Stakenet: P2P Zincirlerarası Bir Ekonomi Modeli

X9 Geliştiricileri

Haziran 2019

Özet

Stakenet; güven gerektirmeyen, zincirlerarası bir ekonomi modeli sunan merkezsiz bir platformdur. Lightning Network, Masternodelar ve merkezsiz uygulamalar(dApps) barındıran Proof of Stake blokzinciri ile güçlendirilmiştir. Amacı, insanların herhangi bir blokzincir üzerinde Stakenet ve Stakenet'in koini XSN'i kullanarak yüksek güvenlikli zincirlerarası işlem yapabilecekleri bir platform sunmaktır.

1 Giriş

Kriptopara topluluğu son yıllarda oldukça büyüdü. Yüzlerce kriptopara bulunmakta ve her gün aralarına yenileri katılmakta. Hangi teknolojilerin, toplulukların ve dağınık veri sistemlerinin farkını göstereceğini, diğerlerinin arasından sıyrılacağını anlamak önemli. Gelecekte tek bir zincirin hakim olduğu bir ortam değil, var olan bütün hizmet, teknoloji ve zincirlerin yer alacağı bir blokzinciri ağının, küresel ortak bir platformun oluşacağına inanıyoruz. Farklı arabirimler üzerinden birbirleri ile iletişim halindeki farklı zincirlerden oluşan birleşik bir ağ. Burdaki zincirlerarası swapler son kullanıcının fark etmeyeceği, görmeyeceği hatta seçmeyeceği bir şekilde gerçekleşecektir.

1.1 Stakenet'in Amacı

Stake kelimesi ilk olarak akla staking'i (pasif gelir) getirse de kelimenin kökeni işletme yönetiminden gelmekte ve pasif gelirden çok daha fazlasını barındıran bir anlama sahiptir. Stakenet pasif gelir sunmaktan çok daha fazlasını yapmaktadır; Stakenet *hissedarlar için bir ağdır*. Bunun anlaşılması için ağ kavramnı açıklamak, *hissedarlık* ve *stake* ile nasıl bağlantılı olduğunu göstermemiz gerekiyor.

- **Ağ** birbirine bağlı benzer parçalardan oluşmuş bir sistemdir.
- **Stake** bir ticari işletmeye ya da faaliyetlerine yapılmış önemli yatırımdır.
- **Hissedar** bir ticari işletmenin misyonuna ve vizyonuna içerden ya da dışardan yatırım yapmış kişi ya da gruptur.

Böylece, bir kriptoparanın hareketlerinden aktif ya da pasif olarak etkilenen kişi, blokzincir ekonomisinin bir hissedarı olmuştur. Buna koin tutarak, varlık ya da hukuki çıkar ilişkisi kurarak, ekonomik ve sosyal bağlılık, topluluk ve geliştirici aktivitelerine dahil olarak ve diğer kripto bağlantılı iş ya da ilişkiler ile dahil olmayı ekleyebiliriz. Böylelikle, kriptopara hissedarı:

- Blokzincir ekonomisini etkiler
- Blokzincir ekonomisinden etkilenir.
- Hem blokzincir ekonomisine etki eder hem de bundan etkilenir.

Hepsini bir araya topladığımızda Stakenet'in geliştirdiği vizyonu anlayabiliriz: Blokzincir ekonomisinin bütün hissedarlarını tek bir dev ağda birleştirecek teknik bir yapı.

1.2 Eylem Planı

Blokzincir ekonomisine başarılı bir zincirlerarası çözüm sunmak için, hissedarların çoğunluğunu tanımlamak, onları birleştirecek bir yöntem bulmak ve bütünlüklerini koruyacak bir yaklaşım geliştirmek zorundayız. Bu yüzden aşağıdaki 3 alt madde eylem planımız için oldukça önemlidir:

1) **Çoğunluğu Tanımlamak**: Blokzincir ekonomisindeki en bilinen hissedar gün geçtikçe güçlenen, elektronik paranın p2p hali olan **Bitcoin**'dir. Son birkaç yıldır yoğun ilgi çeken ve çok sayıda takipçi kazanmayı başaran Bitcoin; sayısız insanı etkilemekte ve gene bu insanların çalışmaları ve aktivitelerinden etkilenmektedir. Bu aktivitelere örnek olarak madencilik endüstrisini, finansal ürünleri, farklı cüzdan çözümlerini ve Bitcoin ile bağlantılı diğer çalışmaları sayabiliriz. Bitcoin'e ek olarak, akıllı sözleşme kapasitesine sahip blokzincirler de popüler ürünler haline geldiler. Bu blokzincirlerin en güzel mimari özelliği hem yan üretime hem de zinciraltı üretime izin vermesidir. Bu sayede merkezsiz uygulamaların geliştirilmesine olanak sağlanmaktadır. En bilinen akıllı sözleşme özelliğine sahip blokzincir, en fazla tokena ev sahipliği yapan **Ethereum**'dur. Diğer ünlü akıllı sözleşme platformu ise, şu anda kriptopara piyasasında en fazla kullanılan blokzincir olan **EOS**'tur. İki platform da iç ve dış çıkarların etkisi altındadır. Hissedar yaklaşımının geçerli olmadığı tek bir blokzincir bile bulunmamaktadır.

2) **Çoğunluğu Birleştirmek:** Hissedarlarımızın kimler olduğunu tanımladıktan sonra onları bir araya getirecek bir yöntem bulmalıyız. Eğer blokzincirler uyumlu arabirimlere sahiplerse, yani benzer ikinci katmanlara sahip ya da aynı şifrelenmiş hash fonksiyonunu kullanıyorlarsa aralarında köprü kurmak mümkündür. Böyle bir durumda farklı blokzincirler arasında güven gerektirmeyen işlemler yapılabilir. Bitcoin örneğini ele aldığımızda, Lightning Network'ü geçerli arabirim olarak kullanarak iki farklı zinciri (daha önce Bitcoin, Litecoin ve Stakenet arasında yapılabildiğini gösterdiğimiz gibi) birleştirebiliriz. EOS ve Ethereum blokzincirlerini hissedar ağımıza bağlamak için bu blokzincirlerin kendi akıllı sözleşme özelliklerini kullanabiliriz. Hash süreli kilitli sözleşmeler veya HTLC'ler yardımı ile, diğer blokzincirlerle kendi zincirimiz arasında güven gerektirmeyen swapları gerçekleştirmek için XSNETH ve XSNEOS tokenlarını geliştiriyoruz. Hashkilitleri ya da sürelikilitleri kullanarak kendi zincirimizde XSN koinler kilitlendiğinde, bu kilitli koinler kadar XSN tokenlar diğer akıllı platform zincirinde serbest kalırlar. Koin ve tokenların değişimi dışında, blokzincirlerin hissedarlarını birleştirmek aynı zamanda bu blokzincirlerin yan endüstrilerini de entegre etmeyi gerektirmektedir. Bu yüzden merkeziyetsiz madencilik havuzları, zincirlerarası stake ve merkeziyetsiz uygulamaların diğer zincirlerin uygulamaları ile uyumlu çalışmasını sağlayacak bir plan hazırladık.

3) **Bütünlüğü Korumak:** Eğer merkezi bir yapı üzerinden çözüm üretseydik, sunduğumuz bütün bu fikirler boş laftan ibaret olurdu. Her blokzincirin güçlü yönlerini tek bir zincirlerarası yönetim mimarisinde birleştirerek, hepsinin bütünlüğünü koruyoruz. Burdaki ana sütunlar, kendi TPoS konsensüsümüz, bekçi kulesi (watchtower) özelliği eklenmiş Masternode katmanı ve özelleştirilmiş swapleri kararlaştıran Lightning Network'tür. Bunların yanına; saklama, takas ve farklı zincirlerdeki varlıklar ile araçları kontrol etmeye yarayan donanım cihazımız XSN Viper'ı da ekleyebiliriz.

Kısaca Stakenet, en büyük dağınık ağlardaki ürünleri bir araya toplayarak, insanların Stakenet arayüzü üzerinden bütün blokzincirler üzerinde işlem yapabilmesini sağlamaktadır.

2 Blokzincir Mimarisi

Stakenet gerçek anlamda merkeziyetsiz, üst düzey güvenliğe sahip ve kâr amaçlı zincirlerarası ağa sahip bir Proof of Stake blokzinciridir. Masternodelar ve Lightning Network nodeları tarafından yönetilen sistem, kendi XSN koini ile güçlendirilmiştir. Stakenet'te doğrulama süresi bir saniyedir ve ana zincir üzerinden saniyede 240 işleme kadar ulaşabilir. 1-4 megabyte'lık bloklar üzerine kurulmuştur ve blok üretim süresi 60 saniyedir. Ek olarak Stakenet blokzinciri, Lightning Network kullanımı ile zincir-dışı işlemlerde sonsuz ölçeğe ve sıfıra yakın transfer ücretlerine sahip olacaktır.

2.1 Diğer Projelerden Alınan Özellikler

Stakenet; Bitcoin, Dash ve Peercoin'den alınan belirli özelliklerle hayata geçirildi. Bitcoin'in çekirdeği üzerine kurulan Stakenet, Dash'ın Masternode mimarisinin geliştirilmiş halini ve Peercoin'in Proof of Stake koin üretme özelliğini kullanmaktadır.

2.2 Konsensüs

Dijital bir parada konsensüs, blokzincire eklenen yeni blokların onaylanma sürecini ifade etmektedir. Basitçe anlatırsak konsensüs, onay merciinin geçmiş işlemlerin doğru olup olmadığını oylamasını sağlayan bir yazılım birleşenidir. Stakenet bunun için, kendi geliştirdiği çevrimdışı stake çözümü TPoS ile güçlendirilmiş Proof of Stake konsensüsünü kullanmaktadır.

2.2.1 Proof of Stake'te Koin Üretimi

Cihazların hash güçlerini kullanarak şifrelenmiş bulmacaları çözdüğü Proof of Work'un aksine, Proof of Stake'te stake yapanlar ellerindeki koin varlığını (coin wealth) belirli bir süre (coinage) hareket ettirmeyerek (24 saate kadar) yeni blok üretimine katkıda bulunurlar. Coinage stake yapanların koinlerini hareket ettirmemeleri gereken süreyi, coin wealth ise stake yapanın elindeki koin sayısını ifade eder. Yeni üretilen blokların kanıtı, coinstake denen özel bir transfer ile oluşturulur. Bu transferin içindeki ilk girilen veri, çekirdek(kernel)'tir. Bu çekirdek, blok üreticisinin rassal (stochastic) bir süreç sonucunda seçildiğinin kesin olması için, belirli bir hash hedef protokolünü sağlamalıdır. Bu süreç sonunda bloğu üreten stake yapıcı, kendisine blok ödülünü alarak coinage süresini sıfırlar ve yeni blok üretiminde diğerlerine göre dezavantajlı hale gelir. Coinage'ini harcayan bir stake yapıcının blok üretimindeki oy hakkının sıfırlanması ile birlikte, arka arkaya blok üretme şansı oldukça azalır.

2.2.2 Trustless Proof of Stake

Proof of Stake protokolüne yapılan en temel eleştiri, 'sistem ancak bütün koinler çevrimiçi olduğunda ve güçlü stake nodelar engellendiğinde tam anlamıyla güvenli olabilir' fikridir. Bugüne kadar üretilen çevrimiçi ya da çevrimdışı çözümler bu soruna çare olamamıştır. Normalde stake yapanların blok üretimine katkıda bulunmak için full-node cüzdanlarını blokzincire bağlı halde bırakmaları gerekir. Ancak Stakenet'in kendi ürettiği konsensüs çözümü Trustless Proof of Stake (Güven Gerektirmeyen POS) ile, kullanıcılar koinlerini Trezor, Ledger Nano gibi soğuk cüzdanlarda tutarken blok üretimine katılabilirler. Diğer çevrimdışı çözümlerin aksine, Stakenet doğrulama nodeları, Delegated Proof of Stake'teki gibi birkaç yetkili node'dan ibaret değildir. Ayrıca bizim çözümümüz, Leasing Proof of Stake'teki gibi eski nodeların sistem üzerinde daha fazla güç sahibi olduğu bir sistem kurmaz. Sistemdeki belirleyici etmenler coinage ve stake yapanların sahip oldukları koin sayılarıdır.

Temel olarak Trustless Proof of Stake, stake yapanlara harcanabilir bakiye ya da private key bilgilerini paylaşmadan, başka bir node üzerinden stake yapma imkanı vermektedir. Bu, **koin sahibinin** kendi adresinin stake hakkını **merchant** adrese verdiği, blokzincirimiz üzeriden yapılan özel bir anlaşma şeklidir. Merchant adresinin yöneticisi stake yapılan koinleri transfer etme hakkına sahip değildir, sadece o adresteki koinleri stake yapma hakkına sahiptir. Koin sahibi sözleşme (contract) süresince koinler üzerindeki kontrolünü sürdürür, istediği zaman koinlerini başka bir adrese taşıyabilir. Stake yapma sözleşmesi OP_RETURN ile imzalanmış özel bir işlemdir. Koin sahibinin kendisine gönderdiği 1 XSN ile yaratılan bu işleme sözleşmenin şartları eklenmiştir. Kullanıcı sözleşmeyi iptal etmek için adresteki koinleri başka bir adrese taşıyabilir ya da kilitli durumda duran 1 XSN'in kilidini kaldırarak sözleşmeyi istediği zaman iptal edebilir.

Sözleşme için gerekenler şunlardır:

- **tposAdresi:** Sözleşmeyi yaratan kişinin adresi (stake yapılacak olan burdaki bakiyedir).
- **merchantAdresi:** Stake yapma hakkına sahip olan kişinin adresi.
- **Komisyon:** Protokole tposAdresine gelen ödüllerin nasıl paylaştırılacağını belirtir.
- **İmza:** Sözleşmeyi yaratan kişinin tposAdresinin sahibi olduğunu gösteren 65 byte'lık imza.

Örnek Sözleşme:

Out 0: { tposAdresi : 1 XSN } (mevduat)

Out 1: { OPRETURN tposAdresi merchantAdresi komisyon imza }

Out 2: { değişimAdresi : değişimMiktarı }

RPC yeni bir TPoS sözleşme çağrısı hazırlar ve ağa bunu bildirir:

- tpossözleşmesi yarat [tposAdresi] [merchantAdresi] [komisyon]
- sendrawtransaction [hex ile kodlanmış sözleşme]

Kullanıcı TPoS'u aktif hale getirdiğinde arkada şu işlemler gerçekleşir:

1- Koin sahibi için tposAdresi oluşturulur.

2- Girilen merchantAdresi kullanılarak TPoS sözleşmesi oluşturulur.

3- Sözleşme ağa duyurulur.

4- Sözleşmede mevduatta yazan kadar koin, koin sahibinin tposAdresine gönderilir.

Buna ek olarak, TPoS özelliğini Masternodeların görevleri ile birleştirerek kullanıcılara zincirlerarası stake yapma imkanını sunacağız. Blok ödülü ödemelerini XSN DEX teknolojisi ile birleştirince, kullanıcılar stake yaptıkları koinin ödülünü farklı bir koin olarak doğrudan soğuk cüzdanlarına alabilecekler. Örneğin, donanım cüzdanınız üzerinden XSN stake ederken, ödülleri Bitcoin ya da Litecoin olarak doğrudan cüzdanınıza alabileceksiniz.

2.3 Şifreleme Algoritması

Blokzincir içerisindeki her parça şifreleme işleminden geçer. Stakenet bu işlem için X11 algoritmasını kullanır. Bu şifreleme algoritması çıkış boyutları birbirinden farklı olan 11 karıştırma sürecine sahiptir. Karmaşık bir yapıya sahip bu algoritma sisteme üst düzey güvenlik ve dijital bir paranın değer aracı olarak kalmasını sağlayacak kalıcılık özelliklerini kazandırır. Diğer tek karıştırmalı çözümlerle karşılaştırıldığında, X11'in yapısını bozmak için bütün 11 algoritmanın aynı anda kırılması gerekmektedir.

X11 şu algoritmalardan oluşmaktadır: NIST hash fonskiyon yarışmasının galibi **Keccak** (SHA-3 olarak da biliniyor). NIST hash fonskiyon yarışmasının finalistleri, **BLAKE**, **Grøstl**, **JH** (Hongjun Wu) ve **Skein**. Son olarak, yarışmada finale çıkamayan ancak 'sorunsuz şekilde çalışan' **Blue Midnight Wish** (BMW), **Luffa**, **Cube-Hash**, **SHAvite**, **SIMD** ve **Echo**.

Sonuç olarak X11, en iyi şifreleme uzmanları tarafından tasarlanmış ve analiz edilmiş algoritmaları sayesinde güçlü bir güvenliğe sahiptir. Gelecekte bu algoritmaların kuantum bilgisayarlar tarafından kırılabileceği söylenmektedir ancak yakın zamanda yapılan çalışmalarda SHA-3 256'ın kuantum bilgisayar tarafından kırılması için gereken sürenin 10^{32} yıl olduğu ortaya çıkmıştır. Bu sayede, görülebilir gelecekte kuantum bilgisayarlar SHA-3 256'ya ve Stakenet'e tehdit oluşturmamaktadır.

2.4 Arz

Stakenet'in ilk arzı POSW'dan XSN'e swap edilen koinler oldu. 76.000.000 XSN İlk blok (genesis block) ile yaratıldı. Swap süresi bittikten sonra, 3.500.000 swap edilmeyen koin, bu adreste imha edildi: XmPe9BHRsmZeThtYF34YYjdnrjmcAUn8bC

2.4.1 Koin Üretimi

Stakenet blokzinciri, asimetrik kazançları önlemek ve swapların tamamlanmasını bekleyerek herkese eşit şans sunmak için ilk 10 gün, 20.000 blok boyunca boş bloklar üretti. Blok üretim süresi 60 saniye iken, blok ödülleri adım adım azaltılarak, her 63.200. blokta 5 XSN azaltıldı ve son olarak 20 XSN oldu.

Aşama 1:	[0 – 20.000]	0 XSN
Aşama 2:	[20.001 – 63.200]	50 XSN
Aşama 3:	[63.201 – 106.400]	45 XSN
Aşama 4:	[106.401 – 149.600]	40 XSN
Aşama 5:	[149.601 – 192.800]	35 XSN
Aşama 6:	[192.801 – 236.000]	30 XSN
Aşama 7:	[236.001 – 279.200]	25 XSN
Aşama 8:	[279.201 – ∞]	20 XSN

Aşama 1 adil başlangıç tarihi: 6 Mart 2018
Aşama 8 başlangıç tarihi: 20 Eylül 2018

XSN blok ödülleri 20 XSN'de sabit kalacağı için, arz teorik olarak sınırsız olacak. Bu yüzden Stakenet, ağ içi bütün transfer ücretlerini imha ederek artan arzı sınırlamakta ve yeni ticari alanlar yaratarak XSN'e değer katmaya çalışmaktadır. Bu değer katma süreci, yeni alanlardan edilen gelirleri imha edip XSN'in arzının düşürülmesi ya da bu gelirlerin yeni projelerin ve ürünlerin fonlanması için hazineye aktarılması şeklinde olur. Bu sayede Stakenet ekosisteminden elde edilen gelirler, XSN koin sahiplerinin faydasına olacak şekilde kullanılır.

2.4.2 Koin Dağılımı

Güçlü ve güvenilir bir altyapıya sahip olmak için ağ güvenliği ile ağ servislerinin aynı önemde olduğuna inanıyoruz. Stakenet blokzincirinin üstünde durduğu iki tip nodeun da (Masternodelar ve stake nodeları) eşit derecede önemli olduğunu düşünüyoruz ve birini diğerinin önüne yerleştirmiyoruz. Bu yüzden stake nodelarının ve masternodeların ödülleri aynıdır, her biri blok ödüllerinin %45'ini alır. Geri kalan %10'luk kısım hazineye gönderilir. Hazine şifrelenmiş bir kilide sahip kamuya açık bir adreste tutulmaktadır. Burdaki koinler Stakenet'te yapılacak geliştirmeleri ve yeni projeleri fonlamak için kullanılır. Ayrıca büyük projeleri, ortaklıkları ve önemli geliştirmeleri fonlamak için uzun vadeli geliştirme fonu bulunmaktadır.

2.5 İkinci Katmanlar

Stakenet blokzinciri zincir-içi, zincir-dışı ve zincirlerarası işlemler için farklı ikinci katman çözümleri kullanmaktadır. En önemlileri kendi Masternodeları ve Lightning Network katmanı ile diğer blokzincirlerdeki Tokenizasyon katmanıdır.

2.5.1 Masternodelar

Masternode dünyanın farklı noktalarındaki serverlarda kurulmuş, sistemin merkeziyetsizliğini garanti eden nodelardır. Stake nodeları blokzincirin doğrulanmasından sorumluyken, Masternode ağ için farklı hizmetler sunar. Masternode çalıştırmak için 15.000 XSN'lik bir teminat gerekmektedir. Teminatın amacı, masternode sayısındaki kontrolsüz artışı engellemek ve kötü niyetli nodeları engellemektir. Masternode'un hızlı transfer ve merkezsiz demokrasi özelliklerine ek olarak, XSN masternodeları kripto endüstrisindeki en güçlü istasyonlar olmayı ve sağladığı hizmetler üzerinden Masternode sahiplerine pasif gelir sağlamayı hedeflemektedir. Bu hizmetler:

- XSN Dex'i tutmak ve çalıştırmak.
- Gerekli bütün blokzincir explorerlarını tutarak gerçek merkeziyetsizliği sağlamak.
- Gerekli bütün blokzincirleri tutarak XSN Dex'in merkeziyetsiz ve 'light' kalmasını sağlamak.
- Lightning swapları ve farklı blokzincirler arasında tokenize swapları gerçekleştirmek.
- Lightning Kanallarını tutmak ve takip etmek için bekçi kulesi (watchtower) görevini üstlenmek
- Teminatları Lightning Network likiditesi için kullanmak.
- Farklı blokzincirler arasında tokenize edilmiş koinlerin transferlerini gerçekleştirmek ve bu transferlerin güvenliğini sağlamak.
- Zincir-içi hızlı ve gizli transferleri gerçekleştirmek.
- TOR hizmeti sunmak ve ağ için güvenli çıkış noktaları sağlamak.
- Stakenet ve diğer blokzincirlerin merkeziyetsiz uygulamalarını tutmak.
- Ağın merkeziyetsiz demokrasisi için araçlar sağlamak.
- Boştaki CPU gücünü ve database kapasitesini Stakenet sistemine sunmak.

Masternodelar sayesinde Stakenet blokzinciri, tek bir birimin kontrolü ele geçiremeyeceği ve bütün ağa hizmet eden bir yapı olmaktadır.

2.5.2 Lightning Network

Lightning Network aynı ya da farklı blokzincirler arasında zincir-dışı P2P işlemlerin yapılmasını sağlayan bir ikinci katman çözümüdür. Likidite sağlamak için sağlayıcıların koinlerini kanallarda kilitlemeleri ve farklı nodelar arasında ödeme yolu açılması gerekmektedir. Lightning Network'un nasıl çalıştığını anlamak için tektaraflı ve çifttaraflı ödeme kanallarını açıklamak gerekmektedir.

Tektaraflı Ödeme Kanalları: Lightning kullanmayan klasik ödeme kanalları sadece iki taraf ya da nokta arasında kurulabilir. Bu teknoloji Çoklu-İmza (MultiSig) ve kilitsüresi (locktime) özelliklerini kullanmaktadır. Multisig mekanizması ile, imzalanması için birden fazla private key gerektiren işlemler gerçekleştirilebilir. Bunun anlamı, transferin gerçekleşmesi için iki tarafın da onayının gerekmesidir. Kilitsüresi de Multisig'deki koinlerin bir süreliğine hareketsiz kalmasını sağlar.

Çifttaraflı Ödeme Kanalları: Yukarda bahsedilen mekanizma sadece bir tarafın diğerine koin göndermesine izin verdiği için 'tekyönlü kanal' olarak tanımlanmaktadır. İki taraf birbirleri ile koin takası yapmak istiyorlarsa 'çiftyönlü kanal' kullanmak zorundadırlar. Ancak bu yöntem ortaya bir sorun çıkarır: Neden bir taraf ortadaki bütün koinlere el koyma şansı varken, kilitsüresinin gerektirdiği zaman boyunca beklesin? Bunu engellemek için Lightning 'ortak koruma' mekanizmasını kullanır. İki taraf da kanalı kurmadan önce, sadece kendilerinin bildiği bir sayıyı şifrelenmiş şekilde karşı tarafa iletir. Tektaraflı ödeme kanalında olduğu gibi, ödeme ortakları bir Multisig adres oluştururlar. Multisig adres ağa bildirilmeden önce, iki taraf da taahhüt belgesi oluştururlar. Bu taahhüt belgesine göre fonlar ayrılır, fonun bir bölümü taahhüt belgesi oluşturana, kalan bölümü de iki tarafın da kilit kalktıktan sonra ulaşabileceği, süreli kilitli bir adrese gönderilir. Bu sayede dolandırıcılığı önleyen bir ortam oluşturulur.

Çiftyönlü ödeme kanallarını da anladıktan sonra, bunları ağa entegre etmenin bir yolunu bulmak zorundayız. Lightning Network'ten önce, her ödeme için yeni bir kanal oluşturulması gerekiyordu. Eğer A ile C ticaret yapmak istiyorsa, iki taraf aralarında yeni bir kanal yaratmak zorundaydılar. Bu ikisinin B ile ödeme kanalı oluşturup oluşturmadıklarının bir önemi yoktu. Peki hem A'nın hem de C'nin B ile önceden oluşturdukları bir kanal varsa, neden aralarında yeni bir kanal yaratsınlar? Burdaki sorun B'nin güvenilir olup olmadığıdır. B dolandırıcı ise onu bu transferi engellemekten ve koinlere el koymaktan ne alıkoyabilir? B'nin Lightning node'unu kapatmayacağından ya da yaşayabileceği teknik sorunlar yüzünden node'un çevrimdışı olmayacağından nasıl emin olabiliriz? Bu sorunlara çözüm olarak, Lightning Network şifreli süreli kilitli sözleşmeler (HTLC'ler)
kullanır ve bu durumların oluşmasını engeller. Örnek olarak: C bir sır tutar (burda sır, kanıt olarak kullanılacak şifreleme ile oluşturulmuş rastgele bir sayıdır). Bu sırrı şifrelenmiş olarak A'ya iletir. Böylece şifrelenmiş sayı bir teminat haline gelir. B ancak bu sırrı öğrendiği zaman ödemeyi alır. A bunu şifreleme ile kontrol eder. B ödeme vaadini gerçekleştireceğini söyleyerek, alıcı taraf da şifrelenmiş halini biliyorsa, ona iletir. Prensip olarak, A ile C arasında şifreyi teminat olarak kullanan başka katılımcılar olabilir. HTLC'ler kullanılarak farklı kişiler arasında birden fazla kanal kurulabilir. Gördüğünüz gibi, kurdukları nodelar ile A ve C arasında köprü olan katılımcılar, sistemin bel kemiğini oluşturmaktadırlar. Önemlerini anlamak için onları, klasik blokzincirlerdeki madenciler veya stake yapanlar ile eş tutabiliriz.

Stakenet mevcut Lightning çözümünü, Masternode teminatlarını kanalları fonlama için kullanarak ve Masternodeların taraflar arasında köprü görevi görmesini sağlayarak geliştirmiştir. Bunu farklı masternodeların teminatlarını tek bir havuzda, yani özelleştirilmiş bir çokimzalı adreste toplanmış gibi düşünebilirsiniz. Bu ana havuzda bütün taraflar, Lightning swaplar sayesinde, farklı blokzincirler arasında bile istedikleri kadar iki taraflı kanal açabilirler. Bu çözüm sadece Stakenet'e değil, Lightning Network desteğine sahip her koine ciddi fayda sağlayacaktır çünkü XSN Bitcoin ve Litecoin işlemleri için de 'aracı koin' işlevi görecektir. Sonuçta Stakenet düşük fonlu kanal riskini ortadan kaldıracak ve farklı Lightning Network ağlarını bir araya getirecek bir çözüm sunmaktadır.

2.5.3 Tokenizasyon

Tokenizasyon bir varlığın haklarının dijital tokenlere çevrilmesine verilen isimdir. Her token belirtilen varlığı temsil eder. Blokzincir bu süreçte sahiplik haklarının korunmasını sağlar. Ethereum ve EOS blokzincirleri için geliştirdiğimiz XSN tokenlar, orjinal XSN koinlerini temsil etmektedir ve istenildiğinde bir köprü protokolü vasıtası ile Stakenet, Ethereum ve EOS arasında çevrilebilirler. Özel çokimzalı adresler, hashkilitler ve sürelikilitler sayesinde kendi zincirimizde XSN'leri kilitleyip, diğer blokzincirler üzerinde XSNETH ve XSNEOS tokenları serbest bırakabiliriz. Stakenet kullanıcıları bu işlemleri kendileri yapmayacaklar, bütün bu süreç akıllı sözleşmeler tarafından yürütülecek ve kendi Masternode katmanımızda takip edilecek.

Bütün bu süreçlerde XSN sayısında bir artış olmayacak: Kilitli olan XSN sayısı serbest kalan tokenlarla eşit olacak ve bu işlemler denetlenebilir olacak. Köprü protokolü oluşturulup XSN koin Ethereum ya da EOS ağında kullanılmak istendiği zaman, XSN'ler özel bir akıllı sözleşmeli hesapta kilitli halde duracak. Böylece kullanıcı diğer tokenlar üzerinde kontrol elde ederken, koinlere ulaşımı engellenecek. Stakenet blokzinciri tokenizasyon yoluyla Ethereum ve EOS'a bağlandığında, bu blokzincirlerdeki bütün tokenları zincirlerarası ağımıza entegre edebileceğiz. Bu sayede kullanıcılar farklı blokzincirlerde yer alan koinler ve tokenlarla istedikleri gibi işlem yapabilecekler. Bu sistemin bir diğer avantajı, tokenları destekleyen her blokzinciri ağımıza ekleme şansına sahibiz. Böylece Stakenet zincirlerarası ağı her gün daha da büyüyerek, yeni geliştiricilerinin ürünlerini kendi üzerinde kullanılabilir hale getirecek.

2.6 Genel Bilgiler

Adı: Stakenet.
Kısaltma: XSN.
Para Tipi: Koin.
Konsensüs: Proof of Stake koin üretimi, Trustless Proof of Stake.
Coinage: Aktif, 24 saat.
Şifreleme Algoritması: X11.
Blok üretim süresi: 60 saniye.
Blok büyüklüğü: 1-4 MB.
Son blok ödülü: 20 XSN.
Blok ödül dağılımı: 45% Masternodelar, 45% stake, 10% hazine.
Masternode teminatı: 15.000 XSN.
Yönetim: Merkeziyetsiz demokrasi.
Fonlama: Merkeziyetsiz hazine, ICO yok, premine yok.
Lightning Network: Mainnet'te aktif
Zincir-içi ölçeklenebilirlik: Saniyede 240 işlem
Zincir-içi işlem ücreti: ~0.00001 XSN/kB.
Zincir-dışı ölçeklenebilirlik: Teorik olarak sınırsız işlem kapasitesi.
Zincir-dışı işlem ücreti: Fiilen sıfır.
Zincirlerarası arayüz: Lightning Swaplar, Tokenizasyon Swapları

3 XSN Ürünleri

XSN Ürünleri, farklı blokzincirlerle uğraşırken kullanıcı-dostu ve güvenli bir ortam sunmak için, yazılımsal ve donanımsal çözümler sunmaktadır.

3.1 Stakenet Cüzdanı

Stakenet Cüzdanı private keyleri sizin kontrolünüzde olan light çoklu-koin cüzdanıdır. Mobil ve masaüstü versiyonları ile Stakenet'in temel ürünü olan bu cüzdanın üzerinden, bütün işlemleri gerçekleştirebilirsiniz. Cüzdanlar kriptopara evreninin temel ve tamamlayıcı parçalarıdır. Bitcoin ve Ethereum gibi dijital paraları saklayabileceğiniz ve transfer edebileceğiniz bir çantadır. Çoğu koinin resmi core ve light cüzdanları var ama karşımıza şu sorun çıkmakta: Kullanıcı sahip olduğu her kriptopara için ayrı bir cüzdan bulundurmak zorunda ve bu kadar cüzdanı yönetmek sıkıcı hale gelmektedir.

Stakenet, Masternode ağının birçok blokzincirin database'ini ve tam node'unu tutması sayesinde farklı blokzincirlerde işlem yapma olanağı sunar ve bu soruna çözüm sağlar. Bu blokzincirlerin ikinci katmanda tutulması Stakenet Cüzdan'ın gerçek anlamda 'light' olarak çalışmasını sağlar. Diğer light cüzdanlardan farklı olarak, Stakenet Cüzdanı koin almak, göndermek ve saklamaktan fazlasını yapacak. Diğer XSN Ürünleri sayesinde, XSN Viper gibi, Stakenet sistemindeki tüm kullanıcılar donanım cüzdanından stake yapabilmek, masternode kurulumu ya da Lightning Network node'u çalıştırmak gibi işlemleri cüzdan üzerinden yapabilecekler. Ek olarak, Stakenet Cüzdanı'nın XSN Dex'e bağlı trade motoru sayesinde kullanıcılar private keylerini riske atmadan farklı blokzincirler üzerinden swap yapabilecekler.

Stakenet Cüzdanı zincirlerarası sistemimize güvenli giriş için TOR desteği sunuyor. Bu hizmet Masternode katmanımız tarafından kontrol edilecektir. TOR, ağ üzerinde anonim bir iletişim sağlamak için IP saklayan bir sistemdir. Bütün Stakenet Masternodeları, kullanıcının konumunu saklaması için blokzincir trafiğimizi binlerce farklı yayın arasından yapmaktadır. Basit şekilde anlatmak gerekirse, kullanıcılar cüzdanlarını TOR ağına bağladıklarında, yaptıkları işlemler dünyanın farklı noktalarına dağılmış sayısız masternode serverı üzerinden ilerler. Her server kendisine bilgi ileten bir önceki serverın bilgilerini siler. Böylece işlem karşı tarafa, yani çıkış noktasına iletildiğinde bağlantının nereden kurulduğuna dair hiçbir bilgi iletilmemiş olur.

3.2 XSN Koin

XSN P2P ödeme yöntemine izin veren son teknoloji ürünü bir kriptoparadır. XSN herhangi bir merkez bankasının bastığı paranın sahip olamayacağı özelliklere sahiptir: Açık, izne veya güvene gerek duymaz, merkeziyetsizdir, sansürlenemez, güvenlidir, mübadele edilebilir, farklı sistemlerle uyumlu çalışabilir ve sabit artış hızına sahiptir. Stakenet ekosistemindeki işlemleri de dikkate alınca, küresel ölçekte gerçek zamanlı bir değişim aracı önümüzde duruyor. Stakenet'in sunduğu hizmetlerinden alınan bütün işlem ücretleri XSN olarak ödenir. Ücretlerin XSN'e çevrilmesi, çoğu zaman kullanıcının fark etmeyeceği şekilde arka planda Lightning Swapler ile gerçekleşir. Bu belgede bahsedilen her hizmet, gas ya da Stakenet'in kurumsal işleyisi, hepsi XSN'in üzerinden ilerlemektedir. Ekosistemin işlemesi için gereken en önemli parçadır.

3.3 XSN Core

XSN Core Stakenet blokzinciri üzerinden gönderme, alma ve saklama görevlerini yerine getiren açık kaynaklı bir yazılımdır. Stakenet ağında Masternode, lightning node, stake node ve merchant node çalıştırmak için gereken full node'dur. Bu nodelar P2P bağlantıları sağlayıp bilgi paylaşımını kontrol ettikleri için blokzincirin temel direkleridir. XSN Core popüler işletim sistemlerinin hepsiyle (Linux MacOS, Windows) uyumludur ve komut istemi (command line) veya grafiksel arayüz ile kontrol edilebilir.

3.4 XSN Excalibur

XSN Excalibur kendi geliştirdiğimiz açık kaynaklı private key yönetimi ve saklanması sistemi. Trezor'un saygın kodu üzerinden geliştirilen sistem, Stakenet Cüzdan'da kelime listesi ile (mnemonic phrase) ile her blokzincir için özel private keyler oluşturmaktadır. XSN Excalibur sayesinde Stakenet kullanıcıları sahip oldukları kelime listesini kullanarak istedikleri zaman tekrardan kriptoparalarını kontrol edebilirler.

3.5 XSN DEX

Kripto borsalar kripto piyasasına likidite sağlayaran sistemin temel unsurlarıdırlar. Kripto dünyası için bu kadar önemli pozisyonda olan kurumların çoğu, merkezi ve birkaç server üzerinden çalışmaktadırlar. Bu durum borsaların sınırlı bir altyapıya sahip olmasına yol açmakta ve hacklere açık bir duruma sokmaktadır. Kullanıcı merkezi bir borsada işlem yapmak istediğinde koinlerini bu yapılara teslim eder ve hem koinlerinin kontrolü hem de koinlerden sağlayacağı faydalardan feragat ederç Stakenet bu soruna XSN Dex ile çözüm getirmeyi hedeflemektedir.

Elimize Stakenet Cüzdanı, Lightning Swaplar ve Tokenize Swapler olunca bu sorunu çözmek zor bir iş değil. Şu an aktif durumda olan birkaç merkeziyetsiz borsa bulunmakta ancak bunların çoğu merkezi unsurlar üzerinden çalışmaktadır. Stakenet, gerçek merkeziyetsizliğe sahip çalışan ilk borsa olacak, bunu da Masternodeları üzerinden başaracak.

Kullanıcıların XSN Dex'te tuttukları koinler işlem tamamlanana kadar cüzdanlarından çıkmaz, böylece devamlı olarak kullanıcıların kontrolünde olurlar. Kullanıcılar bu sayede koinlerin özelliklerini kullanmaya devam edebilirler ve stake yapma gib özelliklerden faydalanmaya devam ederler. Platform kullanıcılarından kimlik bilgisi istemediği için kullanıcılar endişelenmeden anonim bir şekilde işlemlerini yapabilirler. Bütün işlemler merkezi bir yapının işin içine girmediği P2P bağlantılar üzerinden yapılır. Bu sayede işlemler güvenli ve düşük ücretli olur.

XSN Dex'in başka bir önemli özelliği ise diğer merkeziyetsiz borsalarla bağlantı kurabilmesi, yani kümelemedir(aggregate). Tam merkeziyetsizliğe sahip diğer borsaların doğrulama nodelarını Stakenet zincirlerarası ekonomisine bağlamak ve bu borsalardaki emir bloklarından faydalanmak mümkündür. Kümeleme yoluyla diğer borsalardan işlem yapmak ile XSN Dex'in kendi sistemi üzerinden işlem yapmak arasında sadece birkaç saniye fark oluşmaktadır. Bunun sebebi köprü protokolünün iki borsa arasında tokenize varlıkları swap etme zorunluluğudur. Sonuç olarak Stakenet kullanıcıları uyumlu bütün merkeziyetsiz borsalar üzerinden işlem yapabilirler.

3.6 XSN Viper

XS Viper, temel Lightning Network routing özelliklerine sahip olan ve Lightning Network node olarak çalışarak, Stakenet, Bitcoin ve Litecoin için işlem ücretleri kazanabilen özelleştirilmiş bir donanım cüzdanıdır. Gelecek olan versiyonunda birden fazla hub kurulumu ve Masternode çalıştırmak gibi özelliklere sahip olacaktır. Bu sayede kullanıcılar, güvenli bir şekilde farklı zincirler üzerinden işlem yapabilecekler. XSN Viper, açık kaynak kodlu XSN Excalibur sayesinde, private keyleri ayrı bir yerden kumanda edilen çevrimdışı bir alanda saklar. Bu sayede Stakenet kullanıcıları tek bir donanım cüzdanına desteklenen bütün koinleri saklayabilirler.

3.7 XSN Cloud

XSN Cloud, özellikle deneyimsiz XSN kullanıcılarına kolay ve daha iyi hizmet sunmak için oluşturulmuş bir merkezi uygulamadır. XSN Cloud Stakenet blokzincirinden ve merkeziyetsiz ekosisteminden bağımsız bir yapıdır. Basitçe anlatmak gerekirse, https://stakenet.io bilgilendirici bir websitesidir ve XSN Cloud da bu sitenin bir parçasıdır. Stakenet ise blokzincir üzerine kurulmuş merkeziyetsiz bir ağdır. XSN Cloud'un sundukları:

- **Stake Hizmeti (Çevrimiçi stake cüzdanı):** Otomatik olarak stake yapan cüzdanlar. Bu hesaplara gönderilen koinler ana adrese (havuz) aktarılır ve kullanıcılar gerçek zamanlı ve düzenli olarak stake geliri elde ederler.

- **Masternode Hizmeti (Masternode kurulumu):** Kendi sunmuş olduğumuz güven gerektirmeyen Masternode kurulum çözümü. Koinlerin kontrolü sizde olduğu için bu hizmetin herhangi bir riski yoktur.

- **Takip Hizmetleri:** Masternodelar ve TPoS sözleşmeleri için gerçek zamanlı takip hizmeti. Herhangi bir sorun oluştuğunda müşteriler anında e-mail yolu ile uyarılırlar.

- **ROI Hesaplayıcı**: Stake nodeları ile Masternodeları arasındaki ilişki her gün değişir, dolayısıyla kârlılık oranları da aynı kalmaz. ROI Hesaplayıcısı sizin için en kârlı aracı bulmanızı sağlar.

XSN Cloud'un bazı hizmetleri ücretlidir. Bu hizmetlerden elde edilen gelir XSN Cloud hazinesine aktarılır, masraflar ve yeni eklenecek özellikler için gereken harcamalar bu fondan karşılanır. XSN Cloud'a göndermiş olduğunuz koinlerin sizin kontrolünüzde olmadığını ve private keylerine sahip olmayacağınızı unutmayın. XSN Cloud adreslerine büyük miktarda koin yatırmayın, bunun yerine TPos ya da stake kullanmanız sizin için daha uygun olacaktır. XSN Cloud tecrübesiz ve diğer yöntemlerle gelir elde etme şansı olmayan az miktarda koine sahip kullanıcılar için ideal bir çözümdür. Stake Hizmeti haricindeki XSN Cloud hizmetleri güven gerektirmeyen çözümlerdir ve koinlerin kontrolü sizde olduğu için güvenlidir.

4 Özet

Stakenet güven gerektirmeyen zincirlerarası ekonomi sistemi sunan ve hissedarlarına gelir sağlayan dağınık bir ağdır. Lightning Network, Masternodelar ve merkeziyetsiz uygulamalar gibi ikinci katman çözümlerine sahip gelişmiş bir Proof of Stake blokzinciri üzerine temellenmiştir. Zincir-içi bir saniyelik onay süresine sahipyit ve saniyede 240 işlem yapılabilir. İşlemlerin büyük bölümünün yapılacağı Lightning Network üzerinden ise sıfıra yakın ücretlerle, sınırsız sayıda anlık işlem yapılabilir. Stakenet'in amacı, kullanıcıların Stakenet'in kendi coini XSN'i kullanarak Lightning Network ve diğer zincirlerarası teknolojiler sayesinde farklı blokzincirler üzerinde işlem yapabilmelerini sağlamaktır. Stakenet herhangi bir programlala dili sınırı olmadan, XSN Dex benzeri merkeziyetsiz uygulamaları çalıştırır. Bu merkeziyetsiz uygulamalar XSN Masternodelar üzerinden çalışır ve bu uygulamlardan elde edilen gelirleri de Masternode sahipleri alırlar. Diğer kriptoparaların aksine, Stakenet yeni bir standart yaratma iddiasında değildir. Bunun yerine mevcut BTC / LN protokolü ve akıllı sözleşmeleri üzerinden çözümler üretir.

Stakenet Proof of Stake blokzincirler arasında en yüksek güvenliğe sahip olanlardan birisidir. Bir Stakenet buluşu olan TPoS sayesinde çevrimdışı stake yapma özelliğine sahiptir. TPoS, koin sahiplerinin hiçbir risk almadan, koinlerini çevrimdışı cüzdanlarda tutarak pasif gelir elde etmelerini sağlar. Ayrıca Stakenet Masternodelarının devasa merkeziyetsiz bilgisayar ağı, olağanüstü bir işlem gücüne sahiptir. Blokzincir üzerine kurulu merkeziyetsiz uygulamaları çalıştıracak yüksek güçlü bir yapı oluştururlar. Örnek olarak, farklı koinler arasında Lightning Swapler ve Tokenize Swaplar yapabilen Stakenet Dex, XSN Masternode ağının üzerinde çalışır ve Masternode teminatları Ligtning Network kanallarına gerekli likiditeyi sağlarlar.

Stakenet Masternodelu blokzincirler arasında Lightning Network uyumluluğuna sahip ilk koin, Bitcoin ve Litecoin'den sonra Lightning Netwok üzerinden atomik swap (Lightning Swap) gerçekleştiren öncü koindir. Stakenet blokzinciri Lightning Network desteği olan herhangi bir merchant, cüzdan ya da kripto donanım ile uyumludur. Stakenet'in zincirlerarası özellikleri sayesinde kullanıcılar Bitcoin ya da Lightning Network destekli herhangi bir koin ile ödeme yapabilir. Lightning Network destekli ödemeleri kabul eden binlerce satıcı bulunmakta ve sayıları gün geçtikçe artmaktadır.

Stakenet Lightning Network ile akıllı sözleşmeler çözümlerini birleştirerek en güvenli, en hızlı ve en ucuz blokzincir ekonomisini oluşturmakta ve donanım cüzdanlardan güven gerektirmeyen stake, takas ve ödeme yöntemleri geliştirmektedir.