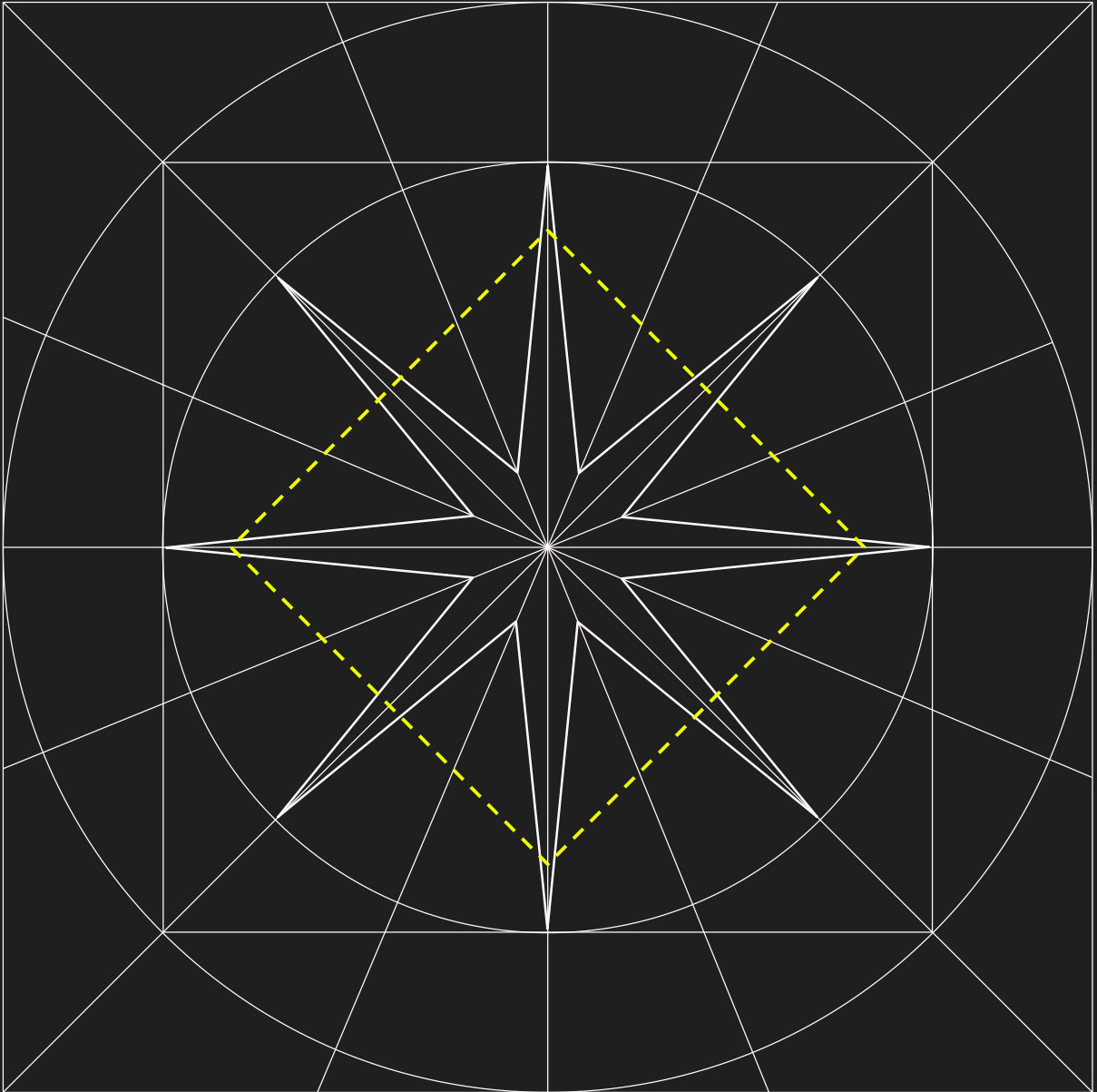




# Evrensel Doğrulama Katmanı İçin Bir Litepaper



Zahary Karadjov ve Magnus Ahmad tarafından  
Ağustos 2025



## Özet

Merkezi olmayan teknolojinin gelişimi iki temel sınırlama ile kısıtlanmıştır: blok zincirlerinin internet ve gerçek dünya ile tam entegrasyonunu engelleyen Bağlantı Engeli ve teknolojiyi dünya ekonomisini gerçekçi bir şekilde güçlendirmek için gerekli kapasiteden yoksun bırakan Verim Engeli. Bu durum, merkezi olmayan uygulamaları nesnel olarak doğrulanabilir mantığın dar bir alanına hapsederek dijital dünyamızı yeniden şekillendirme potansiyellerini sınırlandırmıştır. Blocksense, bu engelleri sistematik olarak ortadan kaldırmak için tasarlanmış yeni, hizmet odaklı bir blok zinciri mimarisi sunuyor. Daha önce ulaşılamayacağı düşünülen bir ölçekte hem nesnel hem de öznel arası gerçekleri güvenli bir şekilde işleyebilen evrensel bir doğrulama katmanı sunuyoruz. Çözümümüz iki temel yenilik üzerine inşa edilmiştir:

- Öznel Arası Doğruluk Makinesi:** Oracle problemini, sıfır bilgi kanıtlarını (ZKP'ler) kullanan rüşvete dayanıklı bir konsensüs mekanizması olan zkSchellingCoin ile çözüyoruz. seçmen gizliliğini sağlamak. Yüksek riskli anlaşmazlıklar için, **Futarchy**'yi nihai bir hakem olarak kullanıyoruz, tüm küresel pazarın kolektif likit sermayesi ile ağı güvence altına alan ve kötü niyetli saldırıları ekonomik olarak mantıksız hale getiren talep üzerine tahmin pazarları oluşturuyoruz.
- Sınırsız Verim Motoru:** Blok zincirini radikal bir şekilde paralelleştiren Ayrıştırılmış Durum Makinesi Çoğaltma (DSMR) mimarisini uyguluyoruz. İşlem sıralaması, birden fazla parçalanmış DAG-BFT mutabakat örneği aracılığıyla yatay olarak ölçeklendirilirken, yürütme, artımlı olarak doğrulanabilir bir hesaplama (IVC) aracılığıyla paralelleştirilir çerçevede. Bu tasarım, ağ veriminin katılımcı düğüm sayısı ile doğrusal olarak artmasını sağlar.

Bu temel yenilikler, yeni bir hesaplama bolluğu ekonomik paradigmasını mümkün kılmaktadır. Blocksense ağı, doğrulanmış hesaplama için birleşik bir pazar yeri olarak çalışarak, büyük kaynakları çeken ve maliyetleri düşüren güçlü bir ekonomik çark oluşturur. Bu verimlilik, özel ve doğrulanabilir yapay zeka ajanları gibi uygulamalar için yeni bir tasarım alanının kilidini açarken, passkey-native hesaplar ve sıfır maliyetli işlemler içeren sürdürülebilir bir kullanıcı deneyimi sunmamızı sağlar. Temel bağlantı ve ölçek sorunlarını çözen Blocksense, yeni nesil merkezi olmayan web için temel ara katman yazılımı olmaya hazırlanıyor.



## 1. Giriş:

# Blockchain'in Engellerini Aşmak

On yılı aşkın bir süredir blockchain teknolojisi daha açık, şeffaf ve kullanıcı merkezli bir dijital gelecek inşa etmeyi vaat ediyor. Ancak, muazzam inovasyona rağmen, dönüştürücü potansiyeli temel mimari kısıtlamalar tarafından engellenmeye devam ediyor. Blokzincirler "dijital adalar" olarak işlemektedir - güvenli ve kendi içinde tutarlı, ancak devrim yaratmayı amaçladıkları dünyadan son derece izole. Bu izolasyon, tüm alanın yörüngesini belirleyen iki temel engel olarak ortaya çıkmaktadır.

Bunlardan ilki **Bağlantı Engelidir**. Blok zincirleri temelde dış sistemlerden kopuktur; küresel ekonominin temelini oluşturan karmaşık, deterministik olmayan ve öznel bilgileri almak ve üzerinde anlaşmak için yerel, güvenli bir mekanizmadan yoksundurlar. Sektörün buna yanıtı olan kehanet, büyük ölçüde merkezi bir yapıda kalmış, ademi merkezizetiğin temel vizyonunda başarısız olmuş ve verimsizliklere ve kapı bekçisi dinamiklerine yol açan bir güç dengesizliği yaratmıştır.

İkincisi ise **Verim Bariyeridir**. Her tam düğümün her bir işlemi işlemesi gereken kanonik blok zinciri tasarımı, ölçeklenebilirlik pahasına güvenliği sağlar. Bu "tüm düğümler-doğrulamalı" paradigması, işlem hızını sınırlayan, maliyetleri artıran ve nihayetinde ana akım benimsemeyi engelleyen bir hesaplama darboğazı yaratır. Mevcut ölçeklendirme çözümleri, yenilikçi olmakla birlikte, genellikle önemli ölçüde karmaşıklık ve ekosistem parçalanması getirmiş, temel mimari sınırlamayı çözmeden kullanıcı deneyimini daha da engellemiştir.

Blocksense bu zorluklara doğrudan bir yanittir. Bu sadece başka bir Katman-1 blok zinciri ya da mevcut oracle tasarımları üzerinde artımlı bir iyileştirme değildir. Yeni bir paradigma sunuyoruz: hem Web3 hem de Web2 için evrensel bir doğrulama katmanı olarak hizmet vermek üzere sıfırdan tasarlanan **hizmet odaklı bir blok zinciri**.

Her türlü bilgi hakkında güvenli bir şekilde akıl yürütebilen ve sınırsız ölçekte çalışabilen yeni bir "Doğrulanmış Otonom Hizmetler" sınıfı için altyapı.

Blocksense, bağlantı ve verim gibi ikili sorunları çözerek, daha önce bilim kurgu dünyasıyla sınırlı kalan uygulamaların önünü açıyor: merkezi olmayan yapay zeka ajanları

Gerçek dünya varlıklarını, canlı internet verileriyle desteklenen karmaşık finansal araçları ve benzeri görülmemiş bir verimlilikle çalışan küresel bilgi işlem pazarlarını yönetmek. Bu makale, Blocksense'in bu vizyonu gerçekleştirmesini sağlayacak temel teknolojik yenilikleri, ekonomik modelleri ve pazara açılma stratejisini detaylandırmaktadır.



## 2. Temel İnovasyon I: Öznelerarası Hakikat Makinesi

Bağlanabilirlik Engelini aşmak için, bir protokolün **özneler arası doğrular** (bir varlığın fiyatı veya bir olayın sonucu gibi, katılımcıların çoğunluğunun aynı görüşü paylaşmasının muhtemel olduğu, ancak yalnızca deterministik hesaplama ile doğrulanamayan **bilgiler**) üzerinde güvenli bir şekilde fikir birliği oluşturabilmesi gerekir. Bunun için temel yaklaşım, ilk olarak Vitalik Buterin tarafından önerilen SchellingCoin oyunudur<sup>[^1]</sup>. Bu oyun, rasyonel ve koordine olmayan aktörlerden oluşan bir ağın, en karlı bireysel stratejileri olduğu için doğru bir cevap üzerinde birleşeceğini varsaymaktadır. Zarif olmakla birlikte, güçlü akıllı sözleşme platformlarının ortaya çıkması, bu fikrin naif uygulamalarında kritik bir güvenlik açığını ortaya çıkarmıştır.

[^1]: Vitalik Buterin, "SchellingCoin: A Minimal-Trust Universal Data Feed," Ethereum Blog, 2014. <https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed>

### 2.1 SchellingCoin'in Aşıl Topuğu: Güvensiz Rüşvet

Tek bir kehanet güncellemesinin milyarlarca doların kaderini etkileyebildiği herhangi bir sistemde, sonucu bozma teşviki çok büyüktür. Halka açık defterler ve Turing-komple akıllı sözleşmelerin birleşimi ölümcül bir saldırı vektörü yaratır: **güvenilmez rüşvet**. Bir saldırgan, programlı ve anonim olarak sofistike bir rüşvet kampanyası yürüten emanet benzeri bir akıllı sözleşmeyi, kendisi ya da katılımcılar için hiçbir risk oluşturmadan devreye sokabilir.

Bu saldırı, katılımcıların oy verme haklarını ve nasıl oy verdiklerini kanıtlayabildikleri herhangi bir oylama protokolüne karşı çalışır. Saldırı şu şekilde gerçekleşir:

1. **Ödül Yerleştirme:** Bir saldırgan akıllı bir sözleşmeye büyük bir ödül koyarak kötü niyetli bir sonuç için oy veren herhangi bir doğrulayıcıya ödül vaat eder.
2. **Güvensiz Koordinasyon:** Doğrulayıcılar sözleşmenin kodunu bağımsız olarak inceleyebilir ve uygunluk halinde ödülün garanti edildiğini doğrulayabilir. ZKP'leri kullanarak, kimliklerini açıklamadan katılmaya istekli olduklarını bile bildirebilirler.
3. **Kötü Amaçlı Oylama ve Ödeme:** Kritik bir katılımcı kitlesine ulaşıldığında, hepsi kötü niyetli oy kullanır. Akıllı sözleşme, katılımlarını kanıtlamalarına olanak tanır - yine ZKP'lerin sofistike kullanımı, saldırıya doğrudan, atfedilebilir bir bağlantı oluşturmadan ödülleri yeni, anonim bir adrese talep etmelerini sağlar.
4. **Risksiz Yürütme:** Saldırı yeterli sayıda katılımcıyı çekemezse, akıllı sözleşme ödülü saldırgana iade eder.



Bu saldırının yıkıcı gücü güvene dayanmayan doğasıdır; kodun soğuk mantığı gerekli olan tek emanettir. Daha ayrıntılı bir sözleşme, peşin bir ödül gereksinimini bile ortadan kaldırabilir ve bunun yerine, elde edilen gelecekteki kârın bir payını temsil eden bir ödeme belirteci koyabilir.

## 2.2 Derinlemesine Savunma: Çok Katmanlı Bir Güvenlik Modeli

Blocksense, özneler arası fikir birliğini güvence altına almak için çok katmanlı, derinlemesine savunma stratejisi kullanır ve saldırıları her aşamada giderek daha zor ve ekonomik olarak mantıksız hale getirir.

### Katman 1: Gizli Alt Komiteler & zkSchellingCoin

İlk savunma hattımız SchellingCoin prensibinin geliştirilmiş bir uygulaması olan zkSchellingCoin'dir. Protokol, herhangi bir veri talebi için oylama yapmak üzere küçük, rastgele ve gizli bir staker alt komitesi seçer. MACI (Minimal Anti-Collusion Infrastructure) gibi zorlamaya dirençli e-oylama protokolleri araştırmalarından yararlanarak, bir seçmenin bir saldırganın sözleşmesinin gerektirdiği kanıt üretmesini kriptografik olarak imkansız hale getirmek için sıfır bilgi kanıtları kullanıyoruz. Sistem, bir seçmenin *hem* belirli bir konuda oy verme hakkını hem de oyunun içeriğini kanıtlamasını imkansız hale getirmektedir. Bu tam kanıt olmadan, güvenilmez rüşvet çöker.

### Katman 2: Dağıtılmış Koordinasyon ve İtibar

MACI seçmenlerin nasıl oy v e r d i k l e r i n i kanıtlamalarını engellerken, standart tasarımında tek bir hata noktası vardır: şifrelenmiş oyları işleyen Koordinatör. Kötü niyetli bir Koordinatör nihai çeteleyi taklit edemez, ancak saldırganlarla işbirliği yaparak oy gizliliğini bozabilir.

Blocksense, **Koordinatör rolünü** MPC destekli ortak SNARK'lar kullanarak **dağıtarak** bu güvenlik açığını ortadan kaldırır. Oy sayımı, kimliklerini açıklayan ve dinamik bir **itibar piyasası** aracılığıyla seçilen bir dizi operatör tarafından gerçekleştirilir. Verilerin nihai kullanıcıları (yüksek TVS'ye sahip protokoller ve dApp'ler), tercih edilen koordinatörleri belirtmek için kullandıkları onay kredileriyle ödüllendirilir. Kötü niyetli güncellemeleri işaretlemeyen koordinatörler, güçlü bir ikinci savunma katmanı oluşturan kesme işlemiyle karşı karşıya kalır: bir saldırgan artık yalnızca stake sistemini değil, aynı zamanda zarar vermek istedikleri varlıklar tarafından kontrol edilen itibar sistemini de yıkmak zorundadır. Bu model, güvenlik için ham sermaye gerekliliklerini önemli ölçüde azaltarak, ekosistemin yerleşik güven ağlarından güç alır, tıpkı günümüzde tamamen itibarla çalışan baskın merkezi oracle'lar gibi.

### Katman 3: Açık Zorluklar ve Anlaşmazlıkların Arttırılması

Bir alt komite ve koordinatörleri bir sonuç ürettiğinde, bu sonuç hemen kesinleşmez. Her veri güncellemesi yapılandırılabilir bir **anlaşmazlık dönemine** girer. **Bekçi düğümleri**, önerilen tüm güncellemeleri sürekli olarak izleyen ve kötü niyetli veya yanlış bir sonuç tespit ettikten sonra milisaniyeler içinde bir anlaşmazlık başlatabilen **otomatik bir yazılım çalıştırabildiğinden**, bu süre minimum olacak şekilde tasarlanmıştır.



Daha da önemlisi, belirli bir veri noktası için devam eden bir anlaşmazlık hizmetin canlılığını etkilemez; müteakip güncellemeyi sağlamak için derhal yeni bir komite seçilir ve protokolün çalışır durumda kalması sağlanır. İhtilaf süresi boyunca, **herkes** bir ihtilaf senedi göndererek orijinal sonuca **itiraz edebilir**. Bu eylem derhal riskleri artırır: anlaşmazlık artık küçük komite ile tek bir meydan okuyucu arasında değildir, ancak **protokoldeki tüm paydaşların bir taraf tutmasını** gerektirir. Kaybeden tarafın destekçileri kesintiye uğrayarak meydan okumaların ciddiye alınmasını sağlar ve kötü niyetli bir güncellemeyi sisteme sokmanın ekonomik maliyetini yükseltir.

#### **Katman 4: Futarchy, Nihai Hakem**

Bir anlaşmazlık tam bir ağı oylamasına dönüşürse, yeterince sermaye sahibi bir saldırgan teorik olarak %51'lik bir hisse saldırısıyla kazanabilir. Bu varoluşsal tehdide karşı koymak için Blocksense son ve en güçlü savunma katmanını entegre eder: **Futarchy**.

Futarchy, "değerlere oy verin, ancak inançlara bahis yapın" özdeyişiyle özetlenen bir yönetim mekanizmasıdır. Bir eylemi doğrudan oylamak yerine, topluluk önce başarıyı yansıtan bir ölçüt (bir değer) üzerinde anlaşır. Ardından, hangi eylemin bu ölçütü (bir inanç) olumlu yönde etkileme olasılığının en yüksek olduğunu belirlemek için tahmin piyasaları kullanılır. Piyasanın en iyi sonucu öngördüğü eylem otomatik olarak seçilir.

Blocksense'de bu, isteğe bağlı bir güvenlik sistemine uyarlanmıştır.

- 1. Tahmin Piyasaları Açılıyor:** Protokol, son derece spesifik sorular içeren iki tahmin piyasasını otomatik olarak oluşturur:
  - ◆ **M Pazarı:** Kötü niyetli M İddiası yayınlanırsa Blocksense tokenının fiyatı önümüzdeki iki hafta içinde %50'den fazla düşecek mi?
  - ◆ **Market T:** Doğru İddia T yayınlanırsa Blocksense token fiyatı önümüzdeki iki hafta içinde %50'den fazla düşecek mi?
- 2. Piyasa Çözüm Mekaniği:** Önceden belirlenmiş bir süre boyunca her iki piyasa da alım satıma açıktır. İşlem süresi sona erdikten sonra protokol, piyasası **fiyat çöküşü olasılığını en düşük** tahmin eden talebi (M veya T) otomatik olarak seçer. Bu karar asimetrik bir çözümü tetikler: Seçilen piyasa (örneğin, T Piyasası) yürürlükte kalır ve gözlem döneminden sonra normal şekilde sonuçlanırken, seçilmeyen piyasa (M Piyasası) geçersiz kılınır ve tüm sermaye bahisçilere iade edilir.
- 3. Kaçınılmaz Piyasa Mutabakatı:** Başarılı, değer çıkaran bir saldırının net bir sonucu vardır: tüm dürüst stakerlar kesilecek, protokol saldırganın eline geçecek ve doğru bir bilgi kaynağı olarak Blocksense protokolüne olan güven yok olacaktır. Token fiyatı kaçınılmaz olarak sıfıra doğru eğilim gösterecektir. Bu nedenle, rasyonel Dünya çapındaki piyasa katılımcıları M Piyasasına "Evet" demek için acele edeceklerdir, çünkü bu sonuç



olasıdır. Tersine, doğru olan T iddiasının yayınlanması halinde fiyatların düşmesini beklemek için hiçbir neden yoktur.

4. **Kazanılmaz Ekonomik Savaş:** Kazanmak için saldırganın bu açık gerçeğe karşı bahis oynayarak tahmin piyasalarını manipüle etmesi gerekir. Özünde, karlı, düşük riskli bir bahse giren dünyadaki her rasyonel aktörü finansal olarak alt etmeleri gerekir. Böyle bir saldırının maliyeti Blocksense'e yatırılan toplam değerle değil, **tahmin piyasasına katılmak için mevcut olan tüm likit sermaye ile ölçülür**. Bir güvenlik krizini küresel bir ticaret fırsatına dönüştüren Futarchy, nihai kripto-ekonomik destek olarak hizmet eder ve herhangi bir rasyonel %51 saldırısını engelleyici derecede pahalı hale getirir.

## 3. Temel Yenilik II: Sınırsız Verim Motoru

Geleneksel blok zincirlerinin monolitik mimarisi, Verim Bariyerinin temel nedenidir. Blocksense, ağ işlevlerini ayıran ve bunları bağımsız olarak ölçeklendiren radikal paralel bir tasarımla bu engeli yıkarak teorik olarak sınırsız verim sağlar.

**3.1 Ayrıştırılmış Mimari: Sıralamayı Yürütmeden Ayırmak** Blocksense, Ayrılmış Durum Makinesi Çoğaltma (DSMR) modeli üzerine inşa edilmiştir. Bu paradigmada, ağın sorumlulukları iki farklı, eşzamansız katmana ayrılmıştır:

1. **Sıralama Katmanı (Mempool):** Bu katmanın tek sorumluluğu kullanıcılardan gelen işlemleri almak ve bunlar için kesin, küresel bir düzen oluşturmaktır.
2. **Yürütme Katmanı:** Bu katman sonlandırılmış işlem dizisini tüketir ve durum geçişlerini işler.

Bu ayırım, her katmanın özel teknikler kullanılarak bağımsız olarak optimize edilmesini ve ölçeklendirilmesini sağlar.

### 3.2 Ölçeklenebilir Sıralama: Paralel DAG Mempool

Sınırsız sipariş kapasitesi elde etmek için Blocksense, çoklu, bağımsız Yönlendirilmiş Asıklık Grafik (DAG) tabanlı BFT konsensüs örneklerinden oluşan yeni bir paralel mempool uygular. Sui'nin Mysticeti ve Aptos'un Raptr gibi, ~100 düğümden oluşan doğrulayıcı setleriyle test koşullarında saniyenin altında kesinlik ve 100.000 TPS'yi aşan verim gösteren en son protokollerden yararlanıyoruz.





Mekanizma basit ancak güçlüdür:

- ◆ **İşlem Parçalama:** İşlemler hash ile paralel DAG örneklerinden birine deterministik olarak atanır ve sıralama yükü eşit olarak dağıtılır.
- ◆ **Bağımsız Sonuçlandırma:** Her DAG örneği kendi yerel işlem dizisini yüksek hızda sonuçlandırır.
- ◆ **Yuvarlak-Robin Tüketimi:** Yürütme Katmanı, her bir DAG'dan gelen sonlandırılmış işlem listelerini adil, yuvarlak robin bir sırayla tüketir ve bunları küresel olarak sıralanmış tek bir akışta bir araya getirir.

Bu mimari, sadece daha fazla paralel DAG örneği ekleyerek ağın işlem sıralama kapasitesini artırmamıza olanak tanır ve herhangi bir talebi karşılamak için mempool'un yatay ölçeklendirilmesini sağlar.

### 3.3 Ölçeklenebilir Yürütme: Simülasyon Öncelikli Paralel Boru Hattı

İşlemler arasındaki potansiyel veri bağımlılıkları nedeniyle paralel yürütme elde etmek oldukça zordur. Blocksense bunu, yürütme sonuçlarını belirleme gibi ucuz bir işi kanıtlama gibi pahalı bir işten ayıran çok aşamalı, simülasyon öncelikli bir işlem hattı ile çözer.

1. **Simülasyon:** Bir işlem grubu Sipariş Katmanı tarafından sonuçlandırıldıktan sonra, ilk olarak **Simülatörler** adını verdiğimiz bir düğüm sınıfı tarafından alınır. Calvin protokolünden ve Spekülatif Çok İş Parçacıklı (SMT) yürütmeden esinlenen Simülatörler, bir toplu işteki tüm işlemleri paralel olarak yürütmeye çalışır.

◆ **Çakışma Çözümü:** İşlemlerde veri çakışmaları varsa (örneğin, aynı durumu değiştirmeye çalışan iki işlem), çakışan işlem bir sonraki partiye ertelenir. Çakışmayı göstermek için özel bir "atlama" kanıtı oluşturulur ve ertelenen işlemin yürütülmesinin ödülü, sonunda işlenmesini sağlamak için artırılır. Saniyenin altındaki partilerde bu işlem ihmal edilebilir bir gecikmeye neden olur.

◆ **Ekonomik Güvenlik:** Hatalı bir simülasyon kullanıcılara doğrudan zarar veremeyeceğinden, simülatörler protokol güvenliği için kritik değildir. Ancak, güven oluşturmak için Simülatörler sonuçlarını imzalamalıdır. Eğer bir Simülatör geçersiz bir sonucu imzalarsa, ücreti kesilebilir. Bu, doğruluk için güçlü bir ekonomik teşvik sağlar ve boru hattının bir sonraki aşamasının ilerlemesine izin verir.

2. **Paralel Kanıtlama:** Simülatörlerden gelen imzalı sonuçlar (her hesaplama adımı için ön ve son koşullar) Doğrulayıcılar ağına yayınlanır. Yürütme yolu artık belirlendiğinden, ZK kanıtları oluşturmanın hesaplama açısından yoğun görevi büyük ölçüde paralelleştirilebilir. Blocksense yürütme katmanı, üç farklı nesnel olarak doğrulanabilir hesaplama türünü paralel olarak kanıtlamak üzere tasarlanmıştır:

◆ **Deterministik Durum Geçişleri:** Bir VM içinde yürütülen standart akıllı sözleşme mantığı.





◆ **Özneler Arası Mutabakat:** zkSchellingCoin oylamalarının sonuçları.

◆ **Doğrulanabilir Gizli Hesaplama:** Özel **BlocksenseOS**<sup>[2]</sup> tarafından yönetilen **Güvenilir Yürütme Ortamlarından (TEE'ler)** kriptografik tasdikler. Bu sayede ağ, verileri veya kimlik bilgilerini zincir üzerinde ifşa etmeden gizli veriler üzerinde (örneğin gizli API anahtarları kullanılarak) belirli, denetlenmiş kodların yürütüldüğünü kanıtlayabilir.

3. **Birleşik Kanıt Toplama:** Katlama kullanan bir ZK kanıtlama sistemi (örn. UltraHONK) kullanılarak, bir bloktaki her hesaplama için ayrı "yaprak" kanıtlar (durum geçişleri, oracle oyları ve TEE onayları) verimli bir şekilde tek ve kısa bir kanıtta birleştirilir. Bu son kanıt, herhangi bir düğümün tümünü yürütmüş veya kanıtlamış olmasını gerektirmeden tüm bloğun durum geçişinin geçerliliğini kanıtlar.

Bu birleşik ZK kanıtı güçlü bir ilkedir. Blocksense'in diğer tüm zincirlere doğal olarak ZK ile bağlanmasını ve bir ZK toplanması ya da validium olarak işlev görmesini sağlar. Ayrıca hafif istemcilerin tek bir ispatı indirip doğrulayarak zincirle anında ve güvenli bir şekilde senkronize olmasını sağlar.

Paralel sıralamadan paralel simülasyon ve kanıtlamaya kadar tüm bu mimari muazzam bir hesaplama kapasitesi gerektirmektedir. Tasarım, geniş bir donanım operatörleri ağını cezbetme becerisine dayanmaktadır. Aşağıdaki bölüm tam olarak bunu yapmak için tasarlanan ekonomik modeli detaylandırmaktadır.

[^2]: **BlocksenseOS**, doğrulanabilir hesaplama için gerekli soyutlamaları sağlayan, Güvenilir Yürütme Ortamlarında çalışmak üzere tasarlanmış minimal, güvenlik açısından güçlendirilmiş bir Linux dağıtımdır. Ayrıntılı bir teknik genel bakış için şu adresteki tasarım belgesine bakın: <https://github.com/blocksense-network/BlocksenseOS/blob/main/docs/BlocksenseOS-Design.md>

## 4. Blocksense Ekonomisi: Kendi Kendini Güçlendiren Bir Volan

Çığır açan teknoloji tek başına yeterli değildir. Başarılı bir protokol, tüm katılımcılar arasındaki teşvikleri hizalayan sağlam, kendi kendini güçlendiren bir ekonomik model gerektirir. Blocksense ekonomisi, hesaplama bolluğu ilkesi etrafında tasarlanmıştır. İşlem hacmini öncelik ücretleriyle açık artırmaya çıkarılan kıt bir kaynak olarak ele alan geleneksel blok zincirlerinin aksine, Blocksense'in sınırsız mimarisi bunu bir emtia olarak ele alır. Bu temel değişim, işlem önceliği ücretlerini ortadan kaldırmamızı sağlıyor. Kullanıcıların dahil olmak için birbirlerine karşı teklif vermeleri yerine, node operatörleri mümkün olan en düşük fiyattan hesaplama sağlamak için rekabet eder, Maliyetleri maddi sınırlarına kadar düşürmek - donanım verimliliği gelişmeye devam ettikçe zaman içinde sıfıra doğru eğilim göstermesini beklediğimiz bir rakam.



#### 4.1 Tokenomik ve Fayda

Yerel Blocksense tokenı ağın can damarıdır ve üç temel işleve hizmet eder:

1. **Staking ve Güvenlik:** Node operatörleri, ağın mutabakat ve yürütme süreçlerine katılmak için Blocksense tokenlarını stake etmelidir. Bu stake, kötü niyetli davranışlar için kesilebilen ve böylece ağı güvence altına alan bir güvenlik depozitosu görevi görür.
2. **Hizmetler için Ödeme:** Blocksense tokenı, tüm ağ hizmetleri için özel hesap birimidir. Buna kod yürütme ücretleri, veri hizmetleri için internet bant genişliği ve kalıcı depolama kirası dahildir. Öncelikli teklifin kullanıldığı tek kıt kaynak, hedef zincirlerdeki blok alanı içindir ve zincirler arası veri dağıtımının verimli olmasını sağlar.
3. **Yönetişim:** Token sahipleri, önemli parametre değişiklikleri ve sistem yükseltmeleri için oy kullanarak protokolün yönetimine katılma hakkına sahip olacaktır.

#### 4.2 Web2 ve Web3 için Birleşik, Yetenek Tabanlı Bir Pazar Yeri

Blocksense ağı bir blok zincirinden daha fazlasıdır; her sektördeki özel hesaplama ağlarıyla rekabet etmek ve onları alt etmek için tasarlanmış **doğrulanmış hesaplama** için küresel bir pazardır. Bunu esnek, **kabiliyet temelli bir yaklaşımla** başarıyoruz.

Blocksense'te hizmetler, özel donanım (örneğin, işleme veya yapay zeka çıkarımı için üst düzey GPU'lar), özel veri akışlarına erişim (örneğin, gerçek zamanlı spor sonuçları) veya diğer benzersiz yetenekler gerektirebilir. Protokolümüz, operatörlerin bu yetenekleri edinmenin gerçek zamanlı karlılığını görebilecekleri bir portal sağlar. Hizmet teklif süreci, operatörlerin hizmetlerini sundukları belirli yeteneklere göre fiyatlandırmalarına olanak tanıyarak her tür hesaplama için dinamik, piyasa odaklı fiyatlandırma yaratır. Bu da doğal olarak pazarı segmentlere ayırarak Blocksense'in tek bir birleşik platform içinde ZK kanıtlama, 3D işleme, yapay zeka ve daha fazlası için özel ağlarla etkili bir şekilde rekabet etmesine olanak tanır.

Bu model, temel bir tasarım ilkesiyle güçlendirilmiştir: Blocksense ağında dağıtılan veri ve hesaplama hizmetleri, hem zincir üzerindeki akıllı sözleşmelere (Web3) hem de geleneksel uygulamalara (Web2) hizmet edebilir. Geleneksel uygulamalar artık Blocksense ağına güç veren aynı kriptografik ve oyun teorisi ilkelerinden faydalanabilir ve **güvenin en aza indirildiği** yeni bir **Web2 hizmetleri** paradigması yaratabilir. Bu, çok yönlü bir doğrulama araç seti ile mümkün kılınmıştır:

◆ **Özneler Arası Hizmetler:** zkSchellingCoin mekanizması, herhangi bir deterministik görev için kripto-ekonomik garantiler sağlar. Halka açık piyasa verileri üzerinde açık kaynaklı bir algoritma çalıştıran bir finansal analiz hizmeti düşünün. Sağlayıcı, Blocksense tokenlarını katılmak için. Bir Web2 istemcisi bir rapor talep ettiğinde, sağlayıcı hesaplamayı çalıştırır, sonucu kriptografik olarak imzalar ve iade eder. İstemci sonucun yanlış olduğundan şüphelenirse, Blocksense ağında bir meydan okuma başlatabilir. Bu, bir zkSchellingCoin komitesinin aynı genel girdilerle aynı hesaplamayı bağımsız olarak yeniden çalıştırmasını tetikler. Komitenin sonucu sağlayıcının imzalı sonucundan farklıysa, sağlayıcının



aldatılmış ve hisseleri düşürülmüştür.

◆ **TEE Hizmetleri:** VEIL hizmetimiz gibi özel veri veya IP içeren görevler için TEE tabanlı yaklaşımımız, ZK onaylı doğruluk tasdikleriyle birlikte donanım destekli gizlilik sağlar.

Hem Web3 hem de Web2 kullanım durumlarına tek ve birleşik bir pazaryerinden hizmet vermenin bu kombinasyonu, ağına güçlü yapısal avantajının kaynağıdır. Düşüm operatörleri silo halinde değildir ve iki farklı iş kategorisine hizmet verebilirler:

◆ **Yüksek Marjlı Doğrulama:** Yüksek değerli DeFi protokolleri için oracle verileri sağlamak gibi temel Web3 görevleri. Bu işin ücreti, genellikle önemsiz olan hesaplama maliyetinden değil, zincir üzerinde güvence altına aldığı muazzam ekonomik değerden kaynaklanır.

◆ **Düşük Marjlı Emtia Hesaplama:** Fiyatların açık piyasa rekabeti tarafından yönlendirildiği genel amaçlı Web2/Web3 görevleri.

Buradaki kilit nokta, yüksek marjlı Web3 işinin operatörleri cezbetmesi ve onların ağına katılımını sübvansede etmesidir. Bir Web3 DeFi protokolü için yüksek marjlı doğrulama gerçekleştiren aynı donanım, bir sonraki anda bir Web2 uygulamasından gelen düşük marjlı bir emtia hesaplama talebine hizmet verebilir. Operatörler daha sonra atıl kapasitelerini, uzmanlaşmış, tek amaçlı ağların rekabet edemeyeceği marjinal bir maliyetle emtia bilgi işlem pazarına sunabilir.

Bu avantaj, Blocksense'in geniş ve çeşitli bir donanım sağlayıcı ağını çekmesine olanak tanıyarak tüm hesaplama hizmetleri için derin likidite ve en düşük fiyatları sağlar. Ayrıca, bu yetenekli operatörler ağı küresel olarak dağıtıldıkça, Blocksense, diyalogsal yapay zeka, çevrimiçi oyun ve artırılmış gerçeklik gibi düşük gecikmeli hizmetler için ideal platform haline gelmek üzere benzersiz bir şekilde konumlandırılmıştır.

#### 4.3 Kullanıcı İndirimi Olarak Oracle Çıkarılabilir Değeri (OEV)

Maksimal Çıkarılabilir Değer (MEV) çoğu blok zinciri ekosisteminde çıkarıcı bir güçtür. Blocksense bu dinamiği yeniden tasarlamaktadır. Mimarimiz, birçok oracle güncellemesini, bunlar üzerinde işlem yapabilen meta işlemlerle birlikte tek bir bölünmez zincir içi işlemde bir araya getirmemize olanak tanır. Bu atomiklik, **Oracle Extractable Value (OEV)** olarak adlandırdığımız bu yeni bilgi üzerinde hareket etmekle ilişkili değeri doğal olarak yakalamamızı sağlar.

Bu değerin üçüncü taraf arama yapanlar tarafından yakalanmasına izin vermek yerine Blocksense, işlemleri bu atomik paketlere dahil etme hakkı için rekabetçi bir açık artırma yürütür. Teklif veren-oluşturan ayrımı tasarımlarından esinlenen bu mekanizma, hiper-rekabetçi bir pazar yaratır. Rasyonel, kâr amacı güden aktörler en kârlı işlem sıralamasını bulmak için rekabet edecek ve rekabet nedeniyle elde edebilecekleri toplam kârdan sadece utangaç bir miktar teklif etmeye zorlanacaklardır. Bu dinamik, mevcut OEV'nin büyük çoğunluğunun kazanan teklif şeklinde açık artırma tarafından yakalanmasını sağlar.



Elde edilen gelir daha sonra programlı bir şekilde, faaliyetleri ilk etapta OEV fırsatını yaratan protokollere ve dApp'lere yeniden dağıtılır. Bu protokoller de bu tasarrufları son kullanıcılarına aktarabilir. Bu, MEV'i kullanıcılar üzerindeki görünmez bir vergiden tüm ekosistem için güçlü bir elde tutma ve büyüme mekanizmasına dönüştürür.

#### 4.4 Hizmet Teklif Sistemi

Ağ kaynaklarının verimli ve mümkün olan en düşük maliyetle tahsis edilmesini sağlamak için Blocksense gizli bir hizmet teklif sistemi kullanır. Düğüm operatörleri, çeşitli görevleri (örneğin, mempool doğrulama, ZK kanıtlama, zkSchellingCoin oylama) gerçekleştirme hakkı için gizlice teklif verir. Protokol içinde çalışan bir hizmet, her görev için bir kesme fiyatı hesaplar ve bu fiyatın altındaki tüm teklif sahiplerini seçer. Merkezileşmeyi ve stratejik düşük tekliflerin güvenliği tehlikeye atmasını önlemek için, seçim mekanizması rastgeleleştirmeyi içerir, teklifleri yüzdelik dilimlere dayalı bantlar halinde gruplandırır ve bir bant içindeki tüm teklif sahiplerine seçilme şansı verir. Bu, sağlıklı rekabeti teşvik ederek kullanıcılar için maliyetleri düşürürken ağın merkezi olmayan ve güvenli kalmasını sağlar.

#### 4.5 Dayanıklı Hendeğimiz: Kendi Kendini Güçlendiren Bir Ağ Etkisi

Blocksense ekonomik modeli, uzun vadeli rekabet hendeğimizi oluşturan güçlü, kendi kendini güçlendiren bir ağ etkisi yaratmak üzere tasarlanmıştır. Volan, paylaşılan kaynak havuzlama mimarimizin benzersiz özellikleri tarafından yönlendirilir.

Bir Blocksense hizmetine ek bir tüketici eklemek (örneğin, mevcut bir veri akışına abone olan yeni bir protokol), o hizmeti çalıştırmanın operasyonel maliyetini artırmaz. Maliyet aşağıdakiler arasında paylaşılır

tüm tüketiciler. Dolayısıyla, **her yeni tüketici mevcut tüm tüketiciler için maliyeti düşürür**. Bu da güçlü bir ekonomik giriş engeli yaratmaktadır. Bir rakibin karşılaştırılabilir bir fiyat sunabilmesi için ağımızın ölçeği ve hacmiyle eşleşmesi gerekir ki bu da kritik bir kitleye ulaşıldığında muazzam bir zorluktur.

Bu maliyet avantajı, Güvence Altına Alınan Toplam Değer (TVS) ve güven arasındaki ilişki ile pekiştirilmektedir. Yeni tüketiciler doğal olarak en yüksek TVS'ye sahip platforma çekilir, çünkü bu güçlü bir sosyal güvenilirlik sinyali olarak hizmet eder. Yeni tüketiciler katıldıkça ağın TVS'si artar ve bu da ödül kazanmak isteyen daha fazla staker ve node operatörünü çeker. Bu sermaye ve donanım akışı, ağın kripto-ekonomik güvenliğini daha da artırarak Blocksense'i bir sonraki tüketici dalgası için daha da çekici ve güvenilir bir platform haline getirir.

## 5. Pazara Giriş:

### Web3 ve Web2 Arasında Köprü Kurmak

Blocksense'in ileri teknolojisi ve sağlam ekonomisi, doğrudan bir dizi yıkıcı hizmete dönüşüyor. Pazara açılma stratejimiz, aşağıdaki sorunları çözmek için bu hizmetlerden yararlanmaya odaklanmıştır



Milyarlarca dolarlık Oracle pazarından başlayarak tüm Web3 ekosistemindeki geliştiriciler ve protokoller için akut sorun noktaları.

### 5.1 ADFS: Hiper Verimli Veri Yolu

Hizmet teklifimizin temel taşı **ADFS'dir (Aggregated Data Feed Store)**. ADFS, hiper verimli bir veri ve işlem veri yolu görevi gören hedef blok zincirlerine yerleştirilmiş bir akıllı sözleşme sistemidir. Gücü toplamadan gelir: Blocksense binlerce farklı veri akışı güncellemesini, zincirler arası mesajı ve meta işlemi tek bir yükte toplayabilir ve bu yükün geçerliliği hedef zincirde tek ve ucuz bir sıfır-bilgi kanıtı ile doğrulanır.

Bu mimari, tipik olarak her güncelleme için ayrı işlemler gönderen mevcut herhangi bir oracle veya çapraz zincir mesajlaşma protokolüne kıyasla büyüklük sırasına göre bir maliyet düşüşü sağlar. ADFS, yapısal olarak daha düşük bir maliyetle üstün hizmet sunmamızı sağlayan sahil noktamızdır.

### 5.2 Oracle Pazarını Yıkma

Oracle pazarı şu anda iki paradigma arasında bölünmüş durumda: itme ve çekme modelleri. Blocksense her ikisini de bozmak için tasarlanmıştır.

◆ **İtmeli Oracle'lara karşı:** Geleneksel "itme" oracle'ları zincir üzerindeki maliyetlerle sınırlıdır ve veri tazeliği ile masraf arasında bir denge kurmaya zorlar. ADFS'nin olağanüstü verimliliği bu değiş tokuşu bozar. Büyük miktarda veriyi marjinal bir maliyetle iterek, yüksek frekanslı zincir içi türevler, blok zinciri oyunları için gerçek zamanlı durum güncellemeleri ve daha sofistike algoritmik stratejiler gibi şu anda yasaklayıcı olan kullanım durumlarını mümkün kılıyoruz.

◆ **vs. Çekme Oracle'ları:** "Çekme" modeli, verileri zincir üzerinde izlemek ve getirmek için protokollerin maliyetli zincir dışı altyapı çalıştırmasını gerektirir. Blocksense, **oracle komut dosyalarımızın programlanabilirliği** sayesinde üstün bir alternatif sunar. Kredi tasfiyesi gibi bir görev şu şekilde kodlanabilir  
merkezi olmayan Blocksense ağı üzerinde çalışan kalıcı, otonom bir hizmettir. Bu hizmet tasfiye koşullarını tespit edebilir ve gerekli verileri koşullu olarak zincire aktarabilir. En önemlisi, bu süreç OEV piyasamızla entegre olur; sofistike aktörler, hepsi aynı atomik ADFS işlemi içinde, talep üzerine gerekli tasfiye sermayesini sağlamak için teklif verebilir. Bu, protokollerin harici botlara fazla ödeme yapma ihtiyacını ortadan kaldırarak hiper verimli bir likidasyon piyasası yaratır. Maksimum esneklik için Blocksense, sık sık rotasyona tabi tutulan Yüksek Frekanslı Güncellemeler Komitesinin zincir dışı imzalı veri sağladığı geleneksel bir çekme modelini de destekler.

### 5.3 Verilerin Ötesinde: Evrensel Bir Çapraz Zincir İlkeli

ADFS bir veri dağıtım mekanizmasından daha fazlasıdır; verimli zincirler arası iletişim için evrensel bir ilkeldir. Rastgele mesajları bir araya getirme ve bunları tek bir ZK kanıtı ile doğrulama yeteneği geniş kapsamlı uygulamalara sahiptir:



◆ **ZK İspat Toplama:** Rollup'lar ve ZK - iş l e m c i l e r i Blocksense'i yüksek verimli bir toplama ve uzlaştırma katmanı olarak kullanabilir ve kanıtlarının pahalı zincir içi doğrulamasını dış kaynak olarak kullanabilir.

◆ **Hesap Soyutlama Paketleyicisi:** Blocksense, ekosistem genelindeki kullanıcı işlemlerini toplayarak ve bunları herhangi bir hedef zincirde tek ve uygun maliyetli bir işlemle çözerek evrensel bir paketleyici olarak hareket edebilir.

◆ **Talep Üzerine Likidite:** Likidasyonlar için sermaye sağlayan aynı OEV piyasa katılımcıları, zincirler arası takaslar ve zincir soyutlaması için isteğe bağlı likidite de sağlayabilir. Bu, kullanıcıların tek bir zincirde fon tutarken, Blocksense'in güven ve mesajlaşma katmanı olarak hareket etmesiyle, herhangi bir zincirdeki dApp'lerle sorunsuz bir şekilde etkileşime girmesine olanak tanır.

## 5.4 Amiral Gemisi Hesaplama Hizmeti: VEIL ile Doğrulanabilir ve Özel Yapay Zeka

Güven minimize edilmiş Web2 hizmetleri pazarına ilk girişimiz, YZ güdümlü yazılım geliştirmedeki kritik güven açığını çözen amiral gemisi bir hizmet olan VEIL (Doğrulanabilir Yürütme ve Çıkarım Katmanı) üzerine odaklanmıştır. Güçlü olsa da, yapay zeka kodlama araçlarının kurumsal olarak benimsenmesi

IP sızıntısı riskleri ve yürütmenin doğrulanabilirliğinin olmaması nedeniyle durmaktadır. VEIL bunu doğrudan ele almaktadır.

Temel, yapay zeka ajanlarını düzenlemek ve denetlemek için açık kaynaklı, git odaklı bir araç seti olan **agents-workflow**'dur ve profesyonel ajan geliştirme için yeni bir standart oluşturur. Maksimum güvenlik gerektiren işletmeler için, tüm ajan yaşam döngüsünü Blocksense ağındaki **Güvenilir Yürütme Ortamı (TEE)** içinde çalıştıran premium bir arka uç sunuyoruz. Bu, kriptografik olarak güçlendirilmiş iki garanti sağlar:

1. **Gizlilik:** TEE, node operatörü dahil hiç kimsenin özel kaynak koduna veya hassas verilere erişememesini sağlar.
2. **Doğrulanabilirlik:** Yürütme Blocksense ağı tarafından onaylanır ve bir sağlayıcının daha ucuz, daha az yetenekli bir AI modeli kullanabileceği "yem ve anahtar" saldırılarını önler.

VEIL, hem açık kaynaklı bir standart hem de premium, güven minimize edilmiş bir arka uç sağlayarak devasa bir üst huni oluşturuyor ve Blocksense Evrensel Doğrulama Katmanının benzersiz gücünü gösteriyor. En önemlisi de, küresel bir operatör ağının hem yüksek marjlı yapay zeka çıkarım görevleri hem de sınırsız iş hacmi motorumuzun muazzam ZK kanıtlama ihtiyaçları için gereken güçlü GPU'ları edinmesi için güçlü bir teşvik sağlayarak tüm bilgi işlem pazarımızın tedarik tarafını başlatıyor.

Sonuç olarak VEIL, Blocksense tezinin güçlü bir göstergesidir. Ağın ekonomik volanı tarafından sübvans edilen rekabetçi bir fiyatla yüksek güvenceli hesaplama sağlar. Evrensel bir doğrulama katmanının soyut gücünü milyarlarca dolarlık bir sorun için somut bir çözüme dönüştürerek, yapay zekanın yazılım mühendisliğinin geleceği haline gelmesi için gerekli güven ve güvenliği sağlar.





## 6. Kullanıcı ve Geliştirici Deneyiminin Yeniden Tanımlanması

Bir protokolün başarısının nihai ölçütü, sağladığı deneyimlerin kalitesidir. Blocksense'in mimari yenilikleri kendi başlarına bir amaç değil, hem son kullanıcılar hem de geliştiriciler için radikal bir şekilde iyileştirilmiş bir deneyim sunarak ana akım benimsemenin yolunu açan araçlardır.

### 6.1 Kullanıcılar için: Görünmez Blok Zinciri

Web3'ün küresel bir izleyici kitlesine ulaşması için temel teknolojinin görünmez hale gelmesi gerekir. Block-sense, yıllardır kullanıcı deneyimini zorlaştıran karmaşıklıkları soyutlamak için tasarlanmıştır.

◆ **Sürtünmesiz İşe Alım:** Tarayıcı uzantılarına ve tohum ifadelerine olan ihtiyacı ortadan kaldırıyoruz. Blocksense, **Paskeys** (WebAuthn) etrafında oluşturulmuş yerel bir hesap soyutlama sistemine sahiptir. Kullanıcılar, telefonlarında ve dizüstü bilgisayarlarında bulunan biyometrik sensörleri (ör. Face ID, parmak izi taraması) kullanarak bir cüzdan oluşturabilir ve işlemleri imzalayarak tanıdık, güvenli ve sorunsuz bir işe alım deneyimi sağlayabilir.

◆ **Sıfır Maliyetli İşlemler:** Yüksek ve öngörülemez gaz maliyeti, giriş için büyük bir engeldir. Blocksense ekonomisinde, işlem ücretleri bir kullanıcı vergisi değil, bir işletme gideridir. Mimarimiz, uygulamaların, protokollerin ve hatta alıcı tarafların işlem maliyetlerine sponsor olabileceği esnek fiyatlandırma modellerine olanak tanıyarak son kullanıcı için "gazsız" bir deneyim yaratır.

◆ **Anında ve Güvenli Senkronizasyon:** Kullanıcılar tam bir node'u senkronize etmek için saatlerce beklemek veya merkezi bir uç noktaya güvenmek zorunda kalmamalıdır. Blocksense light istemcileri, zincirin geçmişinin tek ve kısa bir ZK kanıtını indirip doğrulayarak zincirin en son durumuyla anında ve güvenli bir şekilde senkronize olabilir.

### 6.2 Geliştiriciler için: Bir Olasılıklar Evreni

Blocksense, akıllı sözleşme geliştirmenin geleneksel kısıtlamalarını ortadan kaldırarak yeni nesil güçlü uygulamalar oluşturmak için eksiksiz, genel amaçlı bir platform sağlar.

◆ **Otonom Ajanların Doğuşu:** Üç temel özelliğin birleşimi - **programlanmış/yinelenen işlemler** (setTimeout/setInterval), yerel **AI/ML model çıkarımı** ve

**Herhangi bir zincir içi veya zincir dışı veri kaynağından okuma yeteneği**, gerçek, zincir içi **Otonom Ajanlar** oluşturmak için mükemmel bir ortam **yaratır**. Geliştiriciler, bağımsız olarak çalışan, harici olaylara tepki veren ve karmaşık mantığı yürüten kalıcı hizmetleri dağıtabilir ve otomatik DeFi stratejilerinden merkezi olmayan sosyal medya moderatörlerine kadar kullanım durumlarının kilidini açabilir.





◆ **Evrensel Birleştirilebilirlik:** Blocksense, WASM, Move ve EVM gibi bir dizi yürütme motorunu desteklemek üzere tasarlanmış çok VM'li bir ortamdır. Bu, belirli bir VM'nin yürütüldüğünü kanıtlayan yeni ZK devrelerinin ağ üzerinde düzenli hizmetler olarak konuşlandırılmasına izin vererek elde edilir. VM'ler arası çağrılar için ABI'yi standartlaştırarak, farklı dillerde yazılmış akıllı sözleşmelerin basit bir işlev çağırısı yapıyormuş gibi sorunsuz bir şekilde iletişim kurmasını sağlayacağız. Bu, geliştiricilerin silolara ayrılmadan iş için en iyi araçları kullanabilecekleri zengin, birlikte çalışabilir bir ekosistemi teşvik eder.

◆ **Yerel Gizlilik:** Blocksense'in ZK-yerel mimarisi, onu gizliliği koruyan uygulamalar için önde gelen bir platform haline getirir. Geliştiriciler, gizlilik garantileri olan uygulamalar oluşturmak için protokolün temel kriptografik ilkelerinden yararlanabilirler. Güçlü bir örnek Bağlı herhangi bir blok zinciri ile etkileşime girerken, kurumsal bir hazine için çoklu imza eşikleri ve imzalayanlar gibi hassas **yönetim** ayrıntılarını korumak için ZK kanıtlarını kullanan, gizliliği koruyan, zincirler arası bir akıllı cüzdan, hepsi basit, geçiş anahtarı tabanlı bir arayüz üzerinden yönetilir.

◆ **Oracle Sorununun Sonu:** Geliştiriciler için harici verilere erişmek veya karmaşık bir hesaplama yapmak artık çok partili bir entegrasyon **sorunu** değildir. Bu, yerel bir API çağırısıdır. Blocksense, özneler arası mutabakatı doğrudan yürütme katmanına inşa ederek, tüm interneti akıllı sözleşmeler için okunabilir, doğrulanabilir bir veri kaynağına dönüştürür.

## 7. Yönetişim

Blocksense, aşamalı ademi merkeziyetçilik ilkelerine bağlıdır. Zaman içinde protokol üzerindeki kontrol, Blocksense DAO aracılığıyla yönetilen paydaş topluluğuna devredilecektir. DAO'nun birincil sorumluluğu, ağın uzun vadeli sağlığını ve gelişimini yönetmek olacaktır.

**Protokol Yükseltmeleri:** DAO'nun temel işlevi protokol yükseltmelerini yönetmektir. ZK'ya özgü bir protokol olarak, büyük yükseltmeler yeni ZK devrelerinin ve doğrulayıcı sözleşmelerinin konuşlandırılmasını içerir. Bu süreç, Blocksense token sahiplerinin zincir içi oylamasıyla yönetilir. Ağ istikrarını ve kullanıcı güvenliğini sağlamak için, kabul edilen tüm teklifler bir **zaman kilidi sözleşmesi** aracılığıyla yürütülür. Bu, başarılı bir oylama ile yükseltmenin uygulanması arasında zorunlu bir gecikme getirerek, tüm kullanıcılara ve uygulamalara değişiklikleri gözden geçirmek, bunlara hazırlanmak veya tartışmalı bir teklif durumunda sistemden çıkmak için yeterli zaman verir. Bu mekanizma, düşmanca veya aceleyle yönetişimin ele geçirilmesine karşı kritik bir güvencedir.

**Hazine ve Ekosistem Yönetimi:** Token Oluşturma Etkinliği (TGE) sırasında, token arzının önemli bir kısmı topluluk tarafından yönetilen bir hazineye tahsis edilecektir. Bu fonlar, aşağı yönlü fiyat baskısı yaratmadan uzun vadeli, sürdürülebilir kalkınmayı sağlamak için birkaç yıl içinde kademeli olarak açılacaktır. Blocksense DAO, bu fonların şeffaf gözetimine sahip olacak ve bunları ekosistemi büyüten faaliyetlere yönlendirecektir:



- ◆ **Araştırma ve Geliştirme Hibeleri:** Çekirdek protokolü ilerletmek için ekiplere ve bireylere fon sağlanması.
- ◆ **Ekosistem Yatırımları:** Blocksense üzerine inşa edilen gelecek vaat eden proje ve uygulamalara sermaye sağlanması.
- ◆ **Stratejik Ortaklıklar:** Entegrasyonların ve iş geliştirme girişimlerinin teşvik edilmesi.

## 8. Yol Haritası

Evrensel doğrulama katmanını inşa etme yolumuz pragmatik ve aşamalı olup her adımda güvenlik ve faydaya öncelik vermektedir. Bilinçli bir aşamalı ademi merkeziyetçilik stratejisi yürütüyoruz.

### Aşama 1: Temel ve Canlı Hizmetler (Mevcut)

- ◆ **Canlı Ağ:** Blocksense ağı şu anda bir dizi güvenilir, izinli operatör tarafından güvence altına alınan bir Yetki Kanıtı (PoA) modeli altında canlı ve çalışır durumdadır.
- ◆ **Geliştirici SDK'sı:** Geliştiricilerin bugün özel veri akışları oluşturmaya ve dağıtmasına olanak tanıyan, özneler arası oracle hizmetlerini programlamaya yönelik kapsamlı SDK'mız mevcuttur.
- ◆ **Aşamalı Hizmet Sunumu:** 2025 ve 2026 yılları boyunca PoA ağıımızda bir dizi rekabetçi hizmet başlatıyoruz. Buna amiral gemimiz VEIL hizmetinin, düşük gecikmeli oracle'ların, çekme/şartlı itme oracle'larının, OEV yakalama, çapraz zincir birlikte çalışabilirlik, tahmin piyasaları için spor veri beslemeleri, ZK kanıt toplama ve hesap soyutlama çözümleri.

### 2. Aşama: Merkeziyetsizliğin Önyüklenmesi (Yakında)

- ◆ **EigenLayer Entegrasyonu:** Bir sonraki önemli dönüm noktası, EigenLayer'da Aktif Olarak Onaylanmış Hizmet (AVS) olmaktır. Bu, ETH'yi yeniden oluşturanların Blocksense ağını güvence altına almak için hisselerini devretmelerine izin vererek kripto-ekonomik güvenliğimizi önemli ölçüde artıracak ve ademi merkeziyetçiliğe doğru net bir yol sağlayacaktır.

### Aşama 3: ZK-Native Protokolü (2026)

- ◆ **Testnet Lansmanı (2026 Başları):** Rüşvete dayanıklı zkSchellingCoin devrelerini ve halka açık testler için zincir üzerinde Futarchy mekanizmasını içeren tam ZK yerel mutabakat protokolü için test ağı başlatılacaktır.
- ◆ **TGE & Mainnet Lansmanı (2026 Sonu):** Başarılı bir test ağı aşamasının ardından Token Üretme Etkinliğini (TGE) gerçekleştireceğiz. Bunu, tamamen izinsiz, Blocksense token-stake Proof-of-Stake sisteminin ana ağ lansmanı takip edecektir. TGE ile eş zamanlı olarak, zincir içi yönetim için Blocksense DAO'yu kuracağız.

### 4. Aşama: Ekosistem Olgunluğu (Ötesi)

- ◆ **Hizmet Odaklı Paradigmanın Teşvik Edilmesi:** Temel protokolün tamamlanmasıyla birlikte, odak noktamız canlı ve yenilikçi bir ekosistemi teşvik etmeye kayacaktır. Benzersiz yeteneklere inanıyoruz



geliştiricilerin henüz öngöremediğimiz yeni uygulamalar ve ilkeller yaratmaları için verimli bir zemin oluşturacaktır.

◆ **DAO liderliğinde Büyüme:** Protokolün ve hazinesinin tam kontrolü, gelecekteki araştırma, geliştirme ve büyüme girişimlerini yönetecek olan Blocksense DAO'ya devredilecektir.

## 9. Sonuç

Blok zinciri mimarisindeki hakim paradigmlar sınırlamaları ile tanımlanmıştır. **Bağlantı Bariyeri** onları izole bırakırken, **Verim Bariyeri** onları yavaş ve pahalı bıraktı. Bu kısıtlamalar, muazzam potansiyele sahip bir teknolojiyi dijital dünyanın niş bir köşesine hapsetmiştir.

Blocksense ileriye dönük yeni bir yol sunuyor. Bu iki temel sorunu çözmek için protokolümüzü ilk prensiplerden tasarlayarak, daha hızlı veya daha bağlantılı bir blok zincirinden daha fazlasını yarattık. Evrensel bir doğrulama katmanı inşa ettik. Öznelerarası Doğruluk Makinemiz herhangi bir veriye kırılmaz, ekonomik olarak rasyonel bir güven sağlarken, Sınırsız Verim Motorumuz da bu güveni herhangi bir soruna uygulayacak ölçeği sağlıyor.

Bu kombinasyon, merkezi olmayan uygulamalar için daha önce hayal bile edilemeyen bir tasarım alanının kilidini açıyor. Blocksense, hiper verimli çapraz zincir finansal hizmetlerden gerçek anlamda otonom yapay zeka ajanlarına kadar, bir sonraki merkezi olmayan yenilik dalgası için güvenli, ölçeklenebilir ve ekonomik olarak uyumlu bir temel sağlar. Sizi bu geleceği inşa ederken bize katılmaya davet ediyoruz.