BKM BANKALARARASI KART MERKEZİ | Microsoft | VERİPARK

belgem.io

HERKES İÇİN BLOCKCHAIN

KASIM 2018

İÇİNDEKİLER

GİRİŞ

Dr. Soner Canko
BKM
Genel Müdürü

BKM olarak yapay zekâ, nesnelerin interneti, artırılmış gerçeklik ve blockchain gibi yeni teknolojileri yakından takip ediyoruz. Bu teknolojilerin herkes tarafından anlaşılması ve Türkiye gündeminin üst sıralarında kalması için projeleri hayata geçiriyoruz. Blockchain ile ilgili somut adımlar atmaya da devam ediyoruz. Hyperledger Fabric platformu üzerinde hayata geçirdiğimiz ve çalışma arkadaşlarımızın kullanımına sunduğumuz BBN isimli uygulamamızdan sonra, blockchain tabanlı ikinci ürünümüz olan belgem.io'yu da hayata geçirmenin sevincini yaşıyoruz. Ethereum tabanlı belgem.io ile eğitim sertifikalarınızı artık dijital ortamda güvenli biçimde saklayabileceksiniz.

Uzun yıllar yaptığımız araştırma ve öğrenme süreci ardından geliştirdiğimiz bu uygulamalarla, blockchain'in potansiyelini test ederken kazanımlarımızı da sizlerle paylaşmaya devam ediyoruz. Okumakta olduğunuz bu raporda; belgem.io projesinin amacı, kullandığımız mimari yapı ve diğer teknik detaylarla ilgili değerli bilgiler bulacaksınız.

Blockchain tabanlı çözümlerde başarının doğru ekosistemi oluşturmaktan geçtiğinin bilincinde bir kurum olarak 2018 yılında *Blockchain Türkiye* platformunun kurulmasına öncülük eden şirketler arasında yer almıştık. Bu bilincin bir diğer ürünü olan belgem.io ise VeriPark ve Microsoft ile kurduğumuz konsorsiyumun değerli çalışmalarının bir çıktısı... Blockchain, önümüzdeki dönemde gündemimizin üst sıralarında yer almaya devam edecek ve çalışmalarımızı sizlerle paylaşmayı sürdüreceğiz.

Aslı Derbent Özkan
VeriPark
Genel Müdürü

Dünya genelinde "alıcı" ve "satıcı" arasındaki "iş", "aracı kurumlar" ve "noterlik" servisleri aracılığıyla yürüyor. Bizim B2B dediğimiz iş yapma biçiminde de aslında hiçbir iş akışı firmadan firmaya gerçekleşmiyor, pek çok kurumun, otoritenin, firmanın aracılığı ya da kefaleti gerekiyor.

Blockchain teknolojisi, aracı veya doğrulama otoritelerine gereksinim duymadan, bu ihtiyacı teknoloji ile sağlayarak, iş yapış şekillerini tümden değiştirecek bir yaklaşım, bir fırsat sunuyor.

Bu belgem.io projesi özelinde de olduğu gibi, blockchain artık finans, enerji, sağlık, telekomünikasyon, eğitim ve lojistik gibi bir çok alanda insanların hayatlarını kolaylaştıracak ve bireylerin birbirlerine olan güven problemini ortadan kaldıracak.

Biz de VeriPark olarak blockchain'i geleceği değiştirecek teknolojilerden biri olarak görüyoruz ve bu konuda Ar-Ge ve kavram doğrulama çalışmaları gerçekleştirerek, alt yapımızı geleceğe hazır hale getiriyoruz.

Murat Kansu
Microsoft
Genel Müdürü

İnternet üzerinde yapılan işlemlerin güvenle ilerlemesini sağlayan Blockchain teknolojisi, son günlerde, bankaların da dâhil olduğu farklı oyuncular tarafından e-ticaret, dosya paylaşımı ve haberleşme gibi işlemler için keşfedilmeye ve sıklıkla kullanılmaya başlandı. Yakında, blockchain'in sunduğu fırsatlardan daha fazla faydalanmak üzere, birçok kurumun ortak blokchain altyapısı geliştirmek için iş birliği yapmasını bekliyoruz.

Öngörülerimize göre, gelecek yıl dünyanın en büyük 2 bin şirketinin %25'inden fazlası blockchain teknolojilerine yatırım yapmış olacak. 2019'da prostetik 3D yazıcıların %25'i, güvenli bir blok zincir kullanarak üretim yapacak; bu, güvenli veri paylaşımı sağlayacak ve hastaya özel çözümler geliştirecek. 2020 yılına kadar, dünya genelindeki üst düzey işlem bankalarının %25'i, imalatçıların ve perakendecilerin yaklaşık %30'u ve sağlık kuruluşlarının %20'si, hizmet sunarken blockchain ağları kullanacak. 2021 itibarıyla, açık ağlardaki kaynaklardan elde edilen verilerin %20'si, halka açık bir blockchain ağına kaydedilecek ve bu kayıtları doğrulamak için uygulamalar geliştirilecek. 2022'ye gelindiğinde ise, bir milyardan fazla insanın verisi, bir blok zinciri ağında yer alacak.

Dünyadaki herkesin ve her kurumun daha fazlasını başarması için çalışan Microsoft olarak, dijital dünyanın en önemli unsurlarından biri olan blockchain ile eğitimi bir araya getiren belgem.io projesini Türkiye için büyük bir kazanım olarak görüyoruz. Geliştirdiğimiz belgem.io, Microsoft Azure bulut platformumuz üzerinde çalışan Ethereum Proof-of-Authority Consortium ürünüyle geliştirilen dünyadaki ilk uygulamalardan biri. BKM ve VeriPark iş birliğiyle, işlemleri güvenli hale getiren ve hızlandıran bu teknoloji ile eğitim alanında önemli bir adım attık. Bu projeyle Türkiye'nin dijital dönüşümüne yenilikçi bir katkı daha sunmaktan büyük mutluluk duyuyoruz.

Yönetici Özeti

Blockchain, dijital dünyada kimliklendirme ve yetkilendirme gibi güvene dayalı işlemler için matematiğin bilimselliğine dayanan alternatif çözümler sunan ve bu konularda merkezi yöneticilere duyulan ihtiyacı ortadan kaldıran bir teknolojidir. *Blockchain* teknolojisi;

- Dijital ilişkileri güvence altına aldığı ve düzenlediği için, gelecekte internet işlemlerinin belkemiği olarak gösterilmektedir.
- Verinin gizliliğini kriptografi sağlar, veri transferlerini üçüncü kişilerin kontrolünü gerektirmeksizin güvence altına alır.

Bankalararası Kart Merkezi (BKM), Microsoft ve VeriPark ortaklığı tarafından hayata geçirilen belgem.io uygulaması ile eğitim sertifikaları, *blockchain* altyapısında güvenli ve değiştirilemez bir şekilde saklanmakta, eğitimi alan kişi tarafından dilediği kurum/kişi ile paylaşılabilmektedir.

Güvene dayalı iş modellerinin aracısız olarak kurulmasını sağlayan *blockchain* teknolojisi hakkında deneyim kazanmak kurumlar açısından önemli bir konu haline gelmiştir. Bu sebeple, teknolojinin daha detaylı anlaşılmasını sağlamanın ve ilgili araçların olgunluk seviyesini ölçmenin yanı sıra, teknoloji ile ilgili kazanılan deneyimlerin ekosistem ile paylaşılması da projenin başlıca amaçları arasında yer almaktadır.

Kullanım senaryomuzun oluşturulmasını kolaylaştıran *Ethereum blockchain* platformu, temel inovasyonu olan *Ethereum Virtual Machine (EVM)* sayesinde akıllı sözleşmelerin *blockchain* dünyasına girmesini sağlamıştır. Kod işleme esnekliği sağlayan *Ethereum* platformunda *Solidity* programlama dilini kullanarak *Truffle framework* ile akıllı sözleşmelerimizi test ettik ve geliştirdik. *Proof-of-Authority* konsensüs algoritmasının kullanıldığı *belgem.io* uygulaması, Microsoft Azure üzerinde *Ethereum Proof-of-Authority Consortium* ürünü kullanılarak dünyada geliştirilen ilk uygulamalardan biri olma özelliğini de taşıyor. Bu ürün sayesinde *blockchain* oluşturma ve düğüm ekleme işlemleri kısa sürede tamamlandı. Madencilik gerektirmeyen *Proof-of-Authority* konsensüs algoritması, yönetişim portalı ve blok üretim hızıyla ihtiyaçlarımızı tam olarak karşıladı.

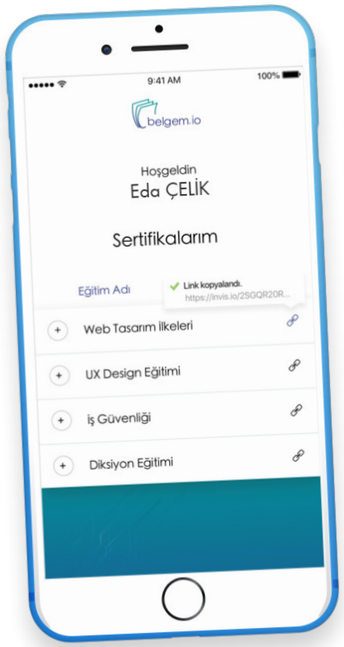
belgem.io uygulamamızda kimlik doğrulama süreçlerinde kurumlar *Ethereum* dünyasının cüzdanı olan *MetaMask,* kullanıcıların verileri de *BKM Express* uygulaması ile doğrulandı. Dijital belgelerin doğruluğu ise asimetrik kriptografiyle sağlandı. Hassas veri yönetiminde ise Azure'un Key Vault ürünü kullanılmış ve *blockchain* üzerinde hassas veri tutulmayan bir yapı inşa edilmiştir.

belgem.io'yu geliştirme aşamasında öğrendiklerimizin detayını bu raporda bulabilirsiniz. BKM dışındaki kurum ve bireylere açık olacak olan *belgem.io*'nun canlı ortamda gözlem imkânı sunacağı tecrübelerin potansiyeli bizi heyecanlandırıyor. Uygulamayı hayata geçirdikten sonra öğrendiklerimiz ile bu raporu güncelleyeceğiz.

1. belgem.io Uygulaması Teknik Altyapısı

1.1 belgem.io Nedir?

belgem.io, kurumlardan eğitim alan bireylerin eğitim sonucunda edindikleri sertifikalarının özel bir Ethereum blokzincirinde saklanması, görüntülenmesi ve paylaşılması için tasarlanmış bir dijital belge platformudur. Bankalararası Kart Merkezi (BKM), Microsoft ve VeriPark ortaklığı tarafından hayata geçirilen bu uygulamada, Ethereum, akıllı sözleşmeler, Proof-of-Authority konsensüs algoritması, kurumlar arası yönetişim uygulaması gibi kavramların test edilmesi amaçlanmıştır. Kurumların oluşturduğu yönetişim yapısı sayesinde belgem.io içerisinde alınmak istenen her karar oylamaya sunulmuş ve %51 çoğunluk şartı gözetilmiştir. Özel ve izin gerektiren bir blockchain ağına sahip olan belgem.io uygulaması, Microsoft Azure bulut platformunda yer alan Ethereum Proof-of-Authority Consortium ürünü üzerine konumlandırılmıştır.



1.2 Blockchain Platformu

belgem.io, Ethereum blockchain platformu üzerinde hayata geçirilmiştir. belgem.io, Temmuz 2018'de Microsoft Azure bulut platformu üzerinde yayına çıkan Ethereum Proof-of-Authority Consortium ürünü ile birlikte geliştirilen dünyadaki ilk uygulamalardan biri olma özelliğini taşımaktadır. Düğümler arası alınacak ortak kararlarda Proof-of-Authority konsensüs algoritmasından faydalanılmaktadır.

BKM ekibi, projeye başlarken platform seçimi için aşağıda yer alan alternatifleri değerlendirdi:

- Ethereum Proof-of-Authority Consortium (Azure)
- Ethereum Proof-of-Work Consortium (Azure)
- Parity Ethereum PoA (Azure)
- R3 Corda
- Hyperledger Sawtooth
- Özelleştirilmiş Bitcoin

Bu platformlar arasında seçim yaparken çeşitli beklentilerin karşılanması hedefleniyordu. Bu beklentiler, aşağıdaki gibi ortaya konuldu:

- Kapalı devre bir sistem ve sadece sistem eşlerinin ortak kararıyla büyüyebilen veya küçülebilen bir yönetişim yapısı,
- MetaMask ve benzeri cüzdan uygulamalarının tecrübe edilebileceği bir blockchain yapısı,
- Akıllı sözleşme geliştirme aşamasında yeni bir yazılım dilinin kullanılması,
- Olası sorunlar karşısında hızlı çözüm üretebilmek için teknik yeterliliği ve destek hizmetleri istenen seviyede olan bir platform.

belgem.io uygulamasında birçok dağıtık uygulama tarafından tercih edilen Ethereum blockchain platformu tercih edildi. Ethereum'un seçilmesindeki bir diğer etken ise birden çok konsensüs algoritmasını desteklemesiydi. Uygulamanın geliştirilmesi aşamasında Azure platformunda hem Proof-of-Work hem de Parity tabanlı Proof-of-Authority'i de denendi ve test edildi. Ethereum işlemlerinde ve akıllı sözleşme testlerinde büyük kolaylık sağlayan Truffle Framework de tecrübe edildi. Sonuç olarak madencilik gerektirmeyen yapısı, yönetişim portalı ve 2-4 saniye arasında blok üretim hızıyla Ethereum Proof-of-Authority Consortium ürününe karar verildi. Projenin başından beri Microsoft ile yapılan ortaklık sayesinde hem belgem.io, hem de Ethereum Proof-of-Authority Consortium birbirlerini besleyerek ortaya çıkarıldı denilebilir.

1.3 Üst Seviye Mimari ve Teknolojiler

Projenin uygulama seviyesinde çoğunlukla açık kaynak temelli teknolojiler kullanılmıştır:

- İşletim sistemi: Windows
- Uygulama sunucusu: Windows Server
- Veritabanı sunucusu: MS SQL
- Blockchain platformu: Ethereum
- Blockchain ürünü: Azure Ethereal Proof-of-Authority Consortium
- Web geliştirme platformu: ASP.NET MVC
- Programlama dilleri: C#, Go, Solidity, JavaScript

belgem.io uygulamasında sertifika verecek ilk 4 kurum Microsoft Cloud Society, FinTech İstanbul, BayBayNakit Akademi ve Blockchain Türkiye Platformu olacaktır. BKM bünyesinde bir hesaba web uygulamasının yöneticiliği ve blockchain ağında eş olma yetkisi verilmiştir. Böylece yönetişim uygulamasında oy hakkı bulunmaktadır. Yeni gelecek bir kurum sisteme önerildiğinde, içerideki kurumlar ve yöneticinin oyları doğrultusunda karar alınacaktır. Blockchain ağındaki her bir eşin yönetişim portalında alınan kararlar için eşit oy hakkı bulunmaktadır. Akıllı sözleşmelerle oluşturulmuş bu yapıda %51 çoğunluk sağlanması şartı gözetilmektedir.

Bir kurumun belgem.io üzerinde sertifika verebilmesi için aşağıdaki iki yapıdan birini tercih etmesi gerekmektedir.

I. Katılacak kurum blockchain düğümü olur

1. Oylama sonucunda özel ağa dahil olmaya hak kazanan her bir eşin, Azure üzerinden bir hesap açarak Ethereum Proof-of-Authority Consortium kurulumu yapması beklenir. MetaMask ya da benzer bir teknoloji/cüzdan ile oluşturulan public key ve belgem.io blockchain'ine ait bilgilerle kurulum tamamlanır.

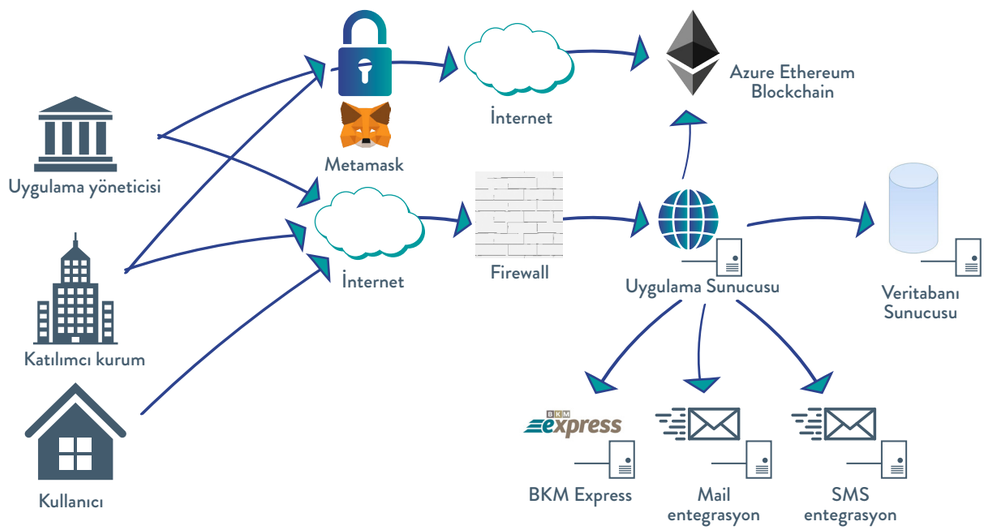
2. Blockchain ağına dahil olan kurumlara, BKM yöneticisi tarafından belgem.io web uygulamasına giriş bilgileri gönderilir. Böylece kurum, web uygulaması üzerinden blockchain'e işlem gönderme yetkisine sahip olur

II. Katılacak kuruma sadece işlem izni verilir

>> Sadece sertifika tanımlamak için uygulamaya katılan kurumlara sertifika tanımlaması için işlem izni sağlanır. Bu kurumlar blockchain düğümü olmadığından yönetişim platformuna dahil edilmez ve yeni katılımcılar için oy hakkı bulunmaz.

belgem.io özel bir blockchain ağı olmasına rağmen bulut istemcisi bilgisi ile içerisindeki sözleşmelere erişilebilir bir yapısı bulunmaktadır. Kötü niyetli kişiler tarafından akıllı sözleşmelere gönderilecek sahte işlemler, ağı şişirerek uygulamanın fonksiyonunu kaybetmesine veya yönetişim üzerinde olumsuzluklara sebep olabilirdi. Bu nedenle, tüm yönetişim portalı ve sertifika oluşturma sözleşmeleri kapsayıcı Transaction Permissioning (işlem izni) akıllı sözleşmesi geliştirilmiştir. Bu kapsamda, sadece belgem.io eşlerinin yetki verdiği adreslerin belgem.io sözleşmelerine ulaşabilmesi ve işlem gönderebilmesi hedeflenmiştir.

Şekil 1: **Üst Seviye Mimari Diyagramı**



1.4 Neden Azure Üzerinde Blockchain?

Microsoft Azure üzerindeki blockchain uygulamaları, giriş seviyesinde Azure ve blockchain altyapısı olan herkes için basit kurulum şablonları destekliyor. Azure portalının sağladığı ürünlerin basit kurulum ekranları sayesinde, blockchain ağ topolojisini dakikalar içinde oluşturuluyor. Bu sayede altyapıyı inşa etmek ve yapılandırmak için saatler harcamak yerine, uygulamamızı ve senaryolarımızı geliştirmeye vakit ayırdık. Proof-of-Authority Consortium ürünü sağladığı özel ve izin gerektiren blockchain ağı, dağıtık yönetişim uygulaması özellikleri ve kurumsal Blockchain projeleri için sağladığı yönetim portal ile belgem.io uygulamamız için oluşturmaya çalıştığımız platform ihtiyacını tam anlamıyla karşıladı. belgem.io uygulamasının platform özelliklerinin girişini Azure portalından yaptıktan sonra tüm ağın fonksiyonel duruma gelmesi (ayağa kalkması) sadece 16 dakika sürdü. Madenciliğin yapılmadığı Proof-of-Authority konsensüs algoritmasında ortalama her 4 saniyede bir yeni blok üretimi yapılıyor.

1.5 belgem.io'da Doğrulama Yapısı

belgem.io uygulamasının en önemli kullanım senaryolarından biri, eğitimi alan kişi adına düzenlenmiş sertifikalara kişinin istediği anda ulaşıp, dijital ortamda paylaşabilmesidir. belgem.io'da, "eğitim veren kurum" ve "kullanıcı" olmak üzere iki genel rol bulunmaktadır. Eğitim veren kurumların MetaMask hesaplarıyla hem dağıtık yönetişim uygulamasına katılarak oy kullanması hem de kullanıcı hesaplarına sertifika üreterek göndermesi kurgulanmıştır. Kullanıcılar ise herhangi bir MetaMask cüzdanıyla ilişkilendirilmemiştir. Böylece kullanıcıların, BKM Express uygulaması sayesinde doğrulanmış kimlik bilgileriyle oluşturdukları profillerine erişmeleri ve sertifikalarını görüntüleyip paylaşmaları sağlanmıştır. MetaMask kullanmayan kullanıcı rolü için BKM Express üzerinden yapılan bağış işlemi karşılığında doğrulanmış kimlik bilgileri belgem.io veritabanına aktarılmıştır. belgem.io çözümünde, kimlik bilgileri kişisel veri olarak değerlendirildiği için sadece kullanıcının onay vermesi halinde uygulamayla/kurumla/blockchain'e paylaşmasına uygun bir gerçekleştirme yapılmıştır. BKM Express uygulaması, kimlik doğrulama fonksiyonu için BKM'nin halihazırda sahip olduğu ve kullandığı bir çözümdür. Gelecekte kurgulanacak yeni kullanım senaryoları için e-Devlet Kimlik Doğrulama Kapısı, bankaların mobil uygulamaları ve opertatörlerin kimlik doğrulama çözümleri de bu fonksiyonun alternatifleri olarak kullanılabilirler.

Kullanıcı, belgem.io'ya ilk kez kaydolurken ilgili kurum bu bilgilerin doğrulama sürecini de gerçekleştirmektedir.

1.5.1 belgem.io'da BKM Express ile Kullanıcı Doğrulaması

Kayıt olurken ekranda oluşturulan QR kodu BKM Express uygulaması ile okutarak bağış işlemi yapar. Bu işlem karşılığında kullanıcının ad, soyad ve TCKN bilgileri doğrulanmış bir şekilde ekrana gelir. Kullanıcı, e-posta ve cep telefonu bilgilerini de doldurarak kayıt işlemini tamamlar.

1.5.2 belgem.io'da MetaMask ile Kurum Doğrulaması

Bir kurumun belgem.io'ya kayıt olması için bir başka kurum tarafından önerilmesi gerekir. belgem.io Kurum Ekranı üzerinden yeni kuruma ait public key ve yetkili bilgileri girilir. Sonrasında yeni kurum kaydı talebini alan kurum yetkilisi, yönetişim uygulaması üzerinden yeni kurum önerisini konsorsiyuma sunar. Yeni kurum katılmaya hak kazanırsa, belgem.io yöneticisi, yeni kurum yetkilisine kayıt işleminin tamamlanması için gerekli bildirimi yapar.

1.5.3 belgem.io'da Dijital Belge Doğrulama

belgem.io üzerinden üretilen her bir sertifikanın biricik linki bulunmaktadır. Bu link oluşturulurken, ilgili kurumun yaptığı MetaMask işlemindeki ViewToken kullanılır. Eğitim alan kişinin özgeçmişine eklediği ve belgem.io platformu üzerinden aldığı sertifikayı doğrulamak için belgem.io sertifikası üzerindeki doğrulama bağlantısı kullanılabilir.

Doğrulama bağlantısının tasarlanmasının arkasındaki senaryo şöyledir:

>> Kullanıcı adına, belgem.io üyesi kurumlardan sertifika üretilmiştir ve kullanıcı bu sertifikaları özgeçmişine eklemiştir.

>> Kullanıcı iş başvurusu yapar.

>> İş başvurusu yapılan kurumun insan kaynakları yetkilileri, CV'de bulunan dijital belgelerin doğruluk kanıtını görmek isteyebilir.

>> Sertifika linkinde bulunan şifrelenmiş ViewToken bilgisi, sertifika alınan kurumun Public Key'i ile çözülerek karşılaştırma yapılır.

>> Karşılaştırma sonucu "doğrulandı" veya "doğrulanmadı" şeklinde ilgili kullanıcılara gösterilir.

2. Alınan Dersler

2.1 Ethereum

2.1.1 Ethereum Blockchain

En basit haliyle Ethereum, geliştiricilerin merkezi olmayan uygulamaları oluşturmasını ve dağıtmasını sağlayan blockchain teknolojisine dayanan açık kaynaklı bir yazılım platformudur.

Bitcoin gibi, Ethereum da halka açık (public) bir blockchain'dir. İkisi arasında bazı önemli teknik farklılıklar olsa da, not edilmesi gereken en önemli özellik, Bitcoin ve Ethereum'un amaç ve kabiliyetlerinin önemli ölçüde farklı olduğudur. Bitcoin, online Bitcoin ödemelerine olanak sağlayan kişiler arası (P2P) elektronik para transfer sistemine özel bir blockchain uygulaması sunar. Bitcoin blockchain, dijital paranın sahipliğini izlemek için kullanılırken Ethereum blockchain, herhangi bir merkezi olmayan uygulamanın programlama kodunu çalıştırmaya odaklanan dağıtık bir sanal bilgisayar gibi düşünülebilir.

Ethereum blockchain'inde madenciler, bitcoin için madencilik yapmak yerine ağı

besleyen bir kripto token olan Ether'i kazanmaya çalışırlar. Ether, kullanışlı bir kripto para birimi olmasının ötesinde, Ethereum ağında uygulama geliştiricileri tarafından yapılan işlemlere ait ücretleri ve hizmetleri ödemek için de kullanılır. Ether dışındaki bir diğer token ise GAS'tir. Her bir işlemin gerçekleşmesi veya bir akıllı sözleşmenin çalışması GAS ile ölçülür ve ödenir. Buna karşın belgem.io'da PoA konsensüs algoritması kullanıldığı için bu ücretlere ihtiyaç duyulmaz. Böylece PoA, kullanıcı ve eğitim kurumlarını kriptopara yönetimi ile uğraşma maliyetinden kurtarmış oldu.

2.1.2 Akıllı Sözleşmeler

Akıllı sözleşme, para, içerik, mülk, hisse veya herhangi bir değerin değişimini kolaylaştıracak bilgisayar kodunu tanımlamak için kullanılan bir ifadedir. Blockchain üzerinde çalışan bir akıllı sözleşmeyi, belirli koşullar karşılandığında kendi kendine otomatik olarak çalışan bir bilgisayar programı şeklinde tanımlayabiliriz.

Tüm blockchain platformları kod işleme yeteneğine sahipken, çoğu ciddi bir biçimde sınırlandırılmıştır. Ethereum sahip olduğu kod işleme esnekliği sayesinde binlerce farklı uygulamanın geliştirilmesine gerekli ortamı sağlar.

Akıllı sözleşmeler aşağıdaki bileşenlerden oluşur:

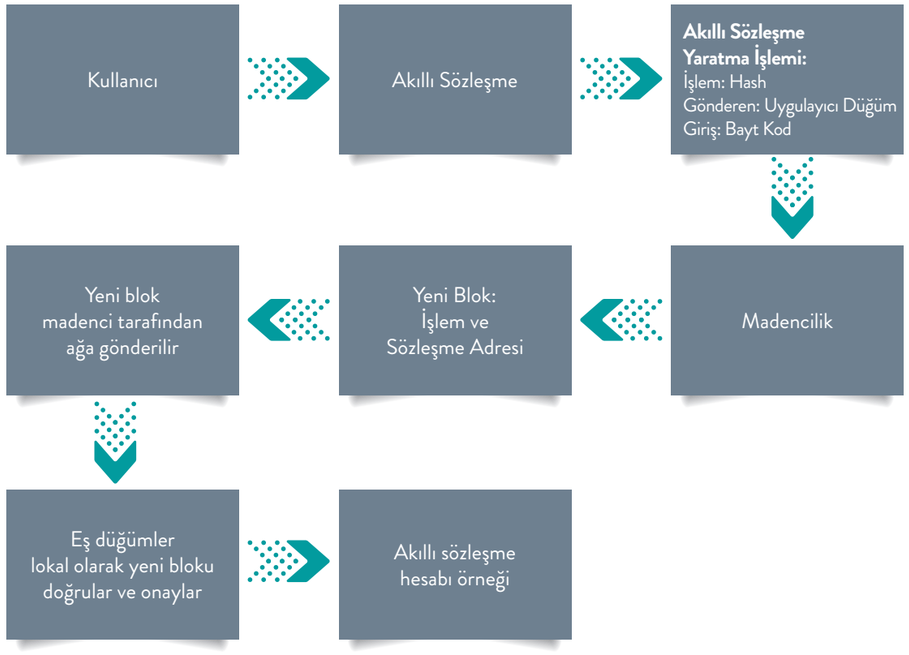
>> State variables (Durum değişkenleri)

>> Functions (Fonksiyonlar)

>> Events (Olaylar)

Akıllı Sözleşmeler Nasıl İşletilir?

Akıllı Sözleşmeler derlenip bayt kodlara dönüştürülür. Bu bayt kodlar, Ethereum Sanal Makinesi'ne (EVM) yüklenir. Aşağıda bir akıllı sözleşmenin üretilme aşamasında hangi süreçlerden geçtiği gösterilmektedir



>> Akıllı sözleşmenin dağıtılma süreci bir işlem ile tetiklenir.

>> İşlemin yürürlüğe girmesi gerekmektedir.

>> Madencilik, eş düğümler tarafından "rekabetçi bir şekilde" gerçekleştirilir.

>> Başarılı bir madencilik işlemi sonrasında oluşan yeni blok içerisinde işlem ve sözleşme adresi bulunur.

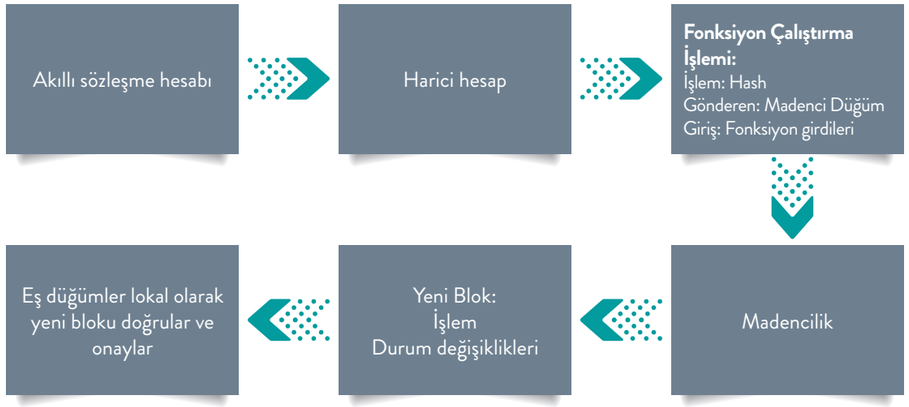
>> Madenci tarafından oluşturulan yeni blok, eş düğümlere yayınlanacaktır.

>> Yeni blok, yerel blockchain'de resmi bir blok haline gelmek üzere eş düğümler tarafından doğrulanacaktır.

>> Akıllı Sözleşmenin yeni örneği benzersiz bir adres içerir. Bu adres sonraki "sözleşme yürütme" için kaydedilmelidir.

Akıllı Sözleşmeler Nasıl Çalışır?

Akıllı sözleşmelerin içerisinde bulunan fonksiyonlar, bir harici hesap veya bir dağıtık uygulama tarafından çalıştırılabilirler.



>> Akıllı sözleşmede tanımlanan bir fonksiyonu yürütmek için akıllı sözleşmenin adresi alınır.

>> State (Durum) değişikliği yapan her fonksiyon bir işlem çağırır.

>> İşlemin onaylanması için madenciler tarafından işlenmesi gerekir.

>> Başarılı bir madencilik işlemi sonrasında oluşan yeni blok içerisinde bu işlem olacaktır.

>> Madenci tarafından oluşturulan yeni blok eş düğümlere yayınlanacaktır.

>> Yeni blok, yerel blockchain'de resmi bir blok haline gelmek üzere eş düğümler tarafından doğrulanacaktır.

2.1.3 Ethereum Sanal Makinesi (EVM)

Ethereum'un temel inovasyonu olan Ethereum Virtual Machine (EVM), Ethereum ağında çalışan bir Turing yazılımıdır. Belirli bir zaman, hafıza ve programlama diline bakılmaksızın herhangi bir programın çalıştırılmasını sağlar. Ethereum Virtual Machine, blockchain uygulamaları oluşturulma sürecini hiç olmadığı kadar kolay ve verimli hale getirir. Her yeni uygulama için tamamen orijinal bir blockchain inşa etmek yerine Ethereum binlerce farklı uygulamanın hepsinin tek bir platformda geliştirilmesini sağlar.

2.1.4 Ethereum Hangi Alanlarda Kullanılabilir?

Ethereum, geliştiricilerin merkezi olmayan uygulamaları oluşturmasına ve dağıtmasına olanak tanır. Merkezi olmayan bir uygulama (dApp), kullanıcıları için belirli bir amaca hizmet eder. Örneğin Bitcoin, kullanıcılarına çevrimiçi Bitcoin ödemelerini sağlayan eşler arası elektronik para transfer sistemi sağlayan bir dApp'tır. Merkezi olmayan uygulamalar, bir blockchain ağı üzerinde çalışan kodlardan oluştuğu için, herhangi bir birey veya merkezi varlık tarafından kontrol edilmezler.

Ethereum ayrıca Merkezi Olmayan Özerk Organizasyonlar (DAO - Decentralized Autonomous Organization) oluşturmak için de kullanılabilir. Bir DAO, tek bir lider olmadan tamamen özerk, merkezi olmayan bir kuruluştur. DAO'lar, Ethereum blockchain'de yazılmış akıllı sözleşmelerin bir koleksiyonunda programlama koduyla çalıştırılır. Bu kod, geleneksel bir organizasyonun kurallarını ve yapısını değiştirmek, insanlar ve merkezi kontrol ihtiyacını ortadan kaldırmak için tasarlanmıştır. Bir DAO, token satın alan herkes tarafından sahip olunur, ancak hisse senetleri ve sahipliklerine eşit olan her bir token yerine, token'lar kişilerin oy haklarını veren katkılar olarak hareket eder. belgem.io uygulamasında akıllı sözleşmelerle otonomlaştırılan yönetişim yapısı kurgulanmış, kurumlar arası bu yapının tasarımında DAO'dan esinlenilmiştir.

2.1.5 Dağıtık Ethereum Uygulamalarının Dezavantajları Nelerdir?

Dağıtık uygulamalar birçok fayda sağlamasına rağmen kusursuz değillerdir. Akıllı sözleşmeler insanlar tarafından yazıldığından, sadece geliştiricisi kadar iyidir denebilir. Kod hataları veya gözetimi, istenmeyen olumsuz davranışlara yol açabilir. Akıllı sözleşme kodundaki bir açık ya da hata, ağ konsensüsünün başkalarının eline geçmesine veya mevcut akıllı sözleşmenin üzerine yeni bir akıllı sözleşme yazılması gibi saldırılara imkân verebilir. Bu durum, değiştirilemez olması hedeflenen blockchain'in amacına ters düşen bir senaryodur. belgem.io uygulamasında bu dezavantajları bertaraf etmek için koruyucu akıllı sözleşmeler geliştirilmiş ve çok sayıda test yapılmıştır.

2.1.6 Özel ve İzin Gerektiren Ethereum Blockchain Yapısı

Blockchain ağları, veri yazma ve okuma haklarına göre farklı kategorilere ayrılmaktadır. Bu kategoriler genellikle "özel" (private) ve "açık" (public) olarak adlandırılsa da önce "izin gerektiren" (permissioned) ve "izin gerektirmeyen" (permissionless) olarak adlandırmak daha doğru olacaktır. Açık ve özel olarak sınıflandırmayı ise aşağıdaki gibi bu kategorilerin altında yapmak mümkündür.

Tablo 2: **Blockchain Yapıları**

İzin Gerektiren (Permissioned)		İzin Gerektirmeyen (Permissionless)	
Özel	Açık	Özel	Açık

İzin gerektiren blockchain'lerde sadece belirlenen eşler (peer) belirli haklarla blok oluşmasına ve mutabakata katkı sağlayabilmektedir. İzin gerektirmeyen blockchain'lerde ise tüm eşler mutabakata ve blok oluşturmaya katkı sağlamaktadır. Özel blockchain yapıları ise bilginin kimlerle paylaşılacağını belirler. Özel blockchain'lerde ağ, herkese açık değildir ancak ağa girenler blockchain verisine erişim iznine sahiptir. Açık blockchain yapılarında ise ağ tüm eşlerin erişimine açıktır.

belgem.io kullanım senaryosunda kurumlar arası yönetişim yapısının özel bir zincirde gerçeklenmesi ve işlemlerin ücretsiz olması hedeflenmiştir. Bu sebeple belgem.io izin gerektiren ve özel kategorisinde yer alan bir blockchain çözümüdür. Veri güvenliği ve gizliliği anlamındaki katma değeri ile bu yapı çoğu kurumsal blockchain çözümünde tercih edilmektedir.

Özel Zincirin Halka Açık Zincire Göre Avantajları Nelerdir?

Blockchain teknolojisinden faydalanmak isteyen kurum ve kuruluşlar için özel blockchain yapısının yüksek potansiyele sahip avantajlarını aşağıdaki gibi sıralayabiliriz.

- İşlemler daha ucuzdur veya ücretsizdir.
- Gecikme yaşama olasılığınız düşer.
- Zincir üzerinde daha fazla yetkiye ve kontrole sahip olursunuz.

2.1.7 Azure Ethereum Proof-of-Authority Consortium

Azure Ethereum Proof-of-Authority Consortium, çok üyeli bir konsorsiyumun asgari düzeyde Azure ve Ethereum bilgisine sahip yetkili otorite ağının yetkilendirilmesini, yapılandırılmasını ve yönetilmesini kolaylaştırmak için tasarlanan bir yönetişim platformudur. Azure portalı aracılığıyla kullanıcılar tek tık ile kurum ismini güncelleme, konsorsiyuma yeni bir kurum ekleme veya mevcut bir kurumun konsorsiyum dışına alınması gibi işlemleri gerçekleştirebilirler.

belgem.io özel bir blockchain ağı olmasına rağmen Ethereum ağında isteyen kullanıcılar belgem.io istemcisiyle (RPC) bilgisi ile ağa bağlanarak, içeride bulunan yönetişim uygulaması ve sertifika tanımlama kontratına işlemler gönderebilirdi. Bu tip fraud işlemleri önlemek için Transaction Permissioning yani işlem izinlerini kapsayan bir kontrat daha yazarak, sadece yetkili hesapların işlem yapabilmesi sağlandı. Özel ağın ilk katılımcısı "admin" kurum, kendinden sonra sisteme katılan hesaplara bu kontrat aracılığıyla yetki vererek, yönetişim uygulamasındaki katılımı artırmış oluyor.

2.1.8 Performans

belgem.io uygulamasının blok oluşturma istatistikleri Azure Monitor üzerinden görüntülenir.

Azure Monitor ile aşağıdaki işlemler yapılabilir:

- Altyapı ve ağ kesintilerinin tespiti
- Her bir düğüme ait ağ istatistiklerinin izlenmesi
- Özelleştirilmiş işlem takibi
- Performans çıktısı oluşturma

2.2 Kullanılan Yazılım Geliştirme Araçları

2.2.1 Truffle

Truffle, Ethereum üzerinde daha kolay uygulama geliştirmek için geliştiricilere sunulan bir framework'tür. Proje boyunca faydalandığımız ve Truffle'ın en çok öne çıkan özellikleri aşağıdaki gibi sıralanabilir.

- Akıllı sözleşmelerin derleme, eşleştirme ve testlerinin yönetimi
- Daha hızlı geliştirme yapmak için otomatik test
- Yapılar arası kolay geçiş ve taşıma
- Özel ve açık ağ yönetimi
- EthPM ve NPM ile paket yönetimi
- Akıllı sözleşme ile doğrudan etkileşime geçebilen konsol

2.2.2 Ganache

Ganache eski adıyla TestRPC, dağıtık uygulamalarınızı test edebileceğiniz, kişisel bir blockchain yapısı sunar. Mac, Windows ve Linux işletim sistemli bilgisayarlarda kullanabileceğiniz bu araç sayesinde uygulamanızı kendi bilgisayarınızda bulunan blockchain üzerinde kolayca test edebilirsiniz.

2.2.3 Parity

Madenciler, servis sağlayıcılar ve borsalar hızlı senkronizasyona ve maksimum çalışma süresine ihtiyaç duyar. Parity Ethereum, hızlı ve güvenilir hizmetler için gerekli temel altyapıyı sağlar. Rust dili ile geliştirilen Parity'nin amacı Ethereum'un en hızlı ve güvenli istemcisi olmaktır.

Parity'nin öne çıkan özellikleri:

- Kolayca kişiselleştirme için modüler kod tabanı
- Gelişmiş CLI tabanlı istemci
- Minimum bellek ve depolama alanı kullanımı
- Warp Sync ile saatler içerisinde senkronizasyon
- Servis veya ürünlerinizle entegrasyon için modüler yapı

2.2.4 Azure CLI 2.0

Microsoft'un Azure kaynaklarını yönetmek için çapraz platform komut satırı olan Azure CLI, kaynaklarınızı script'ler ile yönetmenizi kolaylaştırıyor. Forum ve dokümanlarından çoğu kez faydalandığımız Azure CLI sayesinde, özelliklerini belirlediğimiz blokchain'i yüklerken zaman kazandık. Bunu tarayıcınızda Azure Cloud Shell ile kullanabilir veya macOS, Linux veya Windows'a yükleyebilir ve komut satırından çalıştırabilirsiniz.

2.2.5 Solidity

Solidity, akıllı sözleşmeler yazmak için sözleşme mantığına dayalı bir programlama dilidir. Ethereum ve çeşitli blockchain platformlarında akıllı sözleşmelerin

geliştirilmesi için kullanılır. C ++, Python ve JavaScript dillerinden esinlenerek geliştirilmiştir ve Ethereum Sanal Makinesi (EVM) üzerinde çalışması için tasarlanmıştır. Ethereum'un geliştirilmesine katkıda bulunan çekirdek ekipteki Gavin Wood, Christian Reitwiessner, Alex Beregszaszi, Liana Husikyan, Yoichi Hirai tarafından yaratılmıştır.

2.2.6 Contract ABI (Application Binary Interface)

Akıllı sözleşmeler, sözleşme adresi olarak da bilinen belirli bir adres altında blok zincirine bayt koduna dönüştürülerek kaydedilir. Sözleşmenin bayt koduna erişmek için ABI'e ihtiyaç duyulur ve sözleşme içerisindeki işlevleri çağırmak istediğinizi tanımlar, aynı zamanda çağırdığınız fonksiyonun beklediğiniz formatta veriyi döndüreceğini garanti eder.

2.2.7 Web3.js

Web3.js bir HTTP veya IPC bağlantısı kullanarak yerel veya uzak bir Ethereum düğümü ile etkileşime girmenizi sağlayan bir kütüphane koleksiyonudur. Ethereum'un resmi Javascript API'si olan web3.js, akıllı sözleşmelerle etkileşimde bulunmanızı sağlar.

2.2.8 Nethereum

Nethereum, Ethereum için .Net entegrasyonu kütüphanesi olup hem açık, hem de Geth, Parity veya Quorum gibi özel Ethereum düğümlerinin, akıllı sözleşmelere erişim ve etkileşimini basitleştirmektedir.

2.2.9 Ethereum İstemci Listesi

belgem.io'da Ethereum protokolünün yedi istemcisinden biri olan Parity tercih edilmiştir. Azure Ethereum Proof-of-Authority Consortium ürününü Parity'nin Aura konsensüs motorunu kullanmaktadır.

Aşağıdaki tabloda diğer Ethereum istemcilerini bulabilirsiniz.

İstemci	Dil	Geliştirici
go-ethereum	Go	Ethereum Foundation
cpp-ethereum	C++	Ethereum Foundation
Pyethapp	Python	Ethereum Foundation
Ethereum(J)	Java	<ether.camp>
Ruby-ethereum	Ruby	Jan Xie
Parity	Rust	Ethcore
ethereumH	Haskell	BlockApps

2.3 Hassas Veri Yönetimi

2.3.1 Azure KeyVault

Günümüz şartlarında şifrelenmiş veriler blockchain üzerinde kaydediliyor ancak yükselen bir trend olan quantum computing ile bu şifrelerin kırılması büyük bir risk taşıyor. Ancak her şifreleme algoritmasının bir ömrü vardır. Bu kapsamda belgem.io uygulamasında yapılan işlemler Azure'un Cloud HSM ürünü olan KeyVault tarafından üretilen public key'lere gönderilmiş ve blokchcain'e kritik veri yazılmamıştır. belgem.io uygulamasına kaydolan her kullanıcı için FIPS 140-2 seviye 2 onaylı HSM'lere sahip KeyVault üzerinde public key oluşturulmuş ve sertifikalar bu public key'lere gönderilmiştir. belgem.io üzerindeki işlem seti ve verilerin dağılımını tabloda görebilirsiniz.

	Web Uygulaması	Sunucu Veritabanı	Blockchain
Kullanıcı Girişi	Kullanıcı e-mail ve şifresi	Doğrulama ve yetkilendirme işlemleri	-
Kullanıcı Kaydı	BKM Express ile kimlik doğrulama	Kullanıcı bilgileri (TC kimlik no, ad, soyadı, e-mail ve cep telefonu)	Kullanıcı adına oluşturulan public key
Kurum Kaydı	İşlemin Başlatılması	Kuruma ve kurum yetkilisine ait bilgiler	Kurum public key
Sertifika Talebi	Talep edilen sertifika bilgi girişi	Sertifikanın talep edildiği kurum, talebi yapan kişi ve sertifika bilgileri	-
Sertifika Kaydı	Sertifika bilgi girişi	Sertifikayı veren kurum, sertifika sahibi kişi, sertifika adı ve tarih bilgileri	Sertifikayı veren kurum, sertifika sahibi kişi, sertifika adı ve tarih bilgileri

3. Sonuç

3.1 Özet

Güncel platformlarda öne çıkan ana özellikleri gizlilik, performans (saniye başına işlem sayısı) ve dayanıklılık olarak üçe ayırabiliriz. Blockchain projelerinde dikkat edilmesi gereken kritik husus ise platformların birbirleri arasındaki üstünlüklere odaklanmaktan çok kullanım senaryonuza en uygun yapıyı seçmek diyebiliriz.

belgem.io uygulamasında:

- Sertifika tanımlama ve kurumlar arası yönetişim yapısı için akıllı sözleşmelerin yoğun olarak kullanıldığı açık kaynaklı Ethereum platformu tercih edildi.
- Konsensüs algoritması olan Proof-of-Authority tercih edildi. Düğümler arası demokratik bir yapı oluşturuldu.

>> Kullanım senaryosu yüksek performans talep etmemesine rağmen platformun sağladığı ortalama 4 saniyelik blok oluşturma hızı eklendi.

>> Azure KeyVault ile cloud HSM'leri tecrübe ederek kullanıcıların verileri koruma altına alındı.

3.2 Blockchain Terimler Sözlüğü

>> Adresler (Cryptocurrency address): Adresler, ağ üzerinde işlem almak ve göndermek için kullanılır. Bir adres bir alfasayısal karakter dizisidir ancak taranabilir bir QR kodu olarak da temsil edilebilir.

>> Asimetrik Kriptografi (Genel Anahtar Kriptografi): Asimetrik kriptografi, kamu anahtar şifrelemesi olarak da bilinir. Verileri şifrelemek ve şifresini çözmek için genel ve özel anahtarları kullanır. Anahtarlar, birlikte eşleştirilen ancak aynı olmayan (asimetrik) büyük sayılardır. Herkese açık bir anahtar herkesle paylaşılabilir. Parite içindeki özel anahtar gizli tutulur. SSH, S / MIME gibi protokoller, encyption ve dijital imza fonksiyonları için asimetrik kriptografiye güvenmektedir.

>> Blockchain: Blockchain, blok adı verilen paketlerde (tek bir kağıda harmanlamak yerine) değiştirilemez, dijital olarak kaydedilmiş verilerden oluşan dağıtılmış defter tipidir. Her blok bir kriptografik imza kullanarak sonraki bloğa "zincirlenir". Bu, blok zincirlerinin, uygun izinlere sahip herkes tarafından paylaşılabilen ve erişilebilen bir defter gibi kullanılmasına olanak tanır.

>> Onay: Onay, blockchain işleminin ağ tarafından doğrulandığı anlamına gelir. Bu, bir iş kanıtı sisteminde (örneğin, Bitcoin) madencilik olarak bilinen bir süreçten geçer. Bir işlem onaylandıktan sonra, tersine çevrilemez veya iki kez harcanamaz (değişmez).

>> Konsensüs Algoritması: Konsensüs algoritması, blockchain'de bir sonraki bloğun, gerçeğin tek ve yegane versiyonu olmasını sağlar ve güçlü rakipleri, sistemi raydan çıkarmaktan ve zinciri başarıyla atlatmaktan korur. Konsensüs algoritmalarının en popüler olanları Proof-of-Work, Proof-of-Stake ve Proof-of-Authority'dir.

>> Kriptografi: Kriptografi, verilerin şifrelenmesi ve çözülmesidir. Blockchain, Hashing ve Digital Signatures'te kullanılan iki ana kriptografik kavram vardır. Genelde yaygın olarak kullanılan üç şifreleme şekli vardır: simetrik kriptografi, asimetrik kriptografi ve karmalaşma.

>> dApp (Dağıtık Uygulama): Bir dApp, tamamen açık kaynak olması gereken, merkezi olmayan bir uygulamadır, otonom bir şekilde çalışmalıdır ve herhangi bir token'ın büyük çoğunluğunu kontrol eden bir kuruluş yoktur.

>> Dijital İmza: Dijital imza, bir mesajın belirli bir kişiden ve başka kimseden kaynaklanmadığını kanıtlamanın bir yoludur. Bir web sitesini ziyaret ettiğinizde, SSL kullanıyorsunuz. Bu, sizinle servis arasında güven oluşturmak için dijital bir imza kullanır.

>> Dağıtık Defterler: Dağıtık defterler birden çok siteye, ülkeye veya kuruma yayılmış bir veritabanı türüdür. Dağıtık defter verileri kimin görüntülenebileceğini denetlemek için "izinli" veya "izinsiz" olabilir.

>> Eliptik Eğri Dijital İmza Algoritması (ECDSA): ECDSA, fonların yalnızca hak sahipleri tarafından harcanabilmesini sağlamak için Bitcoin tarafından kullanılan bir şifreleme algoritmasıdır.

>> Şifreleme: Şifreleme, açık metinli bir mesajı (düz metin), bitlerin anlamsız ve rastgele bir sıralamasına benzeyen bir veri akışına (şifre-metni) dönüştürme işlemidir.

>> Ether: Ether, Ethereum blockchain'in, işlem ücretleri, madencilik ödemeleri ve ağdaki diğer hizmetler için ödeme yapmak için kullanılan yerel belirleyicisidir.

>> Ethereum: Ethereum, geliştiricilerin akıllı sözleşmeler yazmasını ve merkezi olmayan uygulamaları oluşturup dağıtmasını sağlayan blockchain teknolojisine dayanan açık bir yazılım platformudur.

>> Ethereum Test Ağı: Ana şebekedeki akıllı sözleşmenizdeki hata riskini azaltmak için, Ana Şebekeye dağıtılmadan önce test edilmesi önemlidir. Ethereum bir kabul ortamı olarak kurabileceğiniz birden fazla test ağına sahiptir. Ethereum Test ağları şunları içerir: Rinkeby, Ropsten ve Kovan.

>> EVM - Ethereum Sanal Makinesi: EVM, Ethereum akıllı sözleşmeler bayt kodu yürütme ortamıdır. Ağdaki her düğüm EVM'yi çalıştırır. Tüm düğümler, EVM kullanarak akıllı sözleşmelere işaret eden tüm işlemleri yürütür, böylece her düğüm aynı hesaplamaları yapar ve aynı değerleri depolar.

>> EVM Bayt Kodu: EVM Bayt kodu, Ethereum blockchain üzerindeki hesapların kod içerebildiği programlama dilidir. Bir hesapla ilişkilendirilen EVM kodu, bu hesaba bir mesaj gönderildiğinde her zaman yürütülür ve depolamayı okuma / yazma ve kendisi de mesaj gönderme özelliğine sahiptir.

>> GAS: Blockchain'in kullanımı paraya mal olur, para, işlemlerinizi doğrulayan ve blockchain'e ekleyen madencileri ödüllendirmek için kullanılır. Ethereum blockchain'indeki tüm işlemlerin, GAS adı verilen bir bedeli vardır. GAS, kod yürütme fiyatını belirlemek için kullanılan karmaşık bir birimdir. GAS karmaşıklığı, eterin mevcut değerine bağlı değildir.

>> Geth Konsolu (Go Ethereum): Geth, Go'da uygulanan tam bir Ethereum düğümünü çalıştırmak için kullanılan komut satırı arabirimidir. Geth'i kurarak ve çalıştırarak, Ethereum sınırında canlı ağda yer alabilir ve gerçek eter alabilir, adresler arasında para transfer edebilir, sözleşmeler oluşturabilir ve işlem gönderebilir, blok geçmişini keşfedebilir ve daha fazlasını yapabilirsiniz.

>> Hash Fonksiyonlar: Hash fonksiyonu dijital imzayı dönüştürür, daha sonra hem hash değeri hem de imza alıcıya gönderilir. Alıcı, hash değerini üretmek için aynı hash işlevini kullanır ve daha sonra mesajla alınanla karşılaştırır. Karma değerler aynıysa, iletinin hatasız iletilmesi olasıdır.

>> Değiştirilemezlik: Değiştirilemezlik, bir blok oluşturulduktan sonra değiştirilemez anlamına gelir. Blockchain'de bloklar birbirine zincirlenir, böylece bir sonraki bloğu değiştirmek zorunda kalmadan bir bloğun içeriğini geri gidemez ve değiştiremezsiniz. Konsensüs protokolüne bağlı olarak, herkes bunu kabul etmeden blokları değiştiremezsiniz. Bu bazen "konsensüsle değişebilir" olarak adlandırılır.

Keccak-256: Bir kriptografik karma işlevi türü. Ethereum Keccak-256 kullanır.

>> Defter: Bir defter, kayıtların değişmez olduğu ve finansal kayıtlardan daha genel bilgi tutabileceği, yalnızca bir kayıt deposudur.

>> Master Düğüm: Bir masternode, gerçek zamanlı olarak blok zincirinin tam kopyasını tutan bir kripto para birimi tam düğüm veya cüzdandır. Her zaman koşuyor. Ana düğümler normal düğümlerden farklıdır, çünkü bunlar işlemin gizliliğini arttırır, anlık işlemler sağlar, yönetişime ve oylamaya katılır ve kriptolarda bütçeleme ve hazine sistemlerini etkinleştirir.

>> MetaMask: MetaMask, tarayıcınızda dağıtılmış web sitesini ziyaret etmenizi sağlayan bir köprüdür. Ethereum dApp'lerini tam bir Ethereum düğümü çalıştırmadan tarayıcınızda çalıştırmanızı sağlar. MetaMask, farklı sitelerdeki kimliğinizi yönetmek ve blockchain işlemlerini imzalamak için kullanıcı arabirimi sağlayan güvenli bir kimlik kasası sağlar.

>> Madencilik: Madencilik, işlemlerin doğrulandığı ve bir blockchain'e eklendiği süreçtir. Bilgisayar donanımını kullanarak kriptografik problemleri çözme süreci de kripto paraların salınımını tetiklemektedir.

>> Düğüm: Bir düğüm, blockchain ağına bağlanan herhangi bir bilgisayardır.

>> Açık Kaynak: Açık kaynaklı yazılım, herkesin inceleyebileceği, değiştirebileceği ve geliştirebileceği kaynak kodlu bir yazılımdır.

>> Solidity: Solidity, akıllı sözleşmeler yazmak için sözleşmeye dayalı bir programlama dilidir. Çeşitli blockchain platformlarında akıllı sözleşmelerin uygulanması için kullanılır.

>> TestRPC: TestRPC, test ve geliştirme için bir Node.js tabanlı Ethereum istemcisidir. Tam istemci davranışını simüle etmek ve Ethereum uygulamalarını çok daha hızlı bir şekilde geliştirmek için ethereumjs kullanır. Ayrıca tüm popüler RPC fonksiyonları ve özellikleri (olaylar gibi) içerir ve gelişmeyi bir esinti yapmak için deterministik olarak çalıştırılabilir.

>> Token: Bir jeton, sahip olunabilecek bir şey için dijital bir kimliktir.

>> İşlem Bloğu: Bir işlem bloğu, Bitcoin ağındaki işlemlerin bir araya getirilmesi, daha sonra blok haline getirilebilecek ve blok zincirine eklenebilecek bir blok halinde toplanır.

>> Truffle: Truffle, Ethereum geliştiricisi olarak hayatı kolaylaştırmayı amaçlayan Ethereum için çerçeve ve varlık boru hattını test eden bir geliştirme ortamıdır.

>> Turing Complete: Turing makinesi, uygun bir algoritma ve gerekli zaman ve bellek verildiğinde, herhangi bir sorunu çözebiliyorsa, bir bilgisayar Turing turudur. Bir programlama diline uygulandığında, bu ifade, Turing tamamlanmış bir bilgisayarın yeteneklerini tam olarak kullanabileceği anlamına gelir.

>> Cüzdan: Bir cüzdan, özel anahtarların bir koleksiyonunu içeren bir dosyadır.

>> Web3.js: Web3.js, bir HTTP veya IPC bağlantısı kullanarak yerel veya uzak bir ethereum düğümüyle etkileşime girmenizi sağlayan bir kütüphane koleksiyonudur. Kaputun altında RPC çağrıları ile yerel bir düğüme iletişim kurar. web3.js bir RPC katmanını ortaya çıkaran herhangi bir Ethereum düğümü ile çalışır.

belgem.io UYGULAMASINI GELİŞTİREN EKİPLER

BANKALARARASI KART MERKEZİ

Celal Cündoğlu
Genel Müdür Yardımcısı

Özge Çelik
İş Geliştirme Direktörü

Okan Yıldız
İş Geliştirme Müdürü

Enes Türk
Mühendis

MICROSOFT

Cavit Yantaç
Yazılım Mühendisliği Genel Müdür Yardımcısı

Behice Funda
Microsoft EMEA Bölgesi Stratejik Programlar Direktörü

Emre Kenci
Yazılım Mimarı

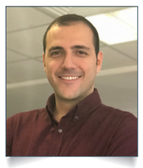
Seda Akdemir
Teknoloji Stratejisti

VERİPARK

Tahir Özmen
Proje Müdürü

Gencay Sazak
Kıdemli Yazılım Geliştirme Uzmanı

Volkan Kavadarlı
Yazılım Geliştirme Uzmanı



Görkem Gökçe
Kıdemli Müşteri Yöneticisi

BKM
BANKALARARASI
KART MERKEZİ

Microsoft

VERİPARK