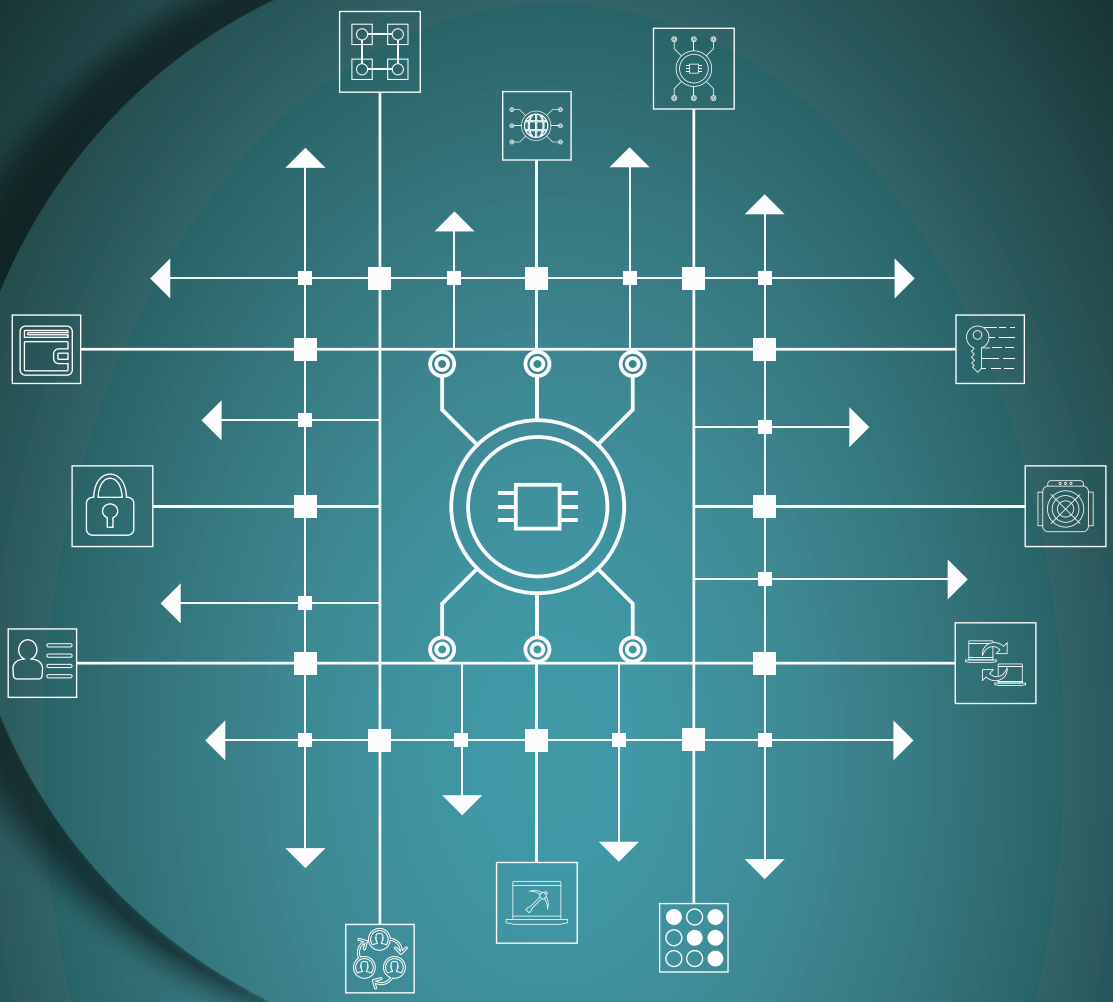
T2 Yazılım A.Ş.

B.B.N.

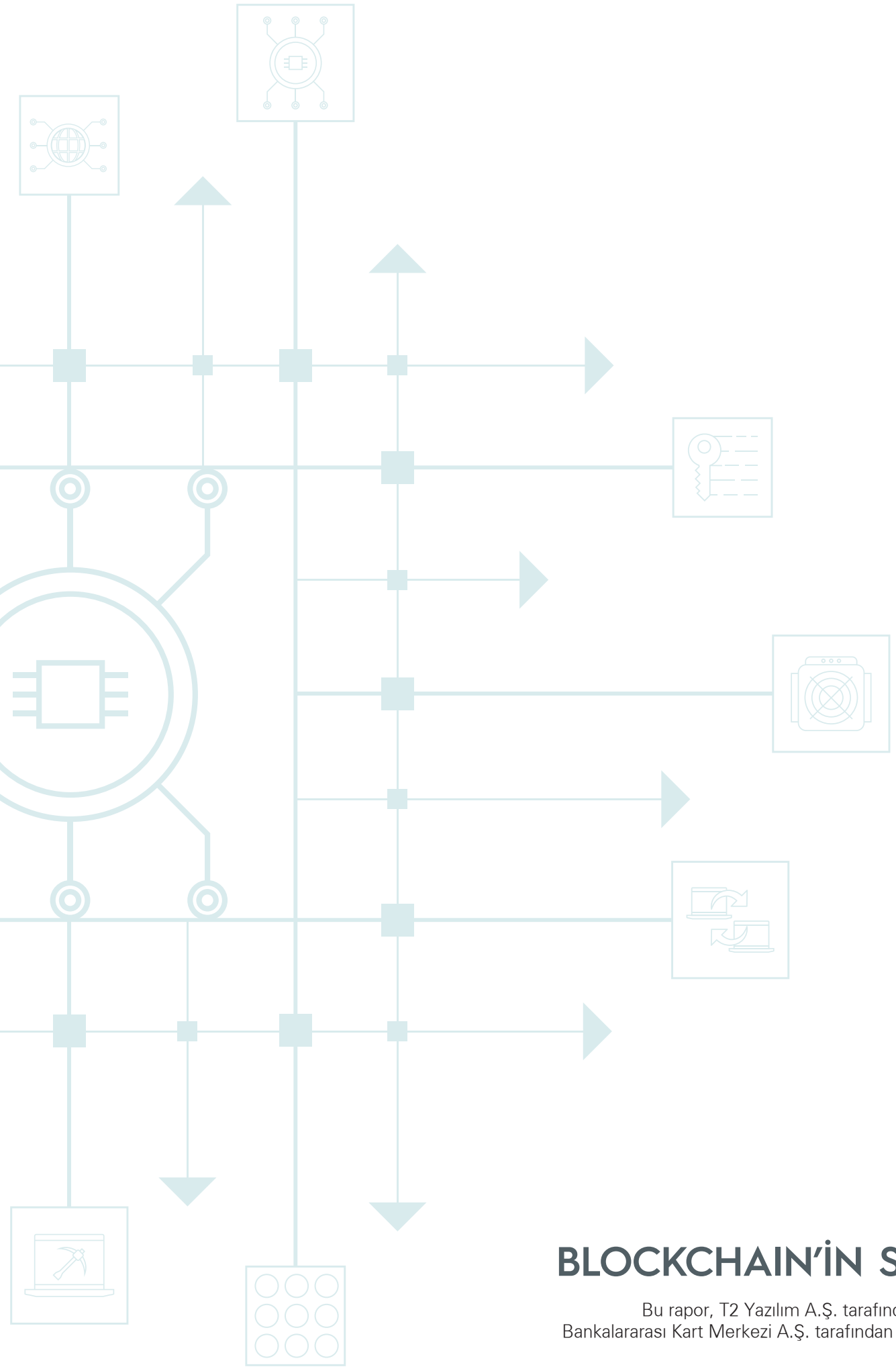
BKM
BANKALARARASI
KART MERKEZİ



KEŞİF:
BLOCKCHAIN'İN SIRLARI

BBN Faz 1

Mart 2018



KEŞİF:
BLOCKCHAIN'İN SIRLARI

Bu rapor, T2 Yazılım A.Ş. tarafından hazırlanmış,
Bankalararası Kart Merkezi A.Ş. tarafından düzenlenmiştir.

"Dijitalleşme çağında araştıran, merak eden ve deneyenler her zaman bir adım önde olacak."

Dr. Soner CANKO

Önsöz

Celal CÜNDOĞLU
Bankalararası Kart Merkezi A.Ş.
Genel Müdür Yardımcısı

Blockchain teknolojisinin önümüzdeki yıllarda finans sektörü de dâhil olmak üzere birçok sektörde iş yapış şekillerini değiştirmesi bekleniyor. Finansal teknolojileri yakından takip eden ve Türkiye'nin bu alanda öncü ülkeler arasında yer alması için çalışmalar yapan Bankalararası Kart Merkezi olarak, olgunlaşma süreci devam eden blockchain'in potansiyelini ve eksiklerini görmek için hayata geçirdiğimiz BBN uygulamamızın ilk çıktılarını sizlerle paylaşmaktan mutluluk duyuyoruz. T2 Yazılım'ın desteğiyle gerçekleştirdiğimiz BBN uygulamamızı, bu teknolojiyi paydaşlarımıza anlatabilmek ve çözüm sunabileceği problemleri birlikte hayal etmek için değerli bir araç olarak görüyoruz.

Bu raporda, BBN'in ilk fazı tamamlanırken teknolojiye dair gözlemlerimizi ve bundan sonra atılacak adımlar için anlamlı bulduğumuz kazanımlarımızı sizlerle paylaştık. Bu anlamda çalışmanın, blockchain üzerine çalışan kişi ve kurumlar için faydalı olmasını dileriz. Önümüzdeki dönemde blockchain ile ilgili yaptığımız çalışmaları çeşitlendirmeyi hedefliyoruz. Yeterli olgunluğa ulaştığında blockchain teknolojisinin ürün ve hizmetlerimizde kullanımının mümkün olup olmadığını araştırmaya devam edeceğiz.

Mustafa SAKALSIZ
T2 Yazılım A.Ş.
Kurucu Ortak, CTO

Bankalararası Kart Merkezi'ne (BKM) blockchain ile ilgili işlerimizi ve fikirlerimizi anlattığımızda, blockchain'i sunumlarda yeterince gördüklerini, artık bu teknolojiyi gerçeğe dönüştürmek istediklerini söylemişlerdi. Ellerinin altında çalışan bir blockchain projesi üzerinde kendi kullanım senaryoları ile denemeler yapmanın ve gerçek sonuçları görmenin zamanının geldiğine inanıyorlardı.

T2 Yazılım olarak, bu bakış açısı ile hayata geçirilmesi planlanan bir projede mutlaka yer almamız gerektiğine inandık ve projeyi gerçekleştirmek için ne kadar istekli olduğumuzu BKM'ye anlattık. Türkiye'nin en StartUp dostu kurumlarından biri olan BKM de bize inandı ve bu projeyi bize verdi.

Dört aylık zaman diliminde birçok özel duruma çareler bulundu, henüz olgunluğa erişmemiş bir teknoloji üzerinde tüm geliştirmeler yapıldı ve canlıya alım başarılı bir şekilde gerçekleştirildi. Bu süreçte özverili çalışmalarıyla yer alan T2 Yazılım mühendisleri ile projeyi olgunlaştıran, test eden ve tanımlayan BKM İş Geliştirme ekibine özel olarak teşekkür ediyorum.

Karşılaştığımız tüm sorunları, çözüm yaklaşımlarımızı, elde ettiğimiz öğretileri ve kazanımları bu raporda anlatmaya çalıştık. Umarım okuyan herkes için faydalı olur.

İçindekiler

Yönetici Özeti

Satoshi Nakamoto takma adıyla kaleme alınan "Bitcoin: A Peer-to-Peer Electronic Cash System" isimli makale ile hayatımıza girdikten sonra zaman içerisinde potansiyeli anlaşılan, teknoloji şirketleri ile girişimler tarafından platformlar geliştirilen ve konsorsiyumlar kurulan blockchain teknolojisini, Bankalararası Kart Merkezi (BKM) de yakından takip eden kurumlar arasında yer aldı. Teknolojinin yeterliliğini görmek ve ülkemizde daha iyi anlaşılmasını sağlayacak bir uygulamaya sahip olmak amacıyla bir kavram kanıtlama çalışması yapmaya karar veren BKM, dijital kimlik tabanlı bir projeyi hayata geçirdi.

Projenin başlıca amaçları arasında; **teknolojinin doğru anlaşılmasını sağlamak, ilgili araçların olgunluk seviyesini ölçmek, akıllardaki soruları yanıtlamak ve teknolojinin çeşitli iş problemlerine çözüm sağlama yeterliliğine dair kazanımları ekosistem ile paylaşmak** ilk sıralarda yer alıyordu.

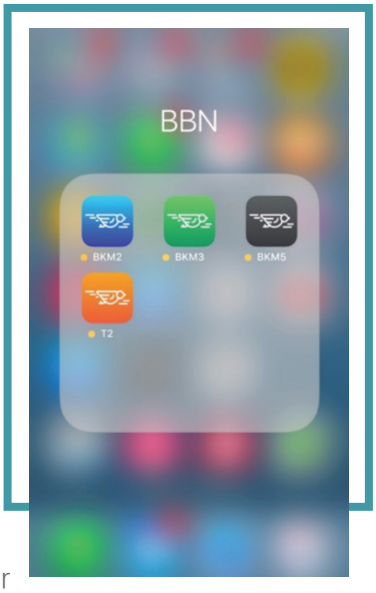
Gelişmekte olan kurumsal blockchain platformları konusunda bilgi birikimi kriterine göre değerlendirme yapıldı ve projenin T2 Yazılım ile birlikte geliştirilmesine karar verildi. Projede geliştirilen uygulamaya, BKM'nin iletişim sloganı **"Bay Bay Nakit"**ten esinlenilerek **BBN** ismi verildi. BBN uygulaması aracılığı ile BKM; çalışanlarının mobil cihazlarına yükleyip kullanabilecekleri uygulamalar üzerinden dijital kimliklerini oluşturmalarını, blockchain'e kaydetmelerini, verilen hedefleri yerine getirmeleri halinde puan kazanmalarını, bu puanları diğer kullanıcılara transfer etmelerini ve uygulamalar içerisindeki mağazalarda listelenen ürünleri puanları ile almalarını sağladı. **Bu işlem seti ile dijital kimliğin yanı sıra dağıtık kayıt defteri (distributed ledger) ve akıllı sözleşmeler (smart contracts) kavramları da uygulamaya geçirildi.** Projede sadakat puanları ise kripto para üzerine kurgulandı.

Bu raporda, blockchain altyapısı ile Ocak 2017'de hayata geçirilen projenin ilk fazına ait sonuçların özetlenmesi, alınan derslerin paylaşılması ve proje hakkında teknik bilgi verilmesi amaçlanmıştır. **Raporda, kullanılan teknolojilerin proje süresince sağladığı avantajlar, karşılaşılan zorluklar ele alınmış ve zorlukların nasıl aşıldığına dair bilgi verilmiştir.** Aynı zamanda rapor içeriğinde, teknolojinin çözdüğü sorunlar ve çözüm olamadığı durumlar üzerinden blockchain teknolojisinin hangi yöne doğru evrilmesi gerektiğine dair çıkarımlar da yer almaktadır.

Türkiye'nin ilk blockchain uygulaması olan BBN'in ilk fazında, teknolojiyi daha yakından tanıma amacına ulaşılırken, **blockchain'in henüz büyük çaplı sistemlerde kullanılabilecek kadar olgunlaşmadığı sonucuna varılmıştır.** İşlevsellik, mutabakat çeşitliliği, işlem hızı ve kapasitesi anlamında platformların gelişmesi ve endüstrilerdeki farklı kurumların ekosistemler oluşturmayı başarması halinde, blockchain teknolojisinin finanstan lojistiğe birçok sektörde çeşitli alanlarda başarılı olabileceğine inanılmaktadır.

Teknolojinin olgunluğunu yakından takip etmek için BKM, çeşitli blockchain platformları ile kavram kanıtlama projeleri yapmaya ve sonuçlarını paylaşmaya devam edecektir.

1. BBN Uygulaması Teknik Altyapısı



1.1. BBN

Bankalararası Kart Merkezi (BKM) tarafından hayata geçirilen BBN, şirket çalışanlarını motive etmek amacıyla verilecek hediyelerin kazanılmasını ve tüketilmesini sağlayan şirket sadakat platformudur. İsmini BKM'nin nakitsiz ödemeler vizyonu ile yaptığı iletişim çalışmalarında kullandığı "Bay Bay Nakit" sloganından alan BBN ile dijital kimlik, dağıtık kayıt defteri, akıllı sözleşmeler ve mutabakat (consensus) gibi kavramların test edilmesi amaçlanmıştır. Ağa dâhil olan eş sayısının artırılması için BKM, tek bir uygulama yerine üç ayrı uygulama olarak temsil edilmiş, çözüm ortağı T2 Yazılım da ağa katılan eşlerden biri olmuştur. BBN blockchain ağında, **izin gerektiren özel bir blockchain yapısı** tercih edilmiştir. Kullanıcıların "keklik" ismi verilen sadakat puanlarını kazandığı ve uygulamalarda yer alan mağazalarda harcayabildiği BBN, 2017 yılının başında hayata geçirilmiş ve 2018 yılının başında ilk faz tamamlanarak ikinci faza geçilmiştir.

1.2. Blockchain Platformu

Projeye başlarken platform seçimi için BKM'nin önünde seçenekler bulunmaktaydı. Bunlardan bazıları aşağıdaki gibiydi:

- Hyperledger Fabric
- Ethereum kapalı test ortamı
- NXT
- Blockstack
- R3 Corda
- Hyperledger Sawtooth
- Özelleştirilmiş bitcoin
- Geliştirilecek tamamen özel ve yeni bir platform

Bu platformlar arasında seçim yaparken çeşitli beklentilerin karşılanması hedefleniyordu. Bu beklentiler;

- Kapalı devre bir sistem ve sadece BKM'nin yetki vereceği eşlerin blockchain ağına dâhil olabileceği izin gerektiren bir yapı,
- Sunduğu imkânları denemek amacıyla akıllı sözleşme desteği,
- Olası sorunlar karşısında hızlı çözüm üretebilmek için teknik yeterliliği ve destek hizmetleri istenen seviyede olan bir platform ihtiyacı şeklinde sıralanabilir.

BBN, Hyperledger Fabric platformunun 0.6 versiyonu üzerinde hayata geçirilmiştir. 2017 yılının ortasında Fabric 1.0 versiyonunun kullanıma açılması sonrasında 2018 yılının başında yeni versiyona güncelleme yapılarak BBN'de ikinci faza geçilmiştir.

Blockchain gelişmekte olan bir teknoloji olduğu için alınacak destek ve yaşanacak olası sorunlarda çözüme hızlı biçimde ulaşmak en önemli unsurlardan biriydi. Bu yüzden yaygın biçimde kullanılan bir platforma ihtiyaç vardı ve sonuç olarak BBN'in, Hyperledger Fabric platformu üzerinde geliştirilmesi kararlaştırıldı. BBN'den sonra dünyada yapılan benzer yapıdaki çalışmalarda da Hyperledger Fabric'in tercih edildiği görülüyor.

1.3. Üst Seviye Mimari ve Teknolojiler

Projenin tamamında açık kaynak temelli teknolojiler kullanılmıştır:

- İşletim sistemi: Linux
- Uygulama sunucusu: Payara
- Veritabanı sunucusu: PostgreSQL
- Blockchain platformu: Hyperledger Fabric
- Mobil geliştirme platformu: React Native
- Container teknolojisi: Docker
- Programlama dilleri: Java, Go, JavaScript

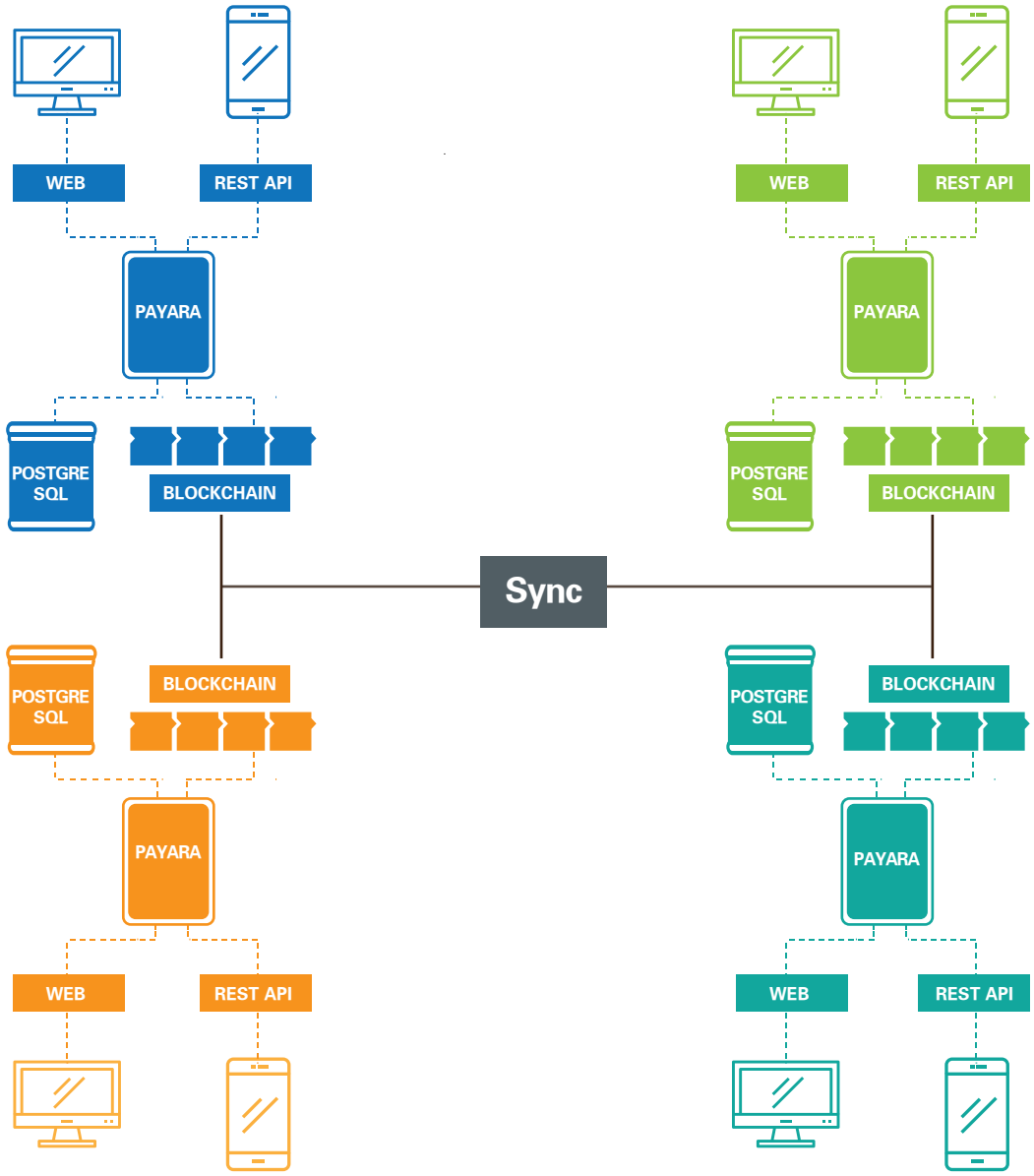
BBN Faz 1'i oluşturan blockchain ağında beş adet eş kullanılmıştır. Bu eşlerden biri T2 Yazılım'a, üçü BKM'ye (her biri ayrı bir kurum / uygulama olarak konumlandırılmıştır) ait olup bir tanesi de son kullanıcı ile etkileşimi olmayan merkezi yönetim katmanıdır. Fabric 0.6'nın yapısı gereği bir eş, temel eş (root peer) olarak tanımlanmak zorundadır. BBN'de merkezi yönetim katmanı, temel eş rolüne de sahipti. Diğer dört eşin ve sistemin üst seviye mimarisi Şekil 1'deki Üst Seviye Mimari diyagramında belirtilmiştir. Buna göre, BBN'deki her bir kurumun (BKM2, BKM3, BKM5, T2) tamamen kendi uygulama sunucusu, veri tabanı, mobil uygulaması ve ilgili servisleri bulunmaktadır. Her bir kurum, BBN blockchain ağında bir eş olarak temsil edilmektedir.

BBN Faz 1'i oluşturan blockchain ağında beş adet eş kullanılmıştır.

Mobil uygulamalarda ayrıca bir cüzdan yapısı kurgulanmamış olup, dijital kimlik barındıracak şekilde geliştirme yapılmıştır. Cüzdan yapılarında kullanıcıların sorumlulukları daha fazladır. İşlemler bloklara yazılırken eşler sürekli cüzdanlarla konuşmak zorundadır. Bu sebeple cüzdan yapısını kullanacak kullanıcıların daha bilinçli ve ileri seviye kullanıcı (power user) olması beklenir. Fakat BBN'de, daha çok eş seviyesindeki işlemlerin gözlemlenmesi hedeflendiğinden ve Fabric'in iyi bir cüzdan yapısı sunmamasından dolayı cüzdan kurgusu, sunucu ve eş seviyesinde kurgulandı. Sahiplik ise dijital kimlik yapısıyla çözüldü. Mobil kullanıcıların hesap yapıları ve işlemleri, sunucu üzerinde bulunan REST servisler vasıtasıyla kurum katmanlarına iletilmektedir ve blockchain üzerinde ilgili eş tarafından gerçekleştirilmektedir.

Uygulama sunucusu üzerindeki geliştirmeler, web arayüzü ve web servisleri Java 8 ile yapılmıştır. Mobil uygulamalar React Native ve Hyperledger Fabric üzerindeki akıllı sözleşmeler ise Go diliyle geliştirilmiştir. Hyperledger Fabric, başka dillerde de geliştirme imkânı verse de Fabric'in kendisinin Go diliyle yazılması, yeniliklerin önce Go API'ına gelmesi ve diğer diller için ayrıca bir vekil (proxy) yapıya ihtiyaç duyulması, Go dilinin seçilmesinde belirleyici oldu. Şekil 1'de Üst Seviye Mimari diyagramındaki her renk, farklı bir kurumu temsil etmektedir ve aralarında blockchain dışında herhangi bir entegrasyon bulunmamaktadır. Ayrıca her kurum için ayrı bir Amazon EC2 ile sanal makine açılmıştır ve farklı bölgelere konulmuştur. Bu yolla gerçek ağ ortamı oluşması sağlanmıştır. Bu sanal makineler arasında sadece Hyperledger Fabric'in kullandığı gRPC iletişim protokolü çalışmaktadır.

Uygulama, kapalı devre bir kavram kanıtlama projesi olduğundan dolayı geliştirme süresini kısa tutmak için bulut ortamı tercih edilmiştir. Öte yandan, blockchain ağında hiçbir şekilde kişisel veri saklanmamaktadır.



Şekil 1: Üst Seviye Mimari Diyagramı

1.4 Blockchain'in Kullanıldığı Alanlar ve Kullanım Şekli

BBN'de birçok bilgi ve işlem kaydı söz konusu olmasına rağmen bu bilgilerin tamamı blockchain üzerinde tutulmamıştır. Kritik verilerin dar bir kapsamda blockchain üzerinde tutulmasına dikkat edilmiştir. İşlem ve kayıt bazında hangi ortamda, hangi bilginin yer aldığına dair ayrıntılı bilgi Tablo 1'de yer almaktadır.

BBN'de birçok bilgi ve işlem kaydı söz konusu olmasına rağmen bu bilgilerin tamamı blockchain üzerinde tutulmamıştır.

Tablo 1: İşlem Setinin ve Bilgilerin Ortam Bazında Dağılımı

	Mobil Uygulama	Sunucu Veritabanı	Blockchain
Kullanıcı Kaydı	Dijital Kimlik	Paylaşılan Kimlik Bilgileri	Dijital Kimliğe Ait Hashcode
Keklik Hesabı	Dijital Kimlik	Kimlik Bilgileri ve Kullanıcı ID Eşleşmesi	Kullanıcı ID ve Keklik Hesap Bilgileri
Keklik Oluşturma	-	Kullanıcı ve İşlem Bilgileri	Oluşturulan Keklikler
Keklik Transferi	İşlemin Başlatılması	Kullanıcı ve İşlem Bilgileri Kaydı	Akıllı Sözleşme İle Transfer İşlemi
Ürün Eklenmesi	-	Ürüne Ait Bilgiler (Ürün adı, Açıklama, Değeri, Fotoğraf)	Her Ürün İçin Tanımlanmış Tekil Kod
Ürün Satın Alınması	İşlemin Başlatılması	Alışveriş İşlemine Ait Kayıtlar	Akıllı Sözleşme ile Ürün ve Keklik Takasının Gerçekleştirilmesi
Kullanıcı Girişi	Dijital Kimlik	Doğrulama ve Yetkilendirme İşlemleri	-

1.5. Dijital Kimlik ve Dijital Kimliğin Blockchain ile Kullanımı

BBN uygulamasının en önemli kullanım senaryolarından biri dijital kimlik ve onun blockchain ile doğrulanması olmuştur. Test edilen bu yapı ile Müşterini Tanı (Know Your Customer - KYC) süreci için pratik bir kullanım sunulması amaçlanmıştır. BBN çözümünde, dijital kimlik kullanıcıya ait bir bilgi olduğu için sadece kullanıcının onay vermesi halinde dijital kimliğinin istediği kurumla/uygulamayla paylaşılmasına uygun bir gerçekleştirme yapılmıştır.

BBN çözümünde, dijital kimlik kullanıcıya ait bir bilgi olduğu için sadece kullanıcının onay vermesi halinde dijital kimliğinin istediği kurumla/uygulamayla paylaşılmasına uygun bir gerçekleştirme yapılmıştır.

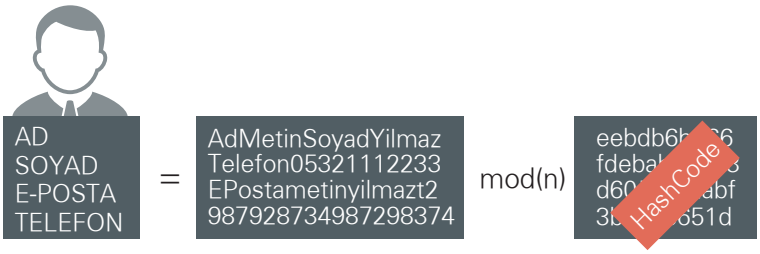
Buna göre dijital kimlik, kullanıcıya ait bir yerde şifreli bir şekilde durmaktadır. BBN'de dijital kimliklerin şifreli şekilde durduğu yer, kullanıcıların kişisel cep telefonları olmuştur. Kullanıcı, BBN'de bir kuruma ilk kez kaydolurken, ilgili kurum bu bilgilerin doğrulama sürecini de gerçekleştirmektedir. BBN'de bu akış aşağıdaki gibi kurgulanmıştır:

- Kullanıcı, kayıt olacağı ilk kurum uygulamasına e-posta adresini, adını, soyadını, telefon numarasını girer ve fotoğrafını da çekerek dijital kimliğini telefonunda oluşturur.

- Ardından kendisine gönderilen e-posta üzerinden onay vererek kuruma başvuruyu kendisinin yaptığını belirtir.
- Ardından başvuru, başvurunun yapıldığı kurumun yetkilisinin ekranına düşer. Başvuruyu yapan kişinin girdiği bilgiler ve fotoğraf üzerinden doğrulama yapılır.
- Yetkilinin onay vermesiyle birlikte dijital kimliğin hashcode'u blockchain'e aktarılır ve kullanıcı, başvuru yaptığı kurum uygulamasına erişebilir.

Gerçek dünyadaki Müşterini Tanı süreçlerinin küçük bir simülasyonu olarak kurgulanan bu yapı; bireylerin, bir bankaya başvuru yaparlarken beyan ettikleri fatura ve kimlik gibi belgelerle kendilerini doğrulamalarına benzetilebilir. Yapılan doğrulamadan sonra kimlik bilgileri, tek yönlü kriptografik özet fonksiyonlar ile hashcode'u oluşturularak blockchain'e atılmış ve tüm ağ ile paylaşılmıştır. Bu sayede kullanıcının cep telefonundaki dijital kimlik, onaylı bir kimlik haline gelmiştir. Tek yönlü kriptografik özet fonksiyonlar (Örneğin, SHA-1 ve SHA-256), tersi alınamayan ve hashcode'dan tekrar bir bilgiye ulaşılabilmesi mümkün olmayan fonksiyonlardır. Bu sayede blockchain üzerinde kullanıcıya ait herhangi bir özel bilginin bulunmaması ve kurumlar arasında herhangi bir kullanıcı verisinin paylaşılmaması sağlanmıştır. BBN'de, dijital kimliğini oluşturan bir kullanıcının aynı ağdaki başka bir kuruma kaydolmak istediğinde tekrar aynı doğrulama süreçlerinden geçmesine gerek olmayan bir yapı kurgulanmıştır. Bilgilerinin, kaydolmak istediği kurumla paylaşılmasına onay vermesi durumunda kullanıcı, telefonda tutulan kimlik bilgilerinin paylaşılmasıyla diğer kurumlara da başvuru yapabilmiştir.

Yapılan doğrulamadan sonra kimlik bilgileri, tek yönlü kriptografik özet fonksiyonlar ile hashcode'u oluşturularak blockchain'e atılmış ve tüm ağ ile paylaşılmıştır. Bu sayede kullanıcının cep telefonundaki dijital kimlik, onaylı bir kimlik haline gelmiştir.



Şekil 2: Dijital Kimlik Hashcode Üretimi

1.6. Dijital Kimliğin Yeniden Oluşturulabilmesi

Blockchain teknolojilerinde kullanıcılara inisiyatif verildiğinde bazı kurtarma senaryoları da karşımıza çıkabiliyor. Örneğin, dijital kimliğin kullanıcı tarafından saklanması ve paylaşılması inisiyatifi, BBN uygulamasında doğrudan kullanıcıya bırakılmıştır. Bu durumda cep telefonunun kaybedilmesi, değiştirilmesi veya şifreli olarak saklanan kimliğin şifresinin unutulması, kullanıcının tüm varlıklarına erişiminde engel oluşturmaktadır. Her ne kadar bu tarz verilerin saklanabilmesi için donanım tabanlı saklama hizmetleri veren kuruluşlar olsa da bir blockchain projesinde bu işlemin de dağıtık olarak sistem üzerinde çözülebiliyor olması gerektiğini düşünerek bu konuda basit ve kullanışlı bir yaklaşım geliştirilmiştir. Buna göre, kullanıcının kimliğini ve o kimlikteki gizli anahtarı blockchain ağındaki seçilen eşlerle paylaşabilmesi ve gerektiğinde bu kurumlardan geri alabilmesi sorunu çözüyordu. Fakat kurumların dijital kimliklere tamamen sahip olması bir güvenlik riski oluşturduğundan, kurumlara gönderilen verinin eşler için anlam ifade etmeyecek bir veri olması gerekiyordu. Bu doğrultuda dijital kimliğin, iki ayrı eşten gelecek parçalı kodlar ile telefonda yeniden oluşturulabildiği bir yapı kurgulanmıştır.

2. Alınan Dersler

2.1. Hyperledger Fabric 0.6

2.1.1. Değiştirilemeyen Akıllı Sözleşme Yapısı

Fabric 0.6 versiyonu için "Fabric'in ara geliştirme sürümü" yorumu yapılabilir. Fabric'te bazı kavramlar sadece deneme amacıyla düşünülmüştü. Örneğin, geliştirme kolaylıkları sağlanması için akıllı sözleşmelerin kullanılabileceği basit bir tablo yapısı sağlanıyordu. Ancak tablodan çekilen kayıtlarda, performans problemi yaşanmaması için satırları getiren fonksiyon için sistem hafızasında sadece 100 kayıt getirecek şekilde bir düzenleme yapılmış. Bu değer, çok fazla işlemin gerçekleşmeyeceği test çalışmaları için yeterli olabilir ancak yaklaşık 150 kişinin kullandığı BBN ve benzer ölçekte uygulamalar için yeterli olmayacaktır. Bu sayıyı artırmak da geçici bir çözüm olacaktı. Bu sebeple BBN kapsamında, kayıtların üzerinde gezebilen farklı bir yapı kurgulandı. İlgili akıllı sözleşmenin istediği kadar veriyi alabilmesine olanak sağlayan yeni bir fonksiyon geliştirilirken, mevcut akıllı sözleşmeler de bu yeni fonksiyonu kullanır hale getirildi.

*Fabric 0.6 versiyonu için "**Fabric'in ara geliştirme sürümü**" yorumu yapılabilir.*

Fabric 0.6'da akıllı sözleşme yapısı bir daha değiştirilmemek üzere kurgulanmıştır. Akıllı sözleşmeler sistem üzerinde devreye alındıktan sonra üzerinde bir değişiklik yapılırsa, sistem onu tamamen yeni bir yapı olarak kurguluyor ve mevcut veriye ulaşamıyor. Sistemin genel yapısını değiştirmeyen hata düzeltmeleri için yapılan güncellemeler de aynı şekilde çalışmakta ve bu durum dezavantaj oluşturmaktadır. Nitekim BBN kapsamında yaşadığımız Fabric 0.6 API'ında bulunan GetRows fonksiyonundaki 100 satırdan fazla kayıt getirme problemini çözerken bir API güncellemesi yapılması gerekti. Yapılan API değişikliği ile beraber akıllı sözleşmeler de değişti ve oluşan yeni sistemde tüm geçmiş kayboldu. Bu durumu çözmek için Fabric 0.6 kodunda değişiklik yapılmak zorunda kalındı.

Tüm bu nedenler düşünüldüğünde, Fabric'teki akıllı sözleşmeleri devreye almadan önce çok iyi tasarlayıp, test edip sonra yüklemek gerektiğini vurgulayabiliriz.

2.1.2. Senkronizasyon Problemi

Fabric 0.6'da eşlerden birinde geçici bir kopma olduğunda ve kopma sonrasında ilgili eş blockchain ağına tekrar bağlandığında, o eş çöktüğü sırada oluşan blokları veya gerçekleşen işlemleri başka bir eşten senkronize edemiyordu. Bu da farklı eşlerde farklı sonuçların oluşmasına sebep oluyordu. Bu sorun aynı zamanda sağlıklı bir mutabakat (consensus) yapısının işlemesini de engelliyordu. Çünkü kurgulanacak bir mutabakat yapısında eşlerin sahip olduğu veriler farklılaştığında yeni eklenecek kayıt, her eşte aynı bütünlüğü sağlayamayacaktı. ***Bu sebeple BBN'de verinin bütünlüğünü koruyan bir mutabakat yapısı yerine daha basit bir yapı kurgulandı.*** Kullanıcı ile etkileşimi daha fazla olan eşlerde kayıt sayısı daha fazla olduğu için problem oluşma ve senkronizasyonun kaybolma riski de daha yüksek oluyor. Bu sebeple kullanıcılar ile etkileşimi olmayan bazı eşlerin sisteme dâhil edilmesi, en uzun zinciri yaşatmak için faydalı olmaktadır. ***Bu anlamda BBN'de kullanıcılarla etkileşimi olmayan merkezi yönetim katmanı, kopmalar sonrası senkronizasyonun tekrar sağlanmasında önemli rol oynamıştır.*** Fabric 0.6'da, çöken eşlerin en uzun zincirden tekrar senkronizasyonu için elle müdahale gerekmiştir ve Fabric, bu sorunun çözümü için hazır bir araç sunmamaktadır. Eşlerdeki verinin diğer taraflara taşınması da bu sorunu çözmemektedir. Çözüm için eşlerin veri tabanındaki ayarları tekrar konfigüre eden bir uygulama geliştirilmesi gerekmiştir.

2.1.3. Performans

İlk fazda çok basit bir mutabakat algoritmasının kullanılması ve eş sayısının az olması nedeniyle sistemde herhangi bir performans problemi yaşanmamıştır. Performans, saniyede dört işlem olarak ifade edilebilir. Fabric 0.6'nın eşler arasındaki senkronizasyonu da pek dikkate almaması sayesinde blokların eklenme hızının çok yüksek olduğu gözlenmiştir. ***Eğer eş sayısı artarsa ve mutabakat algoritması karmaşık hale gelirse (senkronizasyon ihtiyacı artarsa), blok eklenme hızında yavaşlama olması beklenebilir.*** Bu durumda bitcoin'de olduğu gibi bloğun eklenmeden önce bir havuzda bekletilmesi gerekecektir. Sonrasında da bir doğrulama sistemi oluşturmak gerekecektir. Bu yapı, Fabric 1.0 versiyonunda sunulmaktadır.

2.2. Harici Uzlaşma (External Consensus) İhtiyacı

Blockchain kullanım senaryolarına baktığımızda, aslında şu anda çok da gerçekçi olmayan bazı varsayımlarda bulunulduğunu görüyoruz. Bu varsayımlardan karşımıza en çok çıkan ise blockchain üzerinde işlem gören tüm varlıkların dijital olduğu ve gerçekte de blockchain üzerinde temsil edildiği varsayımıdır. Örneğin, tapu ya da araç takas örneklerinde takas işleminin sorunsuz biçimde yapılabilmesi; tapu, ruhsat ve paranın tamamen blockchain üzerinde duran varlıklar olacağı varsayımına dayanır. Eğer öyle olsaydı, tapuyu teslim ederken bir akıllı sözleşme vasıtasıyla aynı blok içerisindeki para da aynı anda karşı tarafın hesabından bizim hesabımıza geçerdi.

Varlıkların dijital olarak temsil edilmesinin ötesinde, büyük boyutlardaki verilerin blockchain üzerinde durmasını gerektirecek senaryolar da çokça konuşulmaktadır. Örneğin, nesnelerin interneti ve sigortacılık alanlarında bu veriler sonucunda bazı uzlaşmaların bir akıllı sözleşmede tanımlanmış ön koşullar yerine geldiğinde hızlıca yapılabilmesi beklenmektedir. Bu örneği detaylandırmak gerekirse, nesnelerin interneti ile birlikte artık cihazlar veri üretebilir ve bazı işlemleri yapabilir duruma geliyor. Bu işlemlerin bir kısmı ise çeşitli ödeme ve mahsuplaşma adımları gerektirecek. Evde elektrik ürettiğimizi ve onu şebekeye geri verdiğimizi hayal edelim. Bu senaryo için blockchain'deki akıllı sözleşmelerin kullanılması söz konusu olabilir. Sigortacılık için de tarım sigortaları örnek verilebilir. Bir bölgedeki olumsuz hava koşullarından dolayı ürünlerimizin zarar gördüğünü varsayalım. Sistem üzerinden bölge ve hava durumu doğrultusunda hasarımız onaylanacak ve uydu görüntüleri ile teyit alınması sayesinde akıllı sözleşmeler zararımızın bedelini sigortalıya ödeyecek. Bu şekilde büyük boyutlardaki veriyi analiz ederek karmaşık kararları vermesi gereken akıllı sözleşme kurguları yapılabilir. Oysa akıllı sözleşmeli blockchain sistemlerinde, her kayıt eklenmesi sırasında bu kaydın herhangi bir akıllı sözleşme tarafından veto edilme olasılığı sebebiyle kaydın eklenip eklenemeyeceğini görebilmek için önce deneme yapılır. Bu işlem, blockchain ağında uzlaşmaya katılan tüm üyeler tarafından uygulanır. Bu sebeple sözleşmelerimiz ne kadar akıllı olursa ve ne kadar çok veriye dayanırsa, kayıt ekleme performansımız da o kadar yavaş olur.

Sözleşmelerimiz ne kadar akıllı olursa ve ne kadar çok veriye dayanırsa, kayıt ekleme performansımız da o kadar yavaş olur.

Son dönemde fiziksel emtia karşılığı içeren blockchain uygulamaları ve token'ları çok popüler oldu. Blockchain sistemleri üzerinde token oluşturmak tamamen dijital ve basit bir işlemdir. Yalnız bu token'ın ya da dijital varlığın fiziksel karşılığının olması iddiası, blockchain'in de dışında bazı harici denetim mekanizmalarını barındırmaktadır. Dolayısıyla sisteme girilen yeni bir varlığın kaydının oluşması sırasında fiziksel varlığın denetimi, akıllı sözleşmelerin yapamayacağı bir şeydir.

Ayrıca bazı durumlarda, insan tecrübesine ve karar yeteneklerine kalan çok sayıda mutabakat adımı gerekmektedir. Örneğin, BBN uygulamasında keklik üretimi, çözümün kapalı devre kavram kanıtlama projesi olması sebebiyle, BKM'nin inisiyatifinde gerçekleşmektedir. Keklik üretimindeki akıllı sözleşme yapısı da, BKM'ye ait özel bir eş vasıtasıyla üretildiği sürece istenildiği kadar keklik üretilmesine olanak vermektedir.

BBN'in Fabric 1.0'da çalışan ikinci fazında keklik üretimi aşamasına harici mutabakat özelliği eklenmiş, keklik üretiminde eşlerin yarısından fazlasının mutabakatı aranarak sistemin otokontrolü artırılmıştır.

Burada blok oluşturma sırasındaki mutabakattan farklı olarak tamamen asenkron ve harici bir uzlaşma yapısı kurgulanmış oluyor. Bu iki mutabakat yapısının beraber çalışması ile gerçek hayattaki senaryoları hayata geçirmek de kolaylaşıyor. Gerek emtia karşılıklarının denetimi, gerekse uzlaşmadaki özel şartlar gibi örnekler, blockchain üzerinde otomatik gerçekleşen bir uzlaşma yapısının kurulmasını engelleyebilmektedir. Bu da çok popüler olan birçok senaryonun bile blockchain üzerinde gerçekleşememesine neden olur. Bu yüzden bu tür otomatik yapılamayan ama sistemin tamamının bloke kalmasını gerektirmeyen ikincil bir mutabakat adımı yapısı ihtiyacı doğmaktadır. Diğer bir deyişle, ***sisteme manuel olarak ya da dışarıdan beslenebilecek mutabakat adımları eklenebilirse blockchain ile gerçekleştirebileceğimiz senaryoların sayısı ve kapsamı da artacaktır.***

3. Hyperledger Fabric 1.0 ile Gelen Yenilikler

Endorser Peer
Oluşturulan işlemlerin uygun olup olmadığını kontrol etmek için öncelikle endorser eşlere işlemleri önermek gerekiyor. Eğer endorser eşlerden olumlu cevap alınırsa, işlemler kayda alınabiliyor. Bu sayede sistem içerisindeki her eşin işlemleri test etmesine gerek kalmıyor. Bu yapı, performansa ve modüler yapıya olan ihtiyaçtan dolayı bu şekilde tasarlanmıştır. Fabric 1.0'da yine endorser olacak eşlere bir zorunluluk ve limit getirilmemektedir. İsteyen eşler, kendilerini endorser eş olarak tanıtabilir ve test sürecine katılabilir.

Orderer Servisi
Mutabakatı işletmek için orderer servisi eklendi. Orderer servisi daha önceden belirlenen sayıda işlemi toplu olarak sıralayıp bir bloğa kayıt edebiliyor. Özellikle aynı anda veya birbirine çok yakın zamanda, farklı eşler tarafından sisteme eklenmesi istenen işlemler yapılmaya çalışılabilir. Bu işlemlerin en nihayetinde bir sıraya konulması gerekmektedir ve bu sıralama sistemin bütünlüğünü bozmamalıdır. Ayrıca bazı durumlarda işlemlerin beraber işlenmesi gerekebilmektedir. Özellikle Fabric 1.0'da konu bazlı işlemlerin beraber işletilmesini ve birleştirilmesini sağlayan Kafka yapısı da getirilmiştir. Bu birleştirilmeleri yapacak servis de orderer servisidir. Orderer servisi tek bir eş tarafından verilmek zorunda değildir. Birden fazla eş tarafından da verilebilmektedir. Bu da sistemin erişilebilirliğini artırmaktadır.

Veritabanı Altlığı ve Sorgulama Özellikleri
Her ne kadar blockchain bir çeşit veritabanı olsa da her sorguda ve işlemde tüm blokları dolaşmak çok pratik olmamaktadır. Bu sebeple oluşan dağıtık defter, veritabanlarında önbelleklenir. Her eşin kendi ön bellek veritabanı vardır. Bu sayede sorgulara daha hızlı cevap verebilir ve blok ekleme sırasında bütünlük testlerini daha kolay yapabilir. Öntanımlı olarak gelen LevelDB yerine CouchDB kullanılırsa ve veri yapısı olarak JSON seçilirse, chain üzerinde zengin sorgulara izin veriliyor.
CouchDB, bir servis gibi kullanıldığından CouchDB ile tak-çıkar veritabanı özelliği de gelmiş oluyor. Bu sayede farklı veritabanlarının farklı sorgulama özelliklerini kullanmak isteyenler, servis üzerine başka veritabanları ekleyerek veri üzerinde farklı sorgulama ve zenginleştirmeler yapabilir.

Key-Value Store
0.6 versiyonda tablo yapıları vardı. Tablo yapıları bazı durumlarda kullanım kolaylıkları sağlasa da özellikle Fabric'i kısıtlayabiliyordu. Key-Value ile daha genişleyebilir ve özelleştirilebilir bir yapıya kavuştu.

Membership Servisi (COP)
Yeni Membership servisi ile MSP (Membership Service Provider) yapısı sunulmaya başlandı. Bu servisi tek eş yerine birden fazla eş verebilmektedir. Bu sayede SPOF (Single Point of Failure) riski de ortadan kalkıyor.

Organizasyon Yapısı
Organizasyon yapısı eklendi. Bir organizasyonun birden fazla eşi olabilir. Bu organizasyonları yöneten birden fazla kullanıcı tanımlanabiliyor. Bu yapı ile organizasyon bazlı kuralların daha kolay verilebilmesi sağlanmıştır.

Channel Yapısı
Channel yapısı eklendi. Böylelikle aynı chain üzerinde birden fazla ledger kullanılabiliyor. Organizasyonlar arası özel channel tanımlanabiliyor. Böylece sadece o channel'a erişim hakkı olanlar söz konusu bilgileri görebiliyor veya oraya bilgi yazabiliyor. Channel yapısına özel endorser eş ve mutabakat kuralları tanımlanarak esnek kullanım senaryoları oluşturulabiliyor. Bu channel'lar oluşturulurken hangi eşlerin katılabileceği belirtiliyor. Daha sonra eş eklenip çıkartılabiliyor.

Güncellenebilen Akıllı Sözleşme Yapısı
0.6 versiyonda güncellendiği zaman ortaya çıkan sorunlar, 1.0 ile beraber chaincode'un güncellenmesini mümkün kılıyor.

Senkronizasyon
Fabric 0.6'da bir eş, diğer eşlerle bağlantısını kaybettiği zaman senkronizasyonunu da kaybediyordu. Geri iletişim sağlandığında, eksik bloklarını tamamlamıyordu. Bu durum farklı eşlerde farklı zincirler bulunmasına yol açıyordu. Fabric 1.0 ile tüm eşlerin aynı zinciri barındırabilmesi ve eksiklerini senkronize etmesi sağlandı ve senkronizasyon sorunu çözülmüş oldu.

4. Blockchain'de Temel Kavramlar

4.1. Dağıtık Kayıt Defteri (Distributed Ledger Technology - DLT)

Günümüzde iş dünyasında birden fazla partinin kullanımına açık olan sistemler, merkezde yer alan ve sistemi işleten güvenilir bir paydaşa ihtiyaç duymaktadır. Blockchain ise bilgilerin birer kopyasının sistemdeki oyunculara eşit olarak tutulmasını sağlayarak ihtiyaç duyulan güven ortamını aracı bir kuruma ihtiyaç duymadan oluşturmayı vadetmektedir. Eğer bir aracı olmadan bu işlemlerin gerçekleşmesi ve bilginin paylaşılması isteniyorsa, DLT bu aşamada ihtiyacı çözen bir teknoloji olarak ortaya çıkmaktadır.

DLT ile veri tüm paydaşlara dağılır ve bilgiler oluşturulurken bilginin doğruluğu, mevcut veri ile tutarlılığı ve mutabakat süreçleri DLT içerisindeki akıllı sözleşmelerle sorgulanabilir ve doğrulanabilir.

DLT ile veri tüm paydaşlara dağılır ve bilgiler oluşturulurken bilginin doğruluğu, mevcut veri ile tutarlılığı ve mutabakat süreçleri DLT içerisindeki akıllı sözleşmelerle sorgulanabilir ve doğrulanabilir. Sadece paydaşların uzlaştıkları veriler sisteme sağlıklı bir şekilde işlenir ve her paydaş tüm verinin bir kopyasını saklar. Ayrıca her kayıt, kendisinden önceki tüm kayıtlarla kriptografik bir şekilde bağlanır. Tüm kayıtların bu şekilde oluşturduğu zincirin bütünlüğü ve değiştirilip değiştirilmediği takip edilebilir.

4.2. Akıllı Sözleşmeler (Smart Contracts)

Bitcoin makalesinde, temelde aracı olmadan kişiler arasında para transferini sağlayan bir yapı anlatılmaktaydı. Bu sebeple bitcoin'in altındaki DLT ile sadece bir kayıt defteri tutuluyordu. Zaman içerisinde aracıyı kaldıran bu teknolojinin farklı senaryolara da çözüm üretebileceği fark edildi. Dağıtık kayıt yapısı verimli iş modelleri ortaya çıkarabiliyor olsa da bu kayıtlar üzerinde işlemler yapabilen yazılım parçalarının oluşturulması, daha akıllı işlemler yapılmasını sağlayabilirdi. Bahsedilen yazılım parçaları DLT'nin dışında da geliştirilebilir. Fakat bu durumda sistemin içindeki her bir paydaş farklı kodlamalar yapabilir, veri her paydaşta farklı bir yorum kazanabilirdi. Sonuç olarak istenmeyen bir durum ortaya çıkabilir ve kurulan yapıda standartlaşmadan bahsedilemezdi. Sanal makine ile erişimi kısıtlanmış biçimde geliştirilebilecek olan DLT'nin içinde çalışan yazılım parçaları ise ağdaki tüm paydaşların aynı programı çalıştırmasını sağlayacak ve kayıtların eklenmesi sırasındaki mutabakatı da daha güvenli hale getirecektir. Bu düşünceden hareketle bitcoin'den bağımsız bir platform olarak Ethereum tasarlandı ve akıllı sözleşme yapısını bizlere kazandırdı.

Akıllı sözleşmelerin avantajları sadece veriyi kontrol etmekle sınırlı değil. Akıllı sözleşmeler, oluşan veriden sonra alınacak bir aksiyon varsa onları da başlatabiliyor ve bazı aksiyonların tanımlı kurallar çerçevesinde otomatik olarak gerçekleşmesini sağlıyor. Bu da aracı kurumların bugün üstlendiği bazı görevlerin de DLT ile yapılabilir hale gelmesini sağlıyor.

4.3. Mutabakat (Consensus)

Blockchain kavramı bitcoin ile hayatımıza girdikten birkaç yıl sonra farklı iş kollarından birçok kurum, blockchain teknolojisine ilgi göstermeye ve kullanım alanlarını araştırmaya başladı. Yapılan ilk çalışmalarda, hâlihazırda yürütülmekte olan süreçlerin blockchain ile tekrar kurgulanmasıyla denemeler yapmak ve teknolojiyi tanımak amaçlandı. Bu kurguların yapılabilmesine olanak sağlayan en büyük etken ise 4.2 bölümünde ayrıntılı biçimde ele alınan Ethereum ile blockchain dünyasına armağan edilen akıllı sözleşmeler olmuştu. Akıllı sözleşmeler, blockchain'i tek boyutlu bir kayıt defteri yapısından sonsuz boyutlu bir yapıya dönüştürdü.

Blockchain'i üç temel kavramın birleşimi olarak tanımlayabiliriz. Bunlar;

1. Veri bütünlüğünü sağlayan zincir şeklinde kayıt imzalama,
2. Verinin dağıtık şekilde bulunması,
3. Sadece mutabakatla kayıt oluşturulabilmesi şeklinde sıralanabilir.

Bu üç maddeden aslında en önemlisi mutabakat kısmıdır. Çünkü ilk iki madde, mutabakat ile eklenen doğru veri oluştuğunda, onun bütünlüğünü koruyup kaybolmamasını sağlarken anlam kazanmaktadır. Hatalı veya hileli biçimde oluşturulan kayıtların bütün ve kaybolmadan durmasının kimseye bir faydası olmayacaktır.

Mutabakat yapısı bazı blockchain'lerde, örneğin bitcoin'de oldukça basittir. Kullanıcılar tarafından imzalanmış transferler, önceden oluşturulmuş ve son blok ve önceki bloklarda yazılı transferlerle tutarlı ise (örneğin, kullanıcının transfer etmek istediği kadar bakiyesi varsa) bir bloğa yazılır ve bloğun belli bir formata uygun özeti oluşturulur. Bitcoin'de akıllı sözleşme yapısı da bulunmamaktadır. Eğer bir blockchain'de akıllı sözleşme varsa, bu bloklara eklenmesi beklenen işlemlerin akıllı sözleşmelerin onayından da geçmesi gerekmektedir.

Blockchain ağlarında mutabakat genellikle çoğunluğun onayına bağlı olarak çalışır. Bu çoğunluk yarıdan bir fazla olarak da değerlendirilebilir (supermajority). Eğer N adet bloğu olan bir ağdan bahsediyorsak, N+1'inci blok için farklı blockchain uygulamalarında farklı yaklaşımlar vardır. Örneğin, bitcoin'de birden fazla N+1 blok oluşur ve blok zincirini birçok dala böler. N+2'nci blok oluşturulmaya başlanınca, madenciler istedikleri N+1 üzerinden devam eder. Bu N+2 ve sonrası bloklar için de aynıdır. Dolayısıyla belli bir zaman sonra zincirin bir dalı diğerinden daha uzun olmaya başlar ve çoğunluk uzun dalı seçtiğinden diğer dallar kaybolur. Eğer her blok oluşturma aşamasına raund (round) dersek, bitcoin gibi herkese açık blockchain ağlarında gerçek mutabakatın oluşması için birden fazla raundun geçmesini beklememiz gerekir. Doğru özet bulunsa bile, eğer blok içinde hatalı işlemler varsa, sonraki raundlarda ilgili blok kabul görmeyecek ve zincir başka dallardan devam edecektir. Bu sayede sistem kendini onaylayarak büyür. Ağın büyük ve çeşitli olması güvenliğini artırır.

Ripple ve Fabric gibi blockchain ağlarında mutabakat süreci daha farklıdır. Bu ağlar, doğası ve kuruluşu itibari ile birbirine güvenen oyunculardan oluşmaktadır. Bu sebeple güvenlikten ziyade performansa odaklanılmaktadır. Bitcoin'den farklı olarak her raundda mutabakatın mutlaka sağlanması beklenir, dallanmalara izin verilmez. Sistemin tamamının mutabakata katılması beklenmez. Bunun için sistemin içinden seçilen bazı eşler bu görevi üstlenir.

Genellikle çoğunluk kuralı uygulansa da sistemi kuran ekip bu kriterleri de iş kuralları çerçevesinde değiştirebilir. Mutabakat, farklı görevleri yerine getiren eşlerin aşamalı onayı ile gerçekleştirilir. Örneğin, yapılacak işlemler öncelikle belli bir grup eşe gönderilir ve onların test etmesi istenir. Bu eşler işlemi reddetmezse, işlemi imzalayarak işlemin oluşturduğu veri değişiklikleri ile beraber işlemi yapan yere geri döndürür. Daha sonra bu değişiklikler sıralama işlemi yapan eşlere gönderilir. Orada bu işlemler belli kriterlere göre sıralanır ve birleştirilir. Sonrasında ise dağıtık deftere işlenmesi için tüm eşlere gönderilir. Ripple'daki yapıda birkaç detay farklı olsa da genel olarak Fabric 1.0 ve Ripple çok benzerdir. Dolayısıyla Fabric ve Ripple'da uzlaşma, bu işlemin bütününü içerir ve farklı aşamalarda ret veya onay alabilir.

4.4. İzin Gerektiren ve İzin Gerektirmeyen Yapılar

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.

BKM tarafından geliştirilen BBN, izin gerektiren ve özel kategorisinde yer alan bir blockchain çözümüdür. Veri güvenliği ve gizliliği anlamındaki katma değeri ile bu yapı, finans sektöründeki oyuncuların yaptığı denemelerde de çoğunlukla tercih edilmektedir. Bitcoin ise izin gerektirmeyen açık blockchain örneklerinden biridir.

İzin gerektiren blockchain'lerde sadece belirlenen eşler (peer) belirli haklarla blok oluşmasına ve mutabakata katkı sağlayabilmektedir.

5. Sonuç

Bankalararası Kart Merkezi olarak Türkiye'nin ilk blockchain projesi olan BBN'i 2017 yılının başında hayata geçirirken tüm yeni teknolojilerde olduğu gibi öğrenmek için denemek gerektiği inancıyla yola çıktık. Henüz yolun başında olduğumuz teknolojiyi test ederken, eksiklerini görmenin yanı sıra potansiyeli hakkında fikir sahibi olup öğrendiklerimizi paydaşlarımıza aktarmayı amaçladık. BBN uygulamamızda tamamladığımız ilk fazda, blockchain teknolojisinin henüz büyük çaplı bir sistemin yerini alacak kadar olgunlaşmadığı sonucuna ulaştık. Bununla birlikte standartların belirlenmesi ve ekosistemdeki oyuncuların ortak paydada buluşması halinde dağıtık kayıt defteri, akıllı sözleşmeler ve mutabakat yapılarının kullanılacağı blockchain tabanlı uygulamaların, orta vadede farklı sektörlerde çeşitli kullanım alanlarında kabul göreceğine inanıyoruz.

Kurum olarak bundan sonraki süreçte BBN uygulamamızı Faz II'de Hyperledger Fabric 1.0 versiyonuna güncelleyeceğiz ve mutabakat, channel gibi yeni yapıları test edebileceğimiz kullanım alanları üreteceğiz. Hyperledger'daki bu çalışmalarımıza ek olarak Ethereum üzerinde bir uygulama geliştirmek de 2018 hedeflerimiz arasında yer alıyor.

Tüm bu çalışmalar sonucunda, doğru zaman geldiğinde teknolojinin katma değer yaratacağı alanlarda blockchain'i kullanmak, yol haritamızdaki önemli bir madde olacak. Bankalararası Kart Merkezi olarak yeni teknolojileri denemeye, öğrenmeye ve anlatmaya devam edeceğiz.

Blockchain Terimler Sözlüğü

Bitcoin: Bilinen ilk kripto paradır. Tamamen dağıtık yapıda ve aracısız çalışmaktadır.

Blockchain (Blok Zinciri): İlk defa bitcoin ile ortaya konulmuş olan, içerisinde kayıtların birbirine kriptografik elementlerle bağlı olduğu sürekli büyüyen dağıtık bir veritabanıdır. Bu veritabanındaki kayıtlar bir blok olarak paketlenmiş ve değişime karşı korunmak amacıyla kendinden önce gelen blokların özet değerleriyle bağlanmıştır.

Onaylama: Bir işlemin blockchain ağı tarafından onaylanmasına denir. Bu işlem, bazı blockchain ağlarında madencilik ile yapılır.

Mutabakat Süreci: Bir grup eşin (peer), dağıtık defter üzerindeki içerik konusunda uzlaşması sırasındaki geçtiği adımlara denir.

Kripto Para: Üretimi bazı matematiksel fonksiyonlarla sınırlandırılmış, kriptografik tekniklerle ve protokollerle güvenliği sağlanmış dijital para türüdür.

Kriptografi: Gizlilik, kimlik denetimi ve bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünüdür.

Ethereum: Halka açık blockchain (blok zinciri) merkezli dağıtılmış bir bilgi işlem platformudur ve akıllı sözleşme işlevselliğine sahiptir.

Ether: Ethereum blok zincirinin değer belirtecine Ether adı verilir. Ether, diğer kripto paralar gibi kripto para borsalarında işlem görmektedir.

EVM: Ethereum Sanal Makinesi (EVM) ile kripto para kullanılarak "akıllı sözleşme" adı verilen P2P sözleşmeleri gerçekleştirilebilmektedir.

Dijital Emtia: Elektronik olarak transfer edilebilen, miktarı sınırlı olan ve pazar değerine sahip fiziksel olmayan değerdir.

Dijital Kimlik: Bir kişinin, organizasyonun ya da elektronik bir cihazın bir ağ içerisinde tanımlanmasını sağlayan kimlik. Dijital kimlik, günümüzde bireylerin çok sayıda kurum ve platformla etkileşim halinde olması sonucunda karmaşıklaşan şifre yönetim süreçlerine çözüm olarak araştırılan blockchain'in kullanım alanlarından biridir.

Dağıtık Kayıt Defteri (Distributed Ledger Technology): Farklı sunucularda kopyaları duran bir veritabanı çeşididir. Kayıtlar birbiri ardına eklenerek sürekli büyür.

Madencilik: Blockchain ağlarında kripto para yaratma işlemine madencilik (mining) denilmektedir. Madencilik, hesaplama yetkisini ve gücünü kullanarak matematiksel işlemleri gerçekleştirme işleminin genel adıdır.

Eş (Node, Peer): Blockchain ağına bağlı olan bir bilgisayar.

Ripple: Uluslararası para transferi için geliştirilen bir blockchain ağı. Ripple Labs tarafından geliştirilmiş sistemin kendi para birimi XRP'dir.

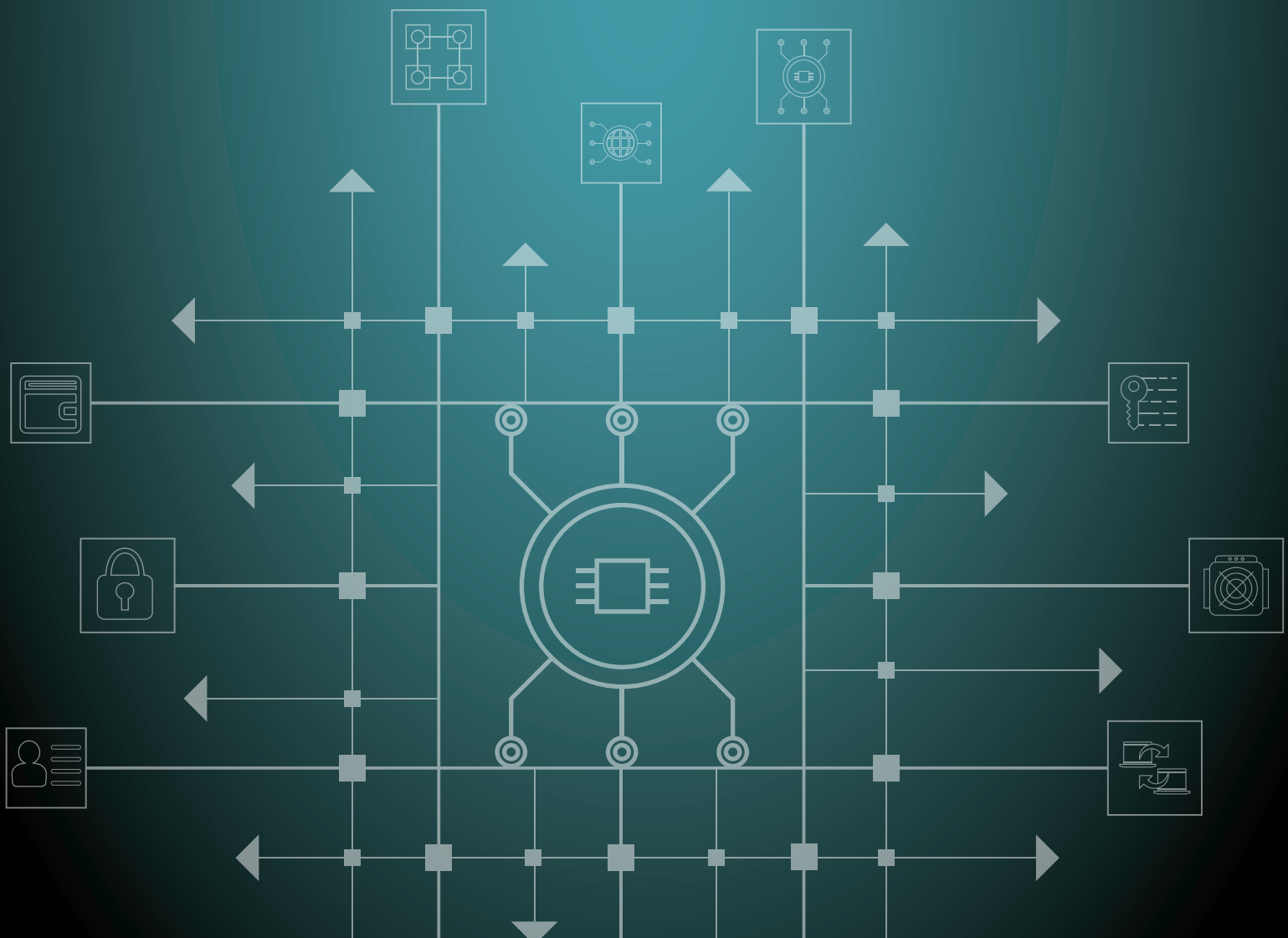
Akıllı Sözleşmeler (Smart Contracts): Programlama diliyle yazılan sözleşmelerdir. Akıllı sözleşmeler otomatik olarak çalıştırılabilirler ve dağıtık defter yapıları üzerinde işlemlerini gerçekleştirirler.

Token: Sahiplik özelliği olan dijital varlıklardır.

İşlem Bloğu (Transaction Block): Belli bir sayıda işlemi bir araya toplayan ve özeti alınarak blockchain'e eklenen sıralı bir işlem kümesidir.

Cüzdan: İçinde sahibine ait gizli anahtarı barındıran yapıdır.

BBN UYGULAMASINI GELİŞTİREN EKİPLER



BBN uygulamasını geliştiren **Bankalararası Kart Merkezi** ekibi üyeleri

Dr. Soner Canko
Genel Müdür

Celal Cündoğlu
Genel Müdür Yardımcısı

Özge Çelik
İş Geliştirme Direktörü

Okan Yıldız
İş Geliştirme Müdürü

Kadir Güzel
Mühendis

BBN uygulamasını geliştiren **T2 Yazılım** ekibi üyeleri

Mustafa Sakalsız
Project Manager - CTO

Dr. Tan Apaydın
Mobile & Blockchain Developer

Mert Çalışkan
Web Developer

Ömer Metehan Danacı
Web & Blockchain Developer

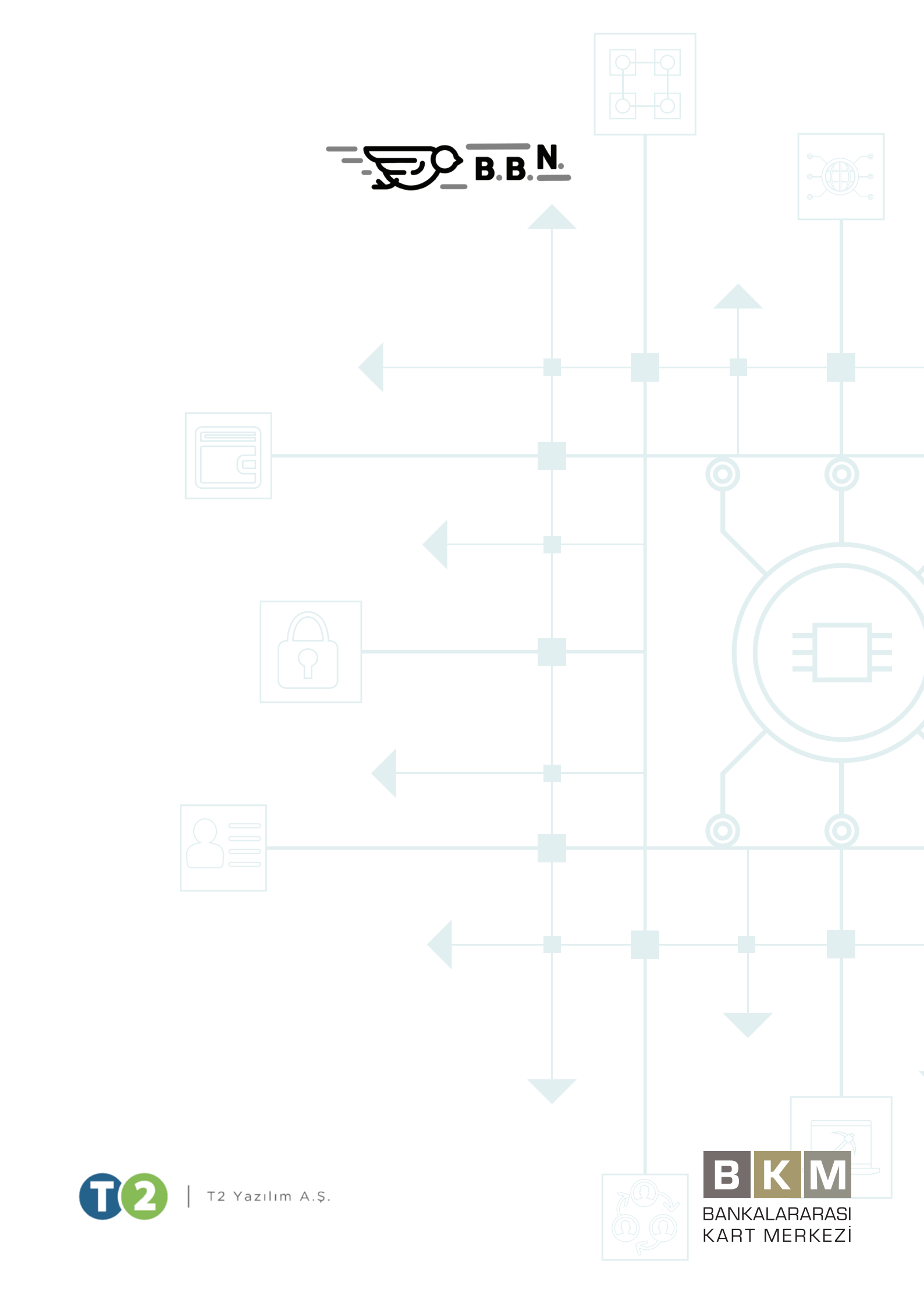
Mustafa İlker Saraç
Mobile Developer

Burak Doma
Scrum Master

Burak Başcı
UI Designer

Dr. Kamer Kaya
Danışman,
Sabancı Üniversitesi

Dr. Ata Türk
Danışman,
Boston University



T2 Yazılım A.Ş.

BANKALARARASI
KART MERKEZİ