Genel Bakış

Trilemma Smart Wallet, Ethereum Virtual Machine (EVM) üzerinde çalışan geleneksel cüzdanların sınırlamalarını aşmayı amaçlayan yenilikçi bir akıllı cüzdan projesidir. Bu cüzdan, kullanıcıların Web3 dünyasına daha kolay, güvenli ve kullanıcı dostu bir şekilde katılmalarını sağlayacak bir dizi özellik sunar. Özellikle hesap soyutlama (Account Abstraction) teknolojisini kullanan Trilemma Smart Wallet, işlemleri daha az maliyetli, daha güvenli ve daha erişilebilir hale getirmeyi hedeflemektedir.

Özellikler:

1. Hesap Soyutlama (Account Abstraction):
    - Trilemma Smart Wallet, ERC-4337 standardını kullanarak geleneksel cüzdanların sınırlarını aşar. Hesap soyutlama, kullanıcıların merkezi olmayan uygulamalarda (dApps) işlemlerini daha kolay ve güvenli bir şekilde yönetmelerini sağlar. Bu teknoloji, işlemlerin blok zincirine gönderilmeden önce çeşitli doğrulama ve güvenlik katmanlarından geçmesine olanak tanır.
2. Gazsız İşlemler:
    - Trilemma Smart Wallet, kullanıcılara gaz ücreti ödemeden işlem yapma imkanı sunar. Bu özellik, özellikle küçük miktarlardaki token transferlerinde maliyetleri minimize eder. Gazsız işlemler, yüksek işlem ücretlerinin olduğu durumlarda bile kullanıcıların ağdan etkin bir şekilde yararlanmasını sağlar.
3. Güvenli Token Transferleri:
    - Trilemma Smart Wallet, token transferlerini daha güvenli hale getiren bir dizi güvenlik mekanizması sunar. Kullanıcılar, cüzdanlarındaki varlıkları belirlenen güvenlik önlemleriyle koruma altına alabilirler, bu sayede cüzdan ele geçirilse bile varlıkların güvenliği sağlanır.
4. Programlanabilirlik:
    - Trilemma Smart Wallet, geliştiricilere programlanabilir bir cüzdan altyapısı sunar. Bu sayede cüzdanın işlevselliği genişletilebilir ve özelleştirilebilir. Geliştiriciler, belirli senaryolara uygun akıllı sözleşmeler yazarak cüzdanın yeteneklerini artırabilirler.

Sorun Tanımı ve Çözüm Önerisi:

Geleneksel EOA Cüzdanlarının Sınırlamaları:

- Mevcut Durum: Geleneksel Externally Owned Account (EOA) cüzdanları, kullanıcıların özel anahtarlarını güvende tutmalarını zorunlu kılar. Özel anahtarların kaybolması veya çalınması durumunda ciddi güvenlik riskleri ortaya çıkar. Ayrıca, bu cüzdanlar gaz ücretleri gerektirir ve sosyal medya hesaplarıyla entegrasyon sunmaz, bu da kullanıcı deneyimini sınırlayan önemli faktörlerdir.
- Çözüm: Trilemma Smart Wallet, özel anahtar kullanımı yerine biyometrik doğrulama ve iki faktörlü kimlik doğrulama gibi alternatif doğrulama yöntemleri sunar. Kullanıcılar, gazsız işlem mekanizmaları sayesinde gaz ücreti ödemeden işlem yapabilirler. Ayrıca, sosyal medya hesaplarıyla entegrasyon özelliği, kullanıcıların mevcut dijital kimliklerini kullanarak cüzdanlarına kolayca erişim sağlamalarını mümkün kılar.

Programlanabilirlik:

- Mevcut Durum: Geleneksel EOA cüzdanları sadece açık ve gizli anahtarları barındırır, ancak herhangi bir programlanabilirlik yeteneğine sahip değildir. Bu, cüzdanların esnekliğini ve işlevselliğini kısıtlar.
- Çözüm: Trilemma Smart Wallet, bir akıllı kontrat olarak işlev görür ve kullanıcı taleplerine göre programlanabilir. Bu esnek yapı, cüzdanın özelleştirilebilir olmasını sağlar ve kullanıcıların ihtiyaçlarına göre yeni özellikler eklenmesine olanak tanır.

ERC-4337 Standardı

Trilemma Smart Wallet, Mart 2023'te duyurulan ve Ethereum Mainnet'te kullanılmaya başlanan ERC-4337 standardını temel alır. ERC-4337, Ethereum'da akıllı sözleşme tabanlı hesapların nasıl oluşturulacağını ve işlemlerin nasıl paketlenip ağa gönderileceğini tanımlar. Bu standart, hesap soyutlama teknolojisinin temelini oluşturur ve kullanıcı deneyimini geliştirir. ERC-4337'nin temel bileşenleri aşağıdaki gibidir:

1. UserOperation
    - Tanım: UserOperation, ERC-4337 standardında tanımlanan, bir kullanıcının gerçekleştirmek istediği bir işlemi temsil eden bir veri yapısıdır. Bu yapı, klasik Ethereum işlemlerinden farklı olarak doğrudan bir Externally Owned Account (EOA) yerine bir akıllı sözleşmeden kaynaklanabilir. Bu, hesap soyutlama (Account Abstraction) hedefleyen uygulamalar için önemlidir.
    - İçerik:
        - İşlem Türü: UserOperation'ın gerçekleştireceği işlemi tanımlar. Örneğin, "transfer" bir varlık transferini ifade ederken, "upgrade" bir varlığın seviyesini yükseltmeyi ifade edebilir.
        - İşlem Verileri: Gerçekleştirilecek işlem için gerekli olan tüm bilgileri içerir. Örneğin, bir varlık transferi işlemi için gönderici ve alıcı adresleri ile transfer edilecek miktar bu veri setine dahildir.
        - İmzalar ve Yetkilendirme: UserOperation, işlemi gerçekleştirme yetkisini kanıtlamak için imzalar içerir. Bu imzalar, işlemin geçerliliği ve güvenliği için kritik öneme sahiptir.
    - İşleyiş: Bir kullanıcı, gerçekleştirmek istediği işlemi temsil eden bir UserOperation oluşturur ve bunu ağa gönderir. Bu işlem, klasik Ethereum işlemlerinden farklı olarak, mutabakat katmanına ulaşmadan önce çeşitli doğrulama ve paketleme aşamalarından geçer.
2. Mempool
    - Tanım: Mempool, henüz blok zincirine eklenmemiş tüm işlemlerin bulunduğu bir havuzdur. UserOperations da bu havuzda yer alır, tıpkı klasik Ethereum işlemleri gibi.

- İşleyiş: Kullanıcılar tarafından gönderilen UserOperations, mempool'a gelir ve burada doğrulanmayı ve blok zincirine eklenmeyi bekler. Mempool, işlemlerin doğrulanması ve sıraya alınması için önemli bir ara katmandır. Burada bulunan işlemler, Bundlerlar tarafından toplanır ve işlenir.

3. Bundler
    - Tanım: Bundler, mempool'deki UserOperations'ı toplayan, doğrulayan ve bunları bir araya getirerek EntryPoint sözleşmesine gönderen bir bileşendir. Bundlerlar, Ethereum ağında bir tür "paketleyici" olarak görev yapar.
    - İşlevler:
        - Mempool Tarama: Bundler, mempool'de bulunan UserOperations'ı belirli kriterlere göre tarar ve toplar. Örneğin, belirli bir kullanıcının işlemleri veya belirli bir işlem türü seçilebilir.
        - Doğrulama: Bundler, topladığı UserOperations'ı doğrular. Bu doğrulama, işlemin geçerliliğini ve güvenliğini sağlamak için kritik öneme sahiptir. Örneğin, işlemin imzaları, yeterli bakiye olup olmadığı ve işlem limitleri kontrol edilir.
        - EntryPoint'e Gönderme: Doğrulanan işlemler, Bundler tarafından EntryPoint sözleşmesine gönderilir. EntryPoint, bu işlemleri işlemek ve blok zincirine eklemek üzere bir sonraki adımı temsil eder.
4. EntryPoint
    - Tanım: EntryPoint, ERC-4337'nin merkezi bir bileşeni olan akıllı sözleşmedir. UserOperations'ı doğrular, işlem maliyetlerini işler ve geçerli işlemleri blok zincirine ekler.
    - İşlevler:
        - UserOperations Doğrulama: EntryPoint, Bundler tarafından gönderilen UserOperations'ı tekrar doğrular. Bu aşamada, işlemin geçerliliği bir kez daha kontrol edilir ve geçersiz işlemler reddedilir.

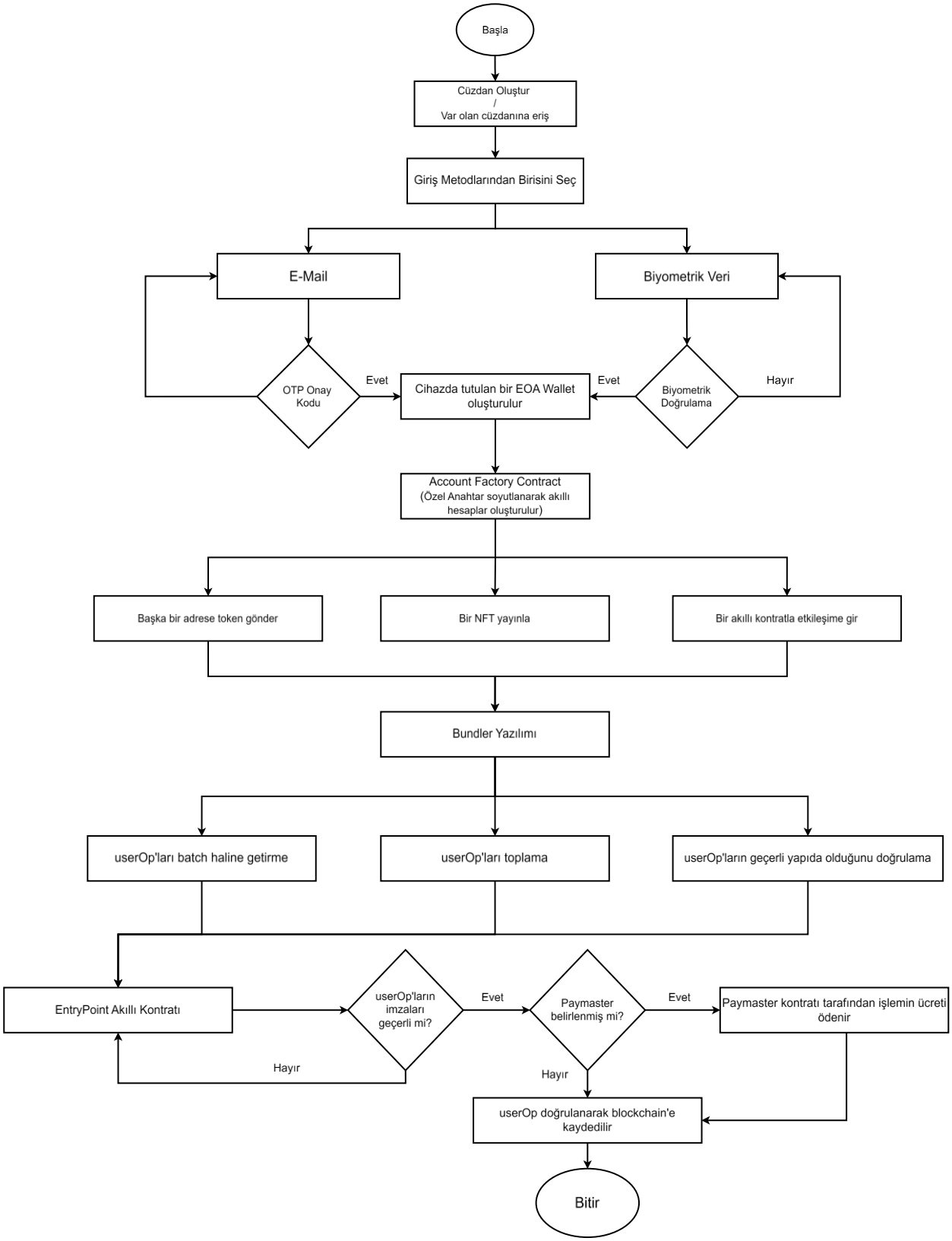
- Blok Zincirine Ekleme: Doğrulanan işlemler, EntryPoint tarafından Ethereum blok zincirine eklenir. Bu, işlemin resmi olarak ağa kaydedildiği aşamadır.
- İşlem Ücretlerinin İşlenmesi: EntryPoint, işlemler için gereken gaz ücretlerini toplar ve işleyerek işlemin tamamlanmasını sağlar. Bu ücretler, genellikle işlem doğrulayıcılarına (madencilere veya doğrulayıcılara) ödenir.

ERC-4337 İşleyişi: ERC-4337 standardı, Ethereum ağında hesap soyutlaması sağlamak amacıyla geliştirilmiştir. Bu standart, klasik Ethereum işlemlerinin aksine, mutabakat katmanında değişiklik yapma gereksinimini ortadan kaldırır ve işlemleri üst katmanlarda işler. Bu, mevcut Ethereum protokolünü bozmadan yeni işlevler eklemeyi sağlar.

Adım Adım İşleyiş:

1. UserOperation Gönderimi: Kullanıcılar, gerçekleştirmek istedikleri işlemleri UserOperation nesneleri olarak mempool'a gönderirler.
2. Bundler'ın İşlemi: Bundlerlar, mempool'deki UserOperations'ı toplar ve belirli kriterlere göre doğrular.
3. Bundler Tarafından Paketleme: Doğrulanan UserOperations, Bundler tarafından tek bir işlem olarak paketlenir. Bu işlem, "Bundle Transaction" olarak adlandırılır.
4. Blok Zincirine Dahil Edilme: Paketlenen Bundle Transaction, EntryPoint tarafından blok zincirine eklenir ve resmi olarak işlenir.

AKIŞ Grafiği



Sonuçlar

Trilemma Smart Wallet, klasik Web3 cüzdanlarının zorluklarını aşarak, Web3 teknolojilerinin daha geniş kitleler tarafından benimsenmesini amaçlayan yenilikçi bir çözüm sunmaktadır. Özellikle Web2 kullanıcılarını hedefleyen proje, Hesap Soyutlama teknolojisi sayesinde kullanıcıların gaz ücreti ödemeden işlem yapmasını, özel anahtar gerektirmeden güvenli doğrulama gerçekleştirmesini ve cüzdanlarını programlanabilir şekilde kullanmasını sağlar.

Proje, iOS, Android mobil uygulamaları ve PWA (Progressive Web App) web uygulamaları ile tam uyumlu olarak tasarlanmıştır. Trilemma Smart Wallet, Web3 dünyasına adım atanlar için güçlü bir çözüm sunmanın yanı sıra, gelişmiş kullanıcı deneyimi ve erişilebilirlik arayanlar için de etkili bir alternatif sunmaktadır. Bu cüzdan, kullanım kolaylığı ve güvenlik odaklı yapısıyla sektörde fark yaratmayı hedeflemektedir.

Ekip Hakkında

Trilemma, Türkiye merkezli bir açık kaynak Web3 geliştirme ekibidir. Ekibin kurucu üyeleri Alperen Bekçi ve Murathan Kağan Bayram, Trio Blockchain Labs hackathon ekibinde edindikleri deneyimle Web3 alanında derin bilgi ve beceriye sahiptir. Trilemma ekibi, Web3 teknolojilerinin herkes tarafından erişilebilir ve kullanılabilir olmasını hedeflemektedir ve kullanıcı deneyimi odaklı projeler geliştirmektedir.

Deloitte tarafından 2022 yılında yapılan bir ankete göre, Web3 teknolojilerine aşina olanların oranı oldukça yüksektir, ancak bu teknolojileri fiilen kullananların oranı düşüktür. Ankete katılanların %74'ü Web3'e aşina olduklarını belirtirken, %20.8'i Web3 uygulaması kullanmamış ve sadece %5.2'si aktif olarak kullanmaktadır. Bu veriler, Trilemma Smart Wallet'ın hedef kitlesinin ihtiyaçlarını net bir şekilde ortaya koymaktadır.

Web3 teknolojilerine aşina olup henüz deneyimlememiş büyük bir kitle mevcut. Bu durum, Trilemma Smart Wallet'ın Web2 kullanıcıları için önemli bir çözüm sunduğunu göstermektedir. Hesap Soyutlama (Account Abstraction) teknolojisi sayesinde, Web3 cüzdanlarının kullanım zorluklarını ortadan kaldırarak bu geniş kitlelerin Web3 ekosistemine dahil olmasını sağlamayı amaçlayan proje, kullanım kolaylığı ve erişilebilirlik sunarak bu teknolojilere yönelik çekinceleri minimize etmeyi hedeflemektedir.

Şu anda ekip, Trilemma Smart Wallet üzerinde yoğun bir şekilde çalışmaktadır. Proje, kullanıcılara daha güvenli, kullanıcı dostu ve programlanabilir bir cüzdan sunmayı amaçlamakta ve kullanıcı geri bildirimlerine büyük önem vererek ürünü sürekli olarak iyileştirmektedir. Trilemma ekibi, Web3 dünyasını daha geniş kitlelere tanıtmayı ve bu teknolojinin günlük kullanımda yer bulmasını sağlamayı hedeflemektedir.

Kaynakça

ERC-4337: Account Abstraction. (n.d.). ERC4337.io. Retrieved June 30, 2024, from https://www.erc4337.io/ ▪AfterDark Labs. (2023, February 21). EIPs Explained: EIP-4337. Medium. Retrieved June 30, 2024, from https://medium.com/@afterdark_labs/eips-explained-eip-4337-e10980b64be4

▪Eth Infinitism. (n.d.). Account Abstraction. GitHub. Retrieved June 30, 2024, from https://github.com/ethinfinitism/account-abstraction/

▪Buterin, V., & Vujin, N. (2023, January 1). EIP-4337: Account Abstraction. Ethereum EIPs. Retrieved June 30, 2024, from https://eips.ethereum.org/EIPS/eip-4337

▪ERC-4337 Account Abstraction via Entry Point Contract Specification. (2023, March 15). Ethereum Magicians. Retrieved June 30, 2024, from https://ethereum-magicians.org/t/erc-4337-account-abstraction-via-entry-pointcontract-specification/7160

İlgili Linkler

LİNKTREE: https://linktr.ee/trilemmadev

Ekip Websitesi: https://trilemmadev.vercel.app/

WhitePaper: https://trilemmadev.vercel.app/trilemmawhitepaper.pdf

İos ve Android App: Yakında...

PWA: https://trilemma-web.vercel.app/