamda ticaret fikri, bir insan ürünüdür. Niyeti belirtmek için son derecede hassas diller, istenmedik sonuçlar durumunda başvurulacak sonsuz teknikler, ve ticarette eşitlik sağlamayı amaçlayan binlerce yıllık yasalar vardır. Hatta yazının en eski örneklerinden bazıları ticari sözleşmelerdir.

Ticarette insan unsurundan; mantığa, makinelere ya da büyük güçler emanet edilen hükümet görevlilerinin aracılık edip etmemesi farketmeksizin kaçınılamaz. Bunlar çoğunlukla insan faktörüne etki edemez.

Herkes hata yapabilir. Herkes fikirlerini değiştirebilir. Herkes kabul ettiği iş yükümlülüklerini her zaman tam olarak anlamayabilir. Herkes yanlış yönlendirilebilir veya dolandırılabilir. Bu konuda durumlar bireysel ve devletsel bazda eşi olmayan çözümler gerektirebilir. Bunun için ise çoğu sözleşme mücbir sebep maddeleri içerir.

Kripto para birimleri ise yazılan koda mükemmel bir şekilde bağlı kalarak, adaleti veya sonucu dikkate almadan, umursamaz bir dijital yargıçlıkla insan anlayışını, şefkatini ve yargısını ortadan kaldırmaya çalışır. İnsanların her zaman kuralları kendi bencil amaçlarıyla değiştirmeye çalıştıkları ve denemeye devam edecekleri göz önüne alındığında, aslında bozulmayan bir sisteme sahip olmak caziptir.

Peki kullanıcılar bu yeni sistemleri geleneksel finansal sistemlerle birlikte kullanması gerektiğinde ne olur? Bu sistemler gerçek dünyada yaşamaya ihtiyaç duyulduğunda ne olur?

Mesela tapu kaydı gibi mülkiyet hakları tamamen fiziksel dünyada yer alır. Arazinin token haline getirilmesinde bile gerçek dünyada var olan yargı yetkisinin az da olsa kabul edilmesini gerekir.

Bir başka noktada, bir külçe altın kendi kendine hareket edemez. Dijital yargıç ise emir verebilir ancak emri uygulayacak insanlar olmadan emri zorlayamaz. Bu nedenle de dijital defterler de gerçeklikten sapabilmektedir.

Bu nedenle bir protokol tasarımcısının kripto para biriminde gerçek dünyadaki gerçeklere ne denli izin verileceği ile ilgili kararlar vermesi gerekir. Bu hususta protokoldeki esnekliğin arttıkça netliğin azalacağı beklenmelidir. Sistemde tüketici koruması ne kadar artarsa geri alma, geri ödeme ve geçmişin düzenlenmesini sağlayan mekanizmaların da o kadar var olması gerekir.

Bu ve yönetmelikle ilgili bir sonraki bölüm Cardano'nun konuya pragmatik yaklaşımını kapsar. Uyumluluk açısından ele alınacak iki ana konu sırasıyla: diğer kripto para birimleri ve gerçek dünyadaki klasik finansal sistemlerdir.

3.2. Eski Sistemlerle Uyumluluk

Finansal teknolojiler (Fintech) tek bir dilden, hatta tek bir standarttan bile oluşmuyor. Konuya yaklaşımlarda, uzlaştırmalarda, takastan sorumlu kuruluşlarda, iş süreçlerinde, muhasebelerde, dönüşümlerde ve değerin hareket etmesindeki alanlarda muazzam çeşitlilik mevcuttur.

Sırf bir teknoloji diğerine üstün olduğu için eski sistemlerin artık pes edip yükseltmeyi kabul edeceğini söylemek saçma olur. Mesela birçok kişi üzerinden 16 yıl geçmesine rağmen hala Windows XP kullanıyor. Bu üzücü durum birinin 1984 yılında çıkan bir Macintosh'u 2000 yılında kullanmasına eşdeğerdir.

Tüketicilerden ayrı olarak işletmeler, güncelleme yapma konusunda genellikle daha yavaştır. Birçok banka hala Cobol ile yazılmış arkayüzleri kullanıyor. Altyapının çalıştığı ve iş gereksinimlerini karşıladığı bilindikten sonra, uyumluluk veya güvenlik endişeleri dışında, tüketicinin yararına yazılım ve protokolleri güncellemek veya iyileştirmek için teşvik azdır.

Cardano için öncelikle eski sistemlerle uyum için kurulacak bir köprünün ne anlama geldiğini belirlememiz lazım. Uyumun yeterli olması için hangi sistemleri, standartları, varlıkları ve protokolleri hedeflemeliyiz? Bu köprüler özerk veya merkeziyetsiz bir şekilde kurulabilir mi? Veya borsalarda olduğu gibi bu köprüler, bilgisayar korsanları, kötü niyetli kişiler veya aşırı hevesli piyasa düzenleyicileri için merkezi başarısızlık noktaları haline gelebilir mi?

Bu noktada ele alınması gereken üç konu var. Birinci konu bilginin temsili ve bilginin doğruluğuna olan inanç, İkinci konu değerin temsili ve mülkiyeti, Üçüncü ve son konu ise varlıkların temsili ve bu tür varlıklara olan güvendir.

Bunun işe yarar bir şey olması için, bilgi ve değerin eski finans dünyası ile Cardano arasında özgürce hareket etmesi, daha sonra güveni sağlamak ve rücu hakkına (ödemeyi geri alma hakkı) zemin oluşturmak için sonuçların belirlenmesi ve kaydedilmesi gerekir. Bunları bir blok zincirinde kodlamak ise işlemleri küresel ve kalıcı hale getirecektir.

Fakat gerçek dünyada değer her zaman özgürce hareket edemez. Ambargolar, yaptırımlar, sermaye kontrolleri ve adli işlemler sonucu varlıklar dondurulabilir. Eski sistemlerle uyumlu olması amaçlanarak değerin bu engellerden sızması için bir kaçış vanası oluşturulamaz.

Son olarak işletmelerin markası ve itibarı, ticari ilişkilerin temellerinden biridir. Markaları kurmak, sürdürmek ve onarmak için pazarlama kampanyalarına her yıl milyarlarca dolar harcanmaktadır. Bir kişi veya kuruluşun haklarındaki karalayıcı, yanlış veya yanıltıcı iddialarla ilgili yasal yollara başvurma hakları vardır; fakat blok zincirler tarihi kalıcı olarak korumaya çalışır.

Programlama dili seçimimizde de olduğu gibi, Cardano'nun bu konuları her yerde ve her konuda doğru bir şekilde çözmesi için ideal bir çözümü yoktur. Bu konularda desteklenen görüşlere bağlı olmak durumundayız.

Bilgi akışı ile ilgili olarak, bu akış güvenilir veri beslemesi olarak bilinir. Kaynağı ve içeriği vardır. Kaynaklar, aldatmak veya dürüstlüğü sürdürmek için güvenilirlik ve teşvik kavramına tabidir. İçerik ise keyfi olarak kodlanabilir.

Protokollerimizde güvenilir donanımı desteklemeyi amaçladığımız için Profesör Ari Juel ve arkadaşlarının Town Crier Protokolünü eklemizin yollarını bulmaya karar verdik. Güvenilir bir veri kaynağının olduğunu varsayarsak Town Crier, akıllı sözleşmelerde ve diğer uygulamalarda kullanım için web içeriğinin güvenli bir şekilde kullanılmasını sağlar.

Kaynakların önyükleme listesi Emurgo, IOHK ve Cardano Vakfı tarafından sağlanacaktır. Liste daha sonra Cardano'nun hazine sisteminden türetilen mekanikleri kullanarak topluluk tarafından oluşturulan bir liste ile değiştirilecektir. Umudumuz, itibar sisteminin iyi veriler etrafında gerçekleşebilmesi; böylece güvenilirliği ve uygunluğun kademeli olarak iyileştirilmesi için olumlu bir geri bildirim döngüsü oluşturmasıdır.

Değerin temsili daha karmaşık bir konudur. Protollerce doğruluğun, güncelliğin ve bütünlüğün güvenilir ve belli bir şekilde davranabildiği bilginin aksine değer, daha hassas bir konudur. Değer token haline geldikten sonra özel bir nesne gibi davranmalıdır. Bilgiler kopyalanabilir ve dağıtılabilir, fakat bir şeyin sahipliğini temsil eden bir token (örnek olarak bir araç plakasını alın) klonlanamaz veya iki farklı defterde takas edilemez. Öyle yapılması sistemin bütünlüğünü yok eder.

Tokenize edilmiş değerlerle uğraşırken eski sistemlerle uyumun zorluğu güvenilen varsayımlar; güvenilirlik ve denetlenebilirlik ve defterler arasında jeton akışıdır. Örneğin, Bob Bitcoin'ini bir borsaya yatırmasına karşılık olarak borsanın kendi Bitcoin'inin defterdeki temsilini alır. MtGOX örneğinde, defterleri gerçeğe uymadı ve kullanıcıların her şeyi kaybetmesine neden oldu.

Sorun, eski sistemlerin bir kripto para biriminde yaşayan tokenları tanıması ihtiyacıyla daha da karmaşıklaşıyor. Daha önce de belirtildiği gibi işletmeler yazılımlarını güncellemeye ve yeni protokolleri desteklemeye dirençlidir. Bu durum net bir çözüm bulmayı zorlaştırmaktadır.

Cardano için en iyi umudumuz, kullanıcılara işlemlerine zengin bir meta veri kaynağı ekleme seçeneği sunmak ve ardından endüstri standartlarının ortaya çıkmasını beklemektir. Interledger çalışma grubu ve R3Cev gibi çabalar, eski finansal protokolleri yükseltmeye yönelik uluslararası yetkiler konusunda bazı ilerlemeler kaydetmiştir.

Fakat hala eski bir sistemden, kripto para birimi defterine gönderilen değeri ölçmek ve nitelendirmek hala zordur. Bununla birlikte, eski bir sistemden bir kripto para birimi defterine gönderilen değeri ölçmek ve nitelemek için daha büyük zorluk devam ediyor. Örneğin Bob bir banka sahibi ve bir stabilcoin çıkaracak. Bob tokenlarını kullanıcı tarafından üretilen bir varlık (bkz. UIAs) olarak Cardano gibi bir deftere göndermek için köprü oluşturabilir.

Cardano Bob için sahipliği tam olarak takip etme, zaman damgası ve denetlenebilirlik gibi bir zincirden istediğimiz tüm özellikleri sunsa da, hiçbir kripto para Bob'u dürüst bir bankacı yapamaz. Bob tüm dolar tokenlarını gerçek dolarlarla desteklemeyerek kısmi rezerv bankası olma imkanına sahiptir. Bu dolandırıcılık, doların kendisinin bir defter tarafından hesaplanan bir token olmadığı sürece bir kripto para birimi tarafından tespit edilemez.[1]

Son olarak, varlıkların çevrimiçi temsili, internetin ilk günlerine kadar uzanan klasik bir ağ sorunudur. Üniversitelerin, işletmelerin, devlet dairelerinin ve herhangi bir kullanıcının bir noktada kimliklerini oluşturması gerekir.

Bunun için web'in Açık Anahtar Altyapısı ve ICANN'ın DNS sistemi gibi pragmatik fakat merkezi yapıda olan çözümler mevcuttur. Modern internetin varlığı, bu çözümlerin hem ölçeklenebilir hem de pratik olabileceğine kanıttır. Ancak bu sistemler bir kişinin herhangi bir işletmeyle iş yapıp yapmamasına karar vermesine odaklı olarak; dayanıklılık, güvenilirlik ve diğer özelliklerle ilgili ticari odaklı bilgi sağlamazlar.

eBay gibi çok taraflı pazaryeri sunucuları, bu bilgiyi sağlamak için bir çerçevenin yanı, sıra bu meta verilerin bir kısmını sağlayan bir iş modeli oluşturmuştur. Bu sistemde genel olarak içeriğin, ticari etkinliklerin ve işletmelerin kalitesiyle ilgili yargılar, yalnızca güvenilir kaynaklardan alınan çevrimiçi değerlendirmelerden etkilenir. Bu değerlendirmeler içeriğin yaratılmasını bile etkiler.[2]

Bu noktanın Cardanoyu ilgilendiren kısmı itibarın merkezileştirilmesi meselesidir. Cardano için hedeflerimizden biri gelişmekte olan ülkeler için finansal altyapı sağlamasıdır. Bunun temel yolu ise birbirini tanımayan kişilerin birbirine güvenmesini sağlamaktır. Kimin iyi veya kötü olarak etiketlendiğine tek bir varlık veya grup kontrol eder ise bu kişi ve grup herhangi bir nedenden dolayı kara listeye alınabilir. Bu güç hem değerlerimize aykırıdır hem de bir kripto para birimi kullanmanın ana nedenini ortadan kaldırır.

Bir itibar ağı oluşturmak için neyse ki hazine önerileri için oy verme, güvenilir veri akışları listesine kaynak ekleme ve bir protokolü forklamada kullanılan aynı mekanizmalar kullanılabilir. Bu konu hala aktif bir araştırma alanıdır. Umudumuz, 2018-2019'da daha temel unsurlar belirlendikten sonra merkeziyetsiz bir itibar ağı için bir katman protokolü sağlamaktır.

[1] Dijital defterler için kripto para birimi borsalarını dürüst tutmanın akıllıca bir yolu olarak rezerv kanıtı önerilmiştir.
[2] Rotten Tomatoes'un film endüstrisini nasıl etkilediğiyle ilgili bu ilgi çekici makaleye bakınız.

3.3. Diğer Kripto Para Birimleri ile Uyumluluk

Gerçek dünyadan dağıtılmış defterlere geçildiğinde uyumluluk konusu basitleşir. .Her defterin kolayla ölçülebilen ağ protokolü, iletişim standartları ve ilgili konsensus (fikir birliği) algoritması hakkında güvenlik varsayımları vardır.

Bilginin hareketi, yabancı bir ağa bağlanarak ve mesajlarını çevirerek sağlanır. Değer hareketi ise bir aktarma (relay) sistemi, atomik swap (çapraz zincir ticareti) veya yan zincirlerin zekice kullanımıyla sağlanabilir.Merkezi bir operatör olmadığı için, varlıkların bir temsili daha çok geliştiricilere, madencilere veya başka bir güç sağlayıcısına duyulan güvenin tartışılmasını kısıtlar.

Cardano için Kiayias, Miller ve Zindros (KMZ) tarafından geliştirilen yeni bir yan zincir protokolünü entegre ediyoruz. Bu protokol, protokolü destekleyen iki zincir arasındaki bir değerin güvenli bir şekilde taşınması için etkileşimli olmayan bir yol sağlar. Bu mekanizma değerin, CSL ve bir CCL katmanı arasında akacağı ana yol olacaktır.

Cardano'nun değeri ve kullanıcı tabanı büyüdükçe, diğer kripto para birimleri için özerk köprüler oluşturulmalıdır. Bu büyümeyi hızlandırmak için Cardano SL, uyumluluk scriptleri için sınırlı bir Plutus sürümünü destekler. Shelley'e ve CSL'ın sonraki sürümlerine özellikle bu ihtiyaçları karşılamak için yeni işlemler eklenecektir.

3.4. Daedalus'un Labirenti

Uyumluluk konusunda bahsedilen noktalar genel bir bakış açısından çıkmıştır. Özel protokoller, yeni işlem türleri, güvenilirliği ve bilgi akışını değerlendiren sistemler, yalnızca tek bir ağ geçidi veya kullanıcıya göre belirlenemez. Aksine bunlar sansür veya herhangi bir ücret olmaksızın herkesin kolayca ulaşabileceği şeyler olmalıdır.

Peki Cardano bir kullanıcının olmazsa olmaz bir protokolünü, işlemini veya uygulamasını desteklemediğinde ne olacak? Biz de mi kapsam dışında olmalıyız? İnternet de 1990'larda benzer bir problemle karşı karşıya kalmıştır.

İnternetin bu problemleri ele alışı kripto para birimlerinde de uygulanabilecek iki farklı çözüm yolu sunuyor. JavaScript herhangi bir web sitesine isteğe bağlı özellikler eklemek için programlanabilirlik sağlar. Tarayıcı eklentileri ve uzantılar ise bunları yüklemek isteyen kullanıcılar için özel yetkiler ekler. Her iki yaklaşım da bize, tüm güvenlik problemleriyle birlikte, modern web'i verdi.

Ethereum, kullanıcıların blok zincirine akıllı sözleşmelerle alt protokolleri yerleştirmelerine izin vererek ikinci seçenekteki yaklaşımı benimsedi. Cardano da bu özelliği CCL aracılığıyla destekliyor. Peki ya özel uzantılar?

Buna güzel bir örnek bir kripto alsatçısı olabilir. Farklı kripto para birimlerini sunan DM isimli verilen merkeziyetsiz bir pazaryeri düşünelim. Bir alsatçı bu marketteki stratejilerini otomatikleştirmek istiyor.

Parçalanmış bir ekosistemde alsatçının her kripto para birimi için düzinelerce istemci kurması; ardından otomatik işlemlerini koordine etmek amacıyla her istemci için özel yazılımlar yazması gerekir. Bir istemci güncellenirse bütün yazılım bozulabilir. Ayrıca, peki ya alsatçı yazılımını satmak isterse?

Webdeki uzantılardan örnek alarak, çeşitli kripto para birimlerinin arayüzü bir web yığınına çekilebilir ise tüccarın görevi büyük ölçüde kolaylaşır. Bunun için evrensel bir arayüz geliştirilebilir. Tek tıkta yükleme. Yazılımın dağıtımı Chrome web mağazasına gibi modellenebilir.

Bunun için Cardanoda referans cüzdanımızın önyüzünü Electron'a yerleştirerek bu yöntemi denemeye karar verdik. Electron hem Node hem de Chrome'u bir araya getiren ve Github'da yürütülen açık kaynaklı bir projedir. Cardano'nun Elektron yapısına Daedalus denir.

Daedalus'un[1] ilk versiyonları harcama şifreleri ve BIP39 gibi endüstri standartlarından beklenen muhasebe ve güvenlik özelliklerinin birçoğunu destekleyen bir HD cüzdan görevi görecek. Sonraki versiyonlarda Daedalus, mağaza, evrensel entegrasyon API'leri ve SDK içeren bir uygulama çerçevesine dönüşecek.

Buradaki anahtar yenilikler programlamacıların uygulamalarını oluşturması için JavaScript, HTML5 ve CSS3 kullanmalarına izin vererek, geliştirme süreçlerinde kolaylık ve çapraz uygulama iletişimi için bir köprü sağlamasıdır. Kriptografi, dağıtılmış ağ yönetimi ve veritabanı mekanikleri gibi karmaşık konular süreçten soyutlanarak, geliştiricinin yalnızca kullanıcı deneyimine ve uygulamasının temel mantığına odaklanmasına izin verilebilir.

[1] Ki şu an Daedaluswallet.io'da mevcut

Daedalus'un evrensel bir çerçeve olması amaçlandığından, yol haritası ve evrimi Cardano'nunkinden nispeten bağımsızdır. 2017'lerde gelişimleri birbirlerine bağlı idi; fakat ilerde Daedalus kullanıcıları için Cardano sadece başka bir uygulama olacak. Ayrıca, yalnızca Intel SGX ile çalışan evrensel bir anahtar yönetim hizmeti gibi son derece özgün özellikleri de keşfetmeyi amaçlıyoruz.

Sonuç olarak, protokol tasarımcılarının tüm ihtiyaçları karşılayamayız. Fakat Daedalus'un CCL üzerinde çalışan kapsamlı akıllı sözleşmelerin getirdiği esnekliğin, tasarım kararlarımızın dışında kalanları tatmin etmesini umuyoruz. Bunun yanı sıra, tüm kripto para birimlerini daha gelişmiş uyumluluk ve güvenlikten yararlanmaya teşvik etmek için daha iyi standartların ortaya çıkabileceğini umut ediyoruz.

4. PİYASA DÜZENLEMELERİ

4.1. Yanlış İkilem

Piyasa düzenlemeleri her ne kadar değişken ve gizemli olursa olsun, altında yozlaşmış kişilerle adalet arayan savcılarının hikayesi olduğu az da olsa çıkarılabilir. Yönetmelikler kanun çıkaranların araç gereçleridir Ancak her araç gibi bunlar da kaba, eski veya yanlış kullanılmış olabilir.

Kripto para birimleri de insanlık faktörünü veya hikayesini değiştirmedi. En iyi niyete sahip olunsa bile dolandırıcılık, kötü kişiler ve korkunç sonuçlar her zaman var olacaktır. Kripto para birimleri insan yargısını denklemden kaldırabilse bile, insan davranışlarını kaldıramazlar.

Bir kripto para tasarımcısı istenmeyen olayları düzeltmek için düzenleyiciye hangi araçları sunacağına dair bir pozisyon almalıdır. Kripto para birimlerinin karşılaştığı özgün zorluk ise aslında düzenleyici ve parasal anlamda devletlerin başarısızlığın bir ürünü olmalarıdır[1].

Kültürel açıdan kripto para birimlerini sahiplenen birçok kişi hükümetlerin eylemlerinin yozlaşmış, beceriksiz veya etkisiz olduğunu düşünüyor. Bu nedenle bir düzenleyicinin veya kanun adamının yanlışları düzeltmesi için protokolde bir arka kapı sağlama fikrine karşı saygıları, sabırları veya istekleri yoktur. Hatta böyle birşey kripto para birimlerinin kullanmanın amacına ters olacaktır.

[1] Hatta Satoshi Bitcoin'in Genesis Bloğunda The Times'tan alınan şu manşeti yerleştirmiştir: The Times 3 Ocak 2009: Şansölye, bankalar için ikinci kurtarma paketini sunma eşiğinde.

Öte yandan, borsa başarısızlıklarını ve tarihi olayları da sayarsak, 3 Ocak 2009'da protokolün başlamasından bu yana Bitcoin'in yüzde 10'undan fazlası kayboldu veya çalındı. 30 Haziran 2017 itibariyle, kaybedilen veya çalınan değer 4 milyar doların biraz üzerindedir; ve bu rakam dolandırıcılık ve kötü halka arzlar nedeniyle kaybedilen Bitcoin ve tokenleri hesaba katmaz.

Bunun üstüne mahremiyet meselesi de var. Değer büyük miktarda düzenlenmiş, meta veriler açısından zengin; kanun uygulayıcılar, hükümetler ve uluslararası düzenleyiciler tarafından aktif olarak izlenen özel kanallardan geçer. Bu sızıntıların işlerin sadece nakit tarafında meydana gelen bir olay olduğu iyi anlaşılmış bir olgudur; ki bu sızıntılar dünya dijital paralara geçtikçe azalıyor[1].

Kripto para birimleri olmasaydı, dünya finansal açıdan mahremiyeti sosyal medya içeriği gibi ele alırdı gibi görünüyor; ki mahremiyetten zerre yok ve yine de kullanmaktan kimse vazgeçemez. Dolayısıyla elimizde bariz bir ikilem var.

Bir kripto para tasarımcısı kullanıcılarının gizliliğini ve dürüstlüğünü, ilkelerinden vazgeçerek ve yargının kodlarına koyduğu taleplere boyun eğerek tehlikeye atabilir. Ya da halihazırda kullanılan en iyi uygulamalardan ve yasalardan ayrı olarak ilkeli fakat anarşist bir felsefeyi benimseyebilir.

Cardano için, bu ikilemin yaratıcılık eksikliğinden doğan yanlış bir durum olduğunu düşünüyoruz. Çoğu kullanıcı gerçekte pazarlarla ilgili kurallarla ilgilenmez. Genellikle kurallardaki, bir veya birden fazla aktörün yararına olacak ani değişikliklerden endişe duyarlar. Yani kimin özel ayrıcalıklara sahip olduğu konusunda şeffaflığın eksikliğinden endişe duyuyorlar.

Bu noktada kişinin haklarıyla piyasanın haklarını ayırmamız gerekiyor. Kripto para birimlerinin küresel bir erişime sahip olduğu göz önüne alındığında, hakların mümkün olduğunca kullanıcı odaklı olması gerekir.

Gizlilik makul ve kullanıcının kontrolünde olmalıdır. Değer akışı serbest bırakılmalıdır. Değerin akışı izinsiz olarak engellenememelidir.

[1] Okuyucunun David Wolman'ın The End of Money kitabını okuması önerilir. Konusu paranın kaybolmasına dair uluslararası hareketleri kapsar.

Piyasa açısından bakıldığında ise, piyasanın verilerin kullanımı, sermayenin kendi içinde nasıl ele alınacağı ve herkesin eşit olması konusunda şeffaf olması gerekir. Ayrıca kullanıcı bir kez onay verdiğinde, rahatsızlık hissettiği durumlardan dolayı aniden fikrini değiştiremez; karşı tarafların da kesinliğe ihtiyacı vardır.

Peki gerçek bir sistem tam olarak nasıl uygulanır? Pratikte ve yasal olarak böyle bir şey nasıl gözükür? Çözümümüzü üç kategoriye ayırdık: meta veriler, kimlik doğrulama ve uyumluluk ile, pazar yeri DAO'ları.

4.2. Meta Veriler

Meta veriler, verilerin kendinden önemli olabilmektedir. Mesela İstanbul'dan Ankara'ya araba sürmek bir veridir. İstanbul'dan Ankara'ya bir Ferrari 488 ile ortalama 200 Km/h hızla gitmek ise meta veridir. Bu ise kesinlikle ortalama 60 Km/h'lik bir Toyota Prius'tan farklı bir deneyim anlamına geliyor.

Finansal işlemler de bu açıdan farklı değildir. İşlemlerin bağlamları ekonomistler, vergi makamları, kanun uygulayıcılar, işletmeler ve diğer kuruluşlar için olağanüstü derecede önemlidir. Ne yazık ki mevcut fiat paraya dayalı sistemimizde çoğu tüketici işlemlerinin meta veriler açısından ne kadar zengin olduğunu veya kimlerle paylaşıldığını göremez[1].

Cardano için kullanıcıların işlem meta verilerini vergi makamları gibi belirli aktörlerle paylaşmaya ihtiyaç duyabileceklerini, veya yasal olarak zorunlu tutulabileceklerini kabul ediyor; fakat bu paylaşımın kullanıcının rızasıyla olması gerektiğine inanıyoruz.

Ayrıca blok zinciri sistemlerinin denetlenebilirlik, zaman damgası ve değişmezlik sağlayarak dolandırıcılığı, israfı ve kötüye kullanımı ortadan kaldırmak için muazzam bir güce sahip olduğuna inanıyoruz. Bunun için bazı meta veriler Cardano blok zincirine aktarılmalıdır.

[1] Bu verilerin büyük bir ölçekte kullanımına örnek Juan Zarate'in Hazinenin Savaşı kitabındadır. Bu kitapta meta verilerinin ABD Hazine Bakanlığı tarafından terörizme karşı savaşta nasıl kullanıldığı hakkında yazıyor. Kitap mevcut küresel finans piyasalarının jeopolitik amaçlar için nasıl kullanılabileceğine dair kapsamlı bir görüş sağlar.

Bu konunun zor kısmı blok zincirimizi şişirmeyen bir denge kurmaktır. Bunu başarmak için ise pragmatik bir çözüm bulduk. İlk olarak, Daedalus önümüzdeki 12 ay boyunca işlemleri ve finansal faaliyetleri etiketlemek için çok sayıda yeni özelliği destekleyecek. Bu meta veriler, talep üzerine kullanıcının gerekli gördüğü kişilerce dışa aktarılabilir ve paylaşılabilir olacak. Ayrıca bu veriler, vergi muhasebesi gibi alana özel amaçlar için üçüncül tarafların uygulamaları tarafından çalıştırılabilir durumda olacak.

İkinci olarak, hashler ve şifreli alanlar içerebilen özel adresler için destek eklemeyi araştırıyoruz. Bu yapı, kullanıcının gizli bir şekilde zincirimize meta veri göndermesini izin verir; ancak verileri paylaşılmak istenirse bir işlemin sahip olduğu tüm denetlenebilirlik, değişmezlik ve zaman damgası güvencesini de taşır.

Bir nitelik alanı içeren bir adres yapısını zaten konuşlandırdık. Şu anda hızlı cüzdan kurtarma için HD cüzdan ağaçları yapısının şifreli bir kopyasını saklamak için kullanılıyor (HD Cüzdan belgelerine bakın). Daha sonraki sürümler bu yapıyı genelleştirecektir.

4.3. Kimlik Doğrulama ve Kanuna Uyum

Sermaye ile işlem yapma hakkı ve mülkiyeti konuları, işlemler açısından önemli kavramlardır. Örneğin alkol almaya yetecek sermayeniz olsa bile yasalar gereği alma yetkiniz kısıtlanmış olabilir.

Sermayenin mülkiyeti ve kaynağı genel olarak müşterini bil (Know Your Customer - K.Y.C.) düzenlemeleri kapsamındadır. Bu düzenlemelere göre banka veya borsa gibi sermayeyi kullanan hizmet ve işletmeler, yeni bir müşteri için hesap açtığında genellikle müşteri ve sermayesinin nereden geldiği hakkında temel bilgiler toplaması gerekir.

Buradaki teknolojik zorluk yasalar gereği bu bilgileri gönderme sürecinde kullanıcının bu bilgilerin nasıl kullanılacağı, saklanacağı ve imha edilip edilmeyeceği konusunda hiçbir güvencesinin olmamasıdır. Uyumluluk bilgileri ise ticari olarak değerli bilgilerdir; kimlik hırsızlığı amacıyla çalınabilir veya kanunun izin verdiği yerlerde satılabilir.

Bu nedenle uyumluluk bilgilerinin aktarıldığı politikalara uymaya zorlanan bir doğrulayıcıya güvenli bir şekilde iletilmesine izin vermek için bir paylaşım politikasının yanı sıra Mühürlü Cam Kanıtları kullanmayı araştırıyoruz. Bunu yaparak ise hem tek tip standartların ortaya çıkmasına hem de müşteri verilerinin çalınma riskini azaltacağına inanıyoruz.

Buna ek olarak Cardano için değeri hesaplamadan ayıran katmanlı model de bu yaklaşımdan yararlanabilir. Hesaplama katmanı borsalar ve bankalar gibi düzenlenmelere uyan kuruluşlar tarafından yürütülüyor ise uyumluluk kontrolleri yapmaları ve kullanıcılara vergi yönetmeliklerini zorlamaları gerekebilir.

Kullanıcı ise mühürlü cam kanıtlarını kullanarak internete sızacağı veya hesaplama katmanının konsensus node'ları tarafından korunup korunmayacağı endişesi olmadan kimlik ibraz edip parasıyla işlem yapabilir. Dahası böylelikle hesaplama katmanı da işlem yapan tüm kullanıcıların kimliğinin doğrulanmış ve meşru olduğundan emin olacaktır.

Bu durum aynı zamanda düzenlemelere uyan kuruluşlar arasında müşteri taşınabilirliğine de izin verir. Bu güvenli kanallar aracılığı ile borsalar müşteriler için bakiyeleri ve hesapları anında aktarabilir ve anlaşmalarının izin verdiği durumlarda piyasa düzenleyicilerle veri paylaşabilir.

Bu teknolojinin ilk beta testini 2018'in ortalarında yapacağız. 2018'in sonundan 2019'un başlarına kadar araştırma sonuçlarına göre ise Cardano'ya entegrasyonunun gerçekleştirilmesini bekliyoruz. Zaman konusunda tahminler ARM ve Intel'in donanımlarında çalışmak üzere imzalanmış kod için işbirliği yaptığını varsayar[1].

[1] bkz: Intel SGX Ticari Lisans Politikası

4.4. Pazar DAO (Merkeziyetsiz ve Özerk Kuruluşlar)'ları

Bundan önceki iki bölüm, dışarıdan da bazı sistemlerce desteklendiğini varsayarak, bilginin üretilmesini ve hareketini ele aldı. Eski sistemlerle uyumlu olmayı sağlamak için bu özellikler her zaman gerekli olacaktır. Ancak bu özellikler blok zinciri tabanlı düzenlemeleri ele almıyorlar.

Akıllı sözleşmeler ilişkilerin baştan sonucu belli, kendi kendini uygulayabilen ve belirsizlikten uzak tamamen yeni bir tür ticari sistemi temsil eder.

Sözleşmeler tahkim, koşula bağlı geri ödemeler ve verilere erişim gibi isteğe bağlı yazılabilen karmaşık yapılardır ve pazar yerleri için kurallar oluşturmak için de kullanılabilirler.

Bu gibi akıllı sözleşmeye dayalı yapılara Pazar DAO'ları diyoruz. Deftere gömülmek için özel protokol desteği veya değiştirilebilirlik gerektirmezler. Hatta tamamen akıllı sözleşmelerden de oluşturulabilirler.

Mimari açıdan amacı, sözleşme kanunlarından ve endüstride görülen en iyi iş uygulamalarından ilham alan bir ticari şablonlar bütünü oluşturmaktır. Bu şablonlar da piyasada belirli standartları uygulamak için geliştiricinin akıllı sözleşmesine bağlanabilir.

Örnek olarak, bir geliştirici halka arzetmek için CCL'de bir ERC20 tokeni çıkarmak istiyor. Bu durum için gönüllü veya yasal koşulları şart koşabilen, sadece halka arzlarla ilgilenen bir Pazar DAO'su kurulabilir. Bu durumda, normalde geliştiricinin ERC20 sözleşmesinde bulunan iadeler, paranın dağıtımı ve ödemelerin dondurulması gibi yetkilerin DAO'larca devralınabilmesi ortaya çıkar.

Bu olgu ise tüketici korunmasını sağlamak için bir pazarın nasıl kontrol edilmesi gerektiği konusunda geniş çaplı bir tartışma başlatır. İkinci bir husus ise yasal koruma ve haklar konusunda işlemlerin, farklı ülkelerdeki farklı yargı alanlarında otomatik olarak uyum sağlamasıdır.

Cardano Vakfı, IOHK ve diğer kuruluşlarla birlikte çalışan Cardano projesi, akıllı sözleşme geliştiricilerinin kullanması için bir Pazar DAO'ları referans kitaplığı oluşturacak. Sigorta ve düzenleyici piyasaların bu DAO'lar etrafında şekillenmesini ve sonuçlara dayalı olarak kendi kendine gelişmesini ümit ediyoruz.

5. SÜRDÜRÜLEBİLİRLİK

Kripto para alanı birçok kavramsal çelişkiyi içerir. Kripto para birimleri değiştirilmesi zor olacak şekilde tasarlanır, ancak tüm teknolojiler gibi tasarım kusurları ve gelişmeler sonucu değişmeleri gerekir. Merkeziyetsiz olmayı amaçlar, ama değişikliklere öncülük etmek veya kodun varlığını sürdürmek için güçlü aktörler gerektirir.

Belki de en kötüsü çoğu paydaşın düzeltilmesi gerektiği konusunda hemfikir olduğu bariz eksiklikler olduğunda ortaya çıktığında fikir birliğinin sağlanamamasıdır.

Bitcoin'in blok boyutu tartışması iki yıldan uzun süredir aktif bir konu. Her gün ağ en yüksek kapasitede olduğu için hacmi bir milyar doları aşan işlemler beklemede.

Geçici çözümlerin varlığında bile basit bir parametre değişimi koordine edilemiyorsa, şirketlerin ve hükümetlerin bu sistemlerin üzerine altyapı inşa etmek için milyarlarca dolar yatırım yapması nasıl beklenebilir? Bir işletme bu gibi mantıklı tasarım yükseltmeleri yapamayan, hesap verebilirlikten uzak protokolleri kullanarak neden kumar oynasın?

İnternet evriminin tarihinde de IPv4'ten IPv6'ya geçmek gibi basit değişiklikler Bitcoine benzer bir örüntü izledi ve gerçekleşmesi onlarca yıl sürdü. Yine de çok farklı bir velayet tarzlarını takip ettikleri için blok zinciri teknolojisi ve internet arasında güçlü bir zıtlık var.

İnternet ilk yıllarında devlet desteği görmüş ve ilgili kişileri atanmış, DARPA'dan (Birleşik Devletler Savunma İleri Araştırma Projeleri Ajansı) akademiye dönen askeri bir projeydi. İnternet, ağı tekelleştirmeye çalışan kurumların oyunlarına maruz kalmadan ve ticari olmayan koşullar altında büyüdü. Hatta e-ticaret 1992'de yürürlükten kaldırılana kadar internetin o yıllarda temeli olan NSF'nin kullanım şartlarını ihlal eden bir kavram idi.

İşletmeler interneti ticarileştirme hakkına sahip olduklarında internetin çoktan güçlü standartları ve ilkelere bağlı savunucuları vardı. Yine de bu standartlar ve savunucular AOL ve Microsoft gibi şirketlerin kendi kapalı platformlarını veya ActiveX gibi tescilli teknolojiler yaratmaya çalışmalarını engellemedi. Bu temel günümüzde de Google gibi yeni nesil aktörlerin devasa kullanıcı tabanları ve büyük sermayeleri ile kendi suni gündemlerini zorlamalarını durduramadı.

Tüccarlardan madencilere kadar rant[1] peşinde koşan aktörler için kripto para birimleri ticari olarak motive edilmiş mükemmel ekosistemlerdir. Bu temel göz önüne alındığında kripto para birimlerinin vesayeti şahsi çıkar etrafında gelişmiştir.

Örneğin, madencinin kar marjını iyileştirdiği için doğrulamasız madencilikle sık sık karşılaşılır; ama bu durum aynı zamanda madenciliğin tüm amacını ve faydasını tamamen göz ardı eder.

Bitcoin'de bir avuç aktörün hash gücünün çoğunluğu temsil etmesiyle madenciliğin merkezileşmesi zaten gerçekleşti.

Kripto para birimlerinde değişiklik yapmak için de, internetin tarihinde de olduğu gibi fikir birliği gerekir. Ancak güç bu kadar hızlı bir şekilde bir avuç rantçıda merkezileşirse ve değişim onlar için uygun olmazsa ne olur?

Çoğu kripto para biriminin başlangıcı internet gibi ticaretten uzak veya akademik yollarla başlamaz. Başlangıçlarından itibaren bazı gruplar kazanç sağlamaya çalışırlar. Bu kazanımları sağlamaya yardımcı olmak için bu gruplarca atanmış güç simsarları bulunur.

Başlangıçta merkezi olmak her kripto para biriminin evriminde olan bir gerçektir. Bundan tam olarak kurtulamayız ama en azından adım adım da olsa merkeziyetsiz olmasını tasarımlarımızla desteklemeliyiz.

Cardano için hangi faktörlerin merkezileşmeyi desteklediğini, ve protokolümüzü yavaş yavaş web gibi kamuya açık bir altyapı haline gelmesine teşvik etmek için hangi tekniklerin uygulanabileceğini dikkatlice düşündük.

Tümden merkeziyetsizliğin hem imkansız hem de verimsiz olabileceğini baştan kabul ediyoruz. Yine de bazı faktörler daha dengeli bir sistem üretmek için teşvik edilebilir.

Birincisi, halka arzda elde edilen fonlarının merkezileştirilmiş gözetimi, protokolün başlangıcında çevik ve hızlı bir şekilde geliştirilmesini sağlar. Sonra finansmanın çeşitlenmesi ve gelişme hızının daha sistematik ve kasıtlı bir hıza çekilmesi gerekiyor. Bu noktadan sonra ise finansmanın kültürel, dilsel ve coğrafi önyargılardan kaçınması gerekir.

[1] Terim hakkında daha detaylı bilgi için şu linke bakınız.

İkincisi, yol haritasıyla ilgili kararlar topluluğun kripto para teknolojisinin doğası hakkında daha fazla bilgi sahibi olmasıyla artık bir grup çekirdek geliştirici veya kuruluşta merkezileştirilemez. Protokolde değişiklik önermek, incelemek ve yürürlüğe koymak için blok zinciri tabanlı bir yöntem olması gerekir.

Üçüncüsü, Cardano SL blok zincirininin arkasındaki teşvikler tüm kullanıcıların ortak arzularıyla uyumlu olmalıdır. Topluluğun iradesinden bağımsız ve orantısız yetki sahibi bir grup aktörün ortaya çıkmasına izin veremeyiz.İlk ilke için Cardano'ya bir hazine sistemi entegre etmeyi seçtik. İkinci ilke için CSL tarafından koordine edilen bir sistem aracılığıyla Cardano İyileştirme Önerileri sunmak için resmi bir süreç uygulayacağız. Üçüncüsü için ise Ouroboros'un zarif bir çözüm sunduğuna inanıyoruz.

Yukarıdaki konular hakkında daha fazla ayrıntı verilebilir, ancak bunlar kendi başlarına ayrı konulardır ve bu gözlem çalışmasının kapsamını aşar. Mekanizma tasarımı, tamamlanmamış teorisi ve temel alacak sağlam bir modeli olmamasıyla, en karmaşık ve birbirine bağlı akademik alanlardan biridir.

İkinci bölümde açıklanan bilim odaklı yaklaşımımız burada bize iyi hizmet ediyor. IOHK'nın Veritas ekibi, Cardano'nun referans hazine modelini geliştirmek için Profesör Bingsheng Zhang yönetiminde Lancaster Üniversitesi'nden bir grup araştırmacı ile ortaklaşa çalışıyor. 2018'de sisteme entegre edilmesi amacıyla, 2017'nin sonuna kadar konuyla ilgili hakemli bir yayın çıkmasını bekliyoruz.

Hem ontolojik kavramları hem de geniş katılımı teşvik etmek için bir mekanizma gerektirdiği için protokolündeki değişikliklerin resmi açıklaması ve incelenmesi konusu en az anlaşılan konudur. Belki bu konuda bir tür temsili demokratik süreç ortaya çıkabilir veya daha rasyonel oylama sağlamak için sıvı geri bildirim kullanılabilir.

Bu yöndeki araştırmaların IOHK'un Cardano'nun[1] gelişimindeki çabasının çoğunu tüketmesini bekliyoruz. Başlangıç noktası olması için referans hazine modelinin yanında çeşitli mekanizmalar da kullanacağız. Kesin bir çözüm bulunması için daha fazla araştırma gereklidir.

Son olarak, Ouroboros'ta teşvikleri iyileştirme çalışmaları Oxford Üniversitesi'nden Profesör Elias Koutsoupias tarafından denetleniyor. Ouroboros'un kriptografik temelleri, gerekli tüm ölçeklenebilirlik çalışmalarıyla sağlamlaştırıldıktan sonra, referans protokolüne daha geniş bir tahvil, ceza ve egzotik teşvik çalışması eklenecektir.

[1] IOHK 2020'nin sonuna kadar Cardano'yu inşa etmeye devam edecek.

6. SONUÇ

Bir kripto para birimi, protokollerinin, kaynak kodunun ve yardımcı programlarının toplamından daha fazlasıdır. Kripto paralar özünde insanlara ilham veren, onları yetkin kılan ve birbirine bağlayan sosyal sistemlerdir. Geçmişteki protokollerin birçok eksik önlemleri, başarısızlıkları ve tutulmayan vaatlerinden hüsrana uğradık, ve daha iyi bir şey inşa etmek için yola çıktık.

Ne bu yolun kolay olduğuna inandık; ne de bir gün bitirebileceğimize. Evrimin özünü yararlı olması için Cardano'ya taşımak istiyoruz.

Evrime ise tek bir el ya da büyük bir tasarım rehberlik etmez. Evrim bitmek bilmeyen hatalardan ve problemlerden ilham alan bir süreçtir. Cardanoyu hem bugünün piyasalarında ayakta kalabilecek kadar fit, hem de geleceğin ihtiyaçlarını karşılayacak kadar kadar esnek olması için bu sürecin dijital olarak somut bir örneği olmayı hedefliyor.

Önceki bölümler, bu hedefe nasıl yaklaştığımıza dair kısa bir bakış açısı içeriyor. Cardano için özenle önyargılardan arınmaya, tarihten ders almaya ve titiz bir süreç izlemeye çalıştık. Hızlı gelişme ihtiyacını, hızlı hareket edemeyecek yöntemlerle dengelemeye çalıştık.

Bu yolculuğa çıkmak olağanüstü bir ayrıcalıktı. Son iki yılda kanıtlanabilir şekilde güvenli bir proof of stake protokolü geliştirdik, Haskell geliştiricilerinden küçük bir ordu topladık ve Cardano'nun geliştirilmesini birçok yetenekli bilim insanının işi haline getirdik.

Kağıt üzerinden gerçek dünyaya geçerken elbette büyüme acılarımız olacak; ancak umudumuz Cardanoyu bir insanmış gibi düşünürsek onu şu cümleyle özetlenebilir hale getirmektir:

"*Cardano, büyüklerinden öğrenen, içinde yaşadığı toplumda iyi bir vatandaş olan ve her zaman faturalarını ödemenin bir yolunu bulan pragmatik bir hayalperesttir.*"

İlerde ne olur bilemeyiz ancak onu herkes için daha iyi hale getirmeye çalışmaktan mutluluk duyuyoruz.

Okuduğunuz için teşekkürler.