ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MATEMATİK VE BİLGİSAYAR BİLİMLERİ

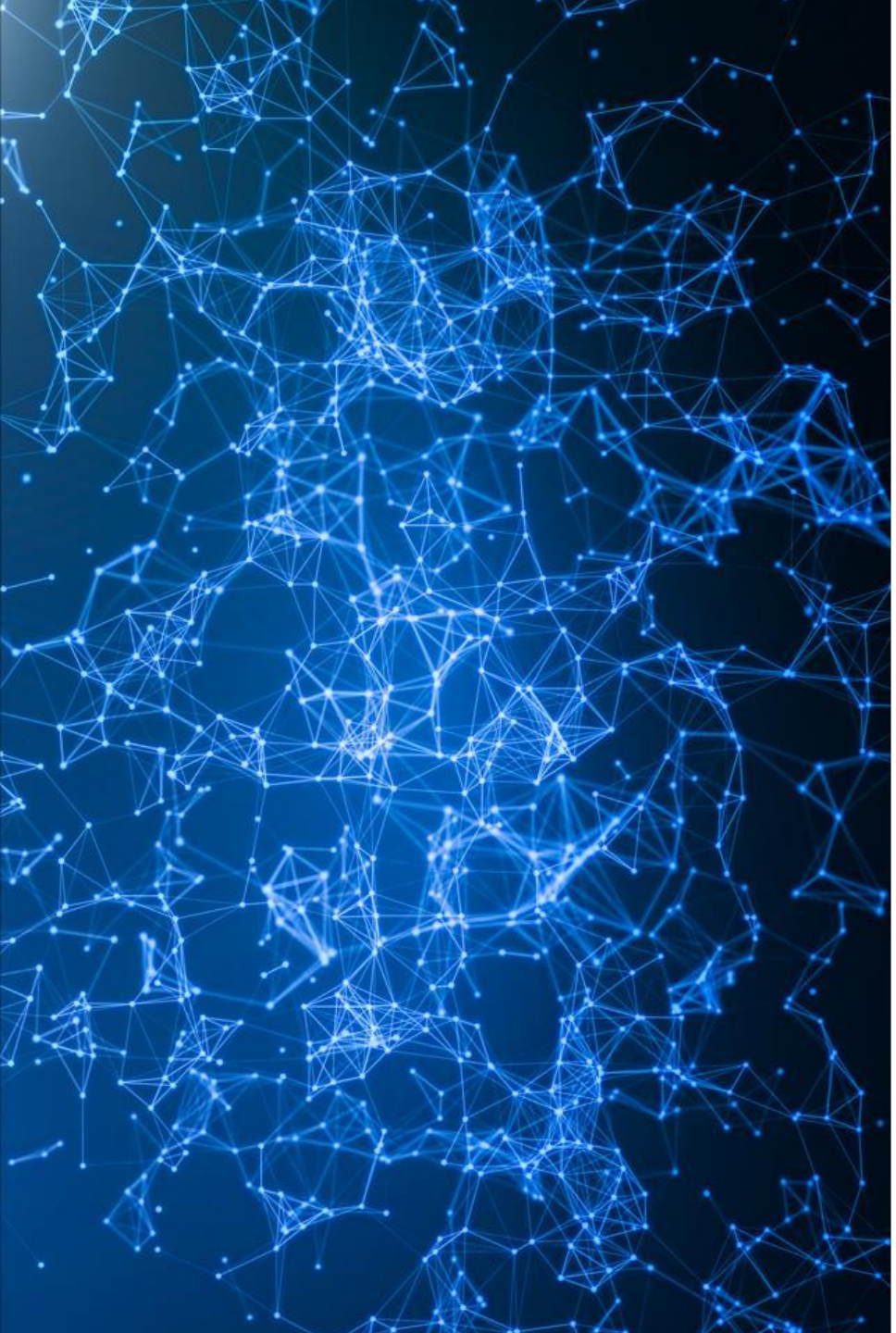
BLOK ZİNCİRİ TABANLI MOBİL YEMEK SİPARİŞ UYGULAMASI GELİŞTİRİLMESİ

NİDA BAŞER

DANIŞMAN: DOÇ. DR. AHMET FARUK ASLAN

YÜKSEK LİSANS TEZİ

2023

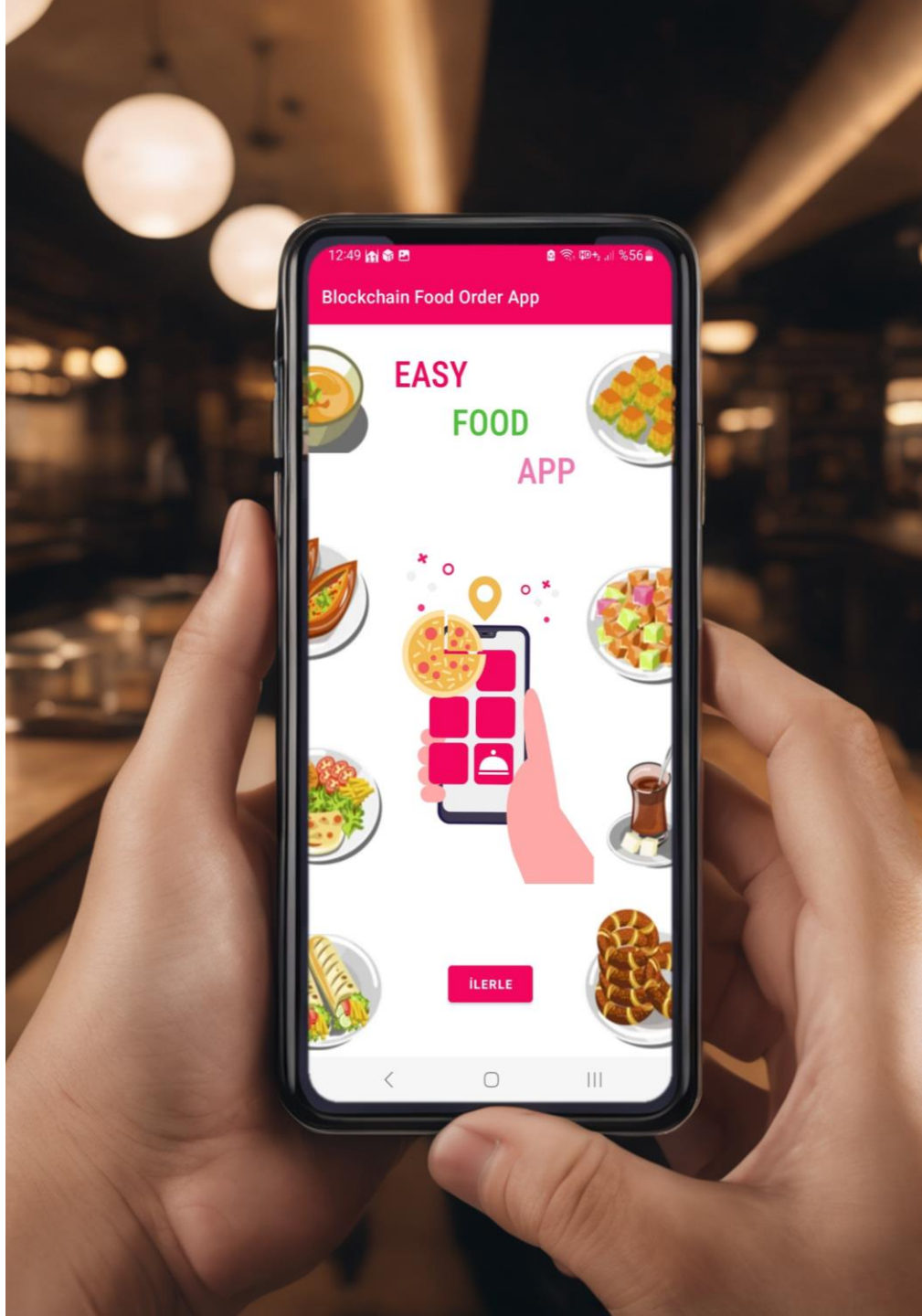


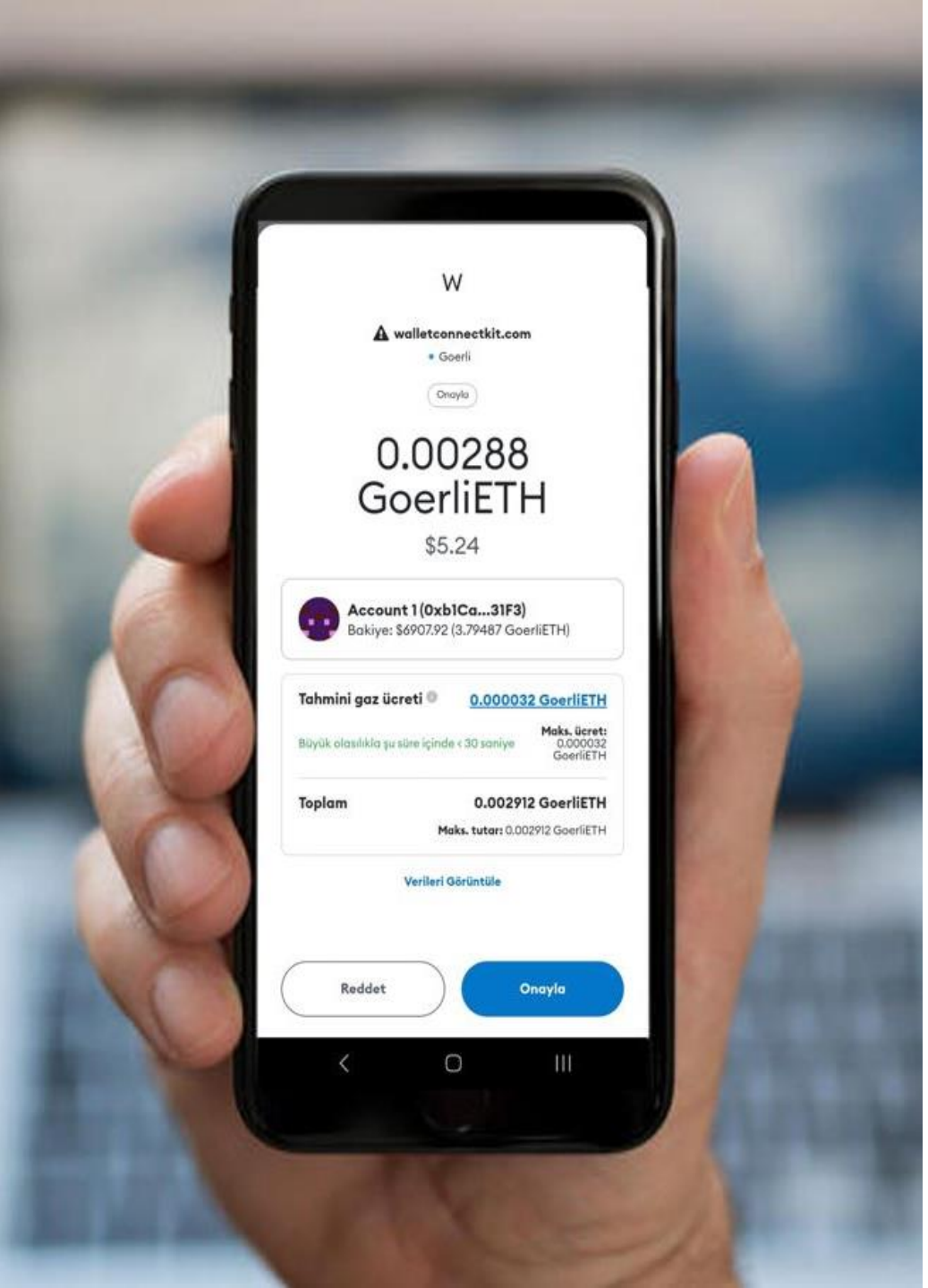
BAŞLIKLAR

- ÇALIŞMANIN AMACI
- ÇALIŞMANIN KONUSU VE ÖNEMİ
- LİTERATÜR İNCELEMESİ
- TEMEL KAVRAMLAR
- TASARIM VE YÖNTEM
- SONUÇLAR VE ÖNERİLER

ÇALIŞMANIN AMACI

Bu çalışmada; blok zinciri tabanlı ethereum kripto para ile ödeme seçeneği sunan bir mobil yemek sipariş uygulaması geliştirilmesi amaçlanmıştır.





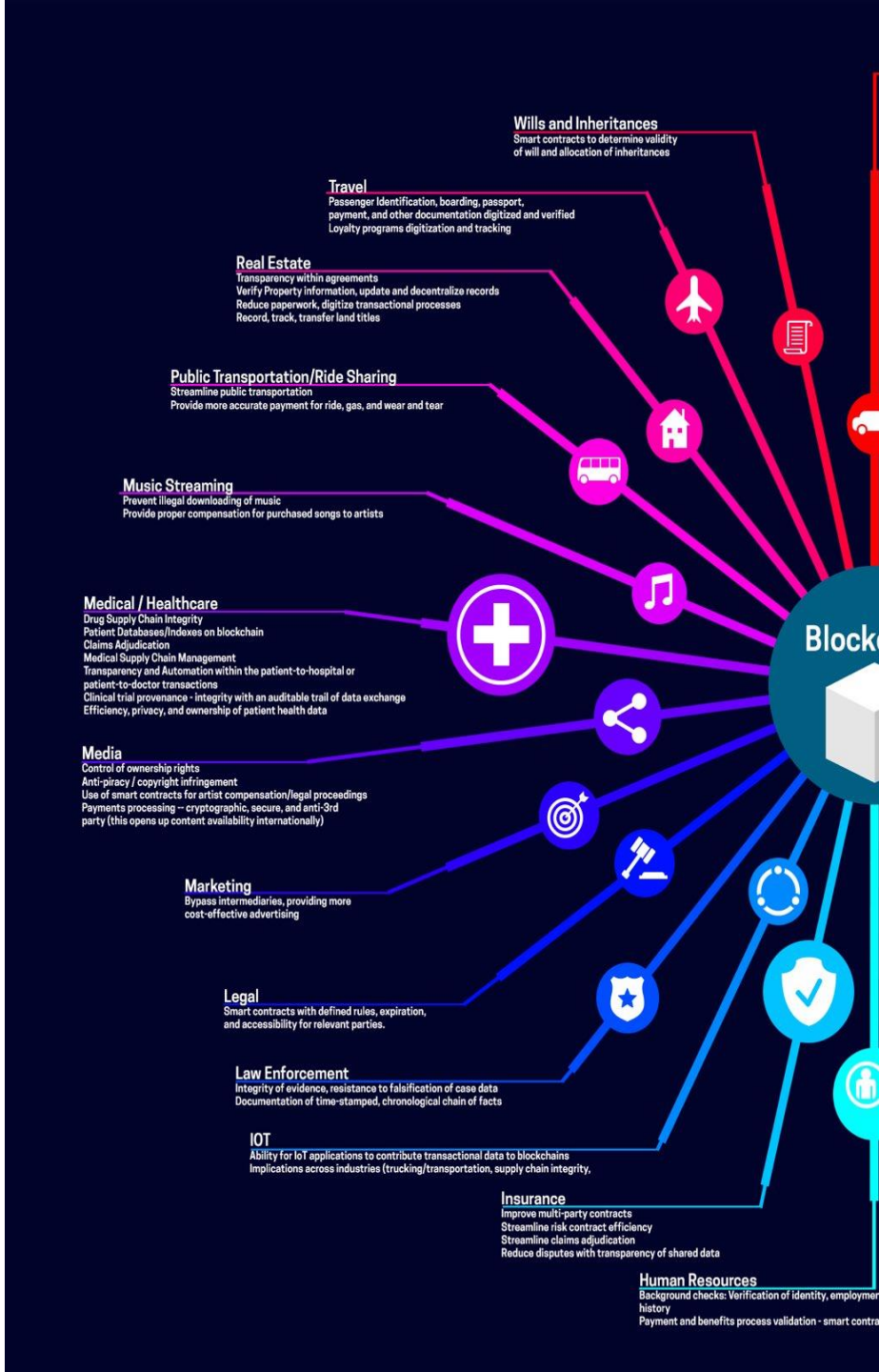
ÇALIŞMANIN KONUSU VE ÖNEMİ

Bu çalışmanın ana konusu ve aslında özgün değerini oluşturan unsur ise; geliştirilen mobil uygulamanın, bir kripto para cüzdanı yazılımı olan Metamask ile bağlantı kurabilmesi ve sepetteki ürünlerin toplam fiyatının ethereum cinsinden kripto para ile ödenerek, ethereum blok zincirine yeni bir blok eklenmesinin sağlanabilmesidir.

LİTERATÜR İNCELEMESİ

Blok zincir ve kripto para kavramları giderek yayılan bir kullanım alanına sahiptir. Ülkemizde de bu kavramları içeren projeler mevcuttur. Örneğin;

- Blok zincir tabanlı oy verme sistemi önerisi (Aydın, 2022),
- Üniversite bağışları için blok zincir tabanlı takip sistemi (Ferwana, 2021),
- Güvenli bir dijital sertifikasyon web uygulaması geliştirilmesi (Ataşen, 2019).
- Tedarik zinciri boyunca ürünlerin izlenebilmesi için blok zinciri tabanlı bir karar destek sistemi geliştirilmesi (Okay, 2022).
- Türkiye'nin yerel gereksinimleri için yapılandırılmış blok zinciri tabanlı bir tapu sistemi önerisi (Mendi vd., 2020).

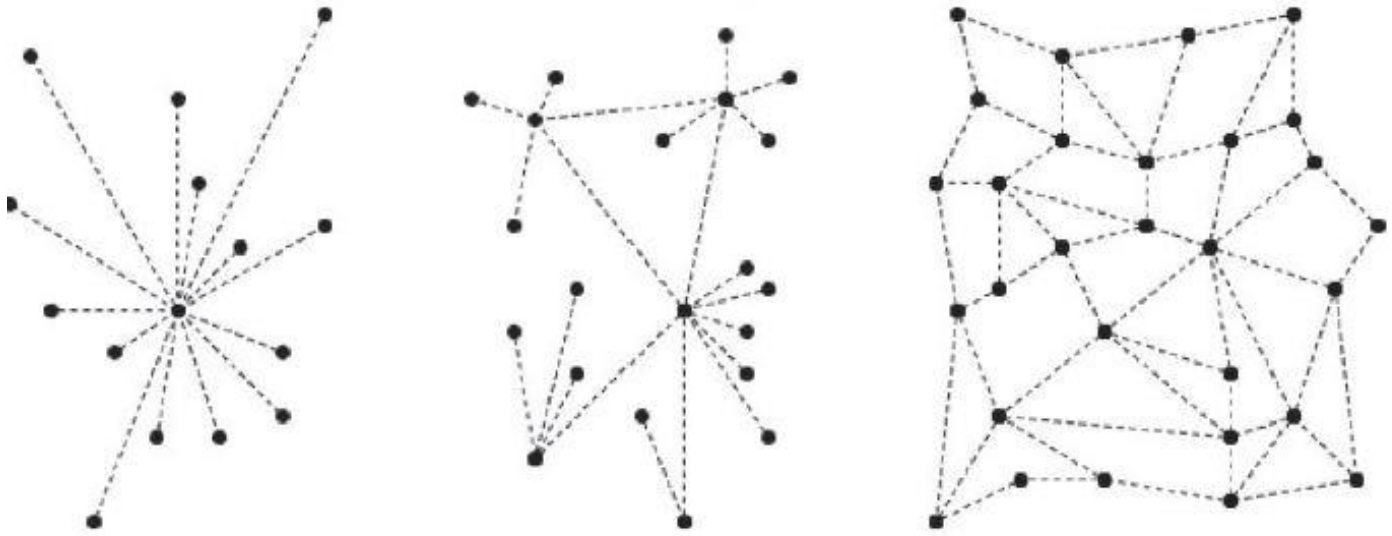


LİTERATÜR İNCELEMESİ

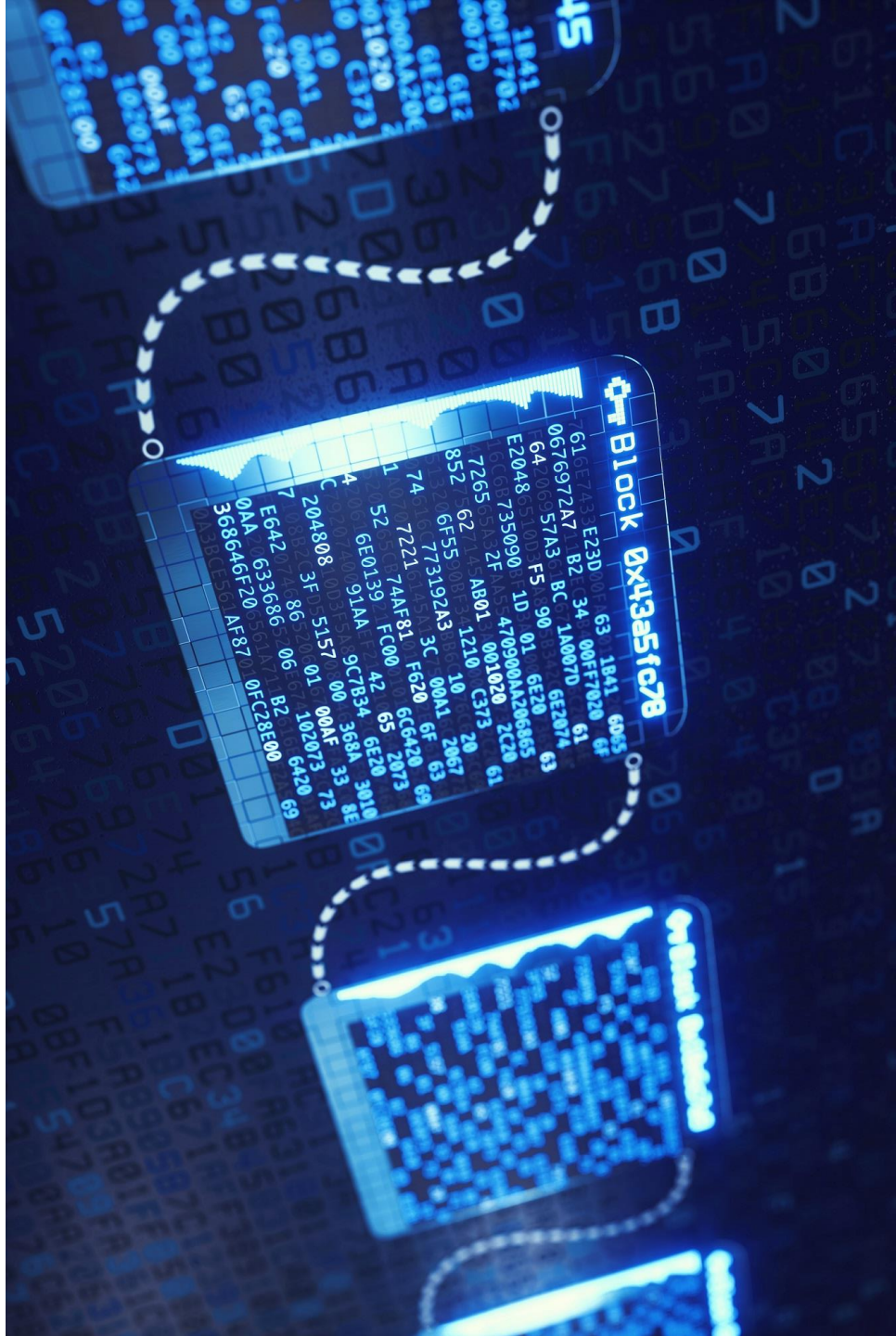
Literatür araştırması sonucunda blok zinciri teknolojisi üzerine yapılmış projelerin genellikle web uygulaması olarak gerçekleştirildiği görülmektedir. Bu projelerin mobil uygulamalara göre yaygınlaşma potansiyelinin düşük olduğu ve son kullanıcıya hitap etme bakımından geride kalabileceği öngörülmektedir. Ayrıca her teknolojinin ilk ortaya çıktığı zamanlarda olduğu gibi, blok zinciri teknolojisi ile ilgili akademik ve bilimsel kaynaklar sınırlıdır. Bu nedenle blok zinciri ve kripto para kavramlarının mobil uygulamalar ile birlikte kullanıldığı projelerin gerçekleştirilmesi literatürde doldurulması gereken bir boşluk olarak görülmüştür.

TEMEL KAVRAMLAR: Blok Zinciri

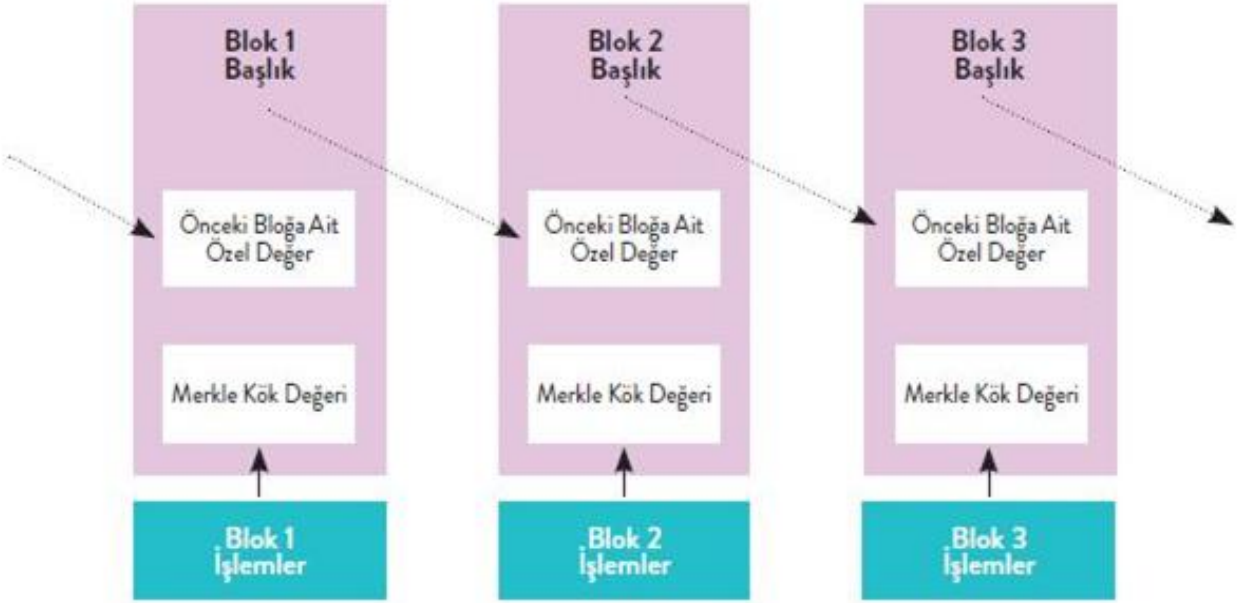
Blok zinciri en genel tanımıyla dijital bir muhasebe defteri olarak da bilinen dağıtılmış defter teknolojisinin bir uygulamasıdır. DDT, blok zinciri teknolojisi ve Bitcoin'den daha önce de var olan bir kavramdır.



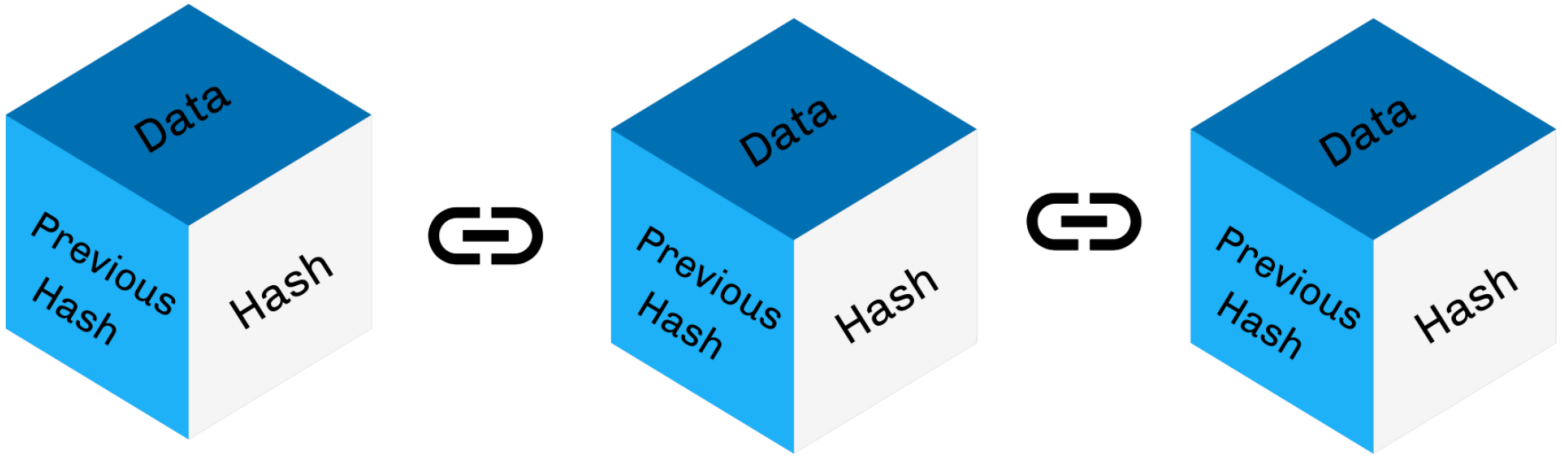
Blok zinciri teknolojisi, merkezi bir otorite olmadan, tüm katılımcılar arasında güvenli, şeffaf ve kalıcı bir şekilde veri paylaşımına olanak sağlar. Bloklar, birbirlerine zincir şeklinde bağlı olduğundan, değişiklik yapmak için önceki blokların hepsini değiştirmek gereklidir. Bu özelliği sayesinde blok zinciri teknolojisi verilerin değiştirilmesini neredeyse imkansız hale getirir.



Blok zinciri iki temel kavramdan meydana gelir: Bloklar ve blokları oluşturan kayıtlar. Kayıtlar, blok zincirin tasarımına göre değişir. Sanal para birimleri için bu kayıtlar para transferi bilgileridir. Kayıtlar birleştirilip belirli aralıklarla işlenerek blokların içine yazılır. Blokların içerisinde kaç tane kayıt bulunacağı ve kayıtların hangi işlemlerden geçtikten sonra bir blok oluşturulacağı gibi kıstaslar, blok zincirin tasarımına mahsustur. Genelde bir bloğun oluşturulması sırasında kriptografik özet algoritmaları ve dijital imza kullanılır. Zincirin en başındaki bloğa "genesis block" denir ve bu blok başka bir bloğa bağlı değildir.

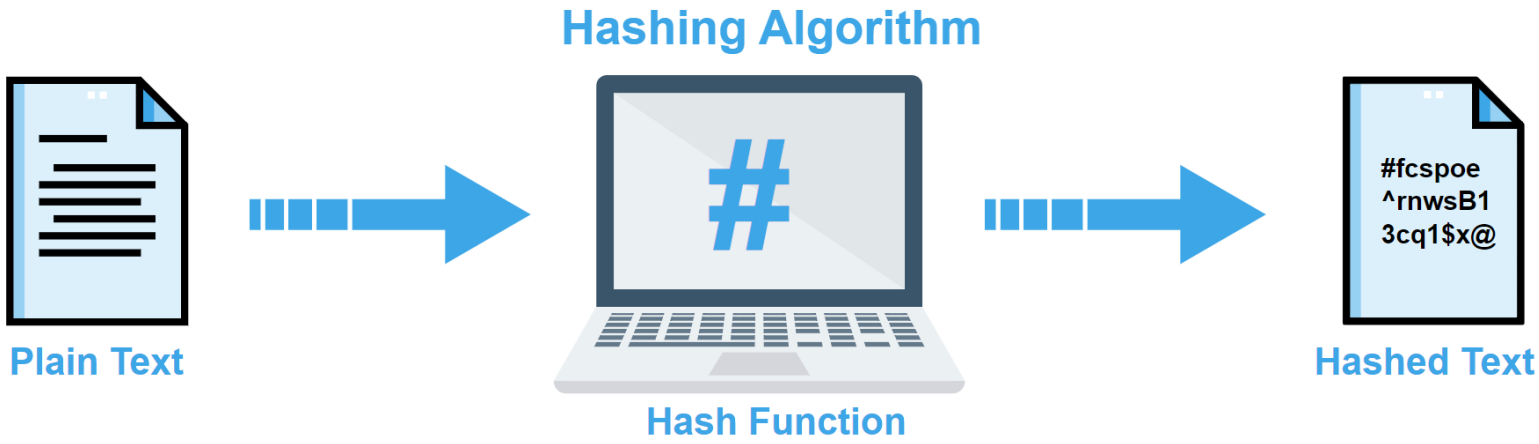


Bloklar arasındaki bağlantılar bilgisayar bilimlerinde veri yapıları başlığı altında anlatılan bağlı liste (Linked List) veri yapısına benzer fakat aradaki tek fark blokların tersine bağlı (Back-Linked List) olmasıdır. Dolayısıyla her blok aslında kendinden bir önceki bloğun adresini kendi içinde barındırır. Ağdaki her düğüm (katılımcı), başlangıçtan itibaren tüm kayıtların bir kopyasını tutar. Bu kayıtların değiştirilmesi özetlerin de değişmesine yol açacağından dolayı, kayıtlar değiştirildiğinde çoğunluk bunu fark edebilir. Herkesin doğrulama yapabildiği dağıtık bir veritabanı sistemi ile kimseye güvenmeye gerek kalmadan doğru bilginin tutulduğu ispatlanabilir.

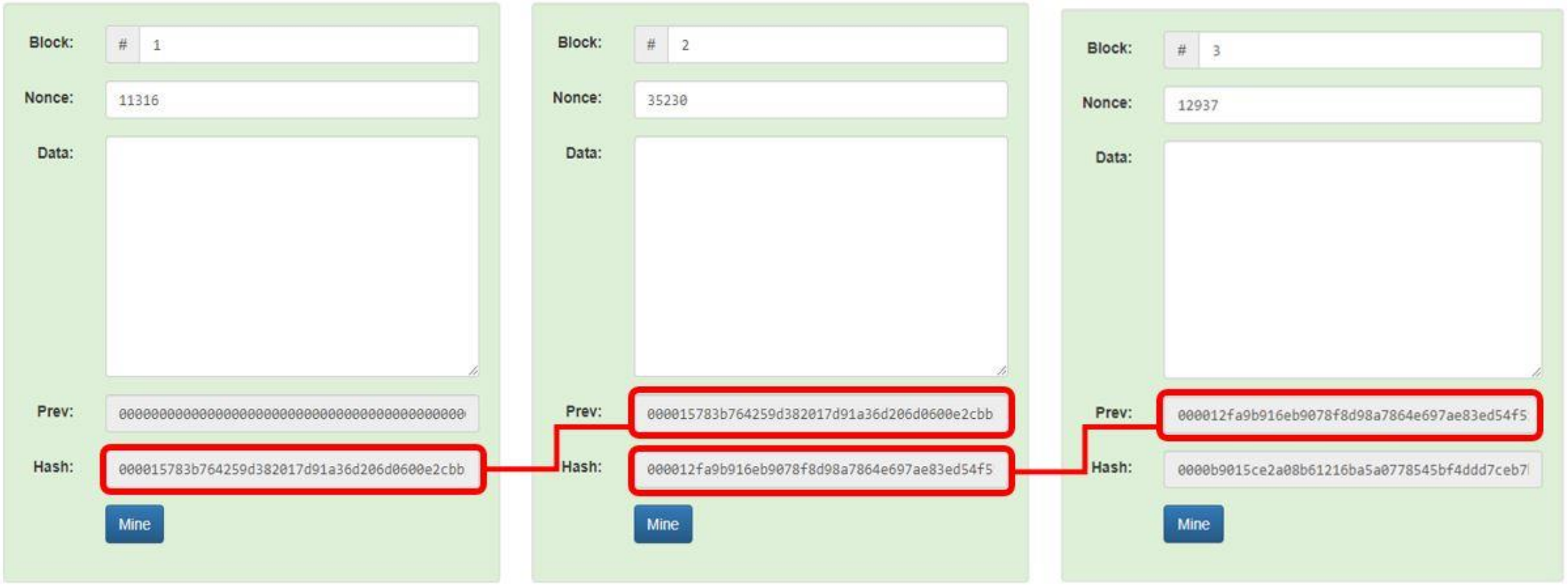


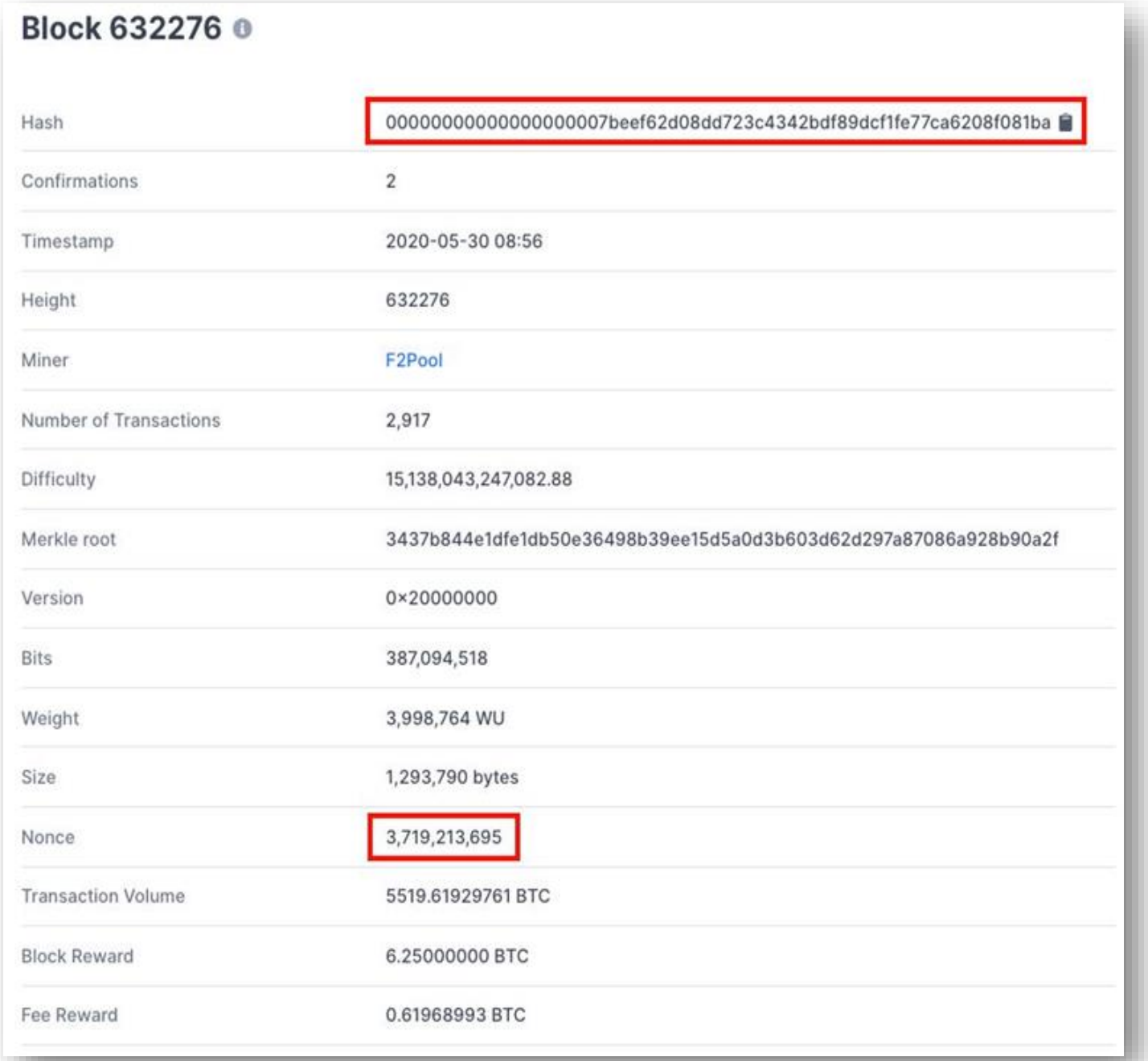
TEMEL KAVRAMLAR: SHA256

Kriptografik özet algoritması, farklı uzunluklardaki verilerin sabit bir uzunluğa dönüştürülmesini sağlayan ve aynı girdi ile her zaman aynı çıktıyı veren tek yönlü bir fonksiyondur. Tek karakterlik bir değişiklik bile metnin özetinin tamamını değiştirir. Bu yüzden hash fonksiyonları veri bütünlüğü kontrolünün sağlanması açısından blok zinciri veri tabanlarında çok büyük öneme sahiptir. Blok zincirinde hash fonksiyonları, yapılan işlemleri doğrularken veya yeni bir bloğu zincire eklerken kullanılmaktadır.



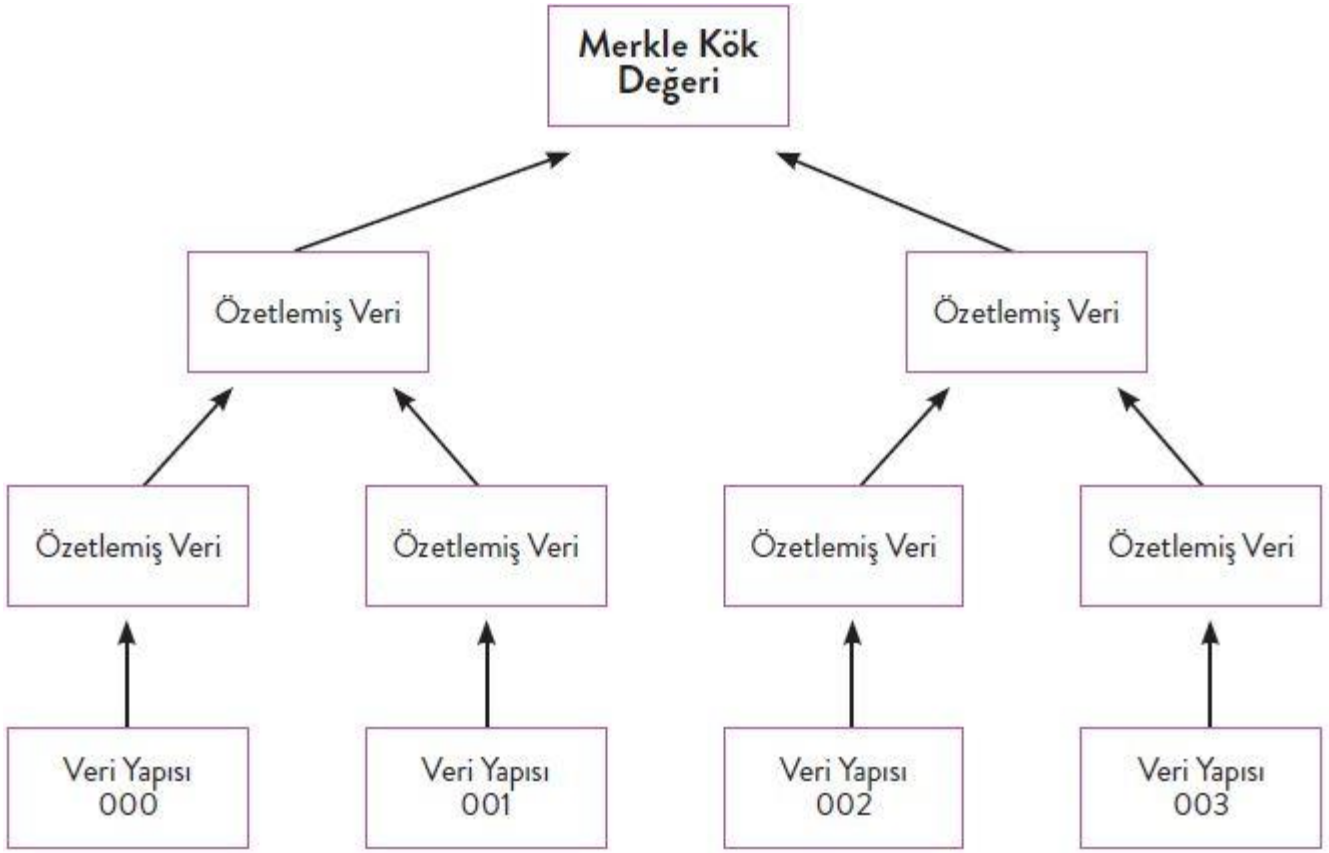
Ağ üzerinde gerçekleştirilen her işlem için benzersiz bir hash değeri oluşturulur. Blokların özetleri alınırken kendisinden bir önceki bloğun özet değeri de o bloğun içine girdi olarak eklenir yani n'inci blok içerisinde n-1'inci bloğun özet değeri de bulunur. Bundan dolayı bir blok kendisinden önceki tüm bloklara ait bilgiyi taşır. Yani herhangi bir blok, kendisinden önceki ve sonraki bloklara hash fonksiyonu ile bağlanmış olur.





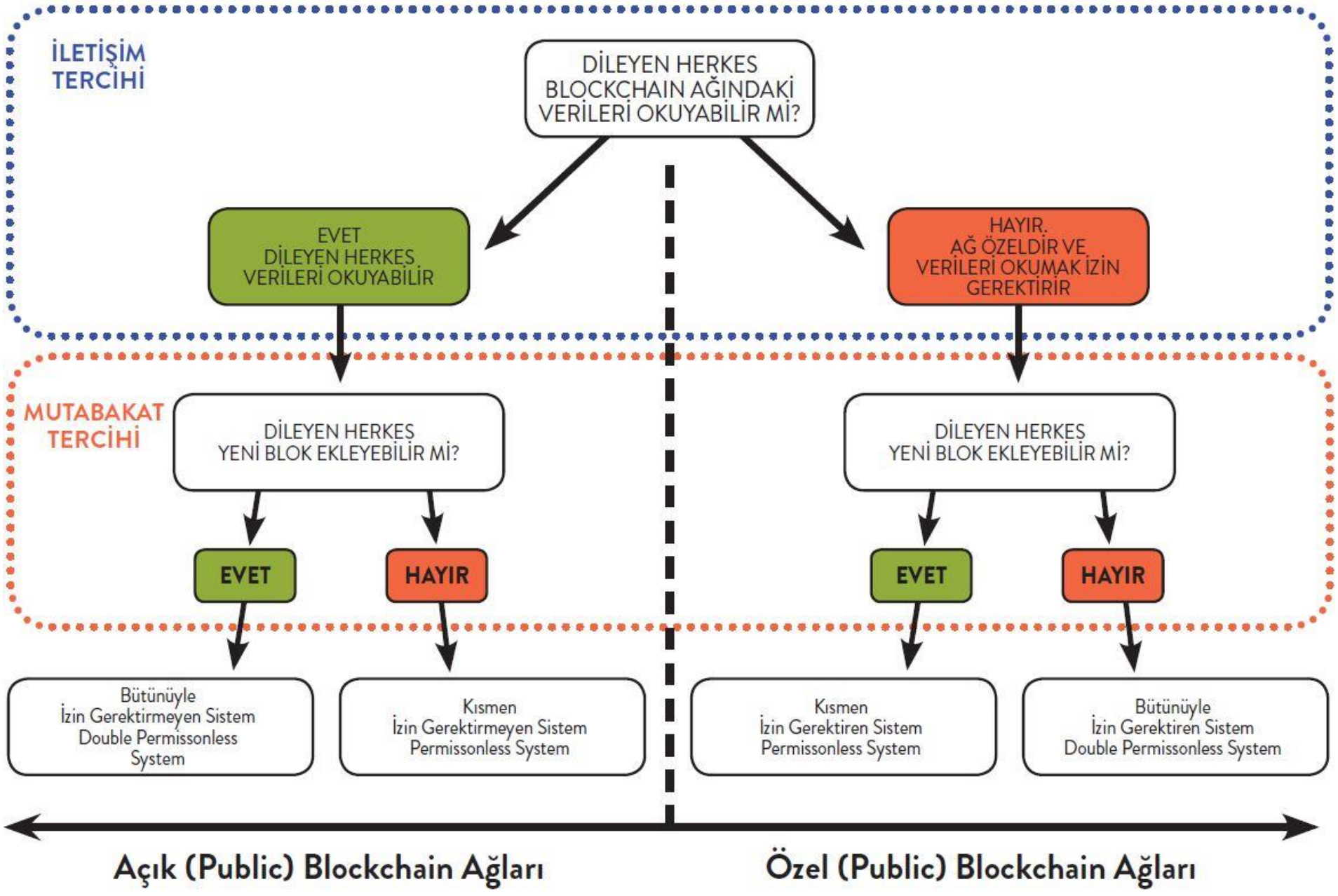
Madenciler, blok zincirine yeni bir blok eklerken, bloğun içerisindeki verileri ve blok özeti olarak da bilinen önceki bloğun hash değerini bir kriptografik hash fonksiyonundan geçirirler. Bu işlem sonucunda elde edilen hash değerinin sol baştan belirli bir kısmının sıfır olması gerekir. Hedeflenen sıfır sayısına ulaşıncaya dek nonce değeri sürekli olarak değiştirilerek hash fonksiyonuna uygulanmaya devam edilir. Hedefe ulaşıldığında, blok zincirine yeni bir blok eklenmiş olur.

TEMEL KAVRAMLAR: Merkle Ağacı



Merkle Ağacı, blok zinciri teknolojisinde kullanılan bir veri yapısıdır. Birden fazla veriyi tek bir özet haline getirerek, bu verilerin güvenliği ve bütünlüğünü sağlar. Bu yapının temel amacı büyük veri kümelerini işlemeyi daha hızlı ve verimli hale getirmektir.

TEMEL KAVRAMLAR: Blok Zincirinin Türleri

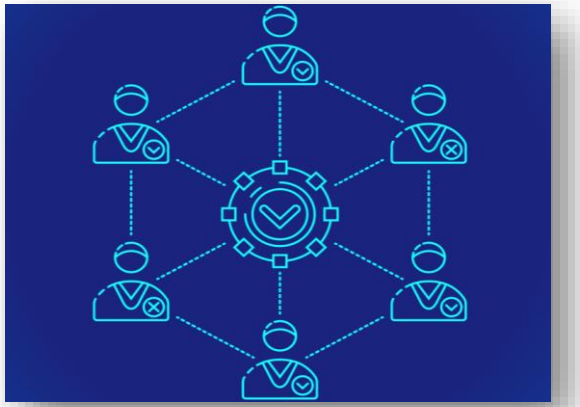


TEMEL KAVRAMLAR: Mutabakat Mekanizmaları

Mutabakat mekanizmaları, ağdaki tüm düğümlerin birbirleriyle anlaşmasını sağlayarak blok zincirinde işlemlerin güvenliğinin, bütünlüğünün ve devamlılığının sağlanmasında kritik bir rol oynamaktadır. Bir çok farklı mutabakat mekanizması vardır ve yenileri de geliştirilmeye devam edilmektedir. Bunlardan İş İspatı (Proof of Work - PoW), Hisse İspatı (Proof of Stake - PoS) ve Yetki İspatı (Proof of Authority - PoA) en yaygın kullanılan mutabakat mekanizmalarıdır.

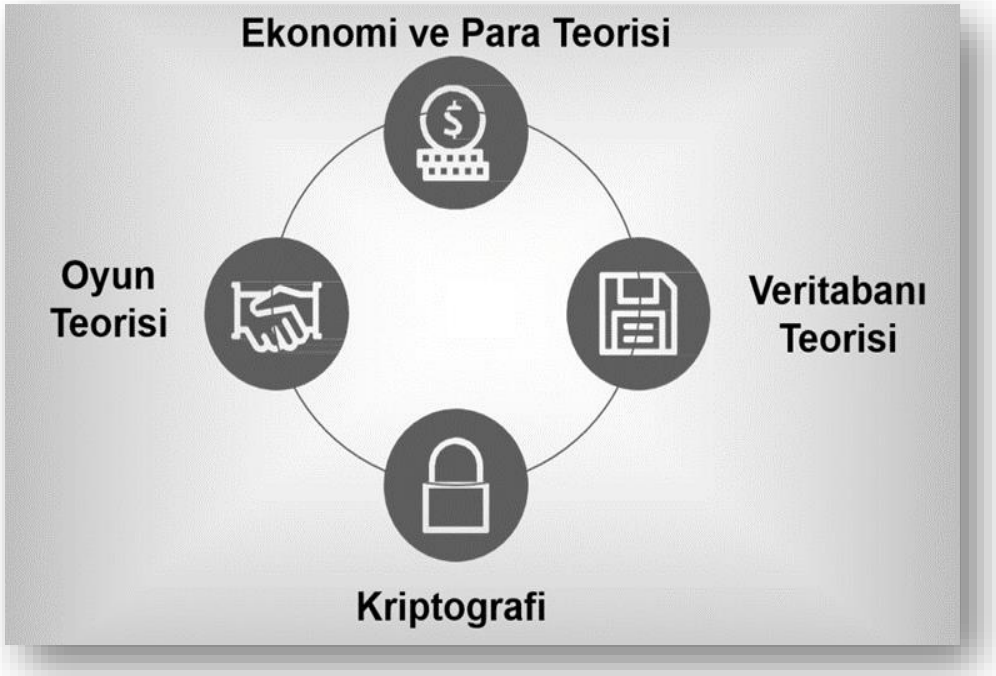
Proof of Work
İş Kanıtı

Proof of Stake
Hisse Kanıtı



Proof of Authority
Yetki Kanıtı

TEMEL KAVRAMLAR: Kripto Paralar



Blok zinciri teknolojisi ilk kullanım alanı olan Bitcoin ile ortaya çıktığında, şekilde gösterildiği üzere bilgisayar bilimlerinde halihazırda mevcut olan bazı bilim dalları, ekonomi ve para teorisiyle bir araya gelmiştir denilebilir. Bu bilim dallarının hepsini bir arada kullanmak Bitcoin'in devrim niteliğinde olmasını sağlamıştır.

- **Ekonomi ve para teorisi yönü**: Bitcoin ile oluşturulan dağıtık güven mekanizmasıyla birlikte bankalardan bağımsız bir para iletişiminin gerçekleştirilmesi sağlanmıştır.
- **Veritabanı teorisi yönü**: Kayıtların ve transferlerin tutulmasındaki yöntem yeni bir veri tabanı yaklaşımı oluşturmuştur.
- **Oyun Teorisi yönü**: Yeni bloklar üretilirken Proof of Work gibi bir fikir birliği mekanizmaları madencilerin teorisini oluşturmuştur.
- **Kriptografi yönü**; Madencileri de tüm bu işlemleri yaparken kriptografik hesaplamaların zorluğunu arkalarına alarak harcanan emeğin bir varlık, bir değer olmasını sağlamışlardır.

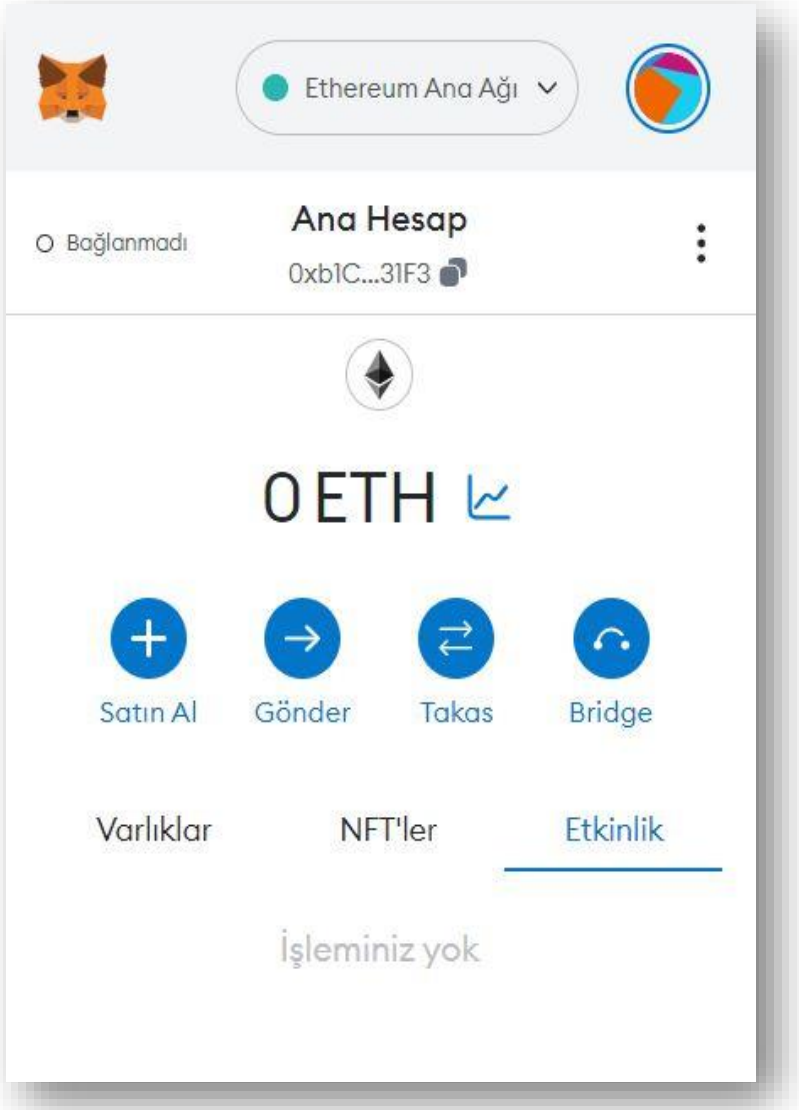
DDT, blok zinciri, kripto para ve bitcoin kavramları aslında birbirinin alt kümesi olarak düşünülebilir. *Blok zinciri;* veri transferi sağlayan dijital bir güven protokolüdür. *Kripto para;* para transferi sağlayan dijital bir finans protokolüdür. *Bitcoin*; ağ üzerinde herhangi bir merkeze bağlı kalmadan kullanıcı mahremiyetini kripto şifrelemeyle koruyup işlem kayıtlarını şeffaflaştırarak, aracısız ve güvenli para transferi sağlayan bir kripto paradır.

Ethereum, geliştiricilerin merkezi olmayan uygulamaları oluşturmasını ve dağıtmasını sağlayan blok zinciri teknolojisi ve akıllı sözleşmeler (smart contracts) konseptini kullanan açık kaynaklı bir yazılım platformudur. Bitcoin gibi, Ethereum da halka açık (public) bir blok zincirdir ancak ikisi arasında bazı önemli teknik farklılıklar vardır. Bitcoin, online ödemeler için eşler arası elektronik para transfer sistemine özel bir blok zinciri uygulaması olup dijital paranın sahipliğini izlemek için kullanılır. Ancak Ethereum, sadece kripto paralara odaklanmaz. Ethereum programlanabilirdir ve merkezi olmayan uygulamalar oluşturup dağıtabilmenize olanak tanır.

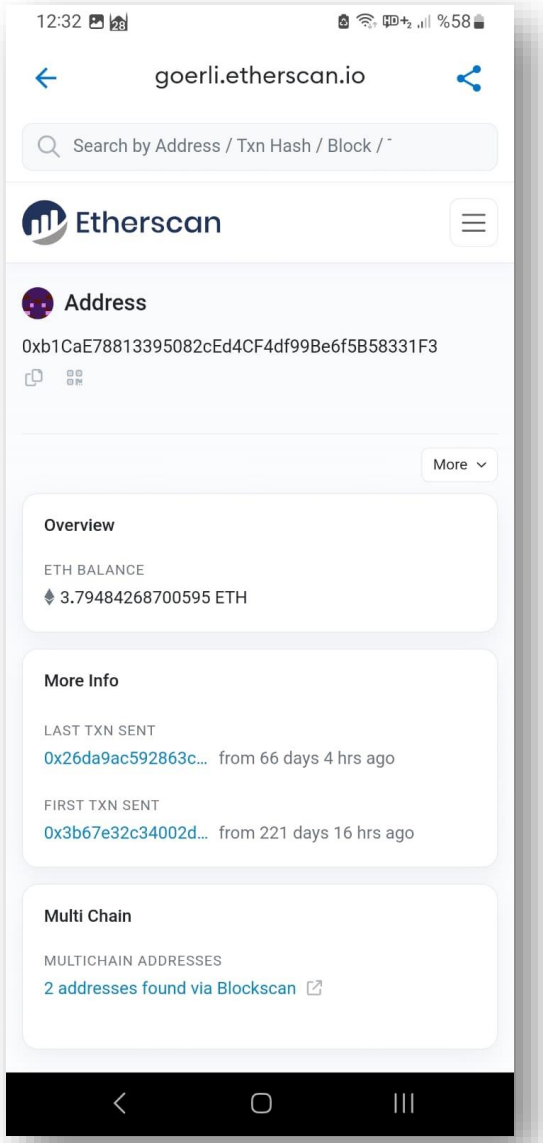
Ethereum blok zincirinde madenciler, Bitcoin blok zincirindeki gibi madencilik yapmak yerine ağı besleyen bir kripto token olan Ether'i kazanmaya çalışırlar. Ether, kullanışlı bir kripto para birimidir ve Ethereum ağında uygulama geliştiricileri tarafından yapılan işlemlere ait ücretleri ve hizmetleri ödemek için de kullanılır. Ethereum ağında işlem yapmak isteyen kullanıcılar Ether satın almalı veya kazanmalıdır. Maksimum üretimi 21 milyon olan Bitcoin'den farklı olarak, oluşturulabilecek ETH miktarı sınırsızdır, ancak bir ETH bloğunu işlemek için geçen süre her yıl ne kadar ether basılabileceğini sınırlar.

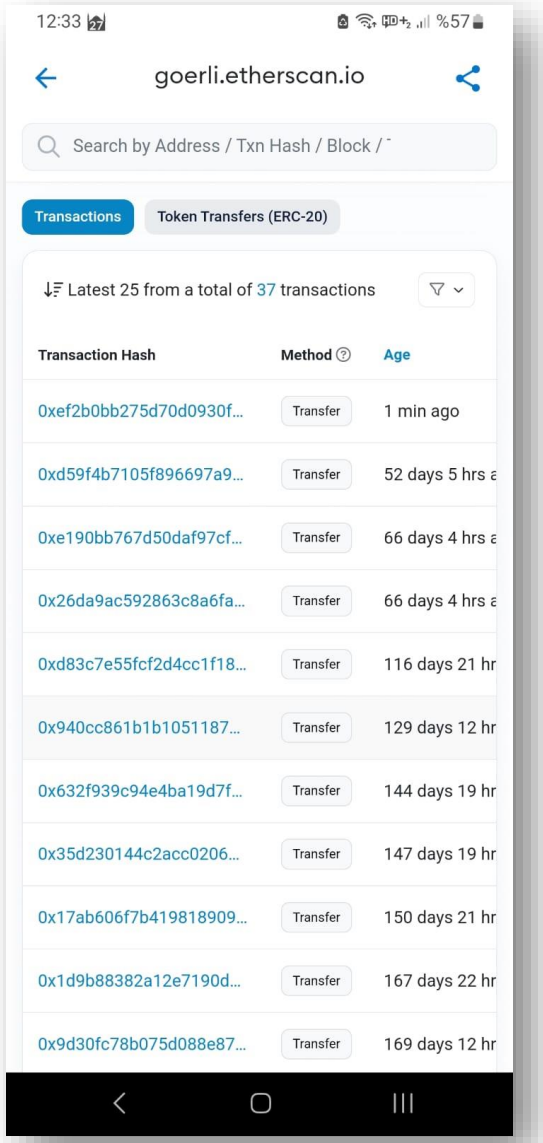
TEMEL KAVRAMLAR: Kripto Cüzdanlar

Metamask, bilgisayarınızda tam bir Ethereum düğümü çalıştırmadan, web tarayıcısı veya mobil uygulama aracılığıyla merkezi olmayan uygulamalara güvenli bir şekilde bağlanılmasını sağlayan bir kripto para cüzdanı yazılımıdır. Kullanıcıların Ethereum hesap anahtarlarını depolamasına, yönetmesine ve Ethereum ağına erişerek işlemlerini imzalamalarına, göndermelerine ve ağda işlemleri takip etmelerine olanak tanır. Doğrudan Ethereum çekirdek ekibi tarafından üretilen Metamask, kullanıcılara güvenli ve esnek işlem kolaylığı sağlamayı amaçlamaktadır.



TEMEL KAVRAMLAR: Blok Zinciri Gezgini





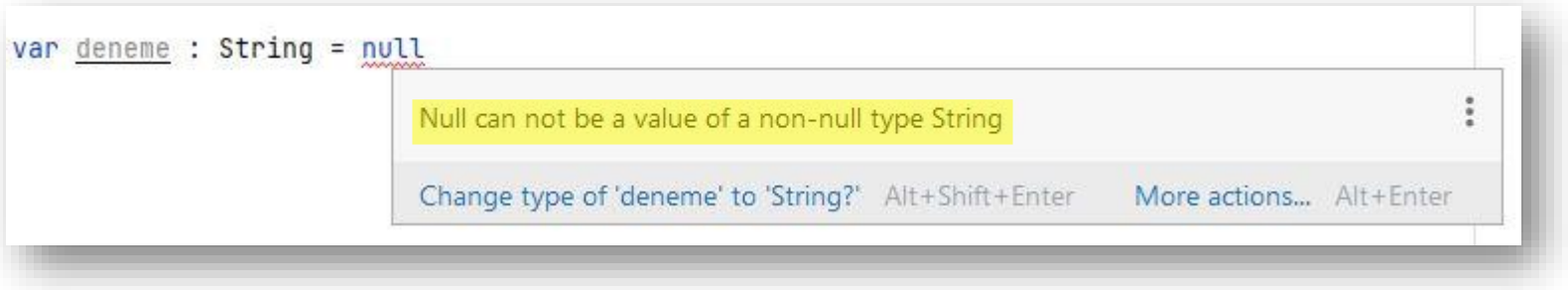
Etherscan, Ethereum blok zinciri üzerindeki işlemlere yönelik herkese açık verileri, akıllı sözleşmeleri, adresleri ve çok daha fazlasını görüntülemeye imkan tanıyan bir blok zincir gezginidir. Ethereum üzerindeki tüm etkileşimler zaten herkese açıktır ve Etherscan bir arama motoru gibi davranarak bunları incelemenize olanak tanır. Bir blok zincir bilgi kaynağı ve akıllı sözleşme veri tabanı olarak hareket eder.

TASARIM VE YÖNTEM

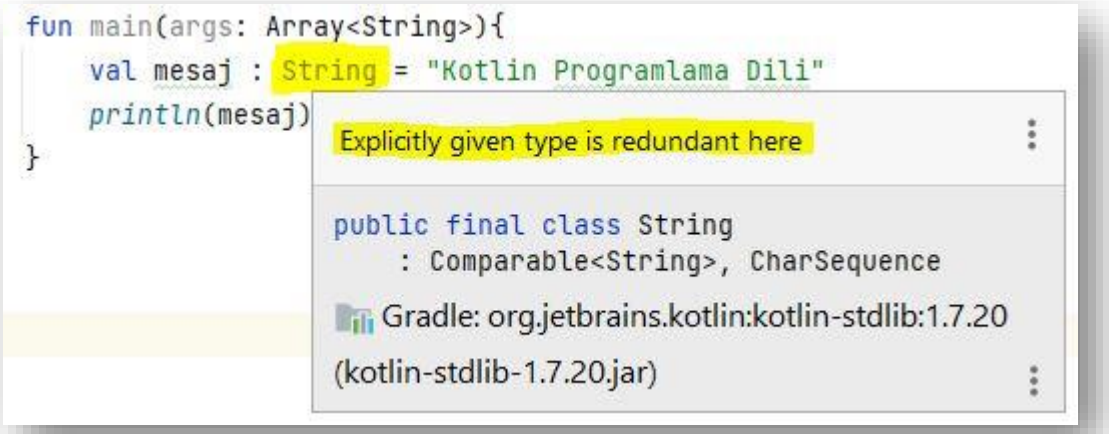
Çalışma, Android Studio geliştirme ortamında, Kotlin programlama dili ve WalletConnect Kotlin SDK (Yazılım Geliştirme Kiti) kullanılarak gerçekleştirilmiştir.

Programlama dili olarak java yerine kotlin'in tercih edilmesindeki sebepler şunlardır:

1. Java gibi nesne yönelimli programlama dillerinde, varsayılan olarak null (boş) değerler sebebiyle Null Pointer Exception (Boş İşaretçi İstisnası) hatalarıyla sıkça karşılaşılmaktadır. Kotlin programlama dilinde varsayılan olarak hiçbir değişkene null değeri atanamamaktadır ve hiçbir metot geriye null değer döndürememektedir.



2. Kotlin programlama dilinde kod yazarken herhangi bir değişkenin türünün tanımlanması esnek hale getirilmiştir. Tür belirtmeye gerek yoksa, şekilde gösterildiği üzere Kotlin, bu işlemin gereksiz olduğunu belirten bir uyarı verir.

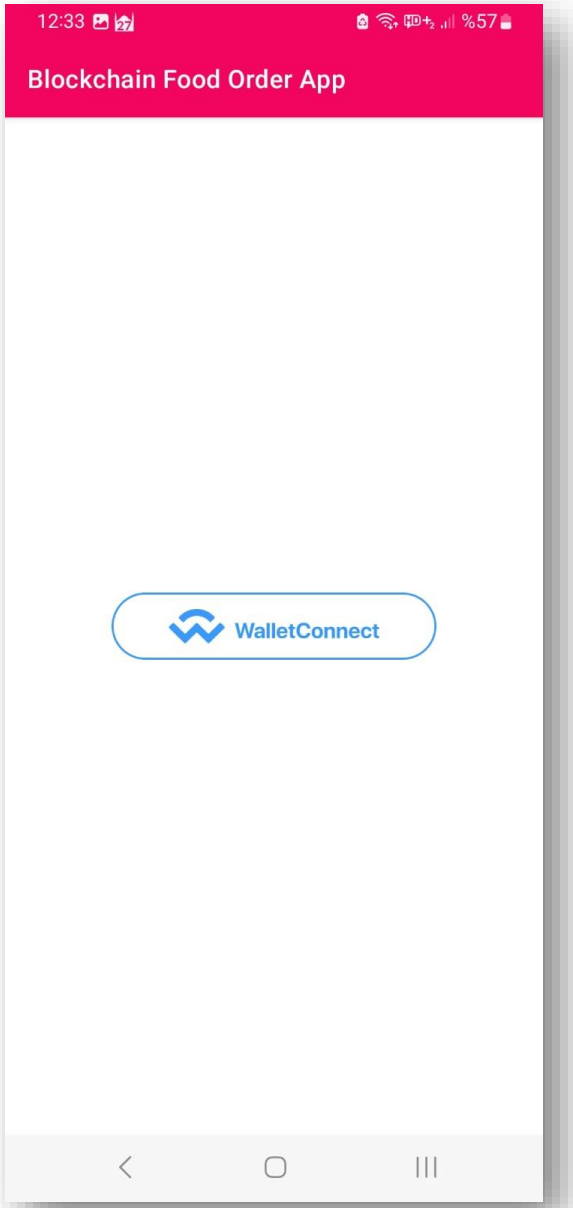



```java
public class User{
        private String name;
        private String surname;
        public User(String name, String surname){
            this.name = name;
            this.surname = surname;
        }
        public string getName(){
            return name;
        }
        public void setName(String name){
            this.name = name;
        }
        public string getSurname(){
            return surname;
        }
        public void setSurname(String surname){
            this.surname = surname;
        }
    }
```

3. Java dilindeki bir sınıf (class) yapısında, kullanılacak her özellik için, get ve set metotlarını tanımlamak gerekmektedir. Ancak Kotlin'de veri sınıfları (data classes) özelliği sayesinde yazılması gereken sınıf ve özellikleri tek satıra indirgenebilmektedir.

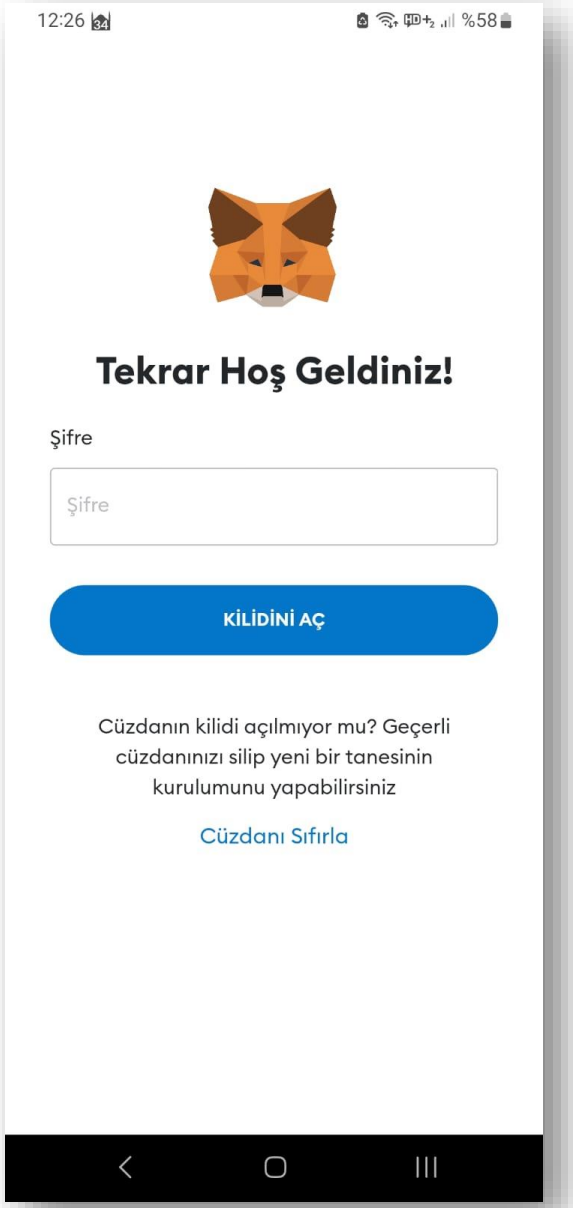
```kotlin
data class User(var name: String, var surname: String)
```

WalletConnect, merkezi olmayan Web3 mesajlaşma katmanıdır ve kripto para cüzdanlarını DApp'lara bağlamak için bir standarttır. Merkezi olmayan uygulamaları QR kodu tarayarak veya derin bağlantıyla (deep link) mobil cüzdanlara bağlamak için kullanılan açık kaynaklı bir protokoldür. WalletConnect, web3 ekosisteminde cüzdan ile merkezsiz uygulamanın birlikte çalışabilirliğini geliştirmektedir ve 150'den fazla kripto cüzdanı desteğini sorunsuz bir şekilde merkezsiz uygulamalara entegre edebilmektedir. Kripto cüzdanlarda WalletConnect entegresyonu için JavaScript, Swift veya Kotlin programlama dillerindeki SDK'lar kullanılabilir. Bu çalışmada Kotlin programlama dili kullanıldığı için WalletConnect'in Kotlin SDK'sı tercih edilmiştir.

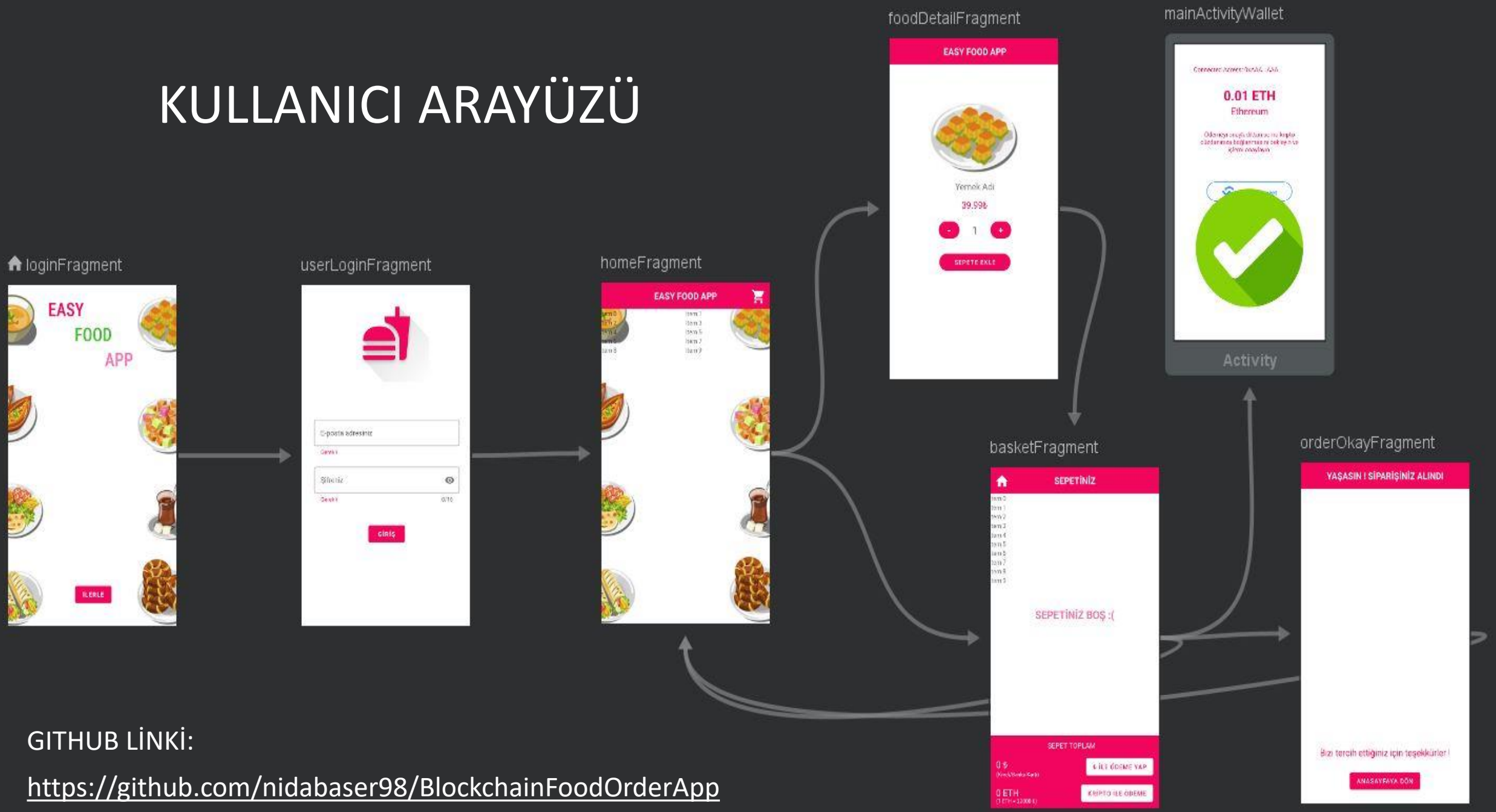


WalletConnect yardımıyla bir kripto cüzdan ile mobil uygulama arasında bağlantı kurmanın genel modeli şu şekildedir:

1. Mobil uygulama, kullanıcıya bir bağlantı düğmesi gösterir.
2. Kullanıcı düğmeye basar ve Android sistemi kripto cüzdana yönlendirir.
3. Cüzdan, kullanıcıdan bağlantı isteğini onaylamasını veya reddetmesini ister.
4. Kullanıcı oturumu onaylar ve mobil uygulamaya döner.
5. Mobil uygulama ile kripto cüzdanı arasında bağlantı kurulmuş olur.
6. Kullanıcı artık transferlerini mobil uygulama içinden gerçekleştirebilir.



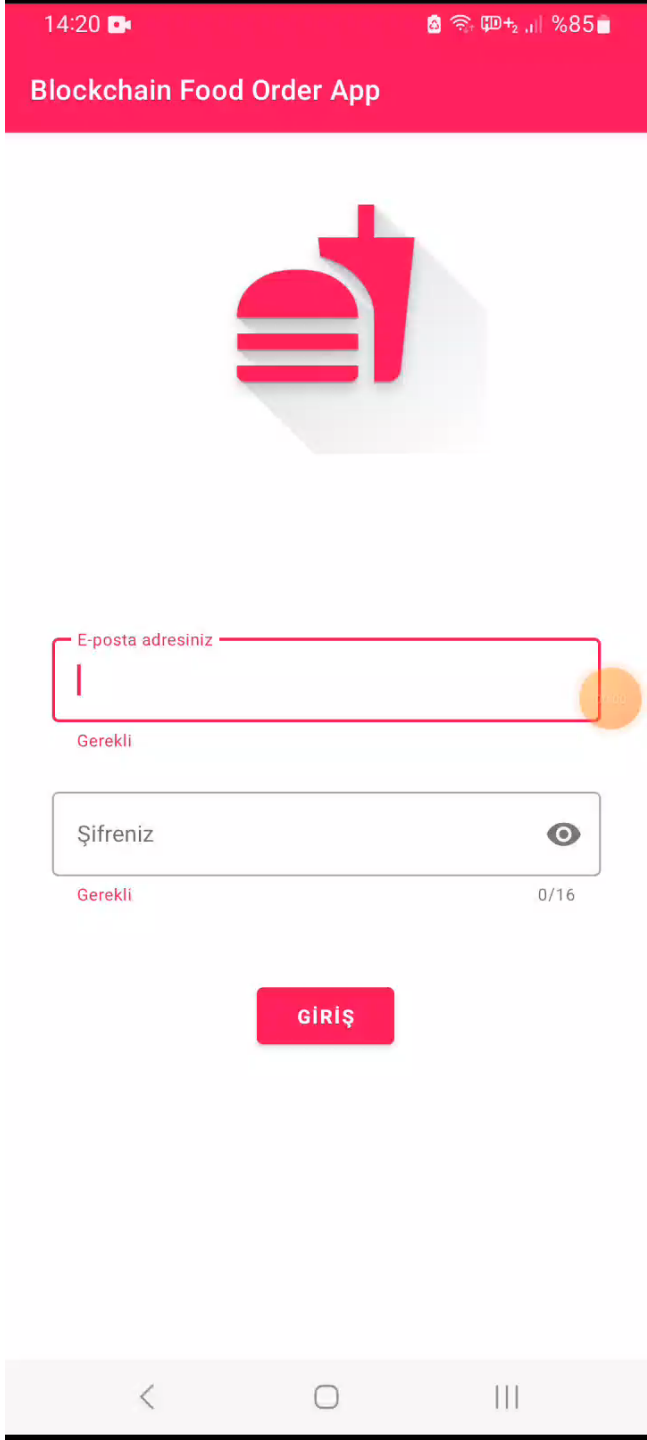
KULLANICI ARAYÜZÜ



GITHUB LİNKİ:

https://github.com/nidabaser98/BlockchainFoodOrderApp

Bu tez çalışması kapsamında geliştirilen mobil uygulamanın içinde yer alan kripto para ile ödeme seçeneğinin kullanıcı tarafından seçilmesi durumunda, sistem kullanıcıyı otomatik olarak Metamask kripto para cüzdanı uygulamasına yönlendirmektedir. Kripto para cüzdanına giriş yaptıktan sonra kullanıcıdan, mobil uygulama ile kripto cüzdan arasında bağlantı kurulması için izin istenmektedir. Kullanıcı bağlantı iznini verdikten sonra toplam ödemeyi onaylayıp onaylamadığı sorulmaktadır. Kullanıcı ödemeyi onaylarsa ve hesabındaki Ethereum miktarı da yeterliyse, transfer işlemi gerçekleşmektedir ve Ethereum blok zincirine yeni bir blok olarak eklenmektedir. Merkezsiz, şeffaf ve kripto güvenlik sağlayan bu ödeme yöntemiyle yapılan işlemler, Ethereum blok zinciri üzerinde saklanır ve değiştirilemezdir.



SONUÇ VE ÖNERİLER

Yaşanan her küresel finans krizinin ardından, bankalara duyulan güven daha da azalmaktadır. Bankalar ve aracı kurumlar üzerinden yapılan para transferlerinde uygulanan yüksek komisyonlar da ek maliyetlere neden olmaktadır. Üstelik bu sistem çeşitli güvenlik açıklarını da barındırmaktadır. Neticede kişiler arası para transferlerine üçüncü bir taraf olarak dahil olan bankacılık sistemi yerine, merkezi olmayan dağıtık bir sistem kurulması düşüncesiyle 2008 yılında Bitcoin ortaya çıkmış ve yepyeni bir ödeme sistemi doğmuştur. Bitcoin'in ortaya çıkışının ardından blok zinciri ve kripto para kavramları giderek yaygınlaşmıştır ve zamanla bir çok farklı kripto para birimi ortaya çıkmıştır. Bunlardan biri olan Ethereum, bu çalışma kapsamında, kripto para ile ödeme yapabilme imkanı sağlayan bir mobil yemek sipariş uygulaması geliştirilmesinde kullanılmıştır.

SONUÇ VE ÖNERİLER

Blok zinciri teknolojisi yeni bir konu olduğu için alanyazındaki akademik ve bilimsel kaynaklar henüz sınırlı sayıdadır. Bu alanda çalışan yazılımcıların tecrübe elde etmesi için de yeterli kaynak bulunmamaktadır. Dolayısıyla aslında küresel ölçekte çok büyük bir sorun teşkil eden insan kaynağındaki yetersizlik sebebiyle blok zincir teknolojisinin sadece finans değil, her alanda çalışılması gerektiği sonucuna ulaşılmıştır.

Ülkemizde blok zinciri teknolojisinin yaygınlaşması adına atılan en önemli adımlardan biri, Cumhurbaşkanlığı tarafından onaylanan 11. Kalkınma Planı 249-5 maddesinde “Blok zincir tabanlı dijital merkez bankası parası uygulamaya konulacaktır.” ifadesine yer verilmiş olmasıdır. Bu madde, blok zinciri alanına gerekli önemin verileceğine dair bir işaret olarak vurgulanmıştır.

DİNLEDİĞİNİZ İÇİN TEŞEKKÜR EDERİM