**Nervos Konumlandırma Belgesi**

**1. Bu Belgenin Amacı**

Nervos Ağı, bir dizi protokol ve yenilikten oluşur. Bir [RFC](https://github.com/nervosnetwork/rfcs) (yorum talebi) sürecinden yararlandığımız temel protokol tasarımı ve uygulamaları hakkında net belgelere ve teknik özelliklere sahip olmak önemlidir. Bununla birlikte, topluluklarımızın neyi başarmaya çalıştığımızı, yaptığımız uzlaşmaları ve mevcut tasarım kararlarımıza nasıl ulaştığımızı anlamalarına yardımcı olmamızın da aynı derecede önemli olduğunu düşünüyoruz.

Bu belgeye, bugün kamuya açık izinsiz(permissionless) blok zincirlerinin karşılaştığı sorunların ve bunları çözmeye çalışan mevcut çözümlerin ayrıntılı bir incelemesiyle başlıyoruz. Bunun, okuyucularımızın bu zorluklara en iyi nasıl yaklaşacağımız konusundaki mantığımızı ve temel tasarım kararlarımızı anlamaları için gerekli kapsamı sağladığını umuyoruz. Ardından, ağın genel vizyonunu desteklemek için birlikte nasıl çalıştıklarına odaklanarak, Nervos Ağı'nın tüm bölümlerinin üst düzey bir incelemesini sunacağız.

**2. Arka Plan**

Ölçeklenebilirlik, sürdürülebilirlik ve birlikte çalışabilirlik, genel izinsiz blok zincirlerinin bugün karşılaştığı en büyük zorluklar arasındadır. Pek çok proje bu sorunlara çözüm getirdiğini iddia etse de bu sorunların nereden geldiğini anlamak ve çözümleri olası takaslar bağlamında ortaya koymak önemlidir.

**2.1 Ölçeklenebilirlik**

Bitcoin [1], eşler arası(peer-to-peer) elektronik nakit olarak kullanılmak üzere tasarlanmış, halka açık ilk izinsiz blok zinciriydi. Ethereum[2], daha fazla kullanım durumunu mümkün kıldı ve genel amaçlı, merkezi olmayan bir bilgi işlem platformu yarattı. Bununla birlikte, bu platformların her ikisi de işlem yeteneklerine sınırlamalar getirir- Bitcoin blok boyutunu ve Ethereum blok gas limitini sınırlar. Bunlar, uzun vadeli ademi merkeziyetçiliği sağlamak için gerekli adımlardır, ancak aynı zamanda her iki platformun da yeteneklerini sınırlar.

Blokzincir topluluğu, son yıllarda birçok ölçeklenebilirlik çözümü önerdi. Genel olarak, bu çözümleri iki kategoriye ayırabiliriz: **zincir içi ölçeklendirme ve zincir dışı ölçeklendirme.**

**Zincir içi** ölçeklendirme çözümleri, mutabakat sürecinin verimini artırmayı ve merkezi sistemlerin tersine yerel veri hacmine sahip blok zincirleri oluşturmayı amaçlar. Zincir dışı ölçeklendirme çözümleri, neredeyse tüm işlemleri üst katmanlara taşırken güvenli bir varlık ve ödeme platformu olarak yalnızca blok zincirini kullanır.

**2.1.1 Tek Blokzincir ile Zincir İçi Ölçeklendirme**

Bir blok zincirinin verimini arttırmanın en basit yolu, blok alanı arzını arttırmaktır. Ek blok alanı ile ağ üzerinden daha fazla işlem akabilir ve işlenebilir. Artan işlem talebine cevaben blok alanı arzını artırmak, işlem ücretlerinin düşük kalmasını da sağlar.

Bitcoin Cash (BCH), eşler arası(peer-to-peer) ödeme ağını ölçeklendirmek için bu yaklaşımı benimser. Bitcoin Cash protokolü, maksimum 8 MB blok boyutuyla başladı, daha sonra 32 MB'a çıkarıldı ve işlem talebi arttıkça süresiz olarak artırılmaya devam edecek. Referans olarak, Bitcoin'in (BTC) Ağustos 2017'de Segregated Witness uygulamasını takiben, Bitcoin protokolü artık yaklaşık 2 MB'lik ortalama bir blok boyutuna izin veriyor.

Bir veri merkezi kapsamında şöyle bir matematik çalışıyor: 7,5 milyar insanın her biri günde 2 zincir içi işlem oluşturursa, ağ her 10 dakikada bir 26 GB blok üretimi gerektirecek ve bu da günde 3,75 TB veya yılda 1,37 PB'lik bir blok zinciri büyüme oranına yol açacaktır [3]. Bu depolama ve bant genişliği gereksinimleri, günümüzün herhangi bir bulut hizmeti için makul düzeydedir.

Bununla birlikte, düğüm operasyonunu bir veri merkezi ortamıyla sınırlamak, tek bir uygulanabilir ağ topolojisine yol açar ve güvenlikten (ağ genelinde veri iletim gereksinimleri arttıkça blok zincirinin çatallanma hızı artacaktır) ve ayrıca ademi merkeziyetçilikten (mutabakata katılım maliyeti arttıkça tam düğüm sayısı azalacaktır) taviz vermeye zorlar.

Ekonomik açıdan, sürekli artan blok boyutu, kullanıcılar tarafından hissedilen ücret baskısını hafifletir. Bitcoin ağının analizi, ücretlerin bir blok yaklaşık %80 dolana kadar sabit kaldığını ve ardından katlanarak arttığını göstermiştir [4].

Büyüyen bir ağın maliyetlerinin yükünü operatörlerine yüklemek makul bir karar gibi görünse de bu, iki nedenden dolayı dar görüşlülük olabilir:

- İşlem ücretlerinin kaldırılması, madencileri ağırlıklı olarak yeni madeni para ihracından (blok ödülleri) elde edilen tazminata güvenmeye zorlar. Enflasyon protokolün kalıcı bir parçası olmadığı sürece, yeni madeni para basımı eninde sonunda duracak (toplam sabit madeni paraya ulaşıldığında) ve madenciler ne blok ödülleri ne de önemli işlem ücretleri alamayacak. Bunun ekonomik etkisi, ağın güvenlik modelini ciddi şekilde tehlikeye atacaktır.

- Tam bir düğümü çalıştırmanın maliyeti aşırı derecede pahalı hale gelir. Bu, normal kullanıcıların bir blok zincirinin geçmişini ve işlemlerini bağımsız olarak doğrulama yeteneğini ortadan kaldırarak, blok zincirinin bütünlüğünü sağlamak için borsalar ve ödeme işlemcileri gibi hizmet sağlayıcılara güvenmeye zorlar. Bu güven gerekliliği, eşler arası, güvene dayalı olmayan dağıtılmış sistemler olarak genel izinsiz blok zincirlerinin temel değer önermesini geçersiz kılar.

Bitcoin Cash gibi işlem maliyeti optimize edilmiş platformlar, geleneksel ödeme sistemlerinin yanı sıra diğer blokaj zincirlerinden (izinli ve izinsiz) önemli bir rekabetle karşı karşıyadır. Güvenliği veya sansüre karşı direnci geliştiren tasarım kararları ilgili maliyetlere yol açacak ve dolayısıyla platformu kullanma maliyetini artıracaktır. Ağın belirtilen hedeflerinin yanı sıra rekabetçi bir ortam dikkate alındığında, diğer tüm hususlar pahasına, ağın genel hedefinin daha düşük maliyetler olması muhtemeldir.

Bu hedef, işlem ağı kullanımına ilişkin gözlemlerimizle tutarlıdır. Bu sistemlerin kullanıcıları, ağı yalnızca kısa bir süre için kullanacaklarından, önemli uzun vadeli ödünleşimlere karşı kayıtsızdırlar. Malları veya hizmetleri alındıktan ve ödemeleri yapıldıktan sonra, bu kullanıcıların artık ağın etkin çalışmasıyla ilgili herhangi bir endişeleri yoktur. Bu değiş tokuşların kabulü, merkezi kripto varlık borsalarının ve daha merkezileştirilmiş blok zincirlerinin yaygın kullanımında açıkça görülmektedir. Bu sistemler, öncelikle kolaylıkları ve işlemsel verimlilikleri nedeniyle popülerdir.

Bazı akıllı sözleşme platformları, blok zinciri verimini ölçeklendirmek için benzer yaklaşımlar benimsedi ve yalnızca sınırlı sayıda "süper bilgisayar" onaylayıcısının fikir birliği sürecine katılmasına ve blok zincirini bağımsız olarak doğrulamasına izin verdi.

Ademi merkeziyetçilik ve ağ güvenliği ile ilgili tavizler daha ucuz işlemlere izin verse de ve bir dizi kullanıcı için uygun olsa da tehlikeye atılmış uzun vadeli güvenlik modeli, işlemleri bağımsız olarak doğrulamak için maliyet engeli ve düğüm operatörlerinin muhtemel yoğunlaşması ve sağlamlaşması bizi şu noktalara götürüyor: bunun halka açık blok zincirlerini ölçeklendirmek için uygun bir yaklaşım olmadığına inanıyoruz.

**2.1.2 Çoklu Zincirler Üzerinden Zincir İçi Ölçeklendirme**

Çoklu Zincirler Üzerinden Zincir İçi Ölçeklendirme, Ethereum 2.0'da görüldüğü gibi parçalama(sharding) veya Polkadot'ta görüldüğü gibi uygulama zincirleri aracılığıyla gerçekleştirilebilir. Bu tasarımlar, ağın küresel durumunu ve işlemlerini etkili bir şekilde çoklu zincirlere ayırarak, her zincirin hızlı bir şekilde yerel fikir birliğine ulaşmasını ve daha sonra ağın tamamının "Beacon Chain" veya "Relay Chain" fikir birliği yoluyla küresel fikir birliğine ulaşmasını sağlar.

Bu tasarımlar, birden çok zincirin paylaşılan bir güvenlik modelini kullanmasına izin verirken, parçalar (Ethereum) veya para zincirleri (Polkadot) içinde yüksek verim ve hızlı işlemlere izin verir. Bu sistemlerin her biri birbirine bağlı bir blok zinciri ağı olsa da her zincirde çalışan protokoller bakımından farklılık gösterirler. Ethereum 2.0'da her parça aynı protokolü çalıştırırken, Polkadot'ta her para-zincir, Substrate çerçevesi aracılığıyla oluşturulan özelleştirilmiş bir protokolü çalıştırabilir.

Bu çok zincirli mimarilerde, her bir dApp (veya bir dApp örneği) yalnızca tek bir zincirde bulunur. Günümüzde geliştiriciler, blok zincirindeki diğer herhangi bir dApp ile sorunsuz bir şekilde etkileşime giren dApp'ler oluşturma yeteneğine alışık olsalar da tasarım modellerinin yeni çok zincirli mimarilere uyum sağlaması gerekecek. Bir dApp farklı parçalara bölünürse, durumu dApp'ın farklı örneklerinde (farklı parçalarda bulunan) senkronize halde tutmak için mekanizmalar gerekir. Ek olarak, hızlı parçalar arası iletişim için katman 2 mekanizmaları konuşlandırılabilse de parçalar arası işlemler küresel fikir birliği gerektirecek ve onay gecikmesine neden olacaktır.

Bu eş zamansız işlemlerle, kötü şöhretli "tren ve otel" sorunu ortaya çıkıyor. İki işlemin atomik olması gerektiğinde (örneğin, iki farklı parça üzerinde bir tren bileti ve bir otel odası rezervasyonu yapmak), yeni çözümler gerekir. Ethereum, bir parçada bağımlı bir sözleşmenin silindiği, ikinci bir parçada (diğer bağımlı sözleşmeyi içeren) oluşturulan ve ardından her iki işlemin de ikinci parçada yürütüldüğü "yanking" sözleşmesini sunar. Ancak, alınan sözleşme daha sonra orijinal parça üzerinde kullanılamayacak, kullanılabilirlik sorunları ortaya çıkaracak ve yine yeni tasarım kalıpları gerektirecektir.

Sharding'in kendi avantajları ve zorlukları vardır. Parçalar gerçekten bağımsız olabiliyorsa ve parçalar arası ihtiyaçlar minimum düzeydeyse, bir blok zinciri, parça sayısını artırarak verimini doğrusal olarak ölçeklendirebilir. Bu, dış durum veya diğer uygulamalarla iş birliği gerektirmeyen bağımsız uygulamalar için en uygun olanıdır.

Parçalanmış bir mimari, "yapı taşı" uygulamalarını bir araya getirerek geliştirilen uygulamalar için sorunlu olabilir (bu, "biçimlendirilebilirlik sorunu" olarak bilinir). Şekillendirilebilirlik, özellikle daha gelişmiş ürünlerin diğer yapı taşı ürünlerin üzerine inşa edilme eğiliminde olduğu merkezi olmayan finans (decentralized finance: DeFi) alanıyla ilgilidir.

Daha teknik bir not olarak, parçalama tipik olarak, N zincirinin bir meta zincire bağlandığı ve bir meta zincirin kendisi ölçeklenebilirlik sorunları yaşamadan destekleyebileceği parça sayısına bir üst sınır getiren bir "1 + N" topolojisi gerektirir.

Web geliştiricilerinin alt düzey endişeler için kitaplıkları ve hizmet entegrasyonu için açık API'leri kullanmasına benzer şekilde, birbirine bağlı uygulamalardan oluşan bir ekosistemin ortaya çıkmasına ve geliştiricilerin kenarlarda yenilik yapmasına izin veren birleşik bir küresel durumda önemli değer gözlemliyoruz. Geliştiriciler, blok zinciri etkileşimlerinin mimari kaygılarındaki tutarlılıktan kaynaklanan üstün bir kullanıcı deneyiminin yanı sıra eşzamanlılığı (parçalar arası varlık aktarımı veya mesajlaşma geçişinde) dikkate almak zorunda kalmadığında çok daha basit bir geliştirme deneyimi sağlanır.

Parçalamanın gelecek vaat eden bir ölçeklenebilirlik çözümü olduğunun farkındayız (özellikle birbirine daha az bağımlı uygulamalar için), ancak en değerli durumu tek bir blok zinciri üzerinde yoğunlaştıran ve şekillendirilebilirliğe izin veren bir tasarıma sahip olmanın faydalı olduğuna inanıyoruz. Bu tasarımla, daha yüksek verime izin vermek için zincir dışı ölçeklendirme yaklaşımlarından yararlanılır.

**2.1.3 Katman 2 ile Zincir Dışı Ölçeklendirme**

Katman 2 protokollerinde, temel katman blok zinciri bir anlaşma (veya taahhüt) katmanı olarak işlev görürken, ikinci katman ağı, katılımcıların kripto para birimini "teslim almasına" olanak tanıyan kriptografik kanıtları yönlendirir. İkinci katmanın tüm faaliyetleri, temeldeki blok zinciri tarafından kriptografik olarak güvence altına alınır ve temel katman, yalnızca ikinci katman ağına giren/çıkan miktarları çözmek ve uyuşmazlık çözümü için kullanılır. Bu tasarımlar, fonların emaneti (veya kayıp riski) olmadan çalışır ve anında, neredeyse ücretsiz işlemlere olanak tanır.

Bu teknolojiler, Bitcoin gibi bir değer saklama ağının günlük ödemeler için nasıl kullanılabileceğini göstermektedir. Katman 2 çözümünün uygulamadaki en tipik örneği, müşteri ile kahve dükkânı arasındaki ödeme kanalıdır. Alice'in her sabah Bitcoin Coffee Shop'u ziyaret ettiğini varsayalım. Ay başında kafe ile birlikte açtığı Lightning ödeme kanalına para yatırıyor. Her gün ziyaret ettiğinde, kahve dükkanının kahvesi karşılığında paranın bir kısmını alma hakkını kriptografik olarak imzalar. Bu işlemler anında gerçekleşir ve tamamen eşler arası, "zincir dışı" olup sorunsuz bir müşteri deneyimi sağlar. Lightning kanalı güvensizdir (katılımcıların sistemin işlemesi için birbirlerini veya üçüncü bir tarafı bilmesine veya güvenmesine gerek olmayan), Alice veya kafeterya ödeme kanalını her an kapatabilir, o sırada alacakları parayı alabilir.

Lightning gibi ödeme kanalı teknolojileri, zincir dışı ölçeklendirme tekniğinin yalnızca bir örneğidir; Blokzincir verimini bu şekilde güvenli bir şekilde ölçekleyebilen birçok olgunlaşan teknoloji var. Ödeme kanalları, iki taraf arasındaki dengeleri yönlendirmek için zincir dışı anlaşmaları içerirken, durum kanalları (bir ağdaki iki kullanıcı veya node arasındaki veya bir kullanıcı ile bir hizmet arasındaki iki yönlü bir iletişim kanalı), kanal katılımcıları arasında keyfi duruma yönelik zincir dışı anlaşmaları içerir. Bu genelleme, ölçeklenebilir, güvene dayalı olmayan, merkezi olmayan uygulamaların temeli olabilir. Tek bir durum kanalı birden fazla uygulama tarafından bile kullanılabilir ve bu da daha fazla verimlilik sağlar. Taraflardan biri kanaldan çıkmaya hazır olduğunda, üzerinde anlaşmaya varılan kriptografik kanıtı blok zincirine sunabilir ve blok zinciri daha sonra anlaşmaya varılan durum geçişlerini yürütür.

Bir yan zincir, güvenilir üçüncü taraf blokzincir operatörleri aracılığıyla artan verime izin veren başka bir yapıdır. Güvenilir ve güvensiz fikir birliğine sahip bir blok zincirine iki yönlü bir bağlantıyla, fonlar ana zincir ve yan zincir arasında ileri geri hareket ettirilebilir. Bu, yan zincirde yüksek hacimli güvenilir işlemlere ve daha sonra ana zincirde net yerleşime izin verir. Yan zincir işlemleri minimum ücrete, hızlı onaya ve yüksek verime sahiptir. Yan zincirler bazı açılardan üstün bir deneyim sunsa da güvenlikten ödün verirler. Bununla birlikte, güvenlikten ödün vermeden aynı performans iyileştirmelerini sağlayabilen güvensiz yan zincirlerle ilgili çok sayıda araştırma vardır.

Güvensiz yan zincir teknolojisine bir örnek, geniş küresel mutabakata sahip bir blok zincirindeki bir güven kökünden yararlanan bir yan zincir mimarisi olan Plasma'dır (5.4'te ele alınmıştır). Plazma zincirleri, merkezi yan zincirlerle aynı performans iyileştirmelerini sunar, ancak bunu yaparken güvenlik garantileri de sunar. Bir Plazma zinciri operatörünün kötü niyetli olması veya hatalı çalışması durumunda, kullanıcılara yan zincir varlıklarını güvenli bir şekilde ana zincire çekmelerine olanak tanıyan bir mekanizma sağlanır. Bu, Plazma zincir operatörünün iş birliği olmadan yapılır ve kullanıcılara yan zincir işlemlerinin rahatlığını ve ayrıca bir katman 1 blok zincirinin güvenliğini sunar.

Zincir dışı ölçeklendirme (off-chain scaling), ademi merkeziyetçilik, güvenlik ve ölçeklenebilirlik sağlar. Uzlaşma işlemleri ve ihtilaflar dışındaki her şeyi zincir dışına taşıyarak, halka açık bir blok zincirinin sınırlı küresel fikir birliği verimli bir şekilde kullanılır. Uygulama gereksinimlerine göre çeşitli katman 2 protokolleri uygulanabilir ve geliştiricilere ve kullanıcılara esneklik sağlar. Ağa daha fazla katılımcı eklendikçe, performans etkilenmez ve tüm taraflar, katman 1 fikir birliği tarafından sunulan güvenlik garantilerini paylaşabilir.

**2.2 Sürdürülebilirlik**

Özerk, sahipsiz bir halka açık (public) blok zincirinin uzun vadeli işleyişini sürdürmek oldukça zorlayıcıdır. Teşvikler, çeşitli paydaşlar arasında dengelenmeli ve sistem, yaygın tam düğüm çalışmasına ve kamu tarafından doğrulanabilirliğe izin verecek şekilde tasarlanmalıdır. Açık, küresel bir ağı desteklerken donanım gereksinimleri makul kalmalıdır.

Ek olarak, halka açık bir blok zincir faaliyete geçtiğinde, protokolü yöneten temel kuralları değiştirmek çok zordur. En başından, sistem sürdürülebilir olacak şekilde tasarlanmalıdır. Bu ilgi doğrultusunda, sürdürülebilir, izinsiz blok zincirleri oluşturma konusundaki zorlukların kapsamlı bir envanterini çıkardık.

**2.2.1 Ademi merkeziyetçilik**

Halka açık blok zincirlerinin karşı karşıya olduğu en büyük uzun vadeli tehditlerden biri, tam düğüm operasyonunun maliyetine yansıyan, bağımsız katılım ve işlem doğrulamanın sürekli artan engelidir. Tam düğümler, blokzincir katılımcılarının zincir üzerindeki durumu/geçmişi bağımsız olarak doğrulamasına ve geçersiz blokları yönlendirmeyi reddederek ağın madencilerini veya doğrulayıcılarını sorumlu tutmasına olanak tanır. Tam düğümlerin maliyeti arttıkça ve sayıları düştükçe, ağdaki katılımcılar hem geçmişi hem de mevcut durumu sağlamak için profesyonel hizmet operatörlerine giderek daha fazla güvenmek zorunda kalıyor ve bu da açık ve izinsiz blok zincirlerinin temel güven modelini aşındırıyor.

Tam bir düğümün blok zincirinin ilerlemesine ayak uydurması için, işlemleri doğrulamak için yeterli hesaplama hacmine, işlemleri almak için bant genişliğine ve tüm küresel durumu depolamak için depolama kapasitesine sahip olması gerekir. Tam bir düğümün işletim maliyetini kontrol etmek için protokolün, bu üç kaynağın iş hacmini veya kapasite artışını sınırlamak için önlemler alması gerekir. Blokzincir protokollerinin çoğu, hesaplama veya bant genişliği verimini sınırlar, ancak çok azı küresel durumun büyümesini sınırlar. Bu zincirlerin boyutu ve operasyon süresi büyüdükçe, tam düğüm operasyon maliyetleri geri döndürülemez şekilde artacaktır.

**2.2.2 Ekonomik Modeller**

Son yıllarda mutabakat protokolleri üzerine pek çok araştırma yapılmış olsa da kripto ekonomisinin yeterince çalışılmamış bir alan olduğuna inanıyoruz. Genel olarak, katman 1 protokolleri için mevcut kripto-ekonomik modeller, öncelikle ağ mutabakatını sağlamak için teşvikler ve cezalara odaklanır ve yerel tokenler çoğunlukla işlem ücretlerini ödemek veya Sybil direnci sağlayan staking gereksinimlerini karşılamak için kullanılır.

İyi tasarlanmış bir ekonomik modelin uzlaşma sürecinin ötesine geçmesi ve protokolün uzun vadeli sürdürülebilirliğini sağlaması gerektiğine inanıyoruz. Ekonomik model özellikle aşağıdaki hedeflerle tasarlanmalıdır:

- ağ, hizmet sağlayıcılarını (genellikle madenciler veya doğrulayıcılar) telafi etmek için sürdürülebilir bir şekilde olmalı ve ağın sürdürülebilir bir şekilde güvenli kalmasını sağlamalıdır.

- ağın, katılıma karşı düşük bir engeli sürdürmek için sürdürülebilir bir yolu olmalı ve ağ zaman içinde merkezsiz kalmalıdır.

- halka açık ağın kaynakları verimli ve adil bir şekilde tahsis edilmelidir.

- blok zincirinin yerel token’i içsel değere sahip olmalıdır.

**2.2.3 Bitcoin'in Ekonomik Modelinin Analizi**

Bitcoin protokolü, blok boyutunu sınırlar ve sabit bir blok süresi uygular. Bu, ağın bant genişliği verimini, kullanıcıların işlem ücretleriyle teklif vermesi gereken kıt bir kaynak haline getirir. Bitcoin Komut Dosyası döngülere izin vermez, bu da komut dosyasının uzunluğunu hesaplama karmaşıklığının iyi bir tahmini yapar. Genel olarak, blok alanı için daha fazla talep, kullanıcılar için daha yüksek işlem ücretleri anlamına gelir. Ek olarak, bir işlemde yer alan girdiler, çıktılar veya hesaplama adımları ne kadar fazlaysa, kullanıcı işlem ücretlerinde o kadar fazla ödeyecektir.

Bitcoin'in içsel değeri neredeyse tamamen parasal priminden (toplumun ona para olarak davranma isteği) ve özellikle onu bir değer saklama aracı olarak tutma isteğinden gelir. Madenci geliri BTC cinsinden olduğundan, Bitcoin'in ekonomik modelinin sürdürülebilir olması için bu algı geçerli olmalıdır. Başka bir deyişle, Bitcoin'in güvenlik modeli daireseldir- ağın sürdürülebilir bir şekilde güvenli olduğuna ve bu nedenle parasal bir değer deposu olarak kullanılabileceğine dair toplu inanca bağlıdır.

Bitcoin'in blok boyutu sınırı, ağa katılım engelini etkili bir şekilde belirler- blok boyutu sınırı ne kadar düşükse, profesyonel olmayanların tam düğümleri çalıştırması o kadar kolay olur. Bitcoin küresel durumu, UTXO (unspent transaction output: harcanmamış işlem çıktısı) kümesidir ve büyüme oranı da blok boyutu sınırıyla etkili bir şekilde sınırlandırılmıştır. Kullanıcılar, UTXO'ları verimli bir şekilde oluşturmaya ve kullanmaya teşvik edilir; daha fazla UTXO oluşturmak, daha yüksek işlem ücretleri anlamına gelir. Ancak, UTXO'ların birleştirilmesini ve küresel durumun boyutunun küçültülmesini teşvik edecek hiçbir teşvik sağlanmamaktadır; Bir UTXO oluşturulduktan sonra, harcanana kadar küresel durumu ücretsiz olarak işgal edecektir.

Bitcoin'in işlem ücretine dayalı ekonomik modeli, protokol tarafından empoze edilen kıt kaynak olan bant genişliği verimini tahsis etmek için adil bir modeldir. Eşler arası bir ödeme sistemi için uygun bir ekonomik modeldir, ancak gerçek bir değer saklama platformu için kötü bir seçimdir. Blok zincirini değer depolamak için kullanan Bitcoin kullanıcıları, işlem ücretlerini yalnızca bir kez öder, ancak daha sonra sürekli kaynak yatırımları yapması gereken madenciler tarafından sağlanan sürekli güvenliğin keyfini çıkararak durumu sonsuza kadar koruyabilir.

Bitcoin'in toplam arz sınırı vardır ve blok ödülleri yoluyla yeni ihraç edilmesi sonunda sıfıra düşecektir. Bu iki soruna neden olabilir:

Birincisi, eğer Bitcoin bir değer deposu olarak başarılı olmaya devam ederse, BTC'nin birim değeri artmaya devam edecek ve ağın güvence altına aldığı toplam değer de artacaktır (ağa daha fazla parasal değer geçtikçe). Bir değer deposu platformu, koruduğu değer zamanla arttığı için güvenlik bütçesini artırabilmelidir, aksi takdirde, saldırganları ikiye katlamaya ve ağ varlıklarını çalmaya davet eder.

Protokol güvenliğini kırmanın maliyeti, dürüst davranarak kazanabilecekleri kârdan az olduğunda, saldırganlar her zaman saldırır. Bu, şehir içindeki zenginlik arttıkça askeri harcamalarını artırmak zorunda olan bir şehre benziyor. Bu yatırım olmazsa er ya da geç şehir saldırıya uğrayacak ve yağmalanacak.

Blok ödüllerinin varlığıyla Bitcoin, güvenliği depoladığı toplam değere göre ölçeklendirebilir- Bitcoin'in fiyatı iki katına çıkarsa, madencilerin blok ödüllerinden elde ettikleri gelir de iki katına çıkar, bu nedenle iki kat hash oranı üretmeyi göze alabilirler ki bu ağa saldırmanın iki kat daha pahalı olması anlamına gelir.

Ancak bu, tahmin edilebilir blok ödülleri sıfıra düştüğünde değişir. Madenciler tamamen işlem ücretlerine güvenmek zorunda kalacaklar; gelirleri artık Bitcoin varlığının değerine ölçeklenmeyecek, ancak ağın işlem talebi tarafından belirlenecek. İşlem talebi, mevcut blok alanını dolduracak kadar yüksek değilse, toplam işlem ücretleri çok küçük olacaktır. İşlem ücretleri kesinlikle blok alanı talebinin bir fonksiyonu olduğundan ve bir Bitcoin fiyatından bağımsız olduğundan, bunun Bitcoin'in güvenlik modeli üzerinde derin bir etkisi olacaktır. Bitcoin'in güvende kalması için, aynı zamanda Bitcoin'in fiyatına göre ölçeklenen, tutarlı, aşırı kapasiteli işlem talebini varsaymamız gerekir. Bunlar çok güçlü varsayımlardır.

İkincisi, tahmin edilebilir blok ödülleri durduğunda, madenciler için blok başına gelirdeki değişkenlik artar ve madencileri blok zincirini ilerletmek yerine çatallamaya teşvik eder. Uç durumda, bir madencinin mempool'u boş olduğunda ve ücretlerle dolu bir blok aldığında, zinciri ilerletmek ve potansiyel olarak geliri olmayan bir blok üretmek yerine, zinciri çatallamak ve ücretleri çalmak onların güdüsüdür [5]. Bu, Bitcoin topluluğunda, Bitcoin'in sabit sınırını kaldırmadan henüz tatmin edici bir çözümün bulunmadığı "ücret kesintisi" sorunu olarak bilinir.

**2.2.4 Akıllı Sözleşme Platformlarının Ekonomik Modelinin Analizi**

Akıllı sözleşme platformlarının tipik ekonomik modeli daha da fazla zorlukla karşı karşıyadır. Örnek olarak Ethereum'u kullanalım. Ethereum'un komut dosyası döngülere izin verir, bu nedenle bir komut dosyasının uzunluğu, komut dosyasının hesaplama karmaşıklığını yansıtmaz. Bu, Ethereum'un blok boyutunu veya bant genişliği verimini sınırlamamasının, ancak hesaplama verimini (blok gaz limitinde ifade edilir) sınırlamasının nedenidir.

İşlemlerinin Ethereum blok zincirine kaydedilmesi için kullanıcılar, işlem ücretlerinde ödemek istedikleri hesaplama başına maliyet üzerinden teklif verirler. Ethereum, ETH'de fiyatlandırılan hesaplama maliyetinin ölçümü olarak "gaz" kavramını kullanır ve "gaz fiyatı" oran kontrolü, hesaplama adımı başına maliyetin yerel tokenin fiyat hareketlerinden bağımsız olmasını sağlar. ETH tokeninin gerçek değeri, merkezi olmayan hesaplama platformunun ödeme tokeni konumundan gelir; ETH, Ethereum'da hesaplamada ödeme yapmak için kullanılabilecek tek para birimidir.

Ethereum'un küresel durumu, tüm hesapların bakiyelerini ve dahili durumunu içeren veri yapısı olan EVM'nin durum trie'si ile temsil edilir. Yeni hesaplar veya sözleşme değerleri oluşturulduğunda, genel durumun boyutu genişler. Ethereum, durum deposuna yeni değerlerin eklenmesi için sabit miktarlarda gas ücreti alır ve değerler kaldırıldığında bir işlemin gas maliyetlerini dengeleyen sabit bir "gas maaşı" sunar.

"Bir kez öde, sonsuza kadar kullan" depolama modeli, madencilerin ve tam düğümlerin devam eden maliyet yapısına uymaz ve model, kullanıcıları gönüllü olarak durumu kaldırmaya veya durumu daha önce kaldırmaya teşvik etmez. Sonuç olarak, Ethereum durum boyutunda hızlı bir büyüme yaşadı. Daha büyük bir durum boyutu, işlem hızını yavaşlatır ve tam düğümlerin işletim maliyetini yükseltir. Durumu temizlemek için güçlü teşvikler olmadan, bu devam edecek bir eğilimdir.

Bitcoin'e benzer şekilde, Ethereum'un talebe dayalı gaz fiyatlandırması, platformun kıt kaynağı olan hesaplama verimini tahsis etmek için adil bir modeldir. Model ayrıca merkezi olmayan bir hesaplama sistemi olarak Ethereum'un amacına da hizmet ediyor. Bununla birlikte, durum depolama ücreti modeli, merkezi olmayan bir durum veya varlık depolama platformu olarak potansiyel önerisiyle eşleşmiyor. Uzun vadeli durum depolama maliyeti olmadan, durumu sonsuza kadar ücretsiz olarak işgal etmek her zaman kullanıcıların çıkarına olacaktır. Durum depolama kapasitesinin kıtlığı olmadan ne bir pazar ne de arz ve talep dinamikleri kurulamaz.

Çekirdek protokolünde blok boyutu sınırını belirleyen Bitcoin'den farklı olarak Ethereum, madencilerin blok ürettikleri zaman blok gaz sınırını dinamik olarak ayarlamalarına izin verir. Gelişmiş donanıma ve önemli bant genişliğine sahip madenciler, bu oylama sürecine etkin bir şekilde hâkim olarak daha fazla blok üretebilir. İlgi alanları, blok gaz limitini yukarı doğru ayarlamak, katılım çıtasını yükseltmek ve daha küçük madencileri rekabetin dışında bırakmaktır. Bu, tam düğüm işleminin hızla artan maliyetine katkıda bulunan başka bir faktördür.

Ethereum gibi akıllı sözleşme platformları, çok varlıklı platformlardır. Tipik olarak "tokenlar" olarak temsil edilen her tür kripto varlığın verilmesini ve işlemlerini desteklerler. Ayrıca yalnızca kendi yerel tokenlarına değil, platformdaki tüm kripto varlıkların değerine de güvenlik sağlarlar. Bu nedenle, çok varlıklı bir bağlamda "değer deposu", hem platformun yerel tokenlarına hem de platformda depolanan kripto varlıklarına fayda sağlayan değer koruma özelliğini ifade eder.

Blok ödülleri ile Bitcoin, mükemmel bir "değer deposu" ekonomik modeline sahiptir. Madencilere BTC cinsinden sabit bir blok ödülü ödenir ve böylece BTC'nin fiyatı ile birlikte gelirleri de artar. Bu nedenle platform, sürdürülebilir bir ekonomik modeli sürdürürken madencilerin güvenliği (saldırı maliyetiyle ölçülen) artırması için gelir artırma yeteneğine sahiptir.

Çok varlıklı platformlar için, bu gereksinimi karşılamak çok daha zor hale geliyor çünkü "değer", yerel tokenların ötesinde kripto varlıklarla ifade edilebilir. Platform tarafından güvence altına alınan kripto varlıkların değeri artar ancak ağ güvenliği artmazsa, platformda depolanan kripto varlıkları iki katına çıkarmak için platformun mutabakat sürecine saldırmak daha karlı hale gelir.

Çok varlıklı bir akıllı sözleşme platformunun bir değer deposu olarak işlev görmesi için, bir ağın varlıklarının değerindeki büyümeyi, temel güvenliğiyle uyumlu hale getirmek için uygun teşviklerin uygulamaya konması gerekir. Veya başka bir deyişle, platformun yerel tokeni, platformun toplam varlık değerinin iyi bir değeri olmalıdır. Bir platformun yerel tokeninin gerçek değeri, işlem ücreti ödemesiyle sınırlıysa, değeri, varlık depolama talebi yerine yalnızca işlem talebi tarafından belirlenir.

Bir değer deposu olarak işlev görecek şekilde tasarlanmamış akıllı sözleşme platformları, devam eden güvenliğini desteklemek için yerel tokenin parasal değerine (insanların tokenleri gerçek değerlerinin ötesinde tutma isteği) güvenmek zorundadır. Bu, yalnızca bir platformun başka bir yerde bulunamayan benzersiz özelliklere hâkim olması veya mümkün olan en düşük işlem maliyetini sunarak diğerleriyle rekabet etmesi durumunda mümkündür.

Ethereum şu anda böyle bir hakimiyete sahip ve bu nedenle parasal primini koruyabilir. Bununla birlikte, birçoğu daha yüksek TPS için tasarlanmış ve benzer işlevsellik sağlayan rakip platformların yükselişiyle, özellikle yerel tokenların açıkça tasarlanmadığı veya inanılmadığı takdirde, tek başına parasal bir prime güvenmenin bir blokzincir platformunun güvenliğini sağlayıp sağlayamayacağı açık bir sorudur. Para olmak ayrıca, bir platform benzersiz özellikler sağlasa bile, parasal değeri kullanıcı arabirimi tarafından verimli takaslar yoluyla soyutlanabilir (büyük olasılıkla sonuçta blok zinciri kitlesel olarak benimsendiğinde). Kullanıcılar, Bitcoin veya istikrarlı madeni paralar gibi en aşina oldukları varlıkları tutar ve işlem ücretlerini ödemek için tam zamanında platform tokenlarını alır. Her iki durumda da bir platformun kripto ekonomisinin temeli çökecektir.

Katman 1 çok varlıklı platformlar, güvenceye aldıkları tüm kripto varlıklar için sürdürülebilir güvenlik sağlamalıdır. Başka bir deyişle, bir değer saklama aracı için tasarlanmış bir ekonomik modele sahip olmaları gerekir.

**2.2.5 Çekirdek Protokol Geliştirmenin Finansmanı**

Genel izinsiz blok zincirleri, halka açık birer altyapıdır. Bu sistemlerin ilk gelişimi büyük miktarda finansman gerektirir ve bir kez çalıştırıldıklarında sürekli bakım ve yükseltmeler gerektirir. Bu sistemlerin bakımını yapan özel kişiler olmadan, yıkıcı hatalar ve yetersiz çalışma riskiyle karşı karşıya kalırlar. Bitcoin ve Ethereum protokolleri, devam eden geliştirmenin finanse edilmesini sağlamak için yerel bir mekanizma sağlamaz, bu nedenle, çıkarların uyumluluğuna ve açık kaynak topluluklarına sahip işletmelerin sürekli katılımına dayanır.

Dash, devam eden geliştirmenin protokol içinde finanse edilmesini sağlamak için bir hazine kullanan ilk projeydi. Bu tasarım, protokolün gelişimini sürdürülebilir bir şekilde desteklerken, kripto para biriminin değerinin sürdürülebilirliği konusunda bir taviz veriyor. Çoğu blokzincir hazinesi gibi, bu model de uzun vadeli varlıkların değerini aşındıran enflasyona dayalı fonlamaya dayanıyor.

Nervos Ağı, temel gelişim için sürdürülebilir finansman sağlayan bir hazine modeli kullanır. Hazine fonları, kısa vadeli token sahiplerinin hedeflenen enflasyonundan gelirken, bu enflasyonun etkileri uzun vadeli token sahipleri için hafifletilir. Bu mekanizma hakkında daha fazla bilgi (4.6)'da açıklanmıştır.

**2.3 Birlikte çalışabilirlik**

Blok zincirleri arasında birlikte çalışabilirlik, sıklıkla tartışılan bir konudur ve özellikle bu zorluğun üstesinden gelmek için birçok proje önerilmiştir. Blok zincirlerindeki güvenilir işlemlerle, merkezi olmayan ekonomide gerçek ağ etkileri gerçekleştirilebilir.

Blokzincir birlikte çalışabilirliğinin ilk örneği, Bitcoin ve Litecoin arasındaki atomik takaslardı. Bitcoin'in Litecoin ile güvene dayalı olmayan değişimi ve bunun tersi, protokol içi mekanizmalar aracılığıyla değil, paylaşılan bir kriptografik standart (özellikle SHA2-256 karma işlevinin kullanımı) aracılığıyla mümkün olur.

Benzer şekilde, Ethereum 2.0'ın tasarımı, tümü aynı protokolü çalıştıran ve aynı kriptografik ilkelleri kullanan birçok parça zincirinin birbirine bağlanmasına izin verir. Bu tekdüzelik, parçalar arası iletişim için protokolü özelleştirirken değerli olacaktır, ancak Ethereum 2.0, aynı şifreleme ilkellerini kullanmayan diğer blok zincirleriyle birlikte çalışmayacaktır.

Polkadot veya Cosmos gibi blok zinciri ağları bir adım daha ileri giderek, aynı çerçeveyle (Cosmos için Cosmos SDK ve Polkadot için Substrate) inşa edilen blok zincirlerinin birbirleriyle iletişim kurmasına ve etkileşime girmesine izin verir. Bu çerçeveler, geliştiricilere kendi protokollerini oluşturma konusunda bir miktar esneklik sağlar ve her zincirin birbirinin bloklarını ayrıştırmasına ve işlemleri çapraz doğrulamasına izin vererek aynı şifreleme ilkellerinin kullanılabilirliğini sağlar. Bununla birlikte, her iki protokol de kendi çerçeveleriyle oluşturulmayan blok zincirlerine bağlanmak için köprülere veya "sabitleme bölgelerine" güvenerek ek bir güven katmanı sunar. Örneklemek gerekirse: Cosmos ve Polkadot "blok zincir ağlarını" etkinleştirse de Cosmos ve Polkadot ağları birlikte çalışacak şekilde tasarlanmamıştır.

Zincirler arası ağların kripto ekonomisi de daha fazla çalışmaya ihtiyaç duyabilir. Hem Cosmos hem de Polkadot için yerel tokenler staking, yönetim ve işlem ücretleri için kullanılır. Tek başına yerel bir token içsel değeri veremeyen (4.2.4'te tartışılan) staking tarafından getirilen kripto-ekonomik dinamikleri bir kenara bırakırsak, ekosistem değerini yakalamak için zincirler arası işlemlere güvenmek zayıf bir model olabilir. Özellikle çapraz zincir işlemleri, çoklu zincir ağlarının gücü değil, bir zayıflığıdır, tıpkı çapraz parça işlemlerinin parçalanmış veri tabanlarının bir zayıflığı olması gibi. Gecikmenin yanı sıra atomiklik ve birleştirilebilirlik kaybı da getirirler. Birbirleriyle etkileşime girmesi gereken uygulamaların, zincirler arası ek yükü azaltmak için sonunda aynı blok zincirinde ikamet etmeye, çapraz zincir işlemlerine olan talebi ve dolayısıyla yerel token talebini azaltmaya yönelik doğal bir eğilimi vardır.

Zincirler arası ağlar, ağ etkilerinden yararlanır- bir ağda ne kadar çok birbirine bağlı zincir varsa, ağ o kadar değerlidir ve ağdaki potansiyel yeni katılımcılar için o kadar çekici olur. İdeal olarak, bu değer yerel tokenlar tarafından yakalanacak ve ağın büyümesini daha da teşvik etmek için kullanılacaktır. Ancak, Polkadot gibi havuzlanmış bir güvenlik ağında, ağa katılımın daha yüksek maliyeti, ağın daha fazla değer kazanması için caydırıcı olur. Cosmos gibi gevşek bağlı bir ağda, aynı zincirler arası işlem talebini ve ücretlerini varsayarsak, staking katılımının daha yüksek maliyeti, doğrulayıcılar için beklenen getiriyi düşürür ve daha fazla staking katılımından caydırıcı etki yapar.

Nervos Network, katmanlı yaklaşımıyla aynı zamanda çok zincirli bir ağdır. Mimari olarak Nervos, gerçek özelleştirmeyi ve kullanıcı tarafından oluşturulan kriptografik ilkelleri desteklemek için hücre modelini ve düşük seviyeli bir sanal makineyi kullanır ve heterojen blok zincirlerinde birlikte çalışabilirliği sağlar (4.4.1'de ele alınmıştır). Kripto-ekonomik olarak, Nervos Network değeri (mesaj iletmek yerine) kök zincirine yoğunlaştırır. Bu mekanizma, ağ tarafından güvence altına alınan toplam değer arttıkça ağın güvenlik bütçesini yükseltir. Bu, ayrıntılı olarak (4.4)'te ele alınmıştır.

**3. Nervos Ağının Temel İlkeleri**

Nervos, merkezi olmayan ekonominin ihtiyaçlarını desteklemek için oluşturulmuş katmanlı bir ağdır. Katmanlı bir yaklaşımın bir blokzincir ağı oluşturmanın doğru yolu olduğuna inanmamızın birkaç nedeni var. Blok zinciri sistemlerinin oluşturulmasında, merkezsizliğe karşı ölçeklenebilirlik, tarafsızlığa karşı uyumlu, gizliliğe karşı açıklık, değer saklamaya karşı işlem maliyeti ve kriptografik sağlamlığa karşı kullanıcı deneyimi gibi birçok iyi bilinen pazarlık(trade-off) vardır. Tüm bu çatışmaların, tamamen zıt endişeleri tek bir blok zinciri ile ele alma girişimlerinden kaynaklandığına inanıyoruz.

Bir sistemi kurmanın en iyi yolunun, her şeyi kapsayan tek bir katman oluşturmak değil, kavramları ayrıştırmak ve farklı katmanlarda ele almak olduğuna inanıyoruz. Bunu yaparak, 1. katman blok zinciri güvenli, tarafsız, merkezi olmayan ve açık kamu altyapısı olmaya odaklanırken, daha küçük, 2. katman ağları kullanım bağlamına en uygun şekilde özel olarak tasarlanabilir.

Nervos Ağında, katman 1 protokolü (Common Knowledge Base- Ortak Bilgi Bankası), tüm ağın değer koruma katmanıdır. Felsefi olarak Bitcoin'den esinlenmiştir ve merkezi olmayan bir değer ve kripto varlık koruyucusu olarak hizmet etmek için maksimum düzeyde güvenli ve sansüre dayanıklı olacak şekilde tasarlanmış, açık, halka açık ve iş tabanlı bir blok zincirinin kanıtıdır. Katman 2 protokolleri, sınırsız ölçeklenebilirlik ve minimum işlem ücretleri sağlamak için katman 1 blok zincirinin güvenliğinden yararlanır ve ayrıca güven modelleri, gizlilik ve kesinlik açısından uygulamaya özel pazarlıklara izin verir.

İşte Nervos Network'ün tasarımına yol açan temel ilkeler:

- Sürdürülebilir, çok varlıklı bir katman 1 blok zinciri, bir değer deposu olacak şekilde kripto-ekonomik olarak tasarlanmalıdır.

- Katman 2, en iyi ölçeklendirme seçeneklerini sunarak neredeyse sınırsız işlem kapasitesi, minimum işlem maliyeti ve geliştirilmiş bir kullanıcı deneyimi sunar. Katman 1 blok zincirleri, katman 2 çözümleriyle rekabet etmek için değil, tamamlamak için tasarlanmalıdır.

- Bir Sybil direnç yöntemi olarak İş Kanıtı, katman 1 blok zincirleri için esastır.

- Katman 1 blok zinciri, etkileşimli protokoller ve blok zinciri birlikte çalışabilirliği için genel bir programlama modeli sağlamalı ve protokolün maksimum düzeyde özelleştirilebilir ve yükseltilmesi kolay olmasına izin vermelidir.

- Kaynakları en iyi şekilde tahsis etmek ve "ortak mallar trajedisinden" kaçınmak için, durum depolamasının net ve ayrıntılı bir mülkiyet modeline sahip olması gerekir. Madencilere tutarlı uzun vadeli ödüller sağlamak için (işlem talebine bakılmaksızın), durum kavramasının devam eden bir maliyeti olmalıdır.

**4. Nervos Ortak Bilgi Bankası (Common Knowledge Base)**

**4.1 Genel Bakış**

"Ortak bilgi", genellikle terimin kullanıldığı toplulukla ilgili olarak, herkes veya neredeyse herkes tarafından bilinen bilgi olarak tanımlanır. Genel olarak blok zincirleri ve özel olarak Nervos Ağı bağlamında, "ortak bilgi", küresel fikir birliği tarafından doğrulanan ve ağdaki herkes tarafından kabul edilen durumu ifade eder.

Ortak bilginin özellikleri, halka açık blokaj zincirlerinde depolanan kripto para birimini toplu olarak para olarak ele almamıza izin verir. Örneğin, Bitcoin'deki tüm adreslerin bakiyeleri ve geçmişi, Bitcoin kullanıcıları için ortak bilgidir, çünkü paylaşılan defteri bağımsız olarak çoğaltabilirler, genesis bloğundan bu yana küresel durumu doğrulayabilirler ve başkalarının da aynı şeyi yapabileceğini bilirler. Bu ortak bilgi, insanların herhangi bir üçüncü tarafa güvenmeden tamamen eşler arası(peer-to-peer) işlem yapmasına olanak tanır.

Nervos Ortak Bilgi Bankası (Common Knowledge Base: CKB), para ile sınırlı olmamak üzere her türlü ortak bilgiyi depolamak için tasarlanmıştır. Örneğin, CKB, misli ve değiştirilemeyen tokenlar (fungible and non-fungible tokens) gibi kullanıcı tanımlı kripto varlıklarının yanı sıra ödeme kanalları (5.2) ve taahhüt zincirleri (5.4) gibi daha yüksek katmanlı protokoller için güvenlik sağlayan değerli kriptografik kanıtları depolayabilir.

Hem Bitcoin hem de Nervos CKB, ortak bilgi depolama ve doğrulama sistemleridir. Bitcoin, küresel durumunu UTXO (unspent transaction output, harcanmamış işlem çıktısı) seti olarak saklar ve işlemlere gömülü kodlanmış kurallar ve betikler aracılığıyla durum geçişlerini doğrular. Nervos CKB, Bitcoin'in veri yapısını ve komut dosyası oluşturma yeteneklerini genelleştirir, küresel durumu etkin programlanabilir hücreler kümesi olarak depolar ve sanal bir makinede çalışan kullanıcı tanımlı, Turing-complete komut dosyaları aracılığıyla durum geçişlerini doğrular.

Nervos CKB, Ethereum ve diğer platformlarınki gibi tam akıllı sözleşme yeteneklerine sahipken, ekonomik modeli, merkezi olmayan hesaplama için ödeme yapmak yerine ortak bilgi koruması için tasarlanmıştır.

**4.2 Konsensüs (Consensus)**

Bitcoin'in Nakamoto Konsensüsü (NC), basitliği ve düşük iletişim yükü nedeniyle iyi karşılandı. Bununla birlikte, NC'nin iki dezavantajı vardır: 1) işlem işleme hacmi tatmin edici olmaktan uzaktır ve 2) saldırganların protokolün öngördüğü davranıştan saparak ek blok ödülleri kazanabilecekleri bencil madencilik saldırılarına karşı savunmasızdır.

CKB mutabakat protokolü, NC'nin performans sınırını ve bencil madencilik direncini artırırken avantajlarını koruyan bir çeşididir. NC'nin blok yayılma gecikmesindeki darboğazı tanımlayıp ortadan kaldıran protokolümüz, güvenlikten ödün vermeden çok kısa blok aralıklarını destekler. Kısaltılmış bir blok aralığı yalnızca verimi artırmakla kalmaz, aynı zamanda işlem onay gecikmesini de azaltır. Tüm geçerli blokları zorluk ayarlama hesaplamasına dahil ederek, bencil madencilik artık protokolümüzde karlı değildir.

**4.2.1 Artan Verim**

Nervos CKB, Nakamoto Consensus'tan türetilen bir konsensüs algoritması ile PoW konsensüsünün verimini artırır. Algoritma, ağ genelinde bağlantının bir ölçümü olarak blok zincirinin yetim oranını (orphan rate) (kanonik zincirin parçası olmayan geçerli blokların yüzdesi) kullanır.

Protokol, sabit bir yetim oranını hedefliyor. Düşük yetim oranına yanıt olarak hedef zorluğu azaltılır (blok üretim hızı artırılır) ve yetim oranı tanımlanmış bir eşiği geçtiğinde hedef zorluğu artırılır (blok üretim hızı azaltılarak).

Bu, ağın tüm bant genişliği yeteneklerinin kullanılmasına izin verir. Düşük yetim oranı, ağın iyi bağlandığını ve daha fazla veri iletimini kaldırabileceğini gösterir; protokol daha sonra bu koşullar altında verimi artırır.

**4.2.2 Blok Yayılım Darboğazının Ortadan Kaldırılması**

Herhangi bir blokzincir ağındaki darboğaz, blok yayılımıdır. Nervos CKB mutabakat protokolü, işlem onayını iki adımlı bir süreçte değiştirerek blok yayma darboğazını ortadan kaldırır: 1) teklif et ve 2) onay ver.

Bir işlem önce bir bloğun (veya amca bloklardan birinin) "teklif bölgesinde" önerilmelidir. İşlem, teklifini takip eden tanımlı bir pencerede bir bloğun "onay bölgesinde" görünürse onaylanacaktır. Yeni bir bloğun onaylanan işlemleri önerildiğinde tüm düğümler tarafından zaten alınmış ve doğrulanmış olacağından, bu tasarım blok yayma darboğazını ortadan kaldırır.

**4.2.3 Bencil Madencilik Saldırılarını Azaltma**

Nakamoto Consensus'a yönelik en temel saldırılardan biri bencil madenciliktir. Bu saldırıda, kötü niyetli madenciler, başkaları tarafından çıkarılan blokları kasten yetim bırakarak haksız blok ödülleri kazanır.

Araştırmacılar, haksız kazanç fırsatının, ağın bilgi işlem gücünü tahmin ederken yetim blokları ihmal eden Nakamoto Consensus'un zorluk ayarlama mekanizmasından kaynaklandığını gözlemliyor. Bu, daha düşük madencilik zorluğuna ve daha yüksek zaman ortalamalı blok ödüllerine yol açar.

Nervos CKB konsensüs protokolü, zorluk ayarlama hesaplamasına amca bloklarını dahil ederek bencil madenciliği artık karlı olmaktan çıkarır. Bu, saldırı stratejisi veya süresinden bağımsız olarak geçerlidir; bir madenci, dürüst ve bencil madenciliğin herhangi bir bileşimi yoluyla haksız ödüller kazanamaz.

Analizimiz, iki adımlı bir işlem onay süreci ile fiili bencil madenciliğin de sınırlı bir saldırı süresi penceresi aracılığıyla ortadan kaldırıldığını gösteriyor.

Mutabakat protokolümüzün ayrıntılı bir şekilde anlaşılması için lütfen [buradan](https://github.com/nervosnetwork/rfcs/blob/master/rfcs/0020-ckb-consensus-protocol/0020-ckb-consensus-protocol.md) okuyun

**4.2.4 İş İspatı (Proof-of-Work) ve Hisse İspatı (Proof-of-Stake)**

Proof of Work (PoW) ve Proof of Stake (PoS) sistemlerinin her ikisi de güç yoğunlaşmalarına karşı savunmasızdır, ancak sistemlerin nitelikleri, iktidardakiler için çok farklı işletim gerçeklikleri sağlar.

PoW madenciliği, titiz bir maliyet denetimi olmadan madencilik gelirlerini aşabilecek gerçek dünya harcamalarına neden olur. İktidardakilerin yenilikçi kalmaları, sağlam iş stratejileri izlemeleri ve hakimiyetlerini sürdürmek için altyapıya yatırım yapmaya devam etmeleri gerekiyor. Madencilik ekipmanı, maden havuzu işlemleri ve ucuz enerjiye erişim, teknolojik yeniliklerden kaynaklanan değişikliklere tabidir. Üçünün de tekelleşmesini uzun süreler boyunca sürdürmek zordur.

Buna karşılık, PoS sistemlerindeki blok oluşturucular, çok düşük operasyonel sermaye gereksinimleriyle, yatırılan miktara dayalı olarak belirleyici bir şekilde ödüllendirilir. Sistem büyüdükçe, ilk hareket eden işletmelere ve bireylere sağlanan doğal avantajların etkisi de artacaktır. Bir PoS sisteminde, gücün birkaç pay sahibinin elinde toplanması mümkündür. PoW sistemlerinin madencilik konsantrasyonuyla ilgili benzer bir sorunu olsa da bir PoS sisteminde güçte kalma maliyeti önemli ölçüde daha düşüktür.

Ek olarak, PoS doğrulayıcılarının benzersiz bir gücü vardır: doğrulayıcı setinin kontrolü. Bir doğrulayıcının konsensus grubuna katılmasına izin veren bir işlemin kabulü, mevcut doğrulayıcıların elindedir. Doğrulayıcı setini işlem sansürü ve talimat manipülasyonu yoluyla etkilemeye yönelik gizli anlaşma çabalarını tespit etmek ve cezalandırmak zor olacaktır. Tersine, PoW sistemlerinde konsensüs katılımı gerçekten açıktır ve mevcut güç yapısına tabi değildir. Avantajlar sistemin erken katılımcılarına verilmez.

Token ekonomisi ile ilgili olarak, staking'in getiri elde etmek (ve dolayısıyla yerel token'a olan talebi artırmak) isteyen sermayeyi çekebileceğine inanılırken, resmin tamamı bu değil. Tüm PoS projeleri sonunda staking oranlarının sabitlendiğini görecek ve bu durumda stake edilen sermaye havuzuna giren ve ayrılan sermaye kabaca aynı olacaktır. Staking mekanizması kendi başına yerel token talebini artırmayacaktır. Başka bir deyişle, bir projenin ilk aşamasında (staking oranı yükseldikçe) staking'in tanıtılması yerel token için talep sağlasa da staking tek başına yerel token için uzun vadeli talep sağlayamaz ve bu nedenle yerel bir tokenin tek gerçek değeri olamaz.

Bir PoS sistemindeki uzun vadeli token sahiplerinin 3 seçeneği vardır: 1) yeni düzenleme almak için altyapıyı yönetebilir ve kendi başlarına bir doğrulama düğümü çalıştırabilirler, 2) tokenlerini üçüncü bir tarafa devredebilir ve onların bütünlüğüne ve altyapısına güvenebilirler veya 3) devam eden ihraçla seyreltilmiş tokenların değerine sahiptir. Bu seçeneklerin hiçbiri, özellikle uzun vadeli, değer deposu odaklı token sahipleri için çekici değildir.

PoW'un izinsiz katılımının, küresel ekonomik faaliyetin temelindeki altyapı için bir gereklilik olduğuna inanıyoruz. Katman 1'in en önemli amacı, blok zincirinin mümkün olduğunca merkezi olmayan, güvenli ve tarafsız olmasını sağlamaktır. PoS sistemlerinin merkezi olmayan ekonomide oynayacağı bir rol olsa da bize göre gerçekten açık ve merkezi olmayan bir katman 1'in gereksinimlerini karşılamıyorlar.

**4.2.5 4 İş İspatı (Proof-of-Work) Fonksiyonu**

Nervos CKB blokları, 1) bloğun geçerli olması ve 2) teklif sahibi, çalışma kanıtı(proof-of-work) adı verilen hesaplama açısından zor bir bulmacayı çözmüştür. Çalışma kanıtı(proof-of-work) bulmacası, önerilen blok açısından tanımlanır; bu, bulmacanın çözümünün bir bloğu benzersiz bir şekilde tanımlamasını garanti eder.

Bitcoin'in çalışma kanıtı(proof-of-work), blok başlığına bir hash işlevi uygulamanın sonucunun belirli bir zorluk seviyesini karşılayacağı şekilde geçerli bir nonce bulmayı gerektirir. Bitcoin için hash işlevi iki kez yinelenen SHA2–256'dır. SHA2 Bitcoin için iyi bir seçim olsa da ondan sonra gelen kripto paralar için aynı şey geçerli değil. Bitcoin madenciliği için büyük miktarda özel donanım geliştirildi, bunların büyük bir kısmı verimlilik iyileştirmeleri nedeniyle geçersiz hale getirildi.

Aynı çalışma kanıtı bulmacasını kullanan yeni bir kripto para birimi, bu kullanımdan kaldırılmış donanımı bir kez daha kullanışlı hale getirecektir. Güncel donanım bile kiralanabilir ve yeni bir madeni para madenciliği yapmak için yeniden kullanılabilir. SHA2 tabanlı bir madeni para için madencilik gücünün dağılımını tahmin etmek çok zor olacak ve ani ve büyük değişikliklere karşı hassas olacaktır. Bu argüman ayrıca, fonksiyonun yazılım hesaplamasını daha ucuz hale getirmek için geliştirilmiş olan SHA2'ye uyarlanmış algoritmik optimizasyonlar için de geçerlidir.

Yeni bir kripto para birimi için, çalışma kanıtı bulmacasını henüz diğer kripto para birimleri tarafından kullanılmayan bir işlev açısından tanımlamak mantıklıdır. Nervos CKB için bir adım daha ileri gittik ve yeni olduğu için erken optimizasyonun konusu olamayacak bir çalışma kanıtı işlevi olarak tanımlamayı seçtik.

Bununla birlikte, madencilik donanımının amaçlanan kullanılamaması yalnızca başlangıçta geçerlidir. Uzun vadede, özel madencilik donanımının konuşlandırılması faydalıdır ve ağa saldırmanın zorluklarını önemli ölçüde artırır. Bu nedenle, yeni olmasının yanı sıra, yeni bir kripto para birimi için ideal bir çalışma kanıtı işlevi de basittir ve donanım geliştirme engelini önemli ölçüde azaltır.

Güvenlik, bariz üçüncü tasarım hedefidir. Bilinen bir güvenlik açığı tüm madenciler tarafından eşit şekilde kullanılabilir ve yalnızca daha yüksek bir zorlukla sonuçlanabilirken, açıklanmayan bir güvenlik açığı keşfeden (ler)e katkıda bulundukları madencilik gücü payını aşan bir avantaj sağlayan bir madencilik optimizasyonuna yol açabilir. Bu durumdan kaçınmanın en iyi yolu, dokunulmazlık için güçlü bir argüman yapmaktır.

**4.2.6 Eaglesong**

Eaglesong, Nervos CKB çalışma kanıtı için özel olarak geliştirilmiş yeni bir sağlama işlevidir, ancak güvenli bir sağlama işlevinin gerekli olduğu diğer kullanım durumlarında da uygundur. Tasarım kriterleri tam olarak yukarıda listelendiği gibiydi: yenilik, sadelik ve güvenlik. Aynı anda hem bilim için ileriye doğru küçük bir adım oluşturacak kadar yeni hem de güçlü bir güvenlik argümanı oluşturacak mevcut tasarımlara yeterince yakın bir tasarım istiyorduk.

Bu amaçla, sünger yapısını (Keccak/SHA3'te kullanıldığı gibi) ARX işlemlerinden (addition, rotation, and xor; toplama, döndürme ve xor) oluşturulan bir permütasyonla somutlaştırmayı seçtik; güvenliğine ilişkin argüman, geniş iz stratejisine dayanmaktadır (AES'in (Advanced Encryption Standard) altında yatan aynı argüman).

Bildiğimiz kadarıyla Eaglesong, üç tasarım ilkesini başarıyla birleştiren ilk hash fonksiyonudur (veya bu konudaki ilk fonksiyondur).

Eaglesong hakkında daha fazla bilgiyi [buradan](https://medium.com/nervosnetwork/the-proof-of-work-function-of-nervos-ckb-3cc8364464d9) okuyabilirsiniz:

**4.3 Hücre Modeli:**

Nervos CKB, UTXO modelinin (Bitcoin'de kullanılan) varlık mülkiyetini ve kanıta dayalı doğrulama özelliklerini korurken, Hesap modelinin (Ethereum'da kullanılan) birçok avantajını sağlayabilen yeni bir yapı olan Hücre Modelini kullanır.

Hücre modeli duruma odaklanır. Hücreler, token miktarı ve sahibi gibi basit veya bir token aktarımı için doğrulama koşullarını belirten kod gibi daha karmaşık olabilen isteğe bağlı veriler içerir. CKB'nin durum makinesi, bir durum geçişinin bütünlüğünü sağlamak için hücrelerle ilişkili komut dosyalarını yürütür.

Hücreler, kendi verilerini depolamanın yanı sıra diğer hücrelerdeki verilere de başvurabilir. Bu, kullanıcıya ait varlıkların ve onları yöneten mantığın ayrılmasını sağlar. Bu durum, akıllı sözleşmenin dahili mülkiyeti olduğu ve akıllı sözleşme arayüzleri aracılığıyla erişilmesi gereken hesap tabanlı akıllı sözleşme platformlarının zıttıdır. Nervos CKB'de hücreler, sahip olunan bağımsız durum nesneleridir ve doğrudan başvurulabilir ve etrafa aktarılabilir. Hücreler, durum geçişlerinin bütünlüğünü sağlayan mantığı tutan bir hücreye atıfta bulunurken, sahiplerine ait gerçek "katlanılabilir varlıkları" ifade edebilir (UTXO'ların Bitcoin sahipleri için katlanılabilir varlıklar olması gibi).

Hücre modeli işlemleri aynı zamanda durum geçiş kanıtlarıdır. Bir işlemin girdi hücreleri etkin hücreler kümesinden çıkarılır ve çıktı hücreleri kümeye eklenir. Aktif hücreler, Nervos CKB'nin genel durumunu içerir ve değişmezdir: hücreler oluşturulduktan sonra değiştirilemezler.

Cell modeli uyarlanabilir, sürdürülebilir ve esnek olacak şekilde tasarlanmıştır. Genelleştirilmiş bir UTXO modeli olarak tanımlanabilir ve kullanıcı tanımlı tokenleri, akıllı sözleşmeleri ve çeşitli katman 2 protokollerini destekleyebilir.

Hücre Modelini daha iyi anlamak için lütfen [buradan](https://medium.com/nervosnetwork/https-medium-com-nervosnetwork-cell-model-7323fca57571) okuyun:

**4.4 Sanal Makine (Virtual Machine)**

Birçok yeni nesil blokzincir projesi, bir blokzincir sanal makinesinin temeli olarak WebAssembly'yi kullanırken, Nervos CKB, RISC-V komut setine dayalı benzersiz bir sanal makine (CKB-VM) tasarım seçeneğini içerir.

RISC-V, yeni donanım ve yazılımların geliştirilmesini kolaylaştırmak için 2010 yılında oluşturulan açık kaynaklı bir RISC komut seti mimarisidir ve telifsiz, geniş çapta anlaşılan ve geniş ölçüde denetlenen bir komut setidir.

RISC-V'yi bir blokzincir bağlamında kullanmanın sayısız avantajı vardır:

- Kararlılık: RISC-V temel komut seti, nihai hale getirildi ve donduruldu, ayrıca geniş çapta uygulandı ve test edildi. Çekirdek RISC-V komut seti sabittir ve hiçbir zaman güncelleme gerektirmez.

- Açık ve Desteklenen: RISC-V, bir BSD lisansı altında sağlanır ve geliştirilmekte olan Rust ve Go dil uygulamaları ile GCC ve LLVM gibi derleyiciler tarafından desteklenir. RISC-V Vakfı, talimat setinin geliştirilmesini ve desteklenmesini ilerleten 235'ten fazla üye kuruluş içerir.

- Basitlik ve Genişletilebilirlik: RISC-V komut seti basittir. 64-bit tamsayı desteği ile set sadece 102 komut içerir. RISC-V ayrıca, yüksek performanslı kriptografik algoritmalar için vektör hesaplama veya 256 bit tamsayılar olasılığını mümkün kılan, genişletilmiş komut setleri için modüler bir mekanizma sağlar.

- Doğru Kaynak Fiyatlandırması: RISC-V komut seti, fiziksel bir CPU üzerinde çalıştırılabilir ve her bir talimatın yürütülmesi için gereken makine döngüleri için ve sanal makine kaynak fiyatlandırması için doğru bir tahmini sağlar.

CKB-VM, esnek, Turing-complete hesaplamaya izin veren düşük seviyeli bir RISC-V sanal makinesidir. Yaygın olarak uygulanan ELF formatının kullanılmasıyla, CKB-VM scriptleri, RISC-V yönergelerine göre derlenebilen herhangi bir dille geliştirilebilir.

**4.4.1 CKB-VM ve Hücre Modeli:**

Devreye alındıktan sonra, mevcut genel blok zincirleri aşağı yukarı sabittir. Kriptografik ilkel öğeler gibi temel öğelerin yükseltilmesi ya çok yıllık taahhütleri gerektirir ya da basitçe imkansızdır.

CKB-VM bir adım geri atıyor ve daha önce özel VM'lerde yerleşik olan ilkelleri sanal makinenin üstündeki hücrelere taşıyor. CKB betikleri, Ethereum'daki akıllı sözleşmelerden daha düşük seviyeli olsa da ilerleyen merkezi olmayan ekonomi için duyarlı bir platform ve temel sağlayan esnekliğin büyük faydasını taşırlar.

Hücreler yürütülebilir kodu depolayabilir ve diğer hücrelere bağımlılık olarak başvurabilir. Neredeyse tüm algoritmalar ve veri yapıları, hücrelerde depolanan CKB scriptleri olarak uygulanır. VM'yi olabildiğince basit tutarak ve program depolamasını hücrelere boşaltarak, anahtar algoritmaları güncellemek, algoritmayı yeni bir hücreye yüklemek ve mevcut referansları güncellemek kadar basittir.

**4.4.2 CKB-VM'de Diğer Sanal Makineleri Çalıştırma**

CKB-VM'nin düşük seviyeli doğası ve RISC-V topluluğundaki araçların kullanılabilirliği sayesinde, diğer VM'leri (Ethereum'un EVM'si gibi) doğrudan CKB-VM'ye derlemek kolaydır. Bunun birkaç avantajı vardır:

- Diğer sanal makinelerde çalışan özel dillerde yazılmış akıllı sözleşmeler, CKB-VM'de çalışacak şekilde kolayca taşınabilir. (Açıkçası, CKB-VM içinde çalışmak üzere derlenmiş kendi sanal makinelerinde çalışıyor olacaklardı.)

- Durum geçişlerinin kuralları CKB-VM dışında bir sanal makinede çalışacak şekilde yazılmış olsa bile, CKB, katman 2 işlemlerinin uyuşmazlık çözümü durum geçişlerini doğrulayabilir. Bu, güvenilir olmayan katman 2 genel amaçlı yan zincirleri desteklemek için temel gereksinimlerden biridir.

CKB-VM'nin teknik incelemesi için lütfen [buradan](https://medium.com/nervosnetwork/an-introduction-to-ckb-vm-9d95678a7757) okuyun

**4.5 Ekonomik Model**

Nervos CKB'nin yerel tokeni "Common Knowledge Byte- Ortak Bilgi Baytı" veya kısaca CKByte'dır. CKBytes, bir token sahibine blok zincirinin toplam durum depolamasının bir kısmını işgal etme hakkı verir. Örneğin, 1000 CKByte tutan bir kullanıcı, 1000 bayt kapasiteli bir hücre veya kapasite olarak 1000 bayta kadar birden çok hücre oluşturabilir.

Verileri CKB'de depolamak için CKByte kullanmak, CKByte sahipleri için bir fırsat maliyeti yaratır; ikincil düzenlemenin bir kısmını almak için işgal edilen CKByte'ları NervosDAO'ya yatıramazlar. CKByte'lar piyasa fiyatına sahiptir ve bu nedenle, genişleyen durumun yüksek talebini karşılamak için kullanıcıların durum depolamasını gönüllü olarak serbest bırakmaları için ekonomik bir teşvik sağlanır. Bir kullanıcı durum depolamasını serbest bıraktıktan sonra, verilerinin kapladığı durum boyutuna (bayt olarak) eşdeğer miktarda CKByte alacaktır.

CKB'nin ekonomik modeli, düşük bir katılım engelini koruyarak ve ademi merkeziyetçiliği sağlayarak, yerel tokenlerin bağlı durum büyümesi verilmesine izin verir. CKByte'lar kıt bir kaynak haline geldikçe, en verimli şekilde fiyatlandırılabilir ve tahsis edilebilirler.

Nervos Network'ün başlangıç bloğu 33,6 milyar CKByte içerecek ve bunun 8,4 milyarı hemen yakılacak. CKBytes'in yeni yayımı iki bölümden oluşur- temel ihraç ve ikincil ihraç. Temel ihraç, Bitcoin'e benzer bir ihraç programı ile sınırlı bir toplam tedarikle (33,6 milyar CKByte) sınırlıdır. Blok ödülü, 0 yeni düzenlemeye ulaşana kadar yaklaşık olarak her 4 yılda bir yarıya iner. Tüm baz ihraçları, ağı korumaya yönelik teşvikler olarak madencilere verilir. İkincil ihraç, yılda 1,344 milyar CKByte sabit bir ihraç oranına sahiptir ve durum depolaması için bir fırsat maliyeti empoze etmek üzere tasarlanmıştır. Baz ihraç durdurulduktan sonra sadece ikincil ihraç yapılacaktır.

Nervos CKB, ikincil ihracın etkilerine karşı “enflasyon sığınağı” işlevi gören NervosDAO adlı özel bir akıllı sözleşme içerir. CKByte sahipleri, tokenlerini NervosDAO'ya yatırabilir ve ikincil ihracın enflasyonist etkilerini tam olarak dengeleyen bir ikincil ihracın bir kısmını alabilir. Uzun vadeli token sahipleri için, tokenlerini NervosDAO'da kilitledikleri sürece, ikincil ihracın enflasyonist etkisi yalnızca nominaldir. İkincil ihracın etkilerinin hafifletilmesiyle, bu kullanıcılar, Bitcoin gibi üst limitli tokenleri etkili bir şekilde ellerinde tutabilirler.

CKByte'lar durumu depolamak için kullanılırken, NervosDAO aracılığıyla ikincil düzenleme ödüllerini kazanmak için kullanılamazlar. Bu, ikincil ihracın sabit bir enflasyon vergisi veya durum depolama işgalinde "durum kirası" olmasını sağlar. Bu ekonomik model, işgalin hem yeri hem de zamanı ile orantılı olarak durum depolama ücretlerini empoze eder. Diğer platformların kullandığı "Bir kere öde sonsuza kadar kullan" modelinden daha sürdürülebilir, açık ödeme gerektiren diğer durum kira çözümlerinden daha uygulanabilirdir ve kullanıcı dostudur.

Madencilere hem blok ödülleri hem de işlem ücretleri ödenir. Blok ödülleri için, bir madenci bir blok çıkardığında, bloğun tam temel düzenleme ödülünü ve ikincil ihracın bir kısmını alır. Bu kısım, durum işgaline dayanmaktadır, örneğin: tüm yerel tokenlerin yarısı durumu depolamak için kullanılıyorsa, bir madenci blok için ikincil düzenleme ödülünün yarısını alacaktır. İkincil ihraçların dağılımına ilişkin ek bilgiler bir sonraki bölümde (4.6) yer almaktadır. Uzun vadede, baz düzenleme durduğunda madenciler, işlemlerden bağımsız ancak Nervos Ortak Bilgi Bankası'nın benimsenmesine bağlı olan "durum kirası" gelirini almaya devam edecektir.

Bir benzetmede, CKByte'lar arazi olarak düşünülebilirken, CKB'de depolanan kripto varlıklar evler olarak düşünülebilir. Bir ev inşa etmek için arazi gerekir ve varlıkları CKB'de depolamak için CKByte'lar gerekir. Varlıkları CKB'de depolama talebi arttıkça, CKByte'lara olan talep de artar. Depolanan varlıkların değeri arttıkça, CKByte'ların değeri de artar.

Nervos CKB, çok sayıda varlığa yönelik talebi tek bir varlığa yönelik talebe çevirmek ve bunu, ağı güvence altına almak için madencileri telafi etmek için kullanmak üzere tasarlanmıştır.

Ekonomik model hakkında daha ayrıntılı açıklama için lütfen [buradan](https://github.com/nervosnetwork/rfcs/blob/master/rfcs/0015-ckb-cryptoekonomiks/0015-ckb-cryptoekonomiks.md) okuyun.

**4.6 Hazine**

1) madencilere veya 2) NervosDAO'da kilitli tokenleri olan uzun vadeli sahiplere gitmeyen ikincil ihraç kısmı bir hazine fonuna gidecektir. Göstermek için: verilen CKByte'ların %60'ı durumu depolamak için kullanılıyorsa ve CKByte'ların %30'u NervosDAO'ya yatırılırsa, madenciler ikincil verilimin %60'ını alacak, NervosDAO (uzun vadeli sahipleri) ise ikinci ihracın %30'unu alacak, ikincil ihracın %10'u da hazineye gidecektir.

Hazine fonu, protokolün devam eden araştırma ve geliştirme çalışmalarının yanı sıra Nervos Ağı ekosistemini oluşturmak için kullanılacaktır. Hazine fonlarının kullanımı herkesin görebileceği şekilde açık, şeffaf ve zincir içinde olacaktır. Enflasyona dayalı bir hazine fonlama modeliyle karşılaştırıldığında, bu model uzun vadeli token sahiplerini (tokenlerini NervosDAO'ya yatıran) seyreltilmez. Protokol geliştirmenin finansmanı, kesinlikle kısa vadeli token sahiplerine yönelik fırsat maliyetinden elde edilir.

Hazine, Nervos Ortak Bilgi Bankası'nın ana ağ lansmanından hemen sonra etkinleştirilmeyecek. Topluluğun onayı ile daha sonra, ancak Nervos Vakfı Genesis bloğunda yer alan Ekosistem Fonunu tükettikten sonra bir hard-fork ile etkinleştirilecektir. Hazinenin etkinleştirilmesinden önce, ikincil ihracın bu kısmı yakılacaktır.

**4.7 Yönetişim (Governance)**

Yönetişim, toplum veya içindeki grupların karar almak için nasıl organize olduklarıdır. Sistemde çıkarı olan ilgili her taraf bu sürece dahil olmalıdır. Bir blok zinciri ile ilgili olarak, bu sadece kullanıcıları, sahipleri, madencileri, araştırmacıları ve geliştiricileri değil aynı zamanda cüzdanlar, borsalar ve madencilik havuzları gibi hizmet sağlayıcıları da içermelidir. Çeşitli paydaş gruplarının farklı çıkarları vardır ve herkesin teşviklerini uyumlu hale getirmek neredeyse imkansızdır. Bu nedenle blokzincir yönetişimi karmaşık ve tartışmalı bir konudur. Bir blok zincirini büyük bir sosyal deney olarak düşünürsek, yönetişim, sistemin diğer herhangi bir parçasından daha karmaşık bir tasarım gerektirir. On yıllık evrimin ardından, hala blok zincir yönetişimi için genel en iyi uygulamaları veya sürdürülebilir süreçleri belirleyemedik.

Bazı projeler yönetişimi "yaşam için hayırsever bir diktatör" aracılığıyla yürütür (Linus Torvalds'ın Linux'u gibi). Bunun bir projeyi son derece verimli, uyumlu ve çekici kıldığını kabul ediyoruz: insanlar kahramanları sever; ancak bu, blok zincirinin temel değeri olan ademi merkeziyetçilikle çelişir.

EOS üzerindeki ECAF (EOSIO Core Arbitration Forum: EOSIO Temel Tahkim Forumu) gibi bazı projeler, geniş kapsamlı karar verme yetkisini seçkin bir zincir dışı komitesine emanet eder. Ancak bu komiteler, katılımcıların bu yılın başlarında ECAF'ın kapatılması kararında rol oynayabilecek olan kararlarına uyacaklarını garanti edecek temel güce sahip değiller.

Tezos gibi bazı projeler daha da ileri gider ve tüm katılımcıların oylanan kararlara uymasını sağlamak için zincir içi yönetişim uygular. Bu aynı zamanda geliştiriciler ve madenciler (veya tam düğüm kullanıcıları) arasındaki herhangi bir anlaşmazlığın etkisini de önler. Zincir içi yönetişimin basit bir zincir içi oylamadan farklı olduğunu unutmayın; önerilen bir özellik veya yama, zincir içi yönetişim yoluyla yeterli oy aldıysa, zincir kodu otomatik olarak güncellenir, madencilerin veya tam düğümlerin bu değişikliği kontrol edebilmesinin herhangi bir yolu yoktur. Polkadot, seçmen katılımını hesaba katmak için seçilmiş bir konsey, hisse ağırlıklı oylama için referandum süreci ve olumlu/olumsuz önyargı mekanizmalarından yararlanarak zincir içi yönetişime daha da sofistike bir yaklaşım getiriyor.

Bununla birlikte, basitliğine rağmen, pratikte zincir içi yönetişimi sunulduğu kadar zarif değildir. Her şeyden önce, oylar yalnızca token sahiplerinin çıkarlarını yansıtırken, diğer tüm tarafları göz ardı eder. İkincisi, düşük oy oranı hem blokzincir dünyasında hem de gerçek dünyada uzun süredir devam eden bir sorundur. Yalnızca bir azınlık oy veriyorsa, sonuçlar nasıl çoğunluğun çıkarına olabilir? Son olarak, ancak en önemlisi, bir hard fork her zaman tüm paydaşlar için nihai başvuru olarak düşünülmelidir. İzinsiz bir blok zincirinin geniş çapta kopyalanmasının sağladığı mükemmel veri kullanılabilirliği göz önüne alındığında, mevcut zincirden tam veri korumasıyla ve kesintisiz olarak ayrılmak her zaman bir seçenek olmalıdır. Zincir içi yönetişim yoluyla bir hard fork asla uygulanamaz.

Yönetişim sorularına henüz uygulanabilir yanıtlar yok, bu nedenle Nervos Network için gelişen bir yaklaşım benimseyeceğiz. Topluluğun ilk günlerde ve zaman içinde organik olarak gelişmesini bekliyoruz, daha fazla token çıkarıldıkça, madencilik daha dağıtık hale geldikçe ve daha fazla geliştirici devreye girdikçe, yönetişim sorumlulukları giderek daha merkezi olmayan hale gelecektir. Uzun vadede, topluluk tabanlı yönetişim, protokol yükseltme sürecini ve hazineden kaynak tahsisini yönetecektir.

Nervos CKB, yüzlerce yıl sürebilecek merkezi olmayan özerk bir altyapı olacak şekilde tasarlanmıştır; bu, bu ağ nasıl gelişirse gelişsin, bir topluluk olarak gerçek olması için elimizden gelenin en iyisini yapmamızı gerektiren belirli şeyler olduğu anlamına gelir. 3 temel değişmez şunlardır:

- İhraç planı tamamen sabittir, bu nedenle asla değişmez.

- Hücrelerde depolanan durum/veriler kurcalanmamalıdır.

- ‘Mevcut scriptlerin‘anlamı değiştirilmeyecektir.

Blok zincirleri için topluluk tabanlı yönetişim çok yeni bir alandır ve devam etmekte olan birçok değerli deney vardır. Bunun önemsiz bir konu olmadığının ve en uygun yaklaşıma ulaşmak için tam olarak çalışmak, gözlemlemek ve yinelemek için zaman gerektiğinin farkındayız. Kısa vadede topluluk temelli yönetişime muhafazakar bir yaklaşım benimserken, uzun vadede bu yöne tamamen bağlı kalıyoruz.

**5. Katman 2 Çözümlerine Genel Bakış**

**5.1 Katman 2 Nedir?**

Bir blokzincir ağının 1. katmanı kısıtlamalarla tanımlanır. İdeal bir 1. katman blok zinciri, güvenlik, ademi merkeziyetçilik ve sürdürülebilirlikten ödün vermez, ancak bu, ölçeklenebilirlik ve işlem maliyetleri ile ilgili zorluklar yaratır. Katman 2 çözümleri, katman 1 protokollerinin üzerine inşa edilmiştir ve hesaplamanın, katman 1 blok zincirine güvenli bir şekilde yerleşmek için mekanizmalarla zincir dışına taşınmasına izin verir.

Bu, bugünün bankacılık sistemindeki net yerleşime veya SEC tarafından zorunlu tutulan düzenleyici dosyalamalara benzer. Ağ, küresel mutabakat gerektiren veri miktarını azaltarak, daha fazla katılımcıya hizmet edebilir ve ademi merkeziyetçilik özelliklerini korurken, başka türlü yapabileceğinden daha fazla ekonomik faaliyeti kolaylaştırabilir.

Katman 2 kullanıcıları, katman 1 blok zinciri tarafından sağlanan güvenliğe bağlıdır ve varlıkları katmanlar arasında taşırken veya bir anlaşmazlığı çözerken bu güvenliği kullanır. Bu işlev bir mahkeme sistemine benzer: mahkemenin tüm işlemleri izlemesi ve doğrulaması gerekmez, yalnızca önemli kanıtları kaydetmek ve anlaşmazlıkları çözmek için bir yer olarak hizmet eder. Benzer şekilde, bir blok zinciri bağlamında, 1. katman blok zinciri, katılımcıların zincir dışı işlem yapmasına izin verir ve bir anlaşmazlık durumunda onlara, blok zincirine kriptografik kanıt getirme ve sahtekarlığı cezalandırma yeteneği sağlar.

**5.2 Ödeme ve Durum Kanalları**

Ödeme kanalları, sıklıkla işlem yapan iki taraf arasında oluşturulur. Doğrudan küresel bir blok zincirinde yapılan işlemlerin asla sağlayamayacağı düşük gecikmeli, anında ödeme deneyimi sağlarlar. Ödeme kanalları bir bar taburesine benzer şekilde çalışır- bir barmenle bir tabure açabilir ve içecek sipariş etmeye devam edebilirsiniz, ancak yalnızca bardan ayrılmaya hazır olduğunuzda tabureyi kapatabilir ve son tutarı ödeyebilirsiniz. Bir ödeme kanalının işletilmesinde katılımcılar, bakiyelerine kriptografik taahhütler içeren mesajlar gönderirler ve bu bakiyeleri, kanalı kapatmaya ve bakiyeleri tekrar blok zincirinde kapatmaya hazır olmadan önce zincir dışında sınırsız sayıda güncelleyebilirler.

Ödeme kanalları tek yönlü veya çift yönlü olabilir. Tek yönlü ödeme kanalları, yukarıdaki bar taburesi örneğine benzer şekilde Taraf A'dan Taraf B'ye akar. A Tarafı, B Tarafına harcayabilecekleri maksimum tutarı yatırır ve ardından mal veya hizmet alırken fonları yavaşça imzalar.

Çift yönlü ödeme kanalları daha karmaşıktır, ancak 2. katman teknolojileri için olasılıkların kapsamını göstermeye başlar. Bu ödeme kanallarında fonlar taraflar arasında gidip gelir. Bu, ödeme kanallarının "yeniden dengelenmesine" izin verir ve paylaşılan bir karşı taraf aracılığıyla kanallar arasında ödeme olasılığını açar. Bu, Bitcoin'in Lightning Network'ü gibi ödeme kanalları ağlarını etkinleştirir. A Tarafı, her iki tarafa da açık bağlantıları olan bir aracı aracılığıyla bir yol bulabildiği sürece, Taraf A'dan Taraf B'ye, aralarında doğrudan bir kanal olmadan fon aktarılabilir.

Ödeme kanallarının zincir içi ödemeleri ölçeklendirebilmesi gibi, durum kanalları da zincir içi işlemleri ölçeklendirebilir. Bir ödeme kanalı, iki taraf arasındaki dengeleri yönetmekle sınırlıyken, durum kanalı, güvene dayalı olmayan bir satranç oyunundan ölçeklenebilir merkezi olmayan uygulamalara kadar her şeyi mümkün kılan keyfi bir durum anlaşmasıdır.

Bir ödeme kanalına benzer şekilde, taraflar bir kanal açar, zaman içinde kriptografik imza alışverişinde bulunur ve zincir içi bir akıllı sözleşmeye nihai durumu (veya sonucu) gönderir. Akıllı sözleşme daha sonra bu girdiye dayalı olarak yürütülecek ve işlemi sözleşmede kodlanmış kurallara göre çözecektir.

"Genelleştirilmiş durum kanalı", tek bir durum kanalının birden çok akıllı sözleşmede durum geçişlerini desteklemesine izin veren güçlü bir durum kanalı yapısıdır. Bu, "uygulama başına bir kanal" mimarisinin doğasında bulunan durum şişkinliğini azaltır ve ayrıca kullanıcıların halihazırda açık olan durum kanallarını kullanma becerisiyle kolay katılıma olanak tanır.

**5.3 Yan-zincirler (Side-chains)**

Yan-zincir, güvene dayalı olmayan bir blok zincire (ana zincir) iki yönlü bir mandalla bağlanan ayrı bir blok zincirdir. Yan-zinciri kullanmak için, bir kullanıcı ana zincirde belirli bir adrese para gönderir ve bu fonları yan-zincir operatörlerinin kontrolü altında kilitler. Bu işlem onaylandıktan ve bir güvenlik süresi geçtikten sonra, yan-zincir operatörlerine para yatırma işleminin ayrıntılarını veren bir kanıt iletilebilir. Operatörler daha sonra uygun fonları dağıtarak yan-zincirde bir işlem oluşturacaktır. Bu fonlar daha sonra yan-zincirde düşük ücretler, hızlı onay ve yüksek verimle harcanabilir.

Yan zincirlerin ana dezavantajı, ek güvenlik mekanizmaları ve güvenlik varsayımları gerektirmeleridir. En basit yan zincir yapısı, birleşik bir yan zincir, çok imzalı bir operatör grubuna güven verir. Akıllı sözleşme platformlarında, güvenlik modellerinde token teşvikleri veya birleştirme/meydan okuma/kesme ekonomik oyunlarla ince ayar yapılabilir.

Diğer zincir dışı genel amaçlı ölçeklendirme çözümleriyle karşılaştırıldığında, yan zincirlerin anlaşılması ve uygulanması daha kolaydır. Kullanıcıları için kabul edilebilir bir güven modeli oluşturmaya izin veren uygulama türleri için yan zincirler pratik bir çözüm olabilir.

**5.4 Onay-zinciri (Commit-chain)**

Plazma[7] gibi onay zincirlerinde[6], geniş küresel mutabakata sahip bir katman 1 blok zincirinde (kök zincir) bir güven kökünden yararlanan bir katman 2 zinciri oluşturulur. Bu onay zincirleri güvenlidir; Bir zincir operatörünün kötü niyetli veya işlevsiz olması durumunda, kullanıcılar her zaman kök zincir üzerindeki bir mekanizma aracılığıyla varlıklarını geri çekebilirler.

İşlemleri doğru bir şekilde yürütmek ve kök zincirde periyodik güncellemeler yayınlamak için bir onay-zinciri operatörüne güvenilir. Kök zincire yapılan uzun süreli bir sansür saldırısı dışında her koşulda, onay-zincirlerindeki varlıklar güvende kalacaktır. Birleştirilmiş yan zincirlere benzer şekilde, onay- zinciri tasarımları, güvenilir olmayan blok zincirlere kıyasla üstün bir kullanıcı deneyimi sunar. Ancak, bunu daha güçlü güvenlik garantilerini sürdürürken yaparlar.

Onay-zinciri, kök zincirde çalışan bir dizi akıllı sözleşme ile güvence altına alınır. Kullanıcılar varlıkları bu sözleşmeye yatırır ve onay-zinciri operatörü daha sonra onlara onay-zincirinde varlık sağlar. Operatör, kullanıcıların daha sonra onay-zinciri varlıklarının kök zincire çekildiği bir "çıkış" olan Merkle kanıtları aracılığıyla varlık sahipliğini kanıtlamak için kullanabilecekleri kök zincir taahhütlerini periyodik olarak yayınlayacaktır.

Bu, Plazma da dahil olmak üzere gelişmekte olan bir protokol ailesinin temeli olan taahhüt zinciri tasarımlarının genel kavramını açıklar. Vitalik Buterin ve Joseph Poon tarafından 2017'de yayınlanan Plazma tanıtım belgesi [7] iddialı bir vizyon ortaya koyuyor. Tüm Plazma zincirleri şu anda varlığa dayalı olmasına ve yalnızca misli ve misli olmayan token sahipliğini (ve transferleri) depolayabilmesine rağmen, güvene dayalı kod yürütme (veya akıllı sözleşmeler) aktif bir araştırma alanıdır.

**5.5 Doğrulanabilir Zincir Dışı Hesaplamalar**

Kriptografi, görünüşte pahalı zincir içi doğrulama ve ucuz zincir dışı hesaplama dinamiklerine göre uyarlanmış bir araç sağlar: Etkileşimli kanıt sistemleri. Etkileşimli bir kanıt sistemi, Prover ve Verifier olmak üzere iki katılımcılı bir protokoldür. Karşılıklı mesajlar göndererek, Doğrulayıcı, Doğrulayıcıyı belirli bir iddianın doğru olduğuna ikna etmek için bilgi sağlarken, Doğrulayıcı sağlananları inceleyecek ve yanlış iddiaları reddedecektir. Doğrulayıcı'nın reddedemeyeceği iddialar doğru kabul edilir.

Doğrulayıcı'nın iddiayı kendi başına naif bir şekilde doğrulamamasının başlıca nedeni verimliliktir- Doğrulayıcı, bir Doğrulayıcı ile etkileşim kurarak, aksi takdirde doğrulaması çok pahalıya mal olacak iddiaları doğrulayabilir. Bu karmaşıklık açığı, çeşitli kaynaklardan gelebilir: 1) Doğrulayıcı, yalnızca uzay sınırlı veya zaman sınırlı (veya her ikisi) hesaplamaları destekleyebilen hafif bir donanım çalıştırıyor olabilir, 2) naif doğrulama, uzun bir deterministik olmayan seçeneklere erişimi gerektirebilir. 3) Doğrulayıcı belirli gizli bilgilere sahip olmadığı için naif doğrulama imkânsız olabilir.

Kripto para birimleri bağlamında önemli bilgilerin gizliliği kesinlikle ilgili bir kısıtlayıcı faktör olsa da ölçeklenebilirlik bağlamında daha ilgili bir kısıtlayıcı faktör, özellikle nispeten ucuz zincir dışı hesaplamanın aksine, zincir içi doğrulamanın maliyetidir.

Kripto para birimleri bağlamında, zk-SNARK'lara (sıfır bilgi, özlü, etkileşimli olmayan bilgi argümanları) büyük ilgi gösterilmiştir. Etkileşimli olmayan ispat sistemlerinin bu ailesi, keyfi bir hesaplamayı sonlu bir alan üzerinde bir toplama ve çarpma devresi olarak kodlayan aritmetik devre etrafında döner. Örneğin, aritmetik devre "Bu Merkle ağacında bir yaprak biliyorum" şeklinde kodlayabilir.

zk-SNARK kanıtları sabit boyuttadır (yüzlerce bayt) ve sabit zamanda doğrulanabilir, ancak bu doğrulayıcı verimliliğinin bir maliyeti vardır: eşleştirmeye dayalı aritmetiğe ek olarak güvenilir bir kurulum ve yapılandırılmış bir referans dizesi gerekir (bunlardan somut kriptografik zorluk endişe kaynağı olmaya devam etmektedir.)

Alternatif ispat sistemleri farklı takaslar sağlar. Örneğin, Bulletproof'ların güvenilir bir kurulumu yoktur ve çok daha yaygın olan ayrık logaritma varsayımına dayanır, ancak logaritmik boyutlu kanıtlara (yine de oldukça küçük olmasına rağmen) ve doğrusal zamanlı Doğrulayıcılara sahiptir. zk-STARK'lar, güvenilir bir kurulum olmaksızın ölçeklenebilirlik açısından zk-SNARK'lara bir alternatif sunar ve üretilen kanıtın logaritmik boyutta olmasına (ve oldukça büyük: yüzlerce kilobayt) rağmen, yalnızca çok sağlam kriptografik varsayımlara dayanır.

Nervos Ağı gibi çok katmanlı bir kripto para birimi ekosistemi bağlamında, etkileşimli ispatlar, pahalı ispatlayan tarafı hesaplamalarını 2. katmana aktarma yeteneği sunarken, 1. katmandan yalnızca mütevazı doğrulayıcı tarafı çalışması gerektirir.

Bu sezgi, örneğin, Vitalik Buterin'in ZK Rollup protokolünde [8] yakalandı: izinsiz bir aktarıcı, zincir dışı işlemleri toplar ve zincirde depolanan bir Merkle kökünü periyodik olarak günceller. Bu tür her kök güncellemeye, yeni Merkle ağacında yalnızca geçerli işlemlerin biriktiğini gösteren bir zk-SNARK eşlik eder. Bir akıllı sözleşme, kanıtı doğrular ve yalnızca kanıt geçerliyse Merkle kökünün güncellenmesine izin verir.

Yukarıda özetlenen yapı, DEX'ler, çoklu tokenlar ve mahremiyeti koruyan hesaplama dahil olmak üzere basit işlemlerin ötesinde daha karmaşık durum geçişlerini destekleyebilmelidir.

**5.6 Katman 2 Çözümlerinin Ekonomik Modeli**

Katman 2 çözümleri etkileyici ölçeklenebilirlik sağlarken, bu sistemlerin token ekonomisi tasarım zorlukları doğurabilir.

Katman 2 token ekonomisi, uygulamaya özel teşvik tasarımının yanı sıra kritik altyapı (doğrulayıcılar ve gözetleme kuleleri gibi) için tazminat içerebilir. Kritik katman 2 altyapısı, süreye dayalı bir abonelik modeliyle daha iyi çalışma eğilimindedir. Nervos Network'te bu fiyatlama yapısı, CKB'nin fırsat maliyetine dayalı ödeme yöntemi ile kolayca uygulanabilmektedir. Hizmet sağlayıcılar, NervosDAO aracılığıyla kullanıcılarının "depozitoları" üzerinden ücret alabilirler. Katman 2 geliştiricileri daha sonra token ekonomik modellerini uygulamalarına özel teşviklere odaklayabilir.

Bir bakıma, bu fiyatlandırma modeli, kullanıcıların CKB'deki durum depolaması için de tam olarak nasıl ödeme yaptıklarıdır. Esasen, NervosDAO tarafından yayınlanan enflasyon ödüllerinin dağıtımı ile madencilere bir abonelik ücreti ödüyorlar.

**6. Nervos Network**

**6.1 Çok Varlıklı Değer Deposu Platformu Olarak Katman 1**

Bir katman 1 blok zincirinin bir değer deposu olarak inşa edilmesi gerektiğine inanıyoruz. Uzun vadeli yerelleşmeyi en üst düzeye çıkarmak için, işlem ücretleri yerine durum depolama işgali etrafında tasarlanmış bir ekonomik modelle çalışma kanıtı mutabakatına dayanmalıdır. Ortak Bilgi Bankası (Common Knowledge Base: CKB), hem programlaması hem de durum etrafında tasarlanmış ekonomik modelleri ile iş tabanlı, çok varlıklı, değer deposu blok zincirinin bir kanıtıdır.

CKB, Nervos Network'ün en yüksek güvenlik ve en yüksek derecede merkezi olmayan temel katmanıdır. CKB'de varlıklara sahip olmak ve işlem yapmak en yüksek maliyetle gelir, ancak ağdaki en güvenli ve erişilebilir varlık depolamasını sağlar ve maksimum şekillendirilebilirliğe izin verir. CKB, yüksek değerli varlıklar ve uzun vadeli varlık koruması için en uygun olanıdır.

Ortak Bilgi Bankası, özellikle katman 2 protokollerini desteklemek için oluşturulmuş ilk katman 1 blok zinciridir:

- CKB, ölçeklenebilirlik gibi üst üste binen katman 2 öncelikleri yerine güvenlik ve dağıtmaya odaklanarak katman 2 protokollerini tamamlamak üzere tasarlanmıştır.

- CKB, defterini hesaplar yerine duruma göre modeller. Hücreler, esas olarak, işlemler tarafından referans alınabilen ve katmanlar arasında dolaşabilen kendi kendine yeten durum nesneleridir. Bu, başvurulan ve katmanlar arasında iletilen nesnelerin hesaplar yerine durum parçaları olduğu katmanlı bir mimari için idealdir.

- CKB, hesaplama motoru yerine genelleştirilmiş bir doğrulama makinesi olarak tasarlanmıştır. Bu, CKB'nin zincir dışı durum geçişlerini doğrulayan bir kriptografik mahkeme olarak hizmet etmesine izin verir.

- CKB, geliştiricilerin özel şifreleme ilkellerini kolayca eklemesine olanak tanır. Bu, çeşitli katman 2 çözümleri tarafından üretilen kanıtların doğrulanmasına izin vererek CKB'yi geleceğe hazırlar.

Ortak Bilgi Bankası (CKB), en ölçeklenebilir ve verimli blokzincir işlemlerini sağlayan sınıfının en iyisi katman 2 ekosistemi ile dünyanın en değerli ortak bilgisini depolamak için altyapı olmayı hedefliyor.

**6.2 Katman 2 Çözümleriyle Ölçeklendirin**

Katmanlı mimarisiyle Nervos Network, 2. katmanda herhangi bir sayıda katılımcıya ölçeklenebilirken, yine de merkeziyetçilikten uzaklaşma ve varlıkların korunması gibi hayati özellikleri koruyor. Katman 2 protokolleri, her türden katman 1 taahhüdünü veya kriptografik ilkeli kullanabilir ve büyüyen katman 2 kullanıcı tabanını desteklemek için işlemsel sistemlerin tasarlanmasında büyük esneklik ve yaratıcılık sağlar. Katman 2 geliştiricileri, uygulamaları ve kullanıcıları bağlamında en iyi şekilde çalışan aktarım hızı, kesinlik, gizlilik ve güven modelleri açısından kendi ödünleşimlerini seçebilirler.

Nervos Ağında, 1. katman (CKB) durum doğrulaması için kullanılırken, 2. katman durum oluşturmadan sorumludur. Durum kanalları ve yan zincirler, durum oluşturma örnekleridir, ancak sıfır bilgi kanıtı oluşturma kümesi gibi her tür oluştur-doğrula modeli desteklenir. Cüzdanlar ayrıca 2. katmanda çalışır, isteğe bağlı mantık yürütür, yeni durum oluşturur ve durum geçişlerini doğrulama için CKB'ye gönderir. Nervos Network'teki cüzdanlar çok güçlüdür çünkü durum geçişleri üzerinde tam kontrole sahip durum oluşturuculardır.

Yan zincirler, geliştirici dostudur ve iyi bir kullanıcı deneyimi sağlar. Ancak doğrulayıcılarının dürüstlüğüne güveniyorlar. Doğrulayıcılar kötü niyetli davranırsa, kullanıcılar varlıklarını kaybetme tehlikesiyle karşı karşıyadır. Nervos Network, "Muta" adlı bir Proof-of-Stake blokzincir çerçevesinden ve buna dayalı “Axon” adındaki bir yan zincir çözümünden oluşan, CKB'de yan zincirleri başlatmak için açık kaynaklı ve kullanımı kolay bir yan zincir yığını sağlar.

Muta, Proof-of-Stake, BFT fikir birliği ve akıllı sözleşmeleri desteklemek için tasarlanmış, oldukça özelleştirilebilir, yüksek performanslı bir blokzincir çerçevesidir. Yüksek verimli ve düşük gecikmeli bir BFT mutabakatı "Overlord" içerir ve CKB-VM, EVM ve WASM dahil olmak üzere çeşitli sanal makineleri destekler. Farklı sanal makineler, VM'ler arası birlikte çalışabilirlik ile aynı anda tek bir Muta blok zincirinde kullanılabilir. Muta, protokollerini kişiselleştirmek için maksimum esnekliğe izin verirken, geliştiricilerin yüksek performanslı blok zincirleri oluşturma engelini büyük ölçüde azaltır.

Axon, geliştiricilere Nervos CKB'ye ek olarak pratik bir güvenlik ve token ekonomik modeli ile anahtar teslimi bir yan zincir sağlamak için Muta ile oluşturulmuş eksiksiz bir çözümdür. Axon çözümleri, güvenli varlık saklama için CKB'yi kullanır ve yan zincir doğrulayıcılarını yönetmek için token tabanlı yönetişim mekanizmasını kullanır. Bir Axon yan zinciri ile CKB arasındaki ve ayrıca Axon yan zincirleri arasındaki etkileşimler için zincirler arası protokoller de yerleşik olacaktır. Axon ile geliştiriciler, altyapı ve zincirler arası protokoller oluşturmak yerine uygulama oluşturmaya odaklanabilir.

Hem Muta hem de Axon şu anda yoğun geliştirme aşamasındadır. Yakında çerçeveleri açacağız ve hem Muta hem de Axon için RFC'ler de yolda.

Katman 2 protokolleri gelişen bir araştırma ve geliştirme alanıdır. Tüm katman 2 protokollerinin standartlaştırıldığı ve sorunsuz bir şekilde birlikte çalıştığı bir gelecek öngörüyoruz. Bununla birlikte, 2. katman çözümlerin hâlâ olgunlaşmakta olduğunu kabul ediyoruz ve çoğu zaman yapabileceklerinin sınırlarını zorlamaya ve kabul edilebilir takasları bulmaya çalışıyoruz. Erken dönem umut verici çözümler gördük, ancak katman 2 tasarımlarında birlikte çalışabilirlik, güvenlik ve ekonomik modeller gibi konularda yürütülecek çok sayıda araştırma var.

**6.3 Sürdürülebilirlik**

Uzun vadeli sürdürülebilirlik adına, Nervos Ortak Bilgi Tabanı durumu sınırlar, zincir içi depolamaya bir maliyet getirir ve kullanıcılara durum depolamalarını temizlemeleri için teşvikler sağlar. Sınırlı bir durum, tam düğüm katılımı için gereksinimleri düşük tutarak düğümlerin düşük maliyetli donanım üzerinde çalıştırılabilmesini sağlar. Sağlam tam düğüm katılımı, merkeziyetçiliği ve buna bağlı olarak güvenliği artırır.

Nervos Ortak Bilgi Tabanı, durum depolamasına zamanla orantılı bir "durum kirası" maliyeti uygulayarak, "bir kez öde, sonsuza kadar sakla" paradigmasında birçok blok zincirinin karşılaştığı müştereklerin trajedisini hafifletir. "Hedefli enflasyon" yoluyla uygulanan bu durum kiralama mekanizması, durum depolamasına bir maliyet getirirken sorunsuz bir kullanıcı deneyimi sağlar.

Bu enflasyon maliyeti hedeflenebilir çünkü kullanıcılar, verilerinin kapladığı mutabakat alanına sahiptir. Bu model aynı zamanda kullanıcıların durumlarını mutabakat alanından kaldırmaları için yerel bir mekanizma içerir. Durum kirasının ekonomik teşvikleriyle birleştiğinde bu, durum boyutunun her zaman ağ katılımcılarının ihtiyaç duyduğu minimum veri miktarına doğru ilerlemesini sağlar.

Bireysel olarak sahip olunan durum, geliştiricilerin maliyetlerini de önemli ölçüde azaltır. Geliştiricilerin, tüm kullanıcılarının durum gereksinimleri için CKByte satın almaları gerekmesi yerine, yalnızca uygulamalarının gerektirdiği doğrulama kodunu depolamaya yetecek kadar CKByte satın almaları gerekir. Her kullanıcı, tokenlerini depolamak için kendi hücrelerini kullanır ve varlıklarından tamamen sorumlu olur.

Son olarak, durum kirası, madencilere yeni token ihracı yoluyla sürekli bir ödül sağlar. Bu öngörülebilir gelir, madencileri işlem ücretlerini almak için karlı blokları çatallamak yerine blok zincirini ilerletmeye teşvik ediyor.

**6.4 Uyumlu Teşvikler (Aligned Incentives)**

Ortak Bilgi Tabanının ekonomik modeli, ekosistemdeki tüm katılımcılar için teşvikleri uyumlu hale getirmek üzere tasarlanmıştır.

Nervos Ortak Bilgi Tabanı, ucuz işlem ücretleri yerine açıkça güvenli değer koruması için oluşturulmuştur. Bu kritik konumlandırma, değişim aracı kullanıcıları yerine Bitcoin kullanıcı topluluğuna benzer şekilde değer deposu kullanıcılarını çekecektir.

Değişim ortamı kullanım durumları, daha fazla verimlilik ve düşük ücretler peşinde her zaman bir blokzincir ağını merkezileştirmeye doğru itme eğilimindedir. Ağı güvence altına alan altyapı operatörleri (madenciler veya doğrulayıcılar) için önemli bir ücret geliri olmadan, güvenlik parasal enflasyon yoluyla finanse edilmelidir veya basitçe yetersiz finanse edilir. Parasal enflasyon, uzun vadeli sahipler için zararlıdır ve yetersiz finanse edilen güvenlik, ağın herhangi bir paydaşı için zararlıdır.

Bununla birlikte, değer deposu kullanıcıları, sansüre karşı direnç ve varlık güvenliği için güçlü taleplere sahiptir. Bunu sağlamak için madencilere güvenirler ve karşılığında rolleri için onları tazmin ederler. Bir değer deposu ağında, bu tarafların ortak çıkarları vardır.

Tüm katılımcıların teşviklerini hizalayarak birleşik bir Nervos topluluğu büyüyebilir ve ağın uyumlu ekonomik sisteminin de hard fork'a dayanıklı olması beklenir.

**6.5 Değer Yakalama ve Değer Yaratma**

Platform tarafından güvence altına alınan varlıkların değeri arttıkça herhangi bir blok zincirinin güvenli kalması için sistemin, güvence altına alınan varlıkların değeri arttıkça değeri yakalayacak bir mekanizmaya sahip olması gerekir. CKB, durumu sınırlayarak, durum alanını kıt ve piyasa fiyatına sahip bir kaynak haline getirir. Ağda varlık depolama talebi arttıkça, sistemin bu tür varlıkları güvence altına almak için madencilere daha iyi ödeme yapması bekleniyor.

Bir değer koruma platformu olarak, bir platform olarak CKB'nin gerçek değeri, koruduğu varlıklara sağladığı güvenlik miktarı ile belirlenir. Güvence altına alınan varlıkların değeri arttıkça, CKB ekonomik modelinin değer yakalama mekanizması, daha fazla maden kaynağı çekmek için CKB'nin güvenlik bütçesini otomatik olarak yükseltebilir ve bu da platformu daha güvenli hale getirir. Bu sadece platformu sürdürülebilir kılmak için önemli olmakla kalmaz, aynı zamanda platformun içsel değeri için bir büyüme yolu sağlar- platform daha güvenli hale geldikçe, aynı zamanda daha yüksek değerli varlıklar için daha çekici hale gelir ve daha fazla talep oluşturur. Tabii ki, bu, sonunda blok zinciri alanına taşınacak olan genel toplam değere bağlıdır.

Zamanla CKB'nin ekonomik yoğunluğunun artmasını bekliyoruz. CKBytes, yüksek değerli varlık depolaması için kullanılacak ve düşük değerli varlıklar, katman 2 yan zincirleri gibi CKB'ye bağlı blok zincirlerine taşınacaktır. CKB, varlıkları doğrudan güvence altına almak yerine, örneğin birkaç yüz baytlık kriptografik kanıtlar aracılığıyla tüm bir yan zincirin ekosistemini güvence altına almak için bir güven kökü olarak kullanılabilir. Bu tür kanıtların ekonomik yoğunluğu olağanüstü derecede yüksektir ve depolama alanının talep eğrisini daha da destekler: küçük bir arazi parseline benzer şekilde, bir gökdeleni destekleyerek ekonomik yoğunluğunu önemli ölçüde artırır.

Son olarak, NervosDAO'nun tasarımı ve "enflasyon sığınağı" işlevi sayesinde, uzun vadeli token sahipleri her zaman sabit bir toplam ihraç yüzdesini elinde tutacak ve yerel tokenin kendisini sağlam bir değer deposu haline getirecektir.

**6.6 Düzenleyici Boşluğu Kapatmak (Bridging the Regulatory Gap)**

İzinsiz blok zincirleri, varlık ihraç ve işlemlerinde tamamen merkezi olmayan bir yapıya izin verir. Onları değerli kılan şey budur, ancak aynı zamanda gerçek dünyadaki finans ve yargı sistemleriyle uyumlu olmamalarının nedeni de budur.

Katmanlı bir mimarinin ortaya çıkışı, düzenlenmemiş, izinsiz bir blok zincirinin düzenleyici uyumlu kısımlarını oluşturma fırsatı sunar. Örneğin, kullanıcılar merkezi olmayan varlıklarını 1. katmanda depolayabilir, bu varlıkların mutlak mülkiyetinin keyfini çıkarabilir ve düzenleyici ve yasal kısıtlamalara tabi oldukları 2. katmanda gerçek dünyadaki işlerini de işleyebilir.

Örneğin, kripto para birimi borsalarını ele alalım- Japonya ve Singapur gibi ülkeler, borsalar için lisanslar vermiş ve düzenleyici gereklilikler oluşturmuştur. Uyumlu bir borsa veya küresel bir borsanın şubesi, 2. katman ticaret zinciri oluşturabilir, kullanıcı kimliklerini ve varlıkları içe aktarabilir ve ardından yerel düzenleyici gerekliliklere uygun olarak yasal işler yürütebilir.

Gerçek dünya varlıklarının ihraç edilmesi ve işlem görmesi, katmanlı bir blok zinciri yapısı içinde mümkün hale gelir. Gerçek dünya varlıkları, düzenlenmiş bir 2. katman yan zinciri aracılığıyla izinsiz 1. katman blok zincirine blok zinciri ekosistemine akabilir ve bu varlıkların birleştirilebilir, merkezi olmayan finansal hizmetlerin en büyük ekosistemine erişmesine olanak tanır.

Gelecekte, Nervos Network'ün, bu alandaki lider şirketlerle iş birliği içinde, büyük ölçekli kullanıcı benimsemesinin temeli olarak katman 2 yan zincirlerini ve uygulamalarını da kullanması bekleniyor.

**Referanslar:**

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 31 Oct 2008, <https://bitcoin.org/bitcoin.pdf>

[2] Vitalik Buterin. "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform". Nov 2013 <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>

[3] With an average Bitcoin transaction size of 250 bytes: (2 \* 250 \* 7,500,000,000) / (24 \* 6) = 26,041,666,666 byte blocks (every 10 minutes); 26,041,666,666 \* (24 \* 6) = 3,750,000,000,000 bytes (blokzincir growth each day); 3,750,000,000,000 \* 365.25 = 1,369,687,500,000,000 bytes (blokzincir growth each year)

[4] Gur Huberman, Jacob Leshno, Ciamac C. Moallemi. "Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System". Bank of Finland Research Discussion Paper No. 27/2017. 6 Sep 2017, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032375>

[5] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, Arvind Narayanan. "On the Instabiliity of Bitcoin Without the Block Reward". Oct 2016, <https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf>

[6] Lewis Gudgeon, Perdo Moreno-Sanchez, Stefanie Roos, Patrick McCorry, Arthur Gervais. "SoK: Off The Chain Transactions". 17 Apr 2019, <https://eprint.iacr.org/2019/360.pdf>

[7] Joseph Poon, Vitalik Buterin. "Plasma: Scalable Autonomous Smart Contracts". 11 Aug 2017, <https://plasma.io/plasma.pdf>

[8] Vitalik Buterin. "On-chain scaling to potentially ~500 tx/sec through mass tx validation". 22 Sep 2018, <https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477>