FAZ II
GÜNCELLENMİŞ
VERSİYON

BKM
BANKALARARASI
KART MERKEZİ

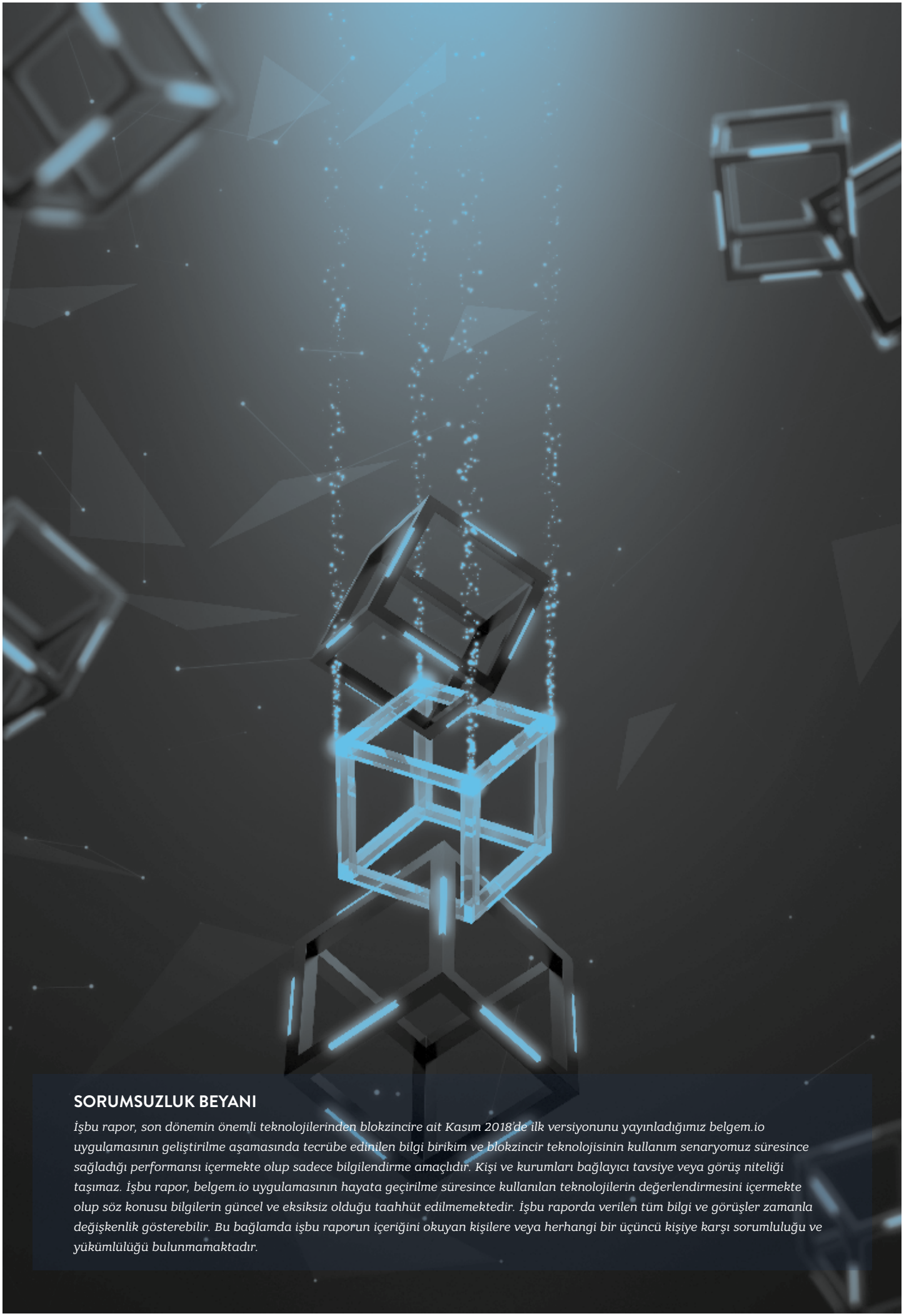
Microsoft

VERİPARK

belgem.io

HERKES İÇİN
BLOKZİNCİR

MART 2020



SORUMSUZLUK BEYANI

İşbu rapor, son dönemin önemli teknolojilerinden blokzincire ait Kasım 2018'de ilk versiyonunu yayınladığımız belgem.io uygulamasının geliştirilme aşamasında tecrübe edinilen bilgi birikim ve blokzincir teknolojisinin kullanım senaryomuz süresince sağladığı performansı içermekte olup sadece bilgilendirme amaçlıdır. Kişi ve kurumları bağlayıcı tavsiye veya görüş niteliği taşımaz. İşbu rapor, belgem.io uygulamasının hayata geçirilme süresince kullanılan teknolojilerin değerlendirmesini içermekte olup söz konusu bilgilerin güncel ve eksiksiz olduğu taahhüt edilmemektedir. İşbu raporda verilen tüm bilgi ve görüşler zamanla değişkenlik gösterebilir. Bu bağlamda işbu raporun içeriğini okuyan kişilere veya herhangi bir üçüncü kişiye karşı sorumluluğu ve yükümlülüğü bulunmamaktadır.

İÇİNDEKİLER

GİRİŞ

Dr. Soner Canko
BKM
Genel Müdürü

BKM olarak yapay zekâ, nesnelerin interneti, artırılmış gerçeklik ve blokzincir gibi yeni teknolojileri yakından takip ediyoruz. Bu teknolojilerin herkes tarafından anlaşılması ve Türkiye gündeminin üst sıralarında kalması için projeleri hayata geçiriyor ve öğrendiklerimizi sizlerle paylaşıyoruz. Blokzincir ile ilgili ideal kullanım alanlarını tespit edip somut adımlar atmaya da devam ediyoruz. Hyperledger Fabric platformu üzerinde hayata geçirdiğimiz ve çalışma arkadaşlarımızın kullanımına sunduğumuz BBN isimli uygulamamızdan sonra blokzincir tabanlı ikinci ürünümüz olan belgem.io'yu 2018 yılının sonunda hayata geçirmiştik. Belgelerinizi dijital ortamda güvenli biçimde saklayıp paylaşmanızı sağlayan belgem.io'nun ilk fazı Ethereum ile geliştirilmişti. belgem.io'nun ikinci fazında Quorum isimli blokzincir platformunu kullanırken özellikle kullanıcı doğrulama adımında yeni çözümleri denedik ve kullanıcı deneyimini iyileştirecek geliştirmeler yaptık.

Uzun zaman ayırdığımız araştırma ve öğrenme süreçlerinin ardından geliştirdiğimiz bu uygulamalarla blokzincirin potansiyelini test ediyoruz ve bilgi dağarcığımızı geliştiriyoruz. Okumakta olduğunuz bu raporda; belgem.io projesinin amacı, her iki fazda kullandığımız mimari yapı ve diğer teknik detaylarla ilgili değerli bilgiler bulacaksınız.

Blokzincir tabanlı çözümlerde başarının doğru ekosistemi oluşturmaktan geçtiğinin bilincinde bir kurum olarak 2018 yılında Blockchain Türkiye Platformu'nun (BCTR) 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 oldu. Blokzincir, önümüzdeki dönemde gündemimizin üst sıralarında yer almaya devam edeceğine inanıyor ve yeni teknolojilerle ilgili çalışmalarımızı sizlerle paylaşmayı sürdüreceğimizin sözünü veriyoruz.

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. Blokzincir 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, blokzincir 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 blokzinciri 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 Blokzincir 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, blokzincirin sunduğu fırsatlardan daha fazla faydalanmak üzere, birçok kurumun ortak blokzincir altyapısı geliştirmek için iş birliği yapmasını bekliyoruz. Öngörülerimize göre, gelecek yıl dünyanın en büyük 2 bin şirketinin %25’inden fazlası blokzincir 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 blokzincir ağları kullanacak. 2021 itibarıyla, açık ağlardaki kaynaklardan elde edilen verilerin %20 ’si, halka açık bir blokzincir 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 blokzincir ile eğitimi bir araya getiren belgem.io projesini Türkiye için büyük bir kazanım olarak görüyoruz. 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

Blokzincir, 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.

Blokzincir teknolojisi:

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

Bankalararası Kart Merkezi (BKM), Microsoft ve VeriPark ortaklığı tarafından hayata geçirilen belgem.io uygulaması ile sertifikalar, blokzincir altyapısında güvenli ve değiştirilemez bir şekilde saklanmakta, belge sahibi kişiler tarafından istenilen kurum veya kişilerle paylaşılabilmektedir. Güvene dayalı iş modellerinin aracısız olarak kurulmasını sağlayan blokzincir teknolojisi hakkında deneyim kazanmak, kurumlar açısından önemli bir konu haline gelmiştir. Bu sebeple teknolojinin daha iyi 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 senaryosunun ilk fazında tercih edilen Ethereum blokzincir platformu, temel inovasyonu olan *Ethereum Virtual Machine (EVM)* sayesinde akıllı sözleşmelerin blokzincir dünyasına girmesini sağlamıştır. Kod işleme esnekliği sağlayan Ethereum platformunda Solidity programlama dili kullanılarak *Truffle framework* ile akıllı sözleşmeler test edilmiş ve geliştirilmiştir. belgem.io, Microsoft Azure üzerinde *Ethereum Proof-of-Authority Consortium* ürünü kullanılarak dünyada geliştirilen ilk uygulamalardan biri olma özelliğine de sahip olmuştur. Bu ürün sayesinde blokzincir oluşturma ve düğüm ekleme işlemleri kısa sürede tamamlanmıştır. Madencilik gerektirmeyen *Proof-of-Authority* mutabakat algoritması, yönetişim portali ve blok üretim hızıyla ihtiyaçları tam olarak karşılamıştır. belgem.io'nun ikinci fazında ise yeni bir blokzincir platformu arayışına başlanmış ve JPMorgan'ın kurumsal Ethereum olarak adlandırılan Quorum blokzincir platformu tercih edilmiştir. Azure Blockchain Service üzerinde konumlandırılan Quroum ile birlikte Istanbul *Byzantine Fault Tolerance (IBFT)* mutabakat algoritması devreye alınmış ve akıllı sözleşmeler güncellenerek yeniden kodlanmıştır.

Dijital belgelerin doğruluğu ise asimetrik kriptografiyle sağlanmıştır. Hassas veri yönetiminde ise Azure'un Key Vault ürünü kullanılmış ve blokzincir üzerinde hassas veri tutulmayan bir yapı inşa edilmiştir.

belgem.io uygulamasında kimlik doğrulama süreçlerinde kurumlar, *Ethereum*

dünyasının cüzdanı olan *MetaMask* ile doğrulanmaktadır. Kullanıcıların bilgileri ise ilk fazda *BKM Express* ile doğrulanmaktayken, belgem.io'nun ikinci fazı kapsamında BKM Express'e ek olarak MERNİS, Plum ve Kimlik Erişim Cihazı ile kimlik doğrulama akışları da denenmiştir.

belgem.io'yu geliştirme aşamasında öğrenilenlerin detayını bu raporda bulabilirsiniz. *TÜBİTAK BİLGEM, TSPB (Türkiye Sermaye Piyasaları Birliği)* gibi kurumların da düzenledikleri eğitim ve organizasyonlara ait sertifikaları dağıttığı belgem.io için alınan geri bildirimler, bizleri yeni teknolojileri denemeye ve paylaşmaya teşvik ediyor. BKM olarak bunu kendimize bir görev olarak addettiğimizi paylaşarak, okumakta olduğunuz bu raporun tüm ekosisteme faydalı olmasını dileriz.

1. belgem.io Uygulaması Teknik Altyapısı

1.1 belgem.io Nedir?

belgem.io, kurumların düzenledikleri eğitim veya organizasyonlara katılan bireylere ait dijital sertifikaların Quorum blokzincirinde saklanması, görüntülenmesi ve paylaşılması için tasarlanmış bir dijital belge platformudur. Bankalararası Kart Merkezi (BKM), Microsoft ve VeriPark ortaklığı tarafından hayata geçirilen bu uygulamanın birinci fazında Ethereum, akıllı sözleşmeler, Proof-of-Authority mutabakat algoritması, kurumlar arası yönetişim uygulaması gibi kavramlar test edilmişti. Uygulamanın ikinci fazında ise platform değişikliğine gidilerek Quorum blokzincir platformu, İstanbul Byzantine Fault Tolerance (IBFT) mutabakat algoritması, güvenlik açısından geliştirilmiş ve güncellenmiş akıllı sözleşmeler, yeni kimlik doğrulama yöntemleri ve arayüz geliştirmeleri hayata geçirilmiştir. Kurumların oluşturduğu yönetişim yapısı sayesinde belgem.io içerisinde alınmak istenen her karar oylamaya sunulmuş ve %51 çoğunluk şartı gözetilmiştir. Özel ve izin gerektiren bir blokzincir ağına sahip olan belgem.io uygulaması, birinci fazında Microsoft Azure bulut platformunda yer alan Ethereum Proof-of-Authority Consortium ürünü, ikinci fazda ise Azure Blockchain Service içerisinde bulunan Quorum üzerine konumlandırılmıştır.

1.2 Blokzincir Platformu

belgem.io, ilk fazında Ethereum blokzincir 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 özelliğine sahip olmuştur. Düğümler arası alınacak ortak kararlarda Proof-of-Authority mutabakat algoritmasından faydalanılmıştır. Uygulamanın ikinci fazında ise Quorum blokzincir platformu tercih edilmiş ve IBFT mutabakat algoritması denenmiştir.

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

- Ethereum Proof-of-Authority Consortium (Azure) (Faz-1)
- Ethereum Proof-of-Work Consortium (Azure)
- Parity Ethereum PoA (Azure)
- R3 Corda
- Hyperledger Sawtooth

- Özelleştirilmiş Bitcoin
- Quorum Istanbul Byzantine Fault Tolerance (IBFT) (Faz-2)

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 blokzincir 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'nun birinci fazında birçok dağıtık uygulama tarafından tercih edilen Ethereum blokzincir 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 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 portali ve 2-4 saniye arasında blok üretim hızıyla Ethereum Proof-of-Authority Consortium ürününe karar verildi. Projenin başından bu yana Microsoft ile yapılan ortaklık sayesinde hem belgem.io, hem de Ethereum Proof-of-Authority Consortium birbirlerini besleyerek ortaya çıkarıldı denilebilir.

İkinci fazda yaptığımız Quorum tercihi ile Ethereum altyapısı için hazırladığımız akıllı sözleşmeleri güncellenen geliştirme araçlarıyla yeniden elden geçirdik ve devreye aldık. İkinci fazda tecrübe ettiğimiz denemeleri *Alınan Dersler: Faz 2* bölümünde detaylı inceleyebilirsiniz.

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
- Blokzincir platformu: Ethereum(Faz-1), Quorum(Faz-2)
- Blokzincir ürünü: Azure Ethereum Proof-of-Authority Consortium (Faz-1) İstanbul Byzantine Fault Tolerance (IBFT) (Faz-2)
- Web geliştirme platformu: ASP.NET MVC
- Programlama dilleri: C#, Go, Solidity, JavaScript

İlk aşamada belgem.io ile sertifika verecek kurumlar FinTech İstanbul, BayBayNakit Akademi ve Blockchain Türkiye Platformu olarak belirlenmiştir.

BKM bünyesinde bir hesaba web uygulamasının yöneticiliği ve blokzincir 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. Blokzincir ağındaki her bir eşin yönetişim portalinde alınan kararlar için eşit oy hakkı bulunmaktadır. Akıllı sözleşmelerle oluşturulmuş bu yapıda %51 çoğunluk sağlanması şartı gözetilmektedir.

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

I. Katılacak kurum blokzincir düğümü olur

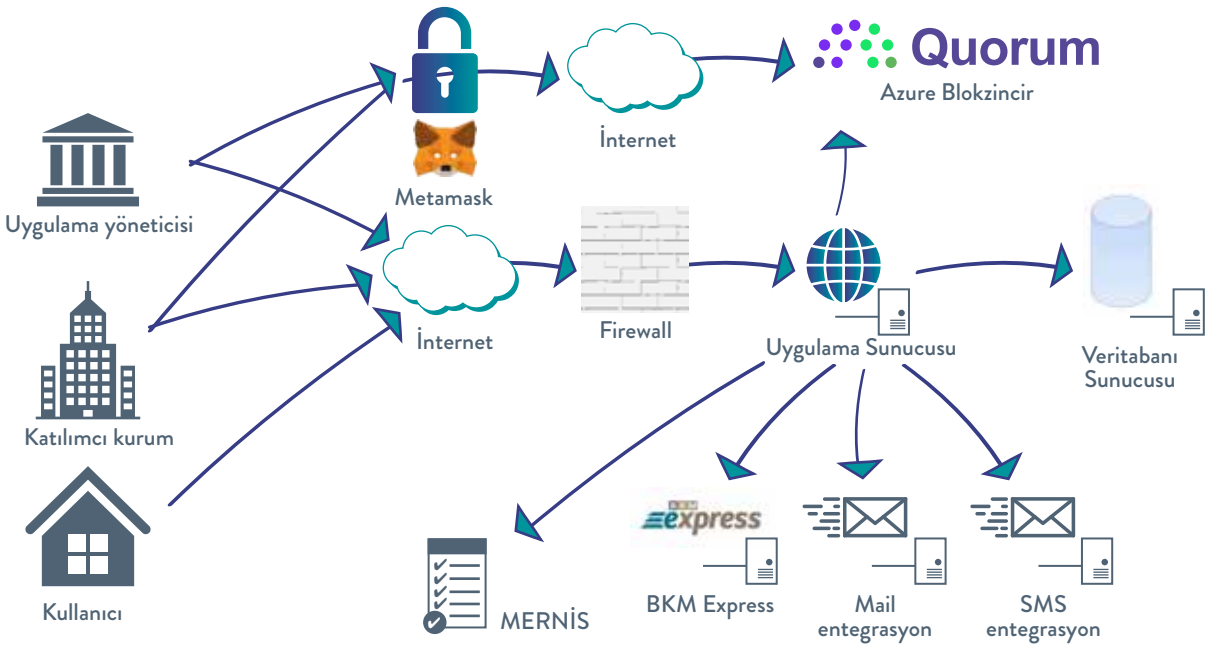
1. Eş olma yetkisine sahip olan kurumlar arasında yapılan oylama sonucunda özel ağa dahil olmaya hak kazanan her bir eşin, Azure üzerinden bir hesap açarak Ethereum Proof-of-Authority Consortium kurulumu yapması beklenir. MetaMask ya da benzer bir teknoloji/cüzdan ile oluşturulan public key ve belgem.io blokzincirine ait bilgilerle kurulum tamamlanır.

2. Blokzincir ağına dahil olan kurumlara, BKM yöneticisi tarafından belgem.io web uygulamasına giriş bilgileri gönderilir. Böylece kurum, web uygulaması üzerinden blokzincire 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 blokzincir düğümü olmadığından yönetişim platformuna dahil edilmez, dolayısıyla yapılacak oylamalara katılmaz.

Şekil 1: **Üst Seviye Mimari Diyagramı**



belgem.io özel bir blokzincir 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 portali 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 sağlanmıştır.

1.4 Neden Azure Üzerinde Blokzincir?

Microsoft Azure üzerindeki blokzincir uygulamaları, giriş seviyesinde Azure ve blokzincir altyapısı olan herkes için basit kurulum şablonlarını destekliyor. Azure portalinin sağladığı ürünlerin basit kurulum ekranları sayesinde, blokzincir ağ topolojisi 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 blokzincir ağı, dağıtık yönetişim uygulaması özellikleri ve kurumsal blokzincir projeleri için sağladığı yönetim portali ile belgem.io uygulamamız için oluşturmaya çalıştığımız platform ihtiyacını tam anlamıyla karşıladı. belgem.io uygulamasının platform özelliklerinin girişini Azure portalinden yaptıktan sonra tüm ağın işler duruma gelmesi sadece 16 dakika sürdü. Madenciliğin yapılmadığı Proof-of-Authority mutabakat algoritmasında ortalama dört 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. Ayrıca ikinci fazda kullanıcılara daha fazla kimlik doğrulama alternatifi sunmak için MERNİS, Plum ve Kimlik Erişim Cihazı (KEC) ile entegrasyon ve denemeler yapılmıştır. Yeni doğrulama yöntemleri ile ilgili detaylı bilgiyi 3.5. bölümde bulabilirsiniz. belgem.io çözümünde, kimlik bilgileri kişisel veri olarak değerlendirildiği için sadece kullanıcının onay vermesi halinde uygulamayla ve kurumla paylaşmasını mümkün

kılan bir akış kurgulanmıştır. Gelecekte kurgulanacak yeni kullanım senaryoları için e-Devlet Kimlik Doğrulama Kapısı, bankaların mobil uygulamaları ve operatörlerin 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 adı, soyadı 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 Merkezi Nüfus İdaresi Sistemi (MERNİS) ile Kullanıcı Doğrulaması

belgem.io'ya kayıt olmak isteyen kullanıcılar kayıt ekranında MERNİS sorgulaması için gereken TCKN, adı, soyadı, doğum yılı bilgilerini girer. T.C. vatandaşı olmayan kullanıcılar ise bu bilgilere ek olarak doğum tarihini gün, ay ve yıl olarak girerler. MERNİS servisine gönderilen sorgunun cevabına göre kullanıcının adı, soyadı ve TCKN bilgileri doğrulanmış bir şekilde ekrana gelir. Kullanıcı, e-posta ve cep telefonu bilgilerini de doldurarak kayıt işlemini tamamlar.

1.5.3 belgem.io'da MetaMask ile Kurun 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.

1.5.4 belgem.io'da Dijital Belge Doğrulaması

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: Faz 1

2.1 Ethereum

2.1.1 Ethereum Blokzinciri

En basit haliyle Ethereum, geliştiricilerin merkezi olmayan uygulamaları oluşturmasını ve dağıtmasını sağlayan blokzincir teknolojisine dayanan açık kaynaklı bir yazılım platformudur. Bitcoin gibi, Ethereum da halka açık (public) bir blokzincirdir. 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 blokzincir uygulaması sunar. Bitcoin blokzincir, dijital paranın sahipliğini izlemek için kullanılırken Ethereum blokzincir, herhangi bir merkezi olmayan uygulamanın programlama kodunu çalıştırmaya odaklanan dağıtık bir sanal bilgisayar gibi düşünülebilir. Ethereum blokzincirinde 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. Blokzincir üzerinde çalışan bir akıllı sözleşmeyi, belirli koşullar karşılandığında kendi kendine otomatik olarak çalışan bir bilgisayar programı şeklinde tanımlayabiliriz.

Tüm blokzincir 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 Makinesine (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.

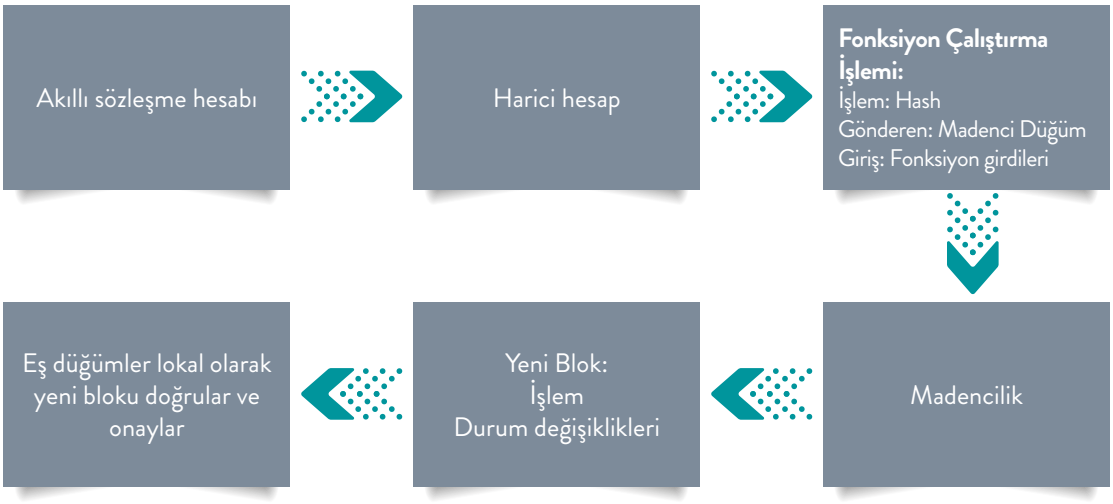
>> Madenci tarafından oluşturulan yeni blok, eş düğümlere yayınlanacaktır.

>> Yeni blok, yerel blokzincirde 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 blokzincirde 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, blokzincir uygulamaları oluşturulma sürecini hiç olmadığı kadar kolay ve verimli hale getirir. Her yeni uygulama için tamamen orijinal bir blokzincir 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 blokzincir 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 blokzincirinde 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 blokzincirin 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 Blokzincir Yapısı

Blokzincir 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 1: **Blokzincir Yapıları**

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

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

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

Özel Zincirin Halka Açık Zincire Göre Avantajları Nelerdir?

Blokzincir teknolojisinden faydalanmak isteyen kurum ve kuruluşlar için özel blokzincir 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 blokzincir 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 blokzincir yapısı sunar. Mac, Windows ve Linux işletim sistemli bilgisayarlarda kullanabileceğiniz bu araç sayesinde uygulamanızı kendi bilgisayarınızda bulunan blokzincir 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 blokzincir 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 blokzincir 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	Blokzincir
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. Alınan Dersler: Faz 2

3.1 Yenilikler

belgem.io'nun yayına alındığı günden bu yana hem blokzincir, hem kullanıcı hem de backoffice tarafları izlenerek iyi bir deneyim elde etmek için geri bildirimler toplanmıştır.

İlk olarak blokzincir performansında iyileştirme yapılmıştır. Azure üzerinde kullandığımız ve zaman zaman kesintiler yaşadığımız Ethereum Proof-of-Authority Consortium ürününden yine Azure Blockchain Service altındaki JPMorgan'ın Ethereum çatalı (fork) olan kurumsal blokzincir platformu Quorum'a geçiş yapılmıştır. Bu aşamada kurumlar tarafından daha önceki zincire kaydedilen sertifikalar, yeni zincire aktarılmıştır.

İkinci iyileştirme konusu ise sertifikaların özelleştirilebilmesi ve kolay yönetimi olarak değerlendirilmiştir. Bu kapsamda, sertifika tasarım ekranı; kurumlar için 5 adet sertifika taslağı ile birlikte uygulamaya eklenmiştir. Bu ekranda kurumlar; tasarladıkları sertifikaları ön izleyebilir, güncelleyebilir, katılım durumuna göre aktif/pasif olarak düzenleyebilirler.

Son olarak sertifika tanımlanırken kullandığımız MetaMask üzerinde iyileştirme yapılmıştır. Her bir sertifika tanımlama işleminde *Gas Price* (işlem ücreti) alanları sıfır olacak şekilde düzenlenerek işlemlerin daha kısa sürede tamamlanması sağlanmıştır.

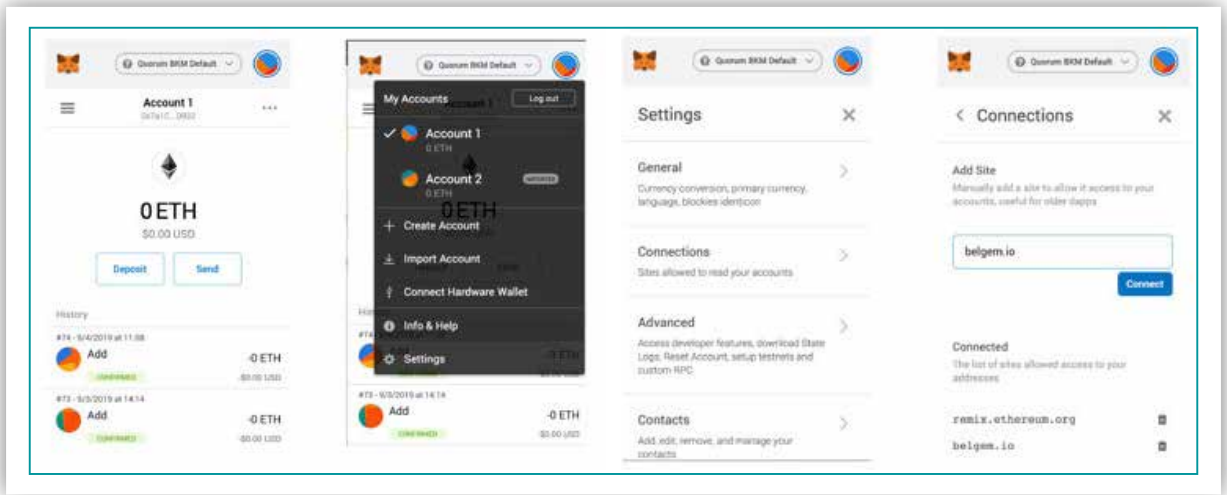
3.2 Kullandığımız Mutabakat Ürününde Yaşadığımız Sorunlar

belgem.io uygulamasının üzerinde inşa edildiği Azure Ethereum Proof-of-Authority Consortium ürünü, dört düğüm ve bir adet işlem iznine sahip kurumun oluşturduğu yapımıza dört ay boyunca kesintisiz ve sorunsuz bir şekilde hizmet verdi. Şubat 2019'un ortalarına geldiğimizde özel blokzincir ağımıza MetaMask cüzdanı üzerinden erişimlerde sorunlar yaşamaya başladık. Azure üzerinden sanal makinelerimizi incelediğimizde zaman zaman ağ kesintilerinin gerçekleştiğini bunun da, düğümler arasında senkronizasyon problemine yol açtığını fark ettik. Bu senkronizasyonu sağlayabilmek için zaman zaman sanal makinelere el yordamıyla müdahale ettik ancak sistemin ayağa kalkması için gerekli süre üç saniyeden otuz dakika mertebelerine ulaşmıştı. Microsoft Türkiye ve Microsoft ABD ofisi mühendisleriyle araştırmalarımıza devam ederken konsorsiyumun ilk düğümüne ait sanal makinenin ağ bağlantısını tamamen kaybettik. Bununla beraber diğer düğümlerin de bağlı olduğu yeni oy verme ekranına da erişemedik. Kurumlar sertifikalarını ayakta kalan diğer üç düğüm üzerinden vermeye devam etti. İncelemeye aldığımız ilk düğüm içerisinde sistem loglarını tutan dosyanın boyutunun bir hayli yüksek olduğu ve neredeyse sanal makinenin disk kapasitesini tamamen doldurduğunu saptadık. Bu sistem dosyası, Ethereum üzerinde Proof-of-Authority mutabakat algoritmasını gerçeklemeyi mümkün

kılan Parity'ye aitti ve problemin bulut uygulamasının kullandığı açık kaynak kodlu proje üzerinden aramaya başladık. İlgili Parity versiyonu içerisinde tıpkı bizim yaşadığımız senkronizasyon probleminin bulunduğunu ve sonraki versiyonlarda düzeltildiğini gördük. Ne yazık ki kullandığımız bulut uygulaması içerisinden Parity versiyonu yükseltilemediği için yeni platform arayışına başladık. Günün sonunda belgem.io bu problemler nedeniyle toplam yüz gün hizmet veremedi.

3.3 MetaMask - v7.1.0

Kurum yetkililerinin belgem.io kayıtlarının bulunduğu zincirle etkileşime geçmek için kullandıkları geleneksel Ethereum cüzdanı üzerinde geliştirmeler ve güncellemeler devam etmektedir. Özellikle güvenlik adına alınan *Privacy Mode* geliştirmesinden sonra v7.1.0 güncellemesiyle birlikte MetaMask, cüzdan uygulamasının etkileşime geçeceği web sitelerinin kaydedildiği *Connections* adlı bir menü tanıttı. Cüzdanınızın etkileşime geçmesine izin verdiğiniz dağıtık uygulama linklerini bu menü içerisindeki listeye ekleyerek, cüzdan bilgilerinizi kullanmak isteyen kötü niyetli etkileşimleri engellemiş oluyorsunuz.



3.4 Yeni Platforma Geçiş

belgem.io uygulamasında yaşadığımız sorunlar devam ederken Azure tarafında detaylarını yakından takip ettiğimiz yeni bir blokzincir altyapısı geliştiriliyordu. Microsoft, Azure kullanıcılarının özel blokzincir yapılarına olan ilgisini görmüş ve içerisinde Quorum ve R3 Corda platformlarının olduğu Azure Blockchain Services adlı ürününü hayata geçirme aşamasındaydı.

3.4.1 Blokzincir Platformu: Quorum

Kurumsal Ethereum olarak da bilinen Quroum, Ethereum protokolünün Go dili uygulaması olan Go Ethereum istemcisinin (geth) minimalist bir çatalıdır ve Ethereum topluluğunun bugüne kadar yaptığı geliştirmelerden yararlanır. ABD merkezli JPMorgan bankası tarafından kurumsal kullanım senaryoları

için geliştirilmiş bu platform sağladığı güvenli, ölçeklenebilir yapısı ile blokzincir ağlarını oluşturma, yönetim ve bakım işlemlerini kolaylaştırıyor. Quorum platformu ile hayata geçirilmiş uygulamalar arasında Takasbank'ın BiGA Dijital Altın hizmeti, Japonya'nın en büyük bankalarından biri olan MUFG'nin dijital ticaret finansmanı ürünü Komgo ve Starbucks'ın kahve üretim takip sistemi gibi uygulamalar bulunuyor.

Tablo 2: **Quorum'un go-ethereum'a Göre Avantajları**

>> Gizlilik: Quorum sahip olduğu özel veya halka açık durum ayrıştırması ve eşler arası şifrelenmiş mesaj değişimi özellikleri sayesinde özel işlemler ve sözleşmeleri kullanabilir. Böylece eşler arasında gizli mesajlaşmalar yapılabilir.	**>> Halka Açık Durum (Public State):** Tüm ağ tarafından erişime açık işlemlerdir. **>> Özel Durum (Private State):** Sadece izinli düğümlerin görüntüleyebileceği şifrelenmiş işlem ve sözleşmelerdir. Bu işlemler dağıtık uygulama üzerinden Quorum içerisindeki bir API ile tüm ağa gönderilir. Blok doğrulamasını yapan düğümler, eğer izinleri varsa bu şifrelenmiş blok içeriğinin şifresini çözer ve bunu EVM'e gönderir. Böylece EVM tarafında herhangi bir kriptografik işlem yapılmasına gerek kalmadan işlemler bir alt katmanda tamamlanır. Özel bir işlem aracılığıyla oluşturulmuş sözleşmelerden elde edilen veriler: izini olan eşlerin veri tabanlarına açık bir şekilde kaydedilirken, izni olmayan eşlerde şifrelenmiş olarak kaydedilir.
>> Alternatif Mutabakat Algoritmaları: Quorum, özel ağlar için tasarlanmış geleneksel Proof-of-Work (İş Kanıtı) ve Proof-of-Stake (Hisse Kanıtı) mutabakat algoritmaları dışında konsorsiyum tabanlı iş modelleri ile uyumlu seçenekleri de destekliyor. Bu algoritmaların ortak özellikleri ise çoklu oylama tabanlı olmalarıdır.	**>> Raft:** Performans odaklı bir mutabakat algoritması olan Raft, hızlı blok üretiminin yanı sıra isteğe göre blok üretme özelliğine de sahiptir. **>> Istanbul BFT:** Bizans Generalleri Probleminin özelleştirilmiş bir uygulaması olan ve belgem.io'da da kullanılan IBFT ile ilgili detaylı bilgiyi bir 2.3 bölümünde bulabilirsiniz.

3.4.2 Mutabakat Algoritması: Istanbul Byzantine Fault Tolerance (IBFT)

Son dönemlerde özel blokzincir yapılarında dikkatimizi çekmeye başlayan IBFT mutabakat algoritmasını özelleştirilmiş bir Proof-of-Authority olarak düşünebiliriz. IBFT, Miguel Castro tarafından 1999 yılında yayınlanmış Practical Byzantine Fault Tolerance makalesindeki yapı üzerinde yapılan birkaç değişiklik ile blokzincir teknolojisine uyarlanmış sürümüdür. Kullanım senaryomuzun ikinci fazı için en uygun mutabakat yapısı olan IBFT'nin öne çıkan özellikleri ise aşağıdaki gibidir.

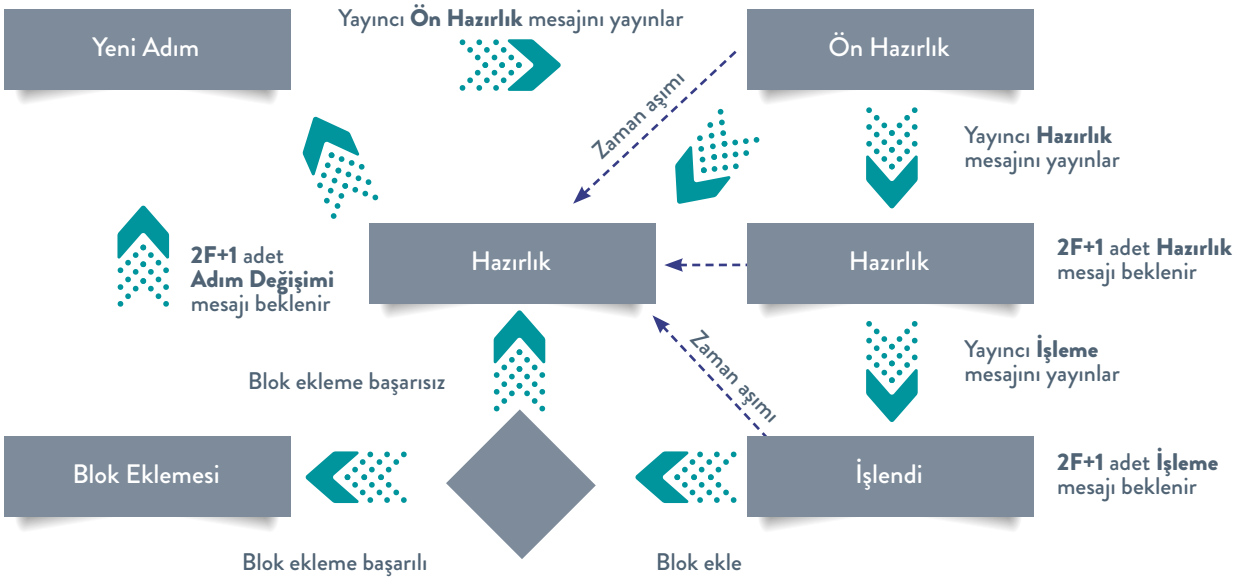
Blok Kesinliği	Bu özellik belirli uzunluğa ulaşmış bir zincire eklenecek olan yeni bloğun sadece bir adet olmasını güvence altına alır. Böylece daha çok açık blokzincir'lerde karşımıza çıkan çatallaşmaları engellenmiş olur.
Daha Sık Blok Üretimi	Daha seri blok üreten yapılarda blokların arasındaki zaman azalır ve ilgili düğümler tarafından bu blokların oluşturulması ve doğrulanması için daha az zaman ve efor harcanır.
Veri Bütünlüğü ve Hata Toleransı	IBFT mutabakat algoritmasında blokların bütünlüğünün sağlanması için doğrulayıcı düğümlerden faydalanılır. Bu düğümlerin en az üçte ikisi zincire eklenecek olan bloğu imzalayarak olası saldırı tehditlerini azaltır. Ayrıca bu düğümler arasındaki liderlik yetkisi belirli aralıklarda değişerek, kötü niyetli bir düğümün ağ üzerindeki etkisi bertaraf edilmeye çalışılır.
Esnek Operasyonel Yapı	Doğrulayıcı düğümlerin yetkileri zaman içinde değiştirilebilir. Böylece ağınızda sadece güvendiğiniz düğümlerin çalışmasını garanti ve kontrol altına almış olursunuz.

IBFT'nin işleyişini dört safha üzerinden incelemek gerekirse bunları aşağıdaki şekilde sıralayabiliriz:

1. Ön Hazırlık | **2.** Hazırlık | **3.** İşleme | **4.** İşlendi

N adet doğrulayıcı düğümün bulunduğu bir ağda, sistemin tolere edebileceği azami kusurlu düğüm sayısı *F* ile gösterilir. *N = 3F+1* olarak formüle edilen sistemde doğrulayıcı düğümler arasından seçilen bir düğüm, üretmek istediği aday bloğu *"Ön Hazırlık"* mesajıyla birlikte tüm ağa yayınlar. *"Ön Hazırlık"* mesajı alan diğer düğümler *"Hazırlık"* safhasına geçerler. Bu sayede ağ üzerindeki tüm doğrulayıcı düğümlerin senkronize bir şekilde aynı blok üzerinde çalışması sağlanır. *"Hazırlık"* mesajı gönderen düğümlerin sayısı *2F+1* olduğunda, blok yayınını yapan düğüm de *"Hazırlık"* aşamasına geçer ve ardından *"İşleme"* mesajını yayınlar. Bu mesaj, düğümlerin işlediği bloğun yayıncı düğüm tarafından onaylandığını ve zincire ekleneceği anlamına gelir. *"İşleme"* mesajı *2F+1* sayısına ulaştığında tüm düğümler kendi zincirlerine eklemelerini yaparlar ve *"İşlendi"* safhasına geçerler. IBFT çalışma prensibini Şekil 2'de görebilirsiniz.

Şekil 2: **IBFT Çalışma Prensibi**



Yukarıdaki akış ile çalışan IBFT protokolündeki bloklar kesindir, bu nedenle zincir üzerinde çatallaşma gerçekleşmemektedir. Hatalı bir düğümün *(F)* ana zincirden farklı bir zincir oluşturmasını önlemek için her bir doğrulayıcı 2F+1 koşulunun sağlanmasını bekler ve *"İşleme"* mesajına ait dijital imzalarını *extraData* adlı alana eklerler. Bu alan dinamik olarak değişebileceğinden blokların özütleri bu alandan bağımsız bir şekilde hesaplanır. Böylece sistemin tutarlılığı sağlanarak zincire eklenecek bloğun başlığına, mutabakatın sağlandığına dair dijital imza eklenir.

3.4.3 Geliştirme Araçlarındaki Yenilikler

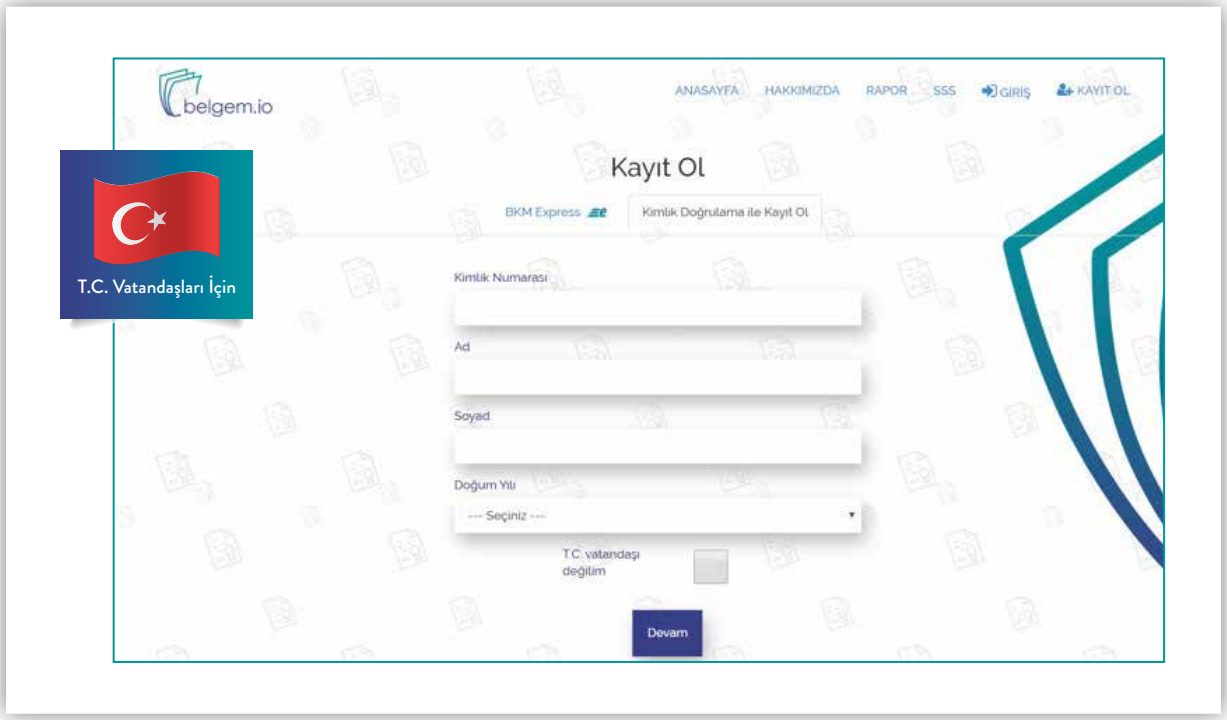
belgem.io içerisindeki akıllı sözleşmeler Solidity dilinde Truffle ile geliştirilmişti. Yeni platforma geçiş öncesinde akıllı sözleşmelerimizin Solidity versiyonlarını 0.4.17'den 0.5.0'a yükselterek EVM üzerinde daha hızlı ve verimli bir işleme özelliğini hayata geçirdik. Yazılım geliştirme editörü VS Code içerisinde Azure Blockchain Service eklentisini yükleyerek Azure hesap bilgilerimizle giriş yaptık ve oluşturduğumuz Quorum konsorsiyumuna kolayca eriştik. Truffle ile geliştirdiğimiz akıllı sözleşmeleri tek tuşla blokzincir'e ekledik.

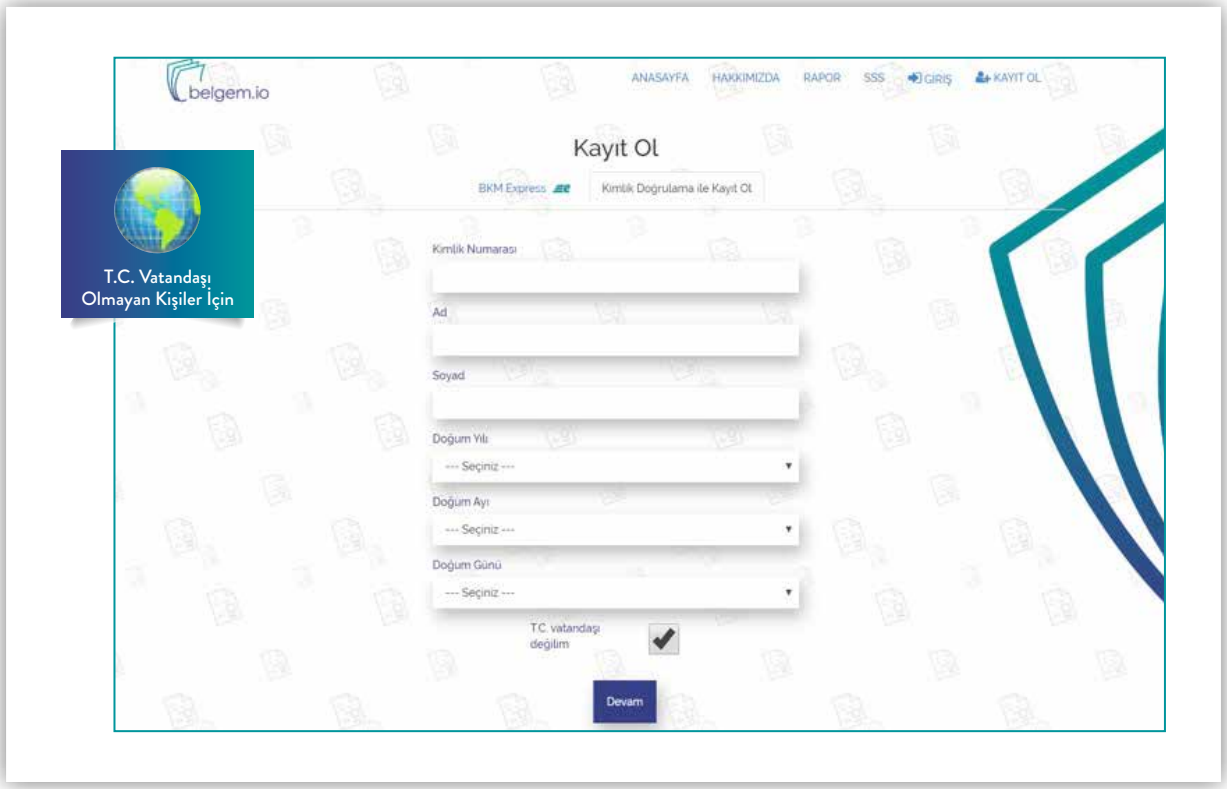
3.5 Yeni Kimlik Doğrulama Yöntemleri

belgem.io'nun kullanıcıların kimliklerini doğrularken kullandıkları yöntemleri çeşitlendirmek için alternatif çözümleri inceledik ve test ettik. 1.5 bölümünde belgem.io'da kullanılan ve denenen kullanıcı kimlik doğrulama yöntemlerinden bahsetmiştik. Tamamladığımız başarılı test süreçlerinin sonucunda MERNİS ile kimlik doğrulama yöntemini üretim ortamına taşıdık. Yakın zamanda Plum. çözümünü de üretim ortamına taşımayı hedefliyoruz.

3.5.1 Merkezi Nüfus İdaresi Sistemi (MERNİS)

Kullanıcılar, ilk fazda BKM Express ile KAÇUV'a yaptıkları 1 bağış karşılığında doğrulanmış adı, soyadı ve TCKN bilgilerini belgem.io'ya aktararak kayıt olma işlemlerini tamamlıyorlardı. belgem.io'nun daha fazla kullanıcı tarafından erişilebilir olması için T.C. İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü'nün hazırlamış olduğu, hem T.C. hem de yabancı uyruklu kullanıcıların kimliklerini doğrulayabileceği servislerin entegrasyonunu tamamladık.



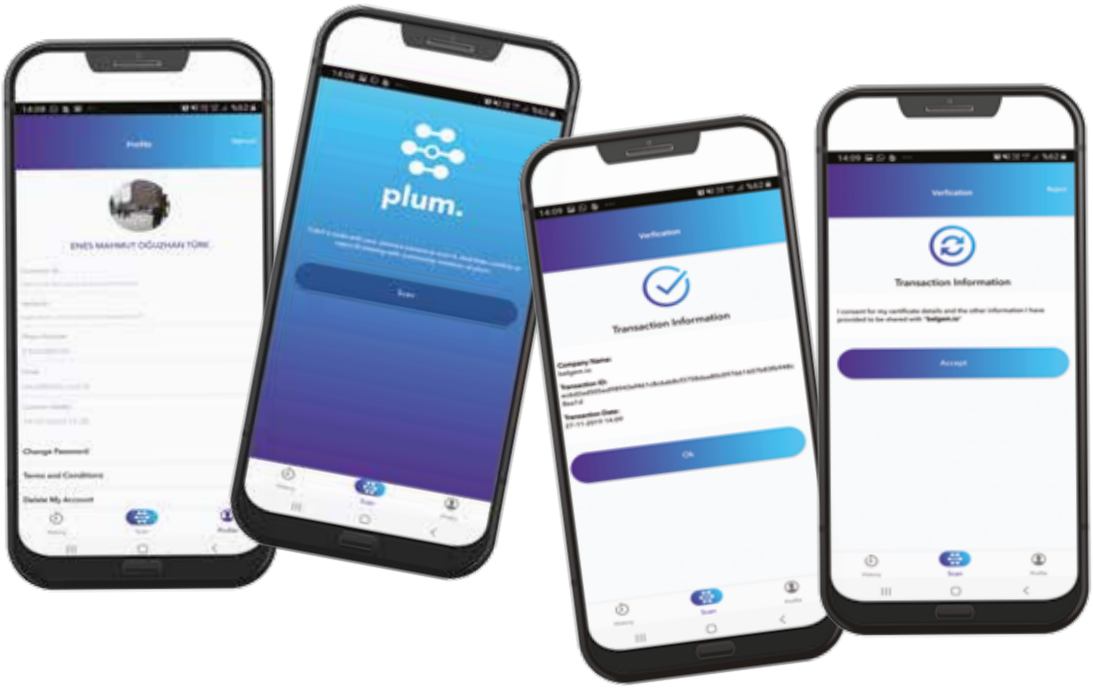


Bu entegrasyon ile T.C. vatandaşı kullanıcılar, kimlik numarası, ad, soyad ve doğum yılı bilgilerini, yabancı uyruklu vatandaşlar ise bu bilgilere ek olarak doğum ay ve gün bilgilerini girerek MERNİS servisleri üzerinden doğrulanarak belgem.io'ya kayıt oldular. Bu aşamada belgem.io kullanıcıların sadece doğrulanmış adı, soyadı ve TCKN bilgilerini tutmaya devam etti.

3.5.2 plum.

plum. uygulaması Plum Technologies B.V. tarafından geliştirilmiş blokzincir tabanlı bir dijital kimlik platformudur. Türkiye'de yayına alınan platform, yurt dışında eIDAS uyumluluğu çalışmalarını sürdürüyor. Platforma üye olabilmek için Türkiye'deki kullanıcıların Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) onayladığı Elektronik Sertifika Hizmet Sağlayıcıları'ndan (ESHS) temin edilen mobil imzaya sahip olmaları gerekmektedir.

Elektronik imza yetkisini alan kullanıcılar, plum. uygulamasına üye olarak imzaladıkları sözleşmede bu bilgilerin plum. blokzincirinde şifrelenmiş bir şekilde saklanmasını kabul ederler. plum. API'ı ile belgem.io'ya entegre ettiğimiz yapıda, kullanıcılar belgem.io'ya kayıt olurken plum. seçeneğini seçerek ekranda oluşturulan QR kodu plum. uygulaması ile okutarak doğrulanmış bilgilerinin belgem.io ile paylaşılması konusunda onay verir. Böylece doğrulanmış TCKN ve adı, soyadı bilgileri belgem.io'ya aktarılmış olur. Test ortamında geliştirmelerini tamamladığımız plum. entegrasyonunu ilerleyen dönemde üretim ortamında hayata geçirmeyi hedefliyoruz.



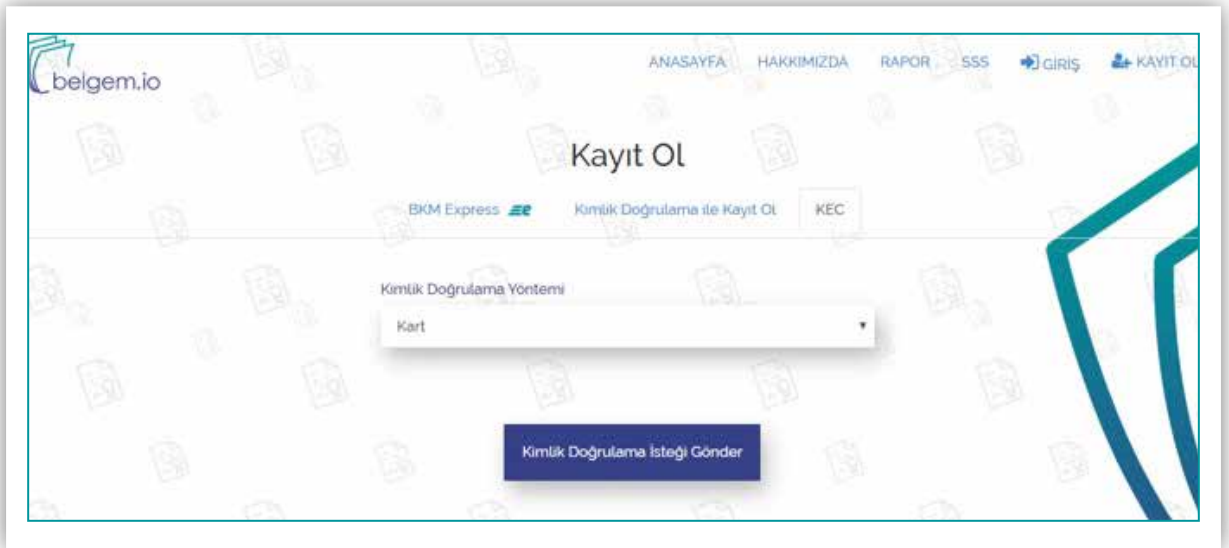
3.5.3. Kimlik Erişim Cihazı (KEC)

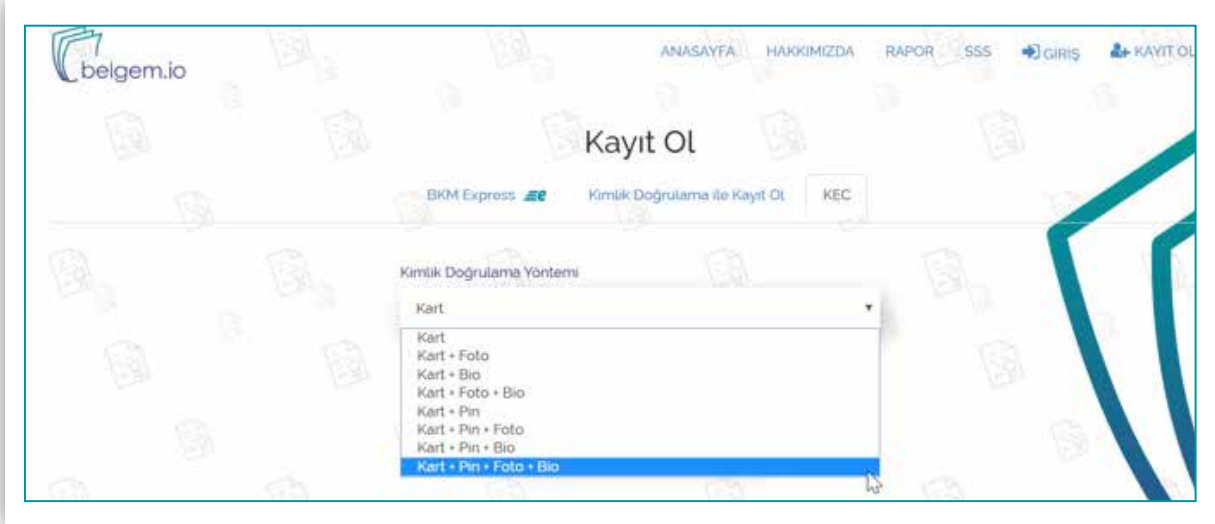
Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünce yürütülen çalışmalar doğrultusunda 2018 yılı itibariyle, 32 milyonu aşkın vatandaşımıza yeni çipli kimlik kartları dağıtılmıştır. Bugün ayda ortalama 1 milyonun üzerinde kart ile devam eden dağıtım süreci, elektronik kimlik doğrulama yöntemlerinin hayatımıza girmesiyle devam edecek. Yapılan kavram ispatı çalışmasında belgem.io için önemli bir süreç olan kullanıcı doğrulama adımı biOnay firmasının geliştirdiği Kimlik Erişim Cihazı (KEC) ile test ettik.

Elektronik Kimlik Doğrulama Nedir?

Kredi kartı PIN kullanımına benzerlik gösteren bu kimlik doğrulama yönteminde kimlik kartı, görevli kişi tarafından göz ile değil, bir terminal aracılığıyla elektronik ortamda doğrulanmaktadır. Ödeme kaydedici cihazlar (ÖKC) sayesinde kredi kartı sahteciliği önlendiği gibi Hazine ve Maliye Bakanlığı tarafından denetlenebilirlik ve vergi kaçakçılığını önlemek için dijital kayıtlar oluşturulmaktadır. Elektronik kimlik doğrulamada sahip olunan, bilinen ve kişiye ait biyometrik özellik olarak 3 farklı unsur kullanılmaktadır. Örneğin; kredi kartlarındaki “Chip&PIN” süreçlerinde, sahip olunan unsur bankanın müşterisine verdiği çipli kredi kartı ve bilinen unsur ise bu karta ait PIN kombinasyonudur. Üç farklı unsurdan

herhangi ikisinin kullanıldığı doğrulamaya 2-faktör kimlik doğrulama, üç unsurun tamamının kullanıldığı doğrulamalara ise 3-faktör kimlik doğrulama olarak adlandırılır. Yeni kimlik kartlarımız hem 2-faktör, hem de 3-faktör kimlik doğrulamayı (çip, PIN, parmak izi) desteklemektedir.





Kavram ispatı çalışması için senaryomuzu, belgem.io'ya kayıt olmak isteyen bir kullanıcının kimlik kartını KEC cihazına okutarak ilgili kimlik doğrulama adımlarını tamamladıktan sonra doğrulanmış TCKN, adı ve soyadı bilgilerinin belgem.io sunucularına aktarılması şeklinde kurguladık. Öncelikle testlerimizi gerçekleştirebilmek için test kimlik kartlarına sahip olmamız gerekiyordu. Bu sebeple TÜBİTAK BİLGEM UEKAE E-Kimlik Uygulamaları Bölümü'ne müracaat ederek test kimlik kartlarımızı bastırdık. Sonrasında her iki uygulamanın test ortamlarında gerekli entegrasyonları gerçekleştirerek, test kimlik kartıyla doğrulama kimlik doğrulaması yapan bir kullanıcının belgem.io'ya kayıt işlemini tamamladık.

3.6 Kurumlara Sertifika Verilmesi

Kurum bünyemizde bulunan Test ve Sertifikasyon ekibimiz, BKM üyelerinin sertifikasyon süreçlerini başarıyla tamamlanmasının ardından ilgili üyeye fiziksel sertifikalar üreterek iletiyordu. Bu senaryonun belgem.io'ya adapte edilebilmesi için PDF dosyalarının dijital olarak imzalanarak bir işlem belirteciyle (viewtoken) temsil edildiği hibrit bir yapı tasarladık.

1. BKM Test ve Sertifikasyon ekibi, ilgili testleri tamamlar ve sertifika almaya hak kazanmış BKM üyesi için sertifikasını PDF formatında hazırlar.

2. belgem.io üzerinde sadece Test ve Sertifikasyon ekibi için oluşturulmuş sayfa üzerinden PDF dokümanını yükler ve bu yüklemenin gerçekleştiğine dair bir işlem belirteci Quroum blokzincirinde oluşturulur.

3. İşlem belirteci ile oluşturulan biricik bağlantı linki, belgem.io'ya yüklenmiş fiziksel PDF dokümanının dizinine erişim sağlamaktadır.

4. Sertifikayı almaya hak kazanmış kurumlar, sertifikalarını ister link üzerinden görüntüleyebilir isterlerse de indirebilirler.

4. Sonuç

4.1 Özet

belgem.io'nun ilk fazının ardından hazırladığımız raporda blokzincir platformlarında öne çıkan gizlilik, performans ve dayanıklılıktan oluşan üç ana özelliğe dikkat çekmiş ve blokzincir projelerinde dikkat edilmesi gereken kritik hususun, platformların birbirleri arasındaki üstünlüklere odaklanmaktan çok kullanım senaryosuna en uygun yapının seçilmesi olduğunu belirtmiştik.

İkinci fazda yaptığımız denemeler sonucunda ise blokzincir platformlarının bağımlı olduğu yazılımlar ve bunların sürdürülebilirliği oldukça önemli bir husus olarak karşımıza çıktı. İhtiyaçlar doğrultusunda yaptığımız arayüz iyileştirmeleri sonucunda ise kurumlar ve kullanıcılar tarafından blokzincir uygulamamızın daha fazla benimsendiğini ve kullanıldığını gözlemledik.

belgem.io uygulamasının birinci fazında:

- Sertifika tanımlama ve kurumlar arası yönetişim yapısı için akıllı sözleşmelerin yoğun olarak kullanıldığı açık kaynaklı Ethereum platform tercih edildi.
- Mutabakat algoritması olan Proof-of-Authority tercih edildi. Düğümler arası demokratik bir yapı oluşturuldu.
- Kullanım senaryosu yüksek performans talep etmemesine rağmen platformun sağladığı ortalama dört saniyelik blok oluşturma hızı eklendi.
- Azure KeyVault ile bulut HSM'leri tecrübe ederek kullanıcıların verileri koruma altına alındı.

belgem.io uygulamasının ikinci fazında:

- Birinci fazda kullanılan Ethereum platformundan, kurumsal blokzincir amaçları için özelleştirilmiş bir Ethereum çatalı olan Quorum platformuna geçiş yapıldı.
- Quorum platformunun sunduğu Istanbul Byzantine Fault Tolerance (IBFT) mutabakat algoritması tercih edildi.
- Kurum ve kullanıcılar için arayüz iyileştirmeleri yapılarak uygulamanın daha çok benimsenmesi hedeflendi.
- MERNİS, Plum ve KEC gibi yeni kimlik doğrulama yöntemleri denendi. Ayrıca kurumlara yönelik belgeler için PDF dokümanlarının imzalanarak saklanacağı hibrit bir yapı kurgulandı.

4.2 Blokzincir 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, encryption ve dijital imza fonksiyonları için asimetrik kriptografiye güvenmektedir.

›› Blokzincir: Blokzincir, blok adı verilen paketlerde (tek bir kâğıda 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, blokzincir 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).

›› Mutabakat Algoritması: Konsensüs algoritması, blokzincirde 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. Blokzincir, Hashing ve Digital Signatures'te kullanılan iki ana kriptografik kavram vardır. Genelde yaygın olarak kullanılan üç şifreleme sekli 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 blokzincirin, 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 blokzincir 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 blokzincir 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: Blokzincirin kullanımı paraya mal olur, para, işlemlerinizi doğrulayan ve blokzincire ekleyen madencileri ödüllendirmek için kullanılır. Ethereum blokzincirindeki tüm işlemlerin, *Gas* adı verilen bir bedeli vardır. *Gas*, kod yürütme fiyatını belirlemek için kullanılan karmaşık bir birimdir.

›› 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. Blokzincirde 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 blokzincir işlemlerini imzalamak için kullanıcı arabirimi sağlayan güvenli bir kimlik kasası sağlar.

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

>> Düğüm: Bir düğüm, blokzincir 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 blokzincir 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

Dr. Soner Canko
Genel Müdür

Celal Cündoğlu
Genel Müdür Yardımcısı

Özge Çelik
İş Geliştirme Direktörü

Okan Yıldız
İş Geliştirme Müdürü

Enes Türk
İş Geliştirme Mühendisi

VERİPARK

Tahir Özmen
Proje Müdürü

Gencay Sazak
Kıdemli Yazılım Geliştirme Uzmanı

Volkan Kavadarlı
Yazılım Geliştirme Uzmanı

BKM BANKALARARASI KART MERKEZİ

Microsoft

VERİPARK