BİGA PROJESİ

TAKAS İSTANBUL

FinTechHub
TAKAS İSTANBUL

TAKAS İSTANBUL

FinTechHub
TAKAS İSTANBUL

FİZİKSEL DAYANAĞI OLAN, REGÜLASYONLA UYUMLU, MAKSİMUM GİZLİLİK VE GÜVENLİK SAĞLAYAN ALTIN

24h GÜVENLİ TRANSFER

Gökhan ELİBOL
Takasbank Genel Müdür Vekili
Yönetim Kurulu Üyesi

İki yılı aşkın bir süredir devam eden ve yoğun bir takım çalışmasının ürünü olarak ortaya çıkan dünyanın ilk fiziksel altına dayalı blokzincir tabanlı transfer sistemi BiGA'yı kamuoyu ile paylaşmaktan büyük mutluluk duyuyoruz.

Günümüz gelişen ve değişen küresel ekonomik eğilimleri zorlu bir rekabetçi ortamı da beraberinde getirmektedir. Özellikle finans teknolojileri alanında yapılan çalışmaların önemi gün geçtikçe artmaktadır.

Kuruluşundan bu yana ilerlemeyi ve gelişmeyi ana hedef olarak benimseyen Bankamız, her geçen gün ülkemiz ekonomisine sağladığı katkının artması için çalışmalarını sürdürmektedir. Bankamız gelişmekte olan teknolojileri daha yakından takip etmek adına ana faaliyet alanlarına ek olarak, 2017 yılı itibariyle FinTechHub Takas İstanbul markasıyla Yerinde Ar-Ge Merkezi olarak da hizmet vermektedir.

Finansal piyasalardaki merkezi konumumuz ve Ar-Ge misyonumuz blokzincir teknolojilerine yönelimimizi olumlu yönde tetiklemiştir.

Finansal teknoloji ekosistemini güçlendirmek amacıyla özel işletmeler ve üniversitelerle işbirlikleri yapılması, banka personeli Ar-Ge teşvikleri, düzenleyici kamu kurumları ve uluslararası organizasyonlarla istişareler konularına büyük önem verilmektedir.

BiGA, içinde bir çok ilkleri barındırıyor olması nedeniyle uluslararası düzeyde, alanında önemli bir dönüm noktası olacak referans bir projedir. Yenilikçi özellikleri nedeniyle BiGA, uluslararası patentleme sürecindedir. BiGA'nın aynı zamanda İstanbul'un Finans Merkezi olma hedefine de katkı sağlayacağı düşünülmektedir.

BiGA Projesinin başarılı bir şekilde gerçekleşmesinde katkıları ve destekleri için Yönetim Kurulu Başkanımıza, Bankamız çalışanlarına ve tüm proje paydaşlarına teşekkür ediyorum.

İÇİNDEKİLER

ÖZET

Blokzincir teknolojisinin popülerliği son yıllarda giderek artmış, finans sektöründe özellikle merkezi konumdaki kurumlar yaygın olarak kullanım alanlarını araştırmaya başlamıştır. İlerleyen yıllarda bu teknolojinin finans sektörüne olabilecek etkilerine yönelik bilgi birikiminin oluşturulması Takasbank'ın en önemli stratejik hedefleri arasında yer almaktadır. Bu hedefe yönelik olarak Takasbank Ar-Ge Merkezi iki yılı aşkın bir süredir blokzincir üzerine detaylı çalışmalar yürütmektedir.
Yapılan araştırmalar, blokzincir teknolojilerinin finans sektöründe kullanılmasının henüz yeterli olgunlukta olmadığını göstermektedir.

Blokzincir teknolojisinin finans sektöründe kullanılabilmesi için mevcut teknolojilere ek geliştirmeler yapılması gerektiği ve Takasbank bünyesinde bu çalışmaların yapılabileceği öngörülmüştür. Özellikle mevcut regülasyonlar ile uyumlu, işlem yapanların mahremiyet beklentilerini karşılayabilen, aynı zamanda finansal otoritelerin işlemleri izleyebileceği, yerinden dağıtık defter teknolojilerinin kullanımı ve fiziksel dayanağı olan varlıkların dijitalleştirilmesi fonksiyonlarının sağlanmasına odaklanmak gerekmektedir. Takasbank tarafından yapılan çalışmalar neticesinde edinilen bilgi birikimi dahilinde, 2017 senesinde blokzincir teknolojisi kullanarak bir platform geliştirme fikri ortaya çıkmıştır. Söz konusu çalışmada fiziksel karşılığı olan dijital altının blokzincir teknolojisiyle taraflar arası transferini sağlayan bir platform oluşturulmuştur. Hem dağıtık defter teknolojisi kullanılmış, hem de işlemlerin mahremiyeti tam

olarak koruma altına alınmıştır. İşlemlerin tam mahremiyet altında yapılabilmesi, fiziksel dayanak varlığı esas alması, kendine ait ayrıca bir değeri olmaması ve mevcut regülasyonlara uyumlu olarak gerçekleşebiliyor olması bu projeyi dünyadaki duyurulan birçok projeden ayırmaktadır. Söz konusu çalışmada farklı teknik yetkinlikleriyle ön plana çıkan iki ayrı blokzincir altyapısıyla geliştirmeler yapılmıştır.

Yapılan bu geliştirmeler sonucu beş Banka ile çok partili test süreci başlamıştır. Albaraka Türk Katılım Bankası, Garanti BBVA, Kuveyt Türk Katılım Bankası, VakıfBank ve Ziraat Bankası ile yapılan testlerin sonucunda BiGA'nın işlevselliği gözlemlenmiş ve yüzde yüz memnuniyetle testler tamamlanmıştır.

Bu doküman, yapılan çalışmaların sonucunda geliştirilen BiGA Projesi hakkında bilgi vermek amacıyla hazırlanmıştır. Marka adı BiGA Dijital Altın olan BiGA Projesi'nde her bir gram fiziksel altın karşılığı olarak üretilen BiGA'ların paydaşlar arasında transferlerinin doğru, kontrollü ve mahremiyet odaklı bir şekilde gerçekleştirilmesi sağlanmıştır. Teknolojinin doğru çalışması ve yeterliliği test edilmiş, teknolojik belirsizlikler gözlemlenmiştir. Ayrıca finans sektöründe diğer çalışmalara öncülük edilmesi amaçlanmıştır. Doküman hem projenin teknik altyapısı hakkında hem de iş modeli hakkında bilgi vermektedir.

GİRİŞ

BiGA Projesi temelleri, Takasbank bünyesinde, 2016 yılının ilk çeyreğinde oluşturulan Takasbank Blokzincir Çalışma Grubu'na dayanmaktadır. Söz konusu tarih itibariyle blokzincir çalışmaları kapsamında sektörel gelişimler yakından takip edilerek Takasbank bünyesinde yapılabilecek projeler hakkında değerlendirmeler yapılmıştır.

Diğer yandan Takasbank, 2017 yılında yerinde Ar-Ge Merkezi statüsüne kavuşmuştur. Ar-Ge vizyonu ile birlikte blokzincir çalışmaları projelendirme aşamasına geçilmiştir. Takasbank, blokzincir hakkında yapılan organizasyonlara gerek ev sahipliği yaparak, gerek aktif katılım sağlayarak üst yönetim seviyesinde katkılar sunmuştur. Takasbank, ülkemizde gelişmekte olan blokzincir finans ekosisteminde bulunan firmalarla çeşitli görüşmeler ve fikir alışverişleri yaparak bu ekosistemin gelişmesine katkılar sağlamıştır.

Teknik altyapısı geleneksel yöntemler ile geliştirilen Altın Transfer Sistemi (ATS) Projesi henüz tasarım aşamasındayken blokzincir teknolojisi kullanarak geliştirilebileceği fikri ortaya çıkmıştır. Bu sayede Altın Transfer Sistemi'nin de blokzincir versiyonu olarak değerlendirilebilecek olan BiGA Projesi çalışmalarına başlanmıştır. Bu raporda ilk fazı tamamlanan BiGA'nın detayları paylaşılmaktadır.

BiGA

Bir Gram Altın

TAKAS İSTANBUL

FinTechHub
TAKAS İSTANBUL

TAKASBANK HAKKINDA

Ülkemiz bankacılık ve sermaye piyasaları açısından stratejik bir öneme sahip olan İstanbul Takas ve Saklama Bankası A.Ş. (Takasbank), "Merkezi Takas Kuruluşu", "Emeklilik Fonları için Saklama Kuruluşu", "Ulusal Numaralandırma Kuruluşu", "Merkezî Karşı Taraf Kuruluşu", "Ödeme ve Menkul Kıymet Mutabakat Sistemi" ve "Yatırım Bankası" lisansları ve yetkilerine sahiptir. Bu kapsamda, Ülkemizde Sermaye Piyasası Kurulu (SPK), Türkiye Cumhuriyet Merkez Bankası (TCMB) ve Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından sürekli gözetim ve denetim altında bulunan tek kuruluştur.

İstanbul Takas ve Saklama Bankası A.Ş. 'nin temel amacı; ilgili mevzuat çerçevesinde takas ve saklama hizmetleri vermek, finansal hizmetleri ve her türlü iktisadi faaliyeti gerçekleştirmek suretiyle ülkemiz piyasalarının rekabet gücünü artırmaktır.
SPK tarafından, Ülkemizin Merkezi Takas Kuruluşu olarak yetkilendirilen Takasbank, başta Borsa İstanbul A.Ş. bünyesindeki pazarlar olmak üzere ülkemizdeki diğer borsalara da (Ürün İhtisas Borsası, Enerji Borsası) takas, teminat ve nakit yönetimi hizmetleri sunmaktadır. Hali hazırda Ödünç Pay Piyasası, Borsa İstanbul Para Piyasası, Pay Piyasası ve Türev Araçlar Piyasası ve SWAP Piyasasında "Merkezi Karşı Taraf (MKT)" hizmeti sunan Takasbank, MKT faaliyeti kapsamında, işlemlerin gerçekleşmesini taahhüt etmekte ve bu anlamda gelişmiş teknolojik altyapısı ile birlikte kapsamlı bir risk yönetimi faaliyeti gerçekleştirmektedir. Ayrıca Ülkemizdeki organize para piyasalarından biri olan fon arz ve talep eden finansal kuruluşları bir araya getiren ve 6 aylık vadeye kadar işlemlerin gerçekleştiği ve bu anlamda emsal piyasa faiz oranlarının oluştuğu Takasbank Para Piyasası da Takasbank tarafından işletilen bir platformdur.

Diğer taraftan, 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun (Kanun)" çerçevesinde; TCMB' den faaliyet izni alan ödeme ve menkul kıymet mutabakat sistem yetkisi olan kurumlardan biri olan Takasbank, EFT-EMKT sistemi içerisinde de bankacılık ve sermaye piyasalarındaki stratejik önemi sebebiyle "Kritik Banka" olarak tanımlanmaktadır.

Takasbank, yurtdışında tesis etmiş olduğu menkul kıymet ve nakit muhabir hesapları ile SWIFT üyeliği vasıtasıyla, "Nakit Takas ve Teminat Hizmeti", "Global Takas ve Saklama Hizmeti" ve "Yerel Takas ve Saklama Hizmeti" ile faaliyet alanını uluslararası platformlara da taşımıştır.

Güvenilir, hızlı ve düşük maliyetli nakit transferi hizmeti sağlayarak para ve sermaye piyasaları arasında köprü görevi üstlenen Takasbank, Sermaye Piyasası ve Borsa İstanbul mevzuatı çerçevesinde Borsa İstanbul bünyesinde faaliyet gösteren piyasalar için tam otomasyon ortamında organize piyasalar ile online bağlantılı olarak takas hizmetleri sunmaktadır.

Takasbank, yıllar içerisinde, bankacılık ürün yelpazesini nakit ve gayri-nakit kredi imkânlarını içeren ve takasın sonlandırılmasını desteklemeyi amaçlayan enstrümanlarla genişletmiştir. Sunduğu nakit kredi imkânlarının yanı sıra, işlettiği Takasbank Para Piyasası (TPP), Türkiye Elektronik Fon Alım Satım Platformu (TEFAS) ve Ödünç Pay Piyasası (ÖPP) gibi nakdi ve gayri nakdi kredi imkânları ile desteklenen bankacılık faaliyetleri ile Türk Sermaye Piyasalarının takas işlemlerini; riskleri en aza indirgeyerek, piyasaya likidite sağlayarak ve takasın hatasız ve zamanında sonlandırılmasını amaçlayarak gerçekleştirmektedir.

Bunların dışında TapuTakas Sistemi, mülkiyet hakkı ve alım satım bedelinin el değiştirmesi sırasında alıcı ile satıcının karşılaştığı olumsuzlukların önlenmesi amacıyla,

- Gayrimenkul ile satış bedeli olan nakdin eş anlı olarak el değiştirmesi,
- Tarafların güven probleminin bertaraf edilmesi,
- Nakit taşıma riskinin ortadan kaldırılması,
- Düşük maliyetle hızlı transfer kolaylığı,
- Sahte para riskinin ortadan kaldırılması

sağlanarak tüm taraflar açısından çağdaş, güvenli ve teknolojik bir altyapı ile zaman, işgücü ve maliyet avantajı yaratılması için Tapu Kadastro Genel Müdürlüğü ile imzalanan protokol çerçevesinde tasarlanmıştır.

Çek Takas Faaliyetleri Hakkında Yönetmeliğin 5 inci maddesi kapsamında çeklerin banka şubeleri arasında hesaben ödenmesini sağlayan, takas ve mutabakat işlemlerine çek takas hizmetinin bünyesinde olmayan teminat yönetimi fonksiyonu da eklenerek tüm işleyişin tekbir merkezden yönetildiği Takasbank Çek Takas Sistemi kurulmuştur.

Enerji piyasasındaki Elektrik ve Doğalgaz Piyasaları için teminat mekanizmasının işletilmesi ve ödemelerin zamanında ve doğru bir şekilde gerçekleştirilerek, piyasadaki nakit akışının sürekli bir şekilde sağlanması amacına yönelik merkezi uzlaştırma bankası olarak Takasbank görevlendirilmiştir.

Piyasa katılımcılarına sınır-ötesi hizmetler de sunan Takasbank, sahip olduğu uluslararası takas kurumu kimliği ile Türkiye'yi global organizasyonlarda da temsil etmektedir. Takasbank'ın uluslararası piyasalarda tercih edilen bir kurum olma vizyonu doğrultusunda, teknolojik alt yapının geliştirilmesi amacı ile birçok projede çalışmalar sürdürülmektedir.

Takasbank mevcut yurt dışı saklama ağı ile dünya çapında 65'in üzerinde piyasada işlem gören yabancı kıymetlere erişim sağlamaktadır. Bu hizmet kapsamında Takasbank, yurtdışında uluslararası takas saklama kuruluşları (Euroclear ve Clearstream) ya da global saklama kuruluşları (Citibank) nezdindeki hesapları aracılığı ile söz konusu sermaye piyasası araçlarının saklanmasını sağlamaktadır.

SPK'nın gözetim ve denetim fonksiyonunu destekleyen ve güçlendiren bir hizmet olarak Bankamız; Kolektif Yatırım Kuruluşları ve Bireysel Emeklilik Fonlarının varlıklarına ilişkin değerleme, kontrol, mutabakat ve SPK'ya raporlama hizmeti de sunmaktadır.

24/07/2014 tarihinde Sermaye Piyasası Kurulu tarafından portföy saklayıcı kurum olarak yetkilendirilen Bankamızca; menkul kıymet yatırım fonları, menkul kıymet yatırım ortaklıkları, borsa yatırım fonları, gayrimenkul yatırım fonları ve girişim sermayesi yatırım fonlarına portföy saklama hizmeti verilmektedir.

Bankamız ayrıca, 5746 Sayılı Kanun kapsamında Türkiye Cumhuriyeti Bilim Sanayi ve Teknoloji Bakanlığı'nın onayı ile 21 Nisan 2017 tarihinde yerinde AR-GE Merkezi olmuştur.

İstanbul Uluslararası Finans Merkezi Projesi'nin en önemli bileşenlerinden biri olan, Bankamız tarafından yazılım ve sistem geliştirmesi yapılan ve Bankaların katılımıyla işleyecek olan "KİŞİDEN KİŞİYE HESAPTAN HESABA" Altın Transfer Sistemi Takasbank tarafından 16 Temmuz 2018 tarihi itibarıyla sistem üyesi bankalara ve müşterilerine hizmet vermeye başlamıştır. Risk, nakit, takas ve teminat yönetimi hizmetleri ile finans ve sermaye piyasalarına önemli katkılar sunan Takasbank, Ekim 2018 ayı itibarıyla Borsa İstanbul A.Ş. ile organize bir döviz SWAP Piyasasını ülkemiz ekonomisinin hizmetine sunmaya başlamıştır. SWAP işlemlerinin yoğun olarak yapıldığı Tezgâh Üstü Piyasalara (OTC) önemli bir alternatif olan Borsa İstanbul SWAP Piyasası, sunulan MKT hizmeti ile de katılımcılarına karşı taraf kredi riski almadan işlemlerini gerçekleştirebilecekleri güvenli bir ortam sunmaktadır.

Takasbank, sözü edilen projeler ve yürütülen kapsamlı çalışmalar ile hem İstanbul Finans Merkezi Projesi'ne aktif olarak destek vermekte, hem de yurt içi ve yurt dışı piyasalardaki konumunu güçlendirerek uluslararası takas ve saklama kuruluşları arasında örnek alınan bir kurum olma hedefine ulaşmayı amaçlamaktadır.

PARA VE SERMAYE PİYASALARI ARASINDAKİ KÖPRÜ

TAKASBANK BLOKZİNCİR VİZYONU

Takasbank'ın yerinde Ar-Ge Merkezi olma düşüncesiyle yenilikçi teknolojilerin araştırılması ve finans sektöründe uygulanabilirliğinin incelenmesi hedefiyle çalışmalara 2016 yılında başlanmıştır. Bu çalışmalar kurum içi yayınlanan bir uzmanlık tezi ile somut bir hale gelmiştir. Aynı dönemde Takasbank bünyesinde konuyla ilgili bir çalışma grubu oluşturularak blokzincir gelişmelerinin yakından takip edilmesi amaçlanmıştır. Çalışma grubu, öncelikle blokzincir yaklaşımını kavrayarak, güncel gelişmeleri yakından takip etmeye başlamış ve bu teknolojinin Takasbank'ın finans piyasalarındaki rolüne etkileri üzerine çalışmalar yürütmüştür. Finansal

teknolojilerde öncü olma vizyonuyla yenilikçi teknolojiler sürekli takip edilmiştir. Takasbank, Nisan 2017'de yerinde Ar-Ge Merkezi ünvanına sahip olmuştur. Bu vizyonla yola çıkılarak FinTechHub Takas İstanbul marka çalışması tamamlanmıştır. Blokzincir alanında finansal teknoloji ekosistemini güçlendirmek amacıyla, yerli ve yabancı şirketlerle, konu hakkında çalışan akademisyenlerle iletişime geçilmiştir. Şirket içi çalışanlar akademik çalışmalarını blokzincir konusunda yapmaya teşvik edilmiştir. Finans sektörü düzenleyici ve denetleyici kamu kurumlarıyla istişareler yapılmış, ayrıca kamu araştırma kurumlarıyla destek anlaşmaları yapılmıştır.

Takasbank bünyesinde bankacılık ve sermaye piyasalarının kamu ve özel şirket bazında üst düzey katılımcılarının yoğun ilgi gösterdiği ve alanında bir ilk olan "Finansal Piyasalarda Dijital Dönüşüm ve Blockchain Çalıştayı" Ekim 2017'de düzenlemiştir. Yurtdışı işbirlikleri kapsamında uluslararası faaliyet gösteren büyük bir bankanın da katkılarıyla üst düzey yöneticilere özel bir panel, Takasbank bünyesinde Kasım 2017'de düzenlenmiştir. Bunların dışında birçok konferans, çalıştay ve panele konuşmacı veya sponsor olarak katkılar sağlanmıştır.

Yapılan çalışmalar sonucunda finans sektöründe kullanılabilecek blokzincir platformları belirlenmiş ve her bir platform için farklı iş senaryoları üzerine çalışılarak, platformlar hakkında bilgi birikimi sağlanmıştır. Oluşan bu bilgi birikimiyle blokzincir platformlarının mevcut durumda finansal projelerde kullanılması için bazı şartları sağlaması gerektiği ve farklı bir yaklaşıma ihtiyaç duyulduğu tespit edilmiştir. Bu sebeple sıfır bilgi algoritmaları üzerine çalışmalar başlatılmıştır.

Takasbank; blokzincir altyapısı kullanılarak kurulması planlanan Güvenilir Varlık Transferi Platformu'nun analiz, tasarım, altyapı, sürekli geliştirme ve yönetiminden sorumlu olmayı önümüzdeki dönem hedeflerinden biri olarak belirlemiştir.


BiGA
1 GRAM ALTIN KARŞILIĞI ŞİFRELİ DİJİTAL VARLIK
ENCRYPTED DIGITAL ASSET EQUIVALENT TO 1 GRAM GOLD
İSTANBUL CLEARING, SETTLEMENT AND CUSTODY BANK INC.
İSTANBUL TAKAS VE SAKLAMA BANKASI A.Ş.

PROJENİN KAPSAMI

Projenin temel amacı, fiziki karşılığı Borsa İstanbul kasalarında Takasbank adına mislen saklamaya alınmış, standartları belirli olan kaydi altının blokzincir teknolojisi kullanılarak transfer işlemlerinin yapılabileceği bir altyapı oluşturmaktır.

Mevcut çözümler incelendiğinde, blokzincir teknolojisiyle üretilmiş birçok dijital değerin arkasında fiziksel bir dayanak varlık bulunmadığı görülmektedir. Ayrıca bu dijital varlıkların gerçek bir değere dayanmamasından ötürü henüz regüle edilmemiş piyasalardaki değerlerinde yüksek volatilite gözlemlenmektedir. Blokzincir tabanlı çözümlerde her bir dijital değer için önceden tanımlı bir fiziksel dayanağın var olması sayesinde, kendine ait ayrıca bir değeri olmayan kaydi bir varlığın transferi sağlanmış olacaktır. Böylece bu dijital varlığa olan güven sağlanacak ve oluşması muhtemel spekülasyonların da önüne geçilecektir.

Bu amaçla konusunda dünyada bir ilk olan Altın Transfer Sistemiyle entegre çalışan bu platform üzerinde oluşturulacak ilk varlığın ismi BiGA'dır.

Proje kapsamında, fiziki altınların kasalarda saklanması ve kaydileştirilmesi süreçlerini yöneten ATS (Altın Transfer Sistemi) ile entegrasyon sağlanmış ve kaydi altınların dijitalize edilerek BiGA'ya dönüştürülmesi ve BiGA'dan kaydi altına çevrilmesi işlemleri mümkün kılınmıştır. Bu sayede uçtan uca fiziki varlık ile dijitalize edilmiş varlık arasında bütün bir yapı kurulmuştur. Geliştirilen blokzincir altyapısıyla, dijital varlıkların transferi, mutabakatı, raporlanması sağlanmıştır. Bu altyapı, diğer değerli varlıkların da dijitalleştirilerek transferine izin veren, modüler bir yapıda tasarlanmıştır.

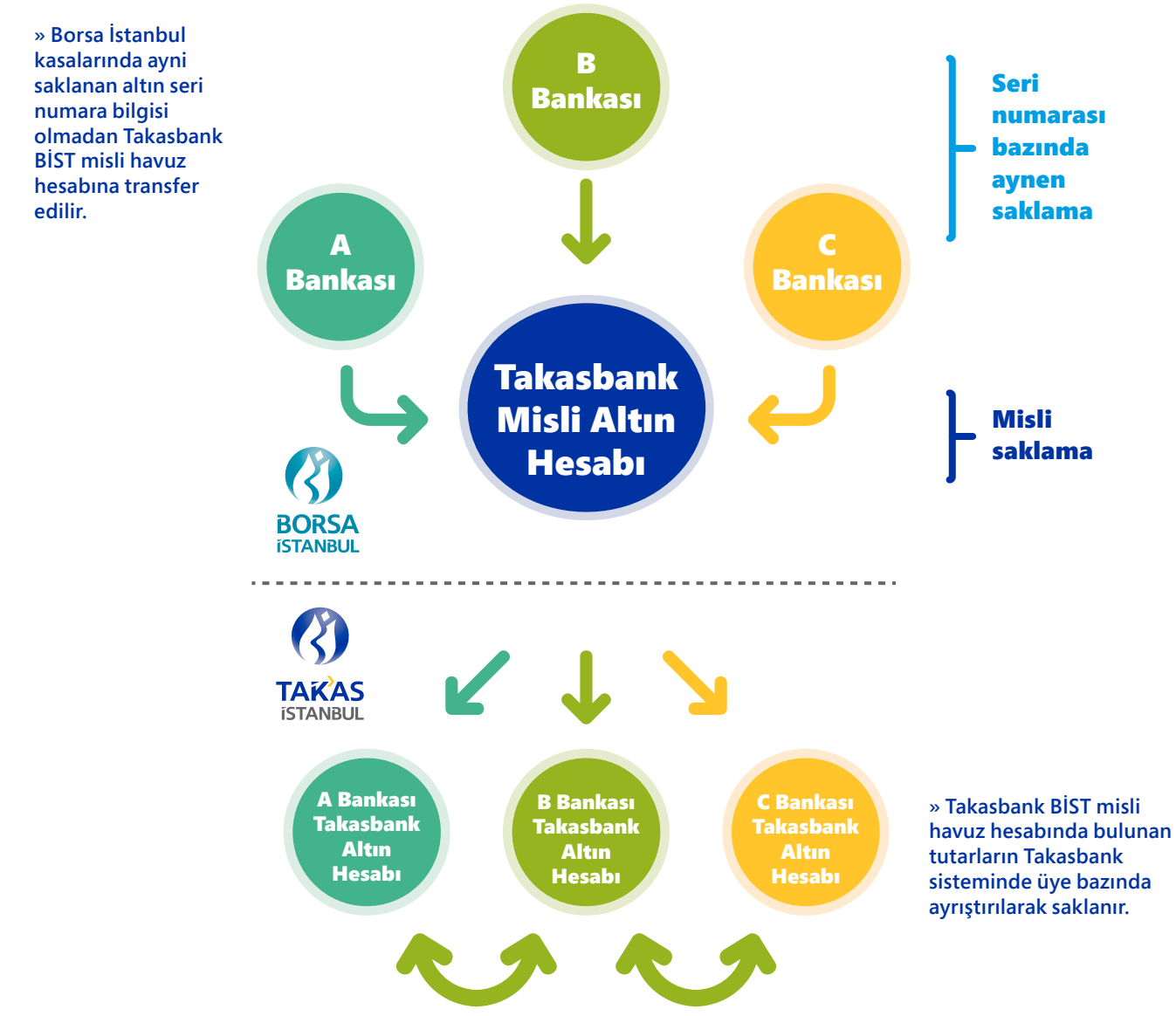
Genel İşleyiş

Bu sistemde dijital varlık için ihraç, itfa ve transfer olmak üzere 3 ana kabiliyet sunulmaktadır. Bunların yanı sıra blokzincir sistemi ile ATS arasında entegrasyon, mutabakat yetkinlikleri, izleme ve raporlama gibi ek kabiliyetler de sağlanmaktadır.

Altın Transfer Sistemi (ATS) Projesi

Takasbank tarafından 16 Temmuz 2018 tarihinde hizmeti verilmeye başlanan "Altın Transfer Sistemi" ile bankalarda tutulan altın bakiyelerinin bankalar arası kaydi olarak transferine olanak sağlanmıştır. Böylelikle altın tasarruflarının ekonomik sistemde yeri sağlamlaşmış ve rekabet ortamının güçlendiği piyasada finansal araç olarak kullanılmasının önü açılmıştır.

Altın Transfer Sistemi, karşılığı Borsa İstanbul kasalarında tutulan fiziki altınların kaydileştirilmesi ve yurtiçinde Takasbank nezdinde bankaların hesabında tutulması, hesaplar arasında elektronik olarak transferinin yapılması işlemlerini gerçekleştirmeyi kapsamaktadır. Sistem sayesinde bireysel ve tüzel kişiler bankalardaki altın hesaplarında yer alan altın tasarruflarını birbirleri arasında diğer para birimlerinde olduğu gibi transfer edebilmektedirler. Kısaca altının EFT'si bu sistemle gerçekleştirilmiştir.

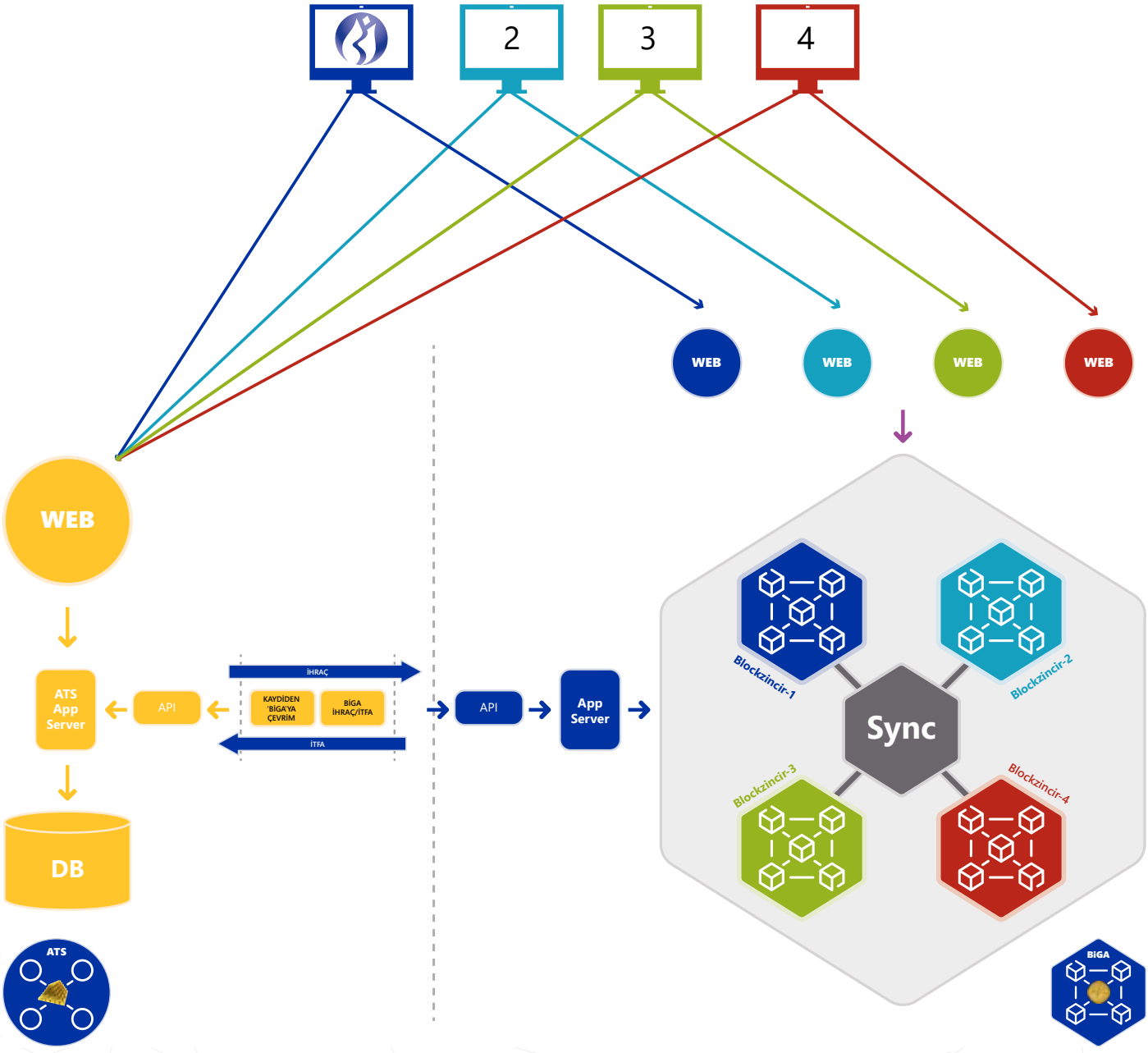


Takasbank Kaydi Altın Saklama ve Transfer Sistemi

ATS-BiGA Entegrasyonu

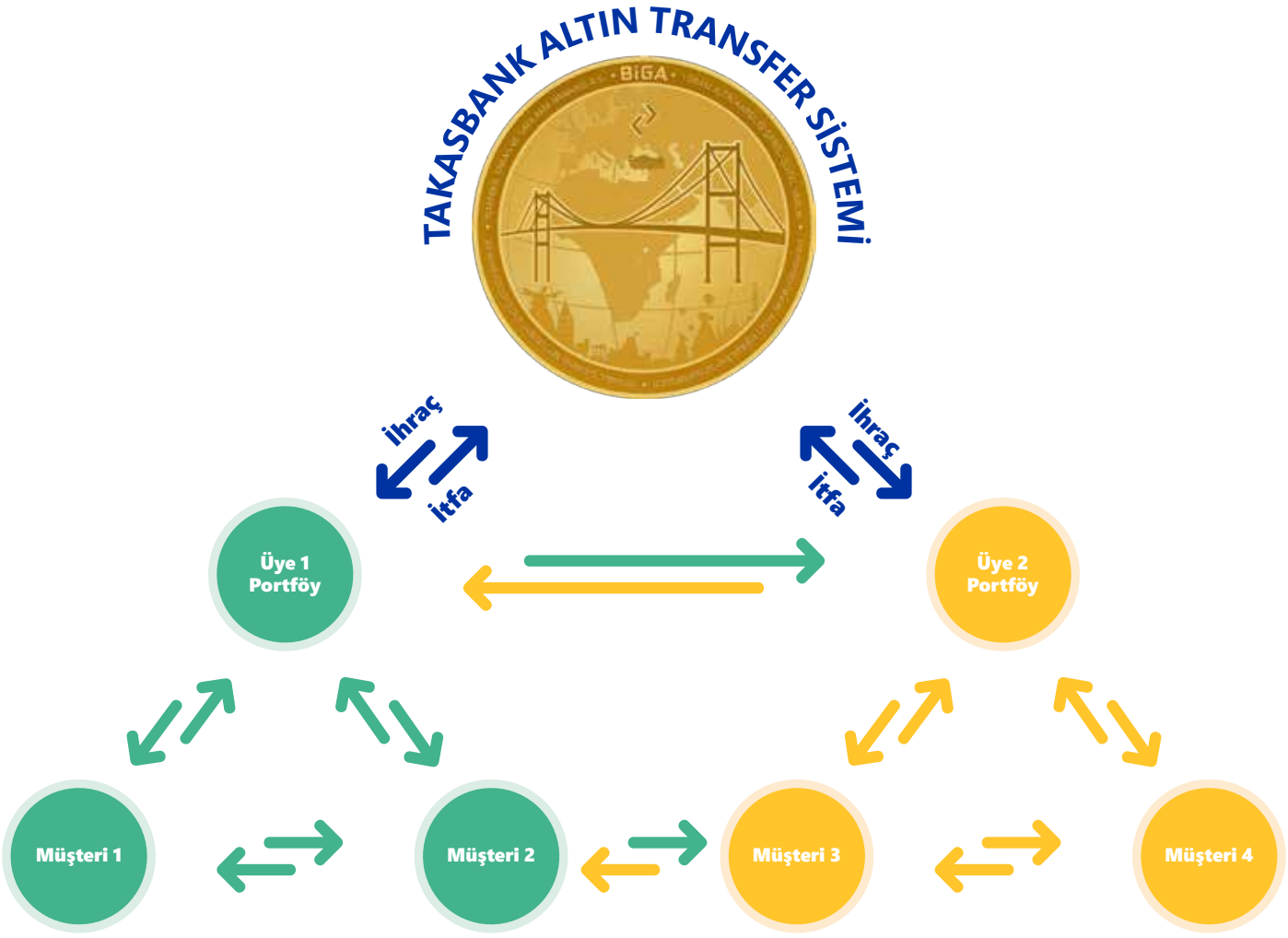
ATS Projesiyle Borsa İstanbul kasalarında fiziki olarak saklanan altınlar BiGA'ya dönüştürülür. Böylece her bir dijital varlık fiziki dayanağına istinaden üretilir. Dijital varlık ile fiziki varlık arasında dönüşüm ve mutabakat yapılmaktadır.

Son kullanıcılar işlemlerini bir banka aracılığıyla yapabilmektedir. Böylelikle kullanıcılar diledikleri zaman BiGA varlıklarını banka (node) üzerinden bozdurarak kaydi altına dönüştürebilir.



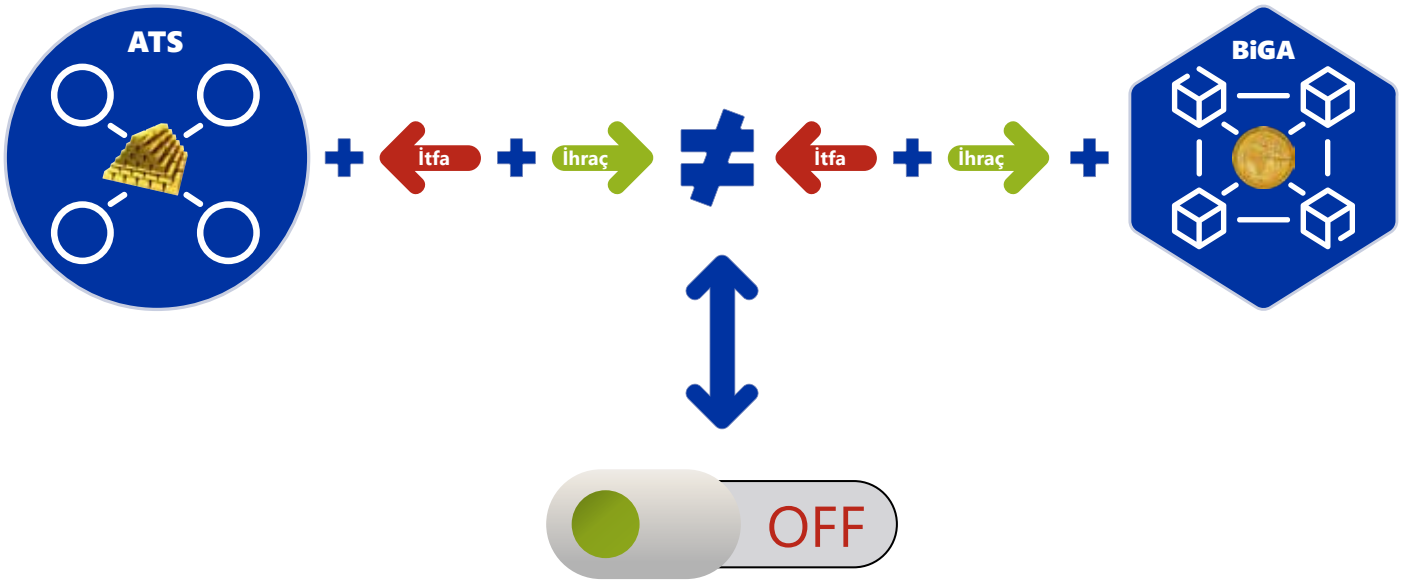
Transfer

Kullanıcı oluşturduğu BiGA varlıklarıyla 7/24 işlem yapabilir. Sisteme katılım sağlayan kurumlar, blokzincir ağı üzerinde birer düğüm (node) olarak tanımlanır. Bu düğümler blokzincir ağı üzerindeki verinin bir kopyasını sürekli olarak güncel bir biçimde bünyelerinde barındırmaktadırlar. Transfer işlemlerinde transfere konu olan BiGA miktarları şifreli olarak gönderilir ve bu değerler blokzincir üzerinde şifreli halde tutulur. Bu sebeple transfere taraf olan kullanıcılar ve regülatör kurum haricinde transfer edilen miktarı kimse bilemez fakat işlemin doğruluğunu onaylayabilir. Onaylanan transfer işlemleri sonucu blokzinciri üzerindeki ilgili şifreli bakiyeler güncellenir. Bu doğrulama konusu dokümanın teknik bölümünde ayrıca detaylandırılmaktadır.



Mutabakat

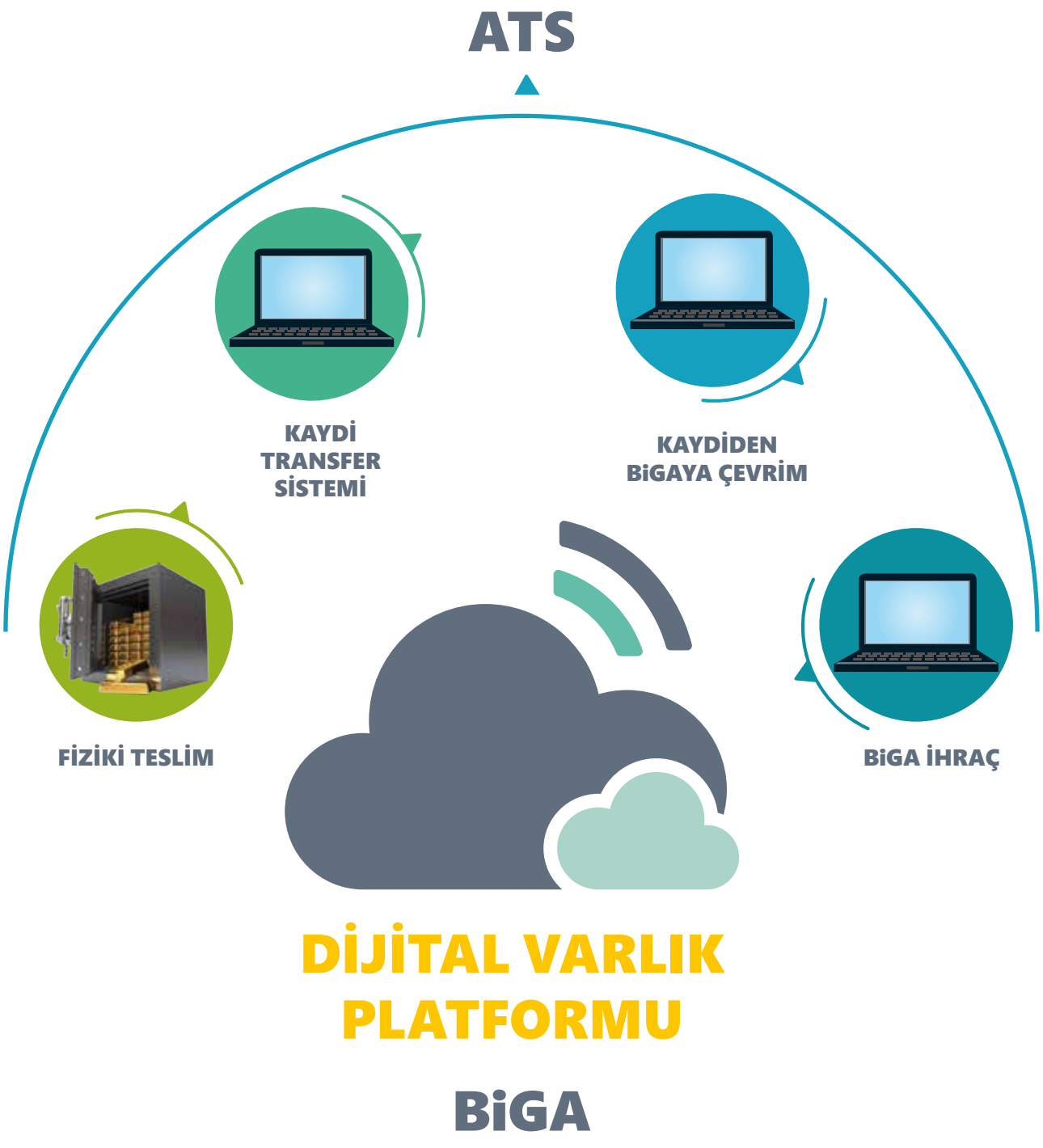
Sistemin tutarlı ve hatasız çalışmasını garanti altına almak için düzenli kontroller yapılmaktadır. Herhangi bir birim zamanda ATS üzerinde bulunan varlıklar ile blokzincir üzerinde bulunan varlıkların toplamının fiziksel kasalarda saklanan altın miktarının toplamına eşit olması bu kontrollerin temel amacını oluşturmaktadır. Herhangi bir olağandışı durum sebebiyle bu tutarlılık sağlanmazsa ihraç, itfa ve transfer işlemleri otomatik olarak durdurulmaktadır. İlgili hata tespit edilip düzeltildikten sonra sistem tekrar aktif hale getirilmektedir.



Fiziksel Karşılığa Sahip Blokzincir Tabanlı Yeni Nesil Transfer Sistemi

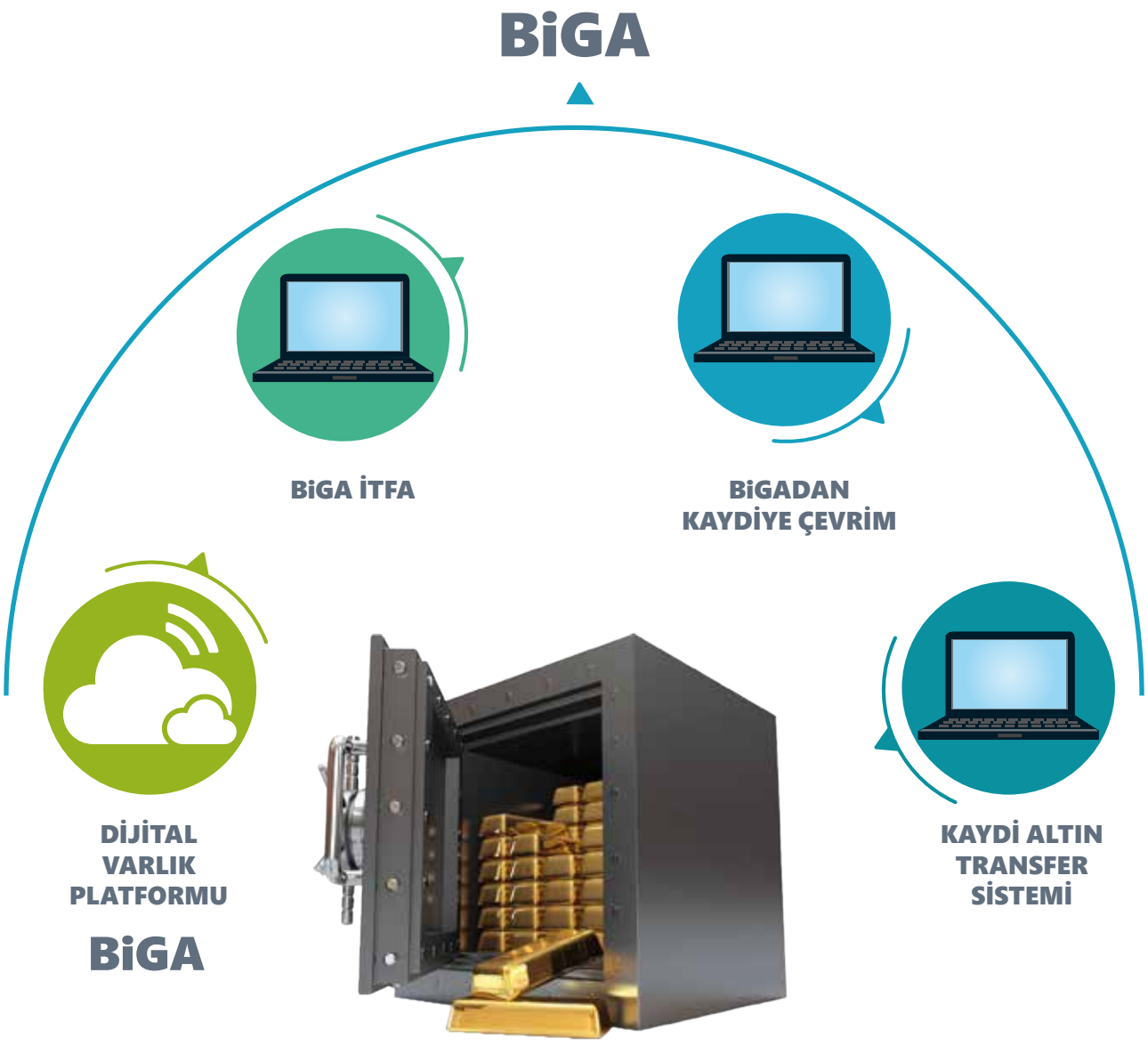
İhraç

Takasbank Altın Transfer Sistemine üye olan kullanıcı, fiziki olarak BİST kasalarında saklaması yapılan 995/1000 saflıkta LBMA içi şartlarına uygun altınlarını kaydileştirir. Bir Gram kaydileşmiş altına karşılık olarak bir BiGA ihracını Altına Dayalı Dijital Varlık Platformu üzerindeki hesaplarına aktarır. İhraç işlemleri ATS'nin çalışma kuralları çerçevesinde belirlenen zaman aralığında gerçekleştirilir.

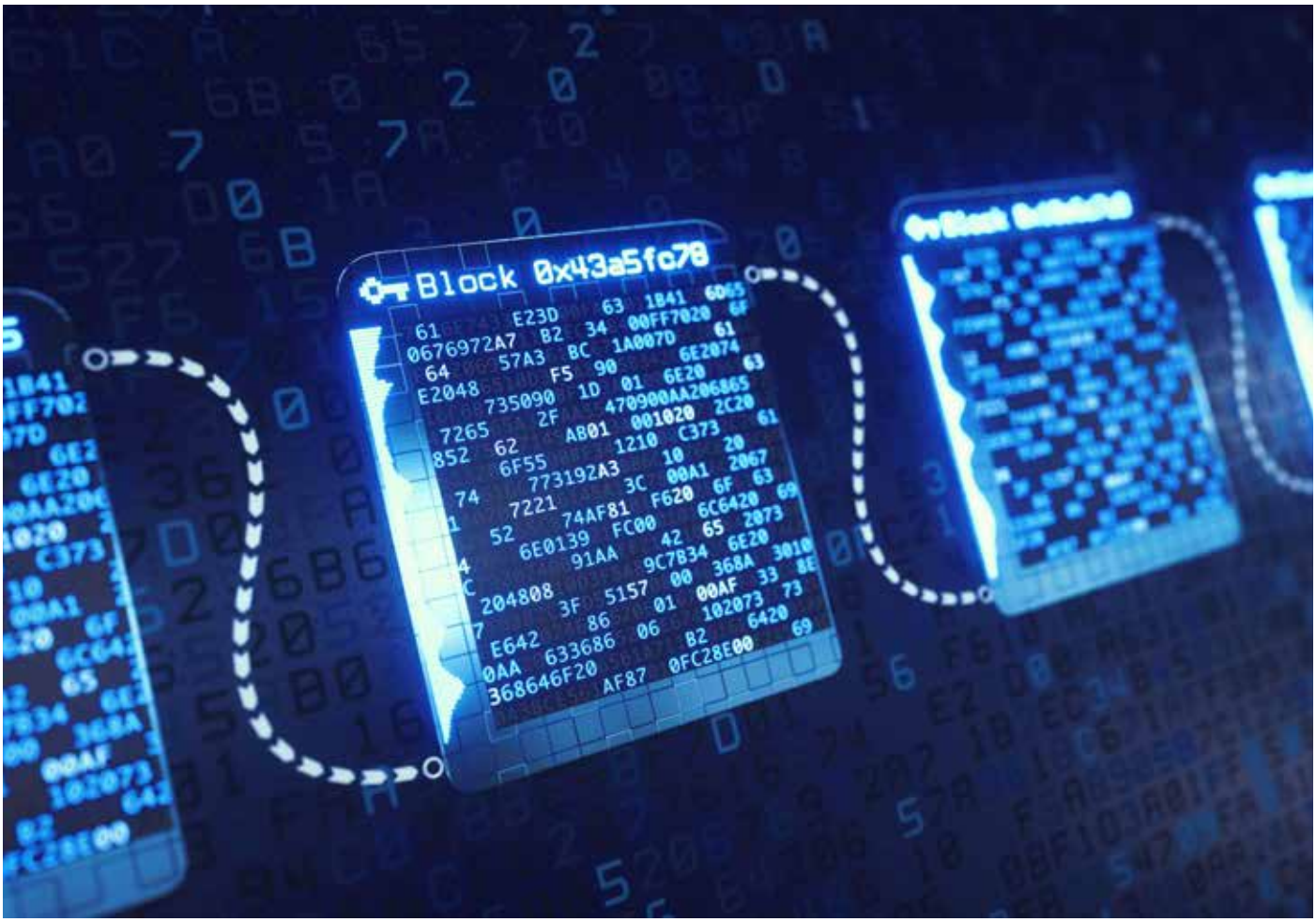


İtfa

Kullanıcı, hesaplarında bulunan BiGA'ları kaydi altına dönüştürerek sistemden çıkışını sağlar. Altına Dayalı Dijital Varlık Platformundaki bir BiGA'yı bir Gram kaydi altına dönüştürerek ATS üzerindeki hesaplarına aktarır. İtfa işlemleri ATS'nin çalışma kuralları çerçevesinde belirlenen zaman aralığında gerçekleştirilir.



FİZİKİ ÇIKIŞ



PROJENİN TEKNİK ARKA PLANI

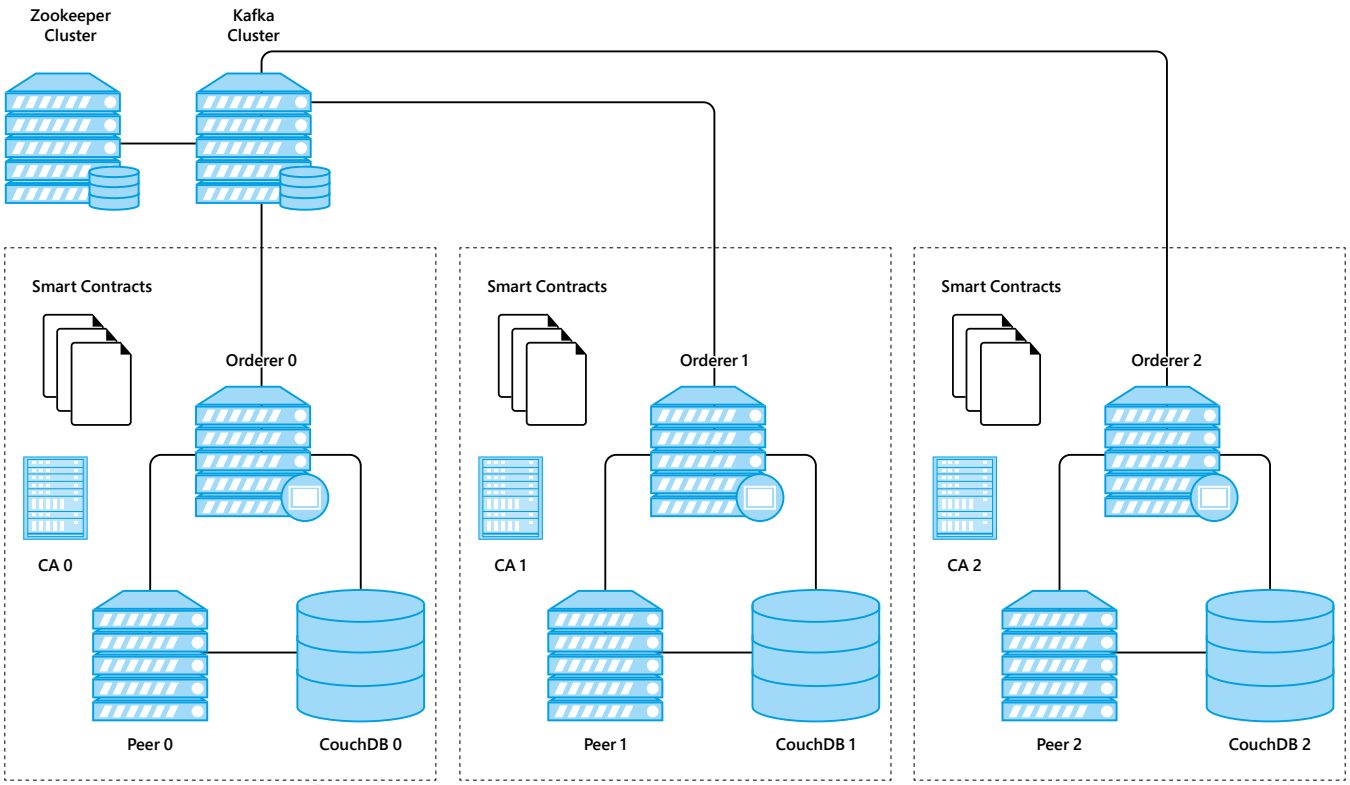
Projenin teknik çalışmaları 2017 yılının son çeyreğinde başlamıştır. Öncelikle Hyperledger Fabric 1.0 platformu ile çalışmalara başlanmıştır. Bu aşamada hem blokzincir teknik çalışmalara giriş hem de finansal teknoloji ekosistemini beslemek amacıyla bu alanda örnek çalışmaları bulunan bir fintek firması ile iş birliğine gidilmiştir. Yine çalışmalara başlanırken Zero Knowledge (Sıfır Bilgi) ihtiyaçları göz önünde bulundurularak TÜBİTAK BİLGEM Blokzincir Araştırma Laboratuvarı ile iş birliği yapılmıştır. Böylece oluşturulan ekosistem ile projenin teknik temelleri farklı disiplinlerin uzmanlıklarının bir araya gelmesi ile sağlanmıştır. Proje ilerleyen safhalarda tamamen Takasbank personelinin çalışmalarıyla devam etmiştir. Hyperledger Fabric ile başlayan geliştirmeler ikinci aşamada Quorum platformuyla devam etmiştir. Bu çalışmalarda sadece söz konusu blokzincir platformları üzerinde çalışılmamıştır. Docker gibi tamamlayıcı ve kolaylaştırıcı yeni nesil teknolojiler bu proje kapsamında sıklıkla kullanılmıştır.

Bu bölümde projede kullanılan teknik bileşenler ve edinilen tecrübelere yönelik bilgiler verilmektedir.

Hyperledger

Hyperledger, Aralık 2015'de Linux Vakfı tarafından desteklenen açık kaynak kodlu bir platformdur. İzin gerektiren ve akıllı kontratlarla (chaincode) işlemlerin yapıldığı ve bir kripto para birimine sahip olmayan ilk platformdur. Bu yönüyle kurumsal araştırma projelerinde hızla karşılık bulmuştur. Hyperledger servis katmanı üç ana mantıksal kategori içerisinde değerlendirilmektedir. Bunlar sırasıyla üyelik servisleri, blokzincir servisleri ve chaincode servisleridir.

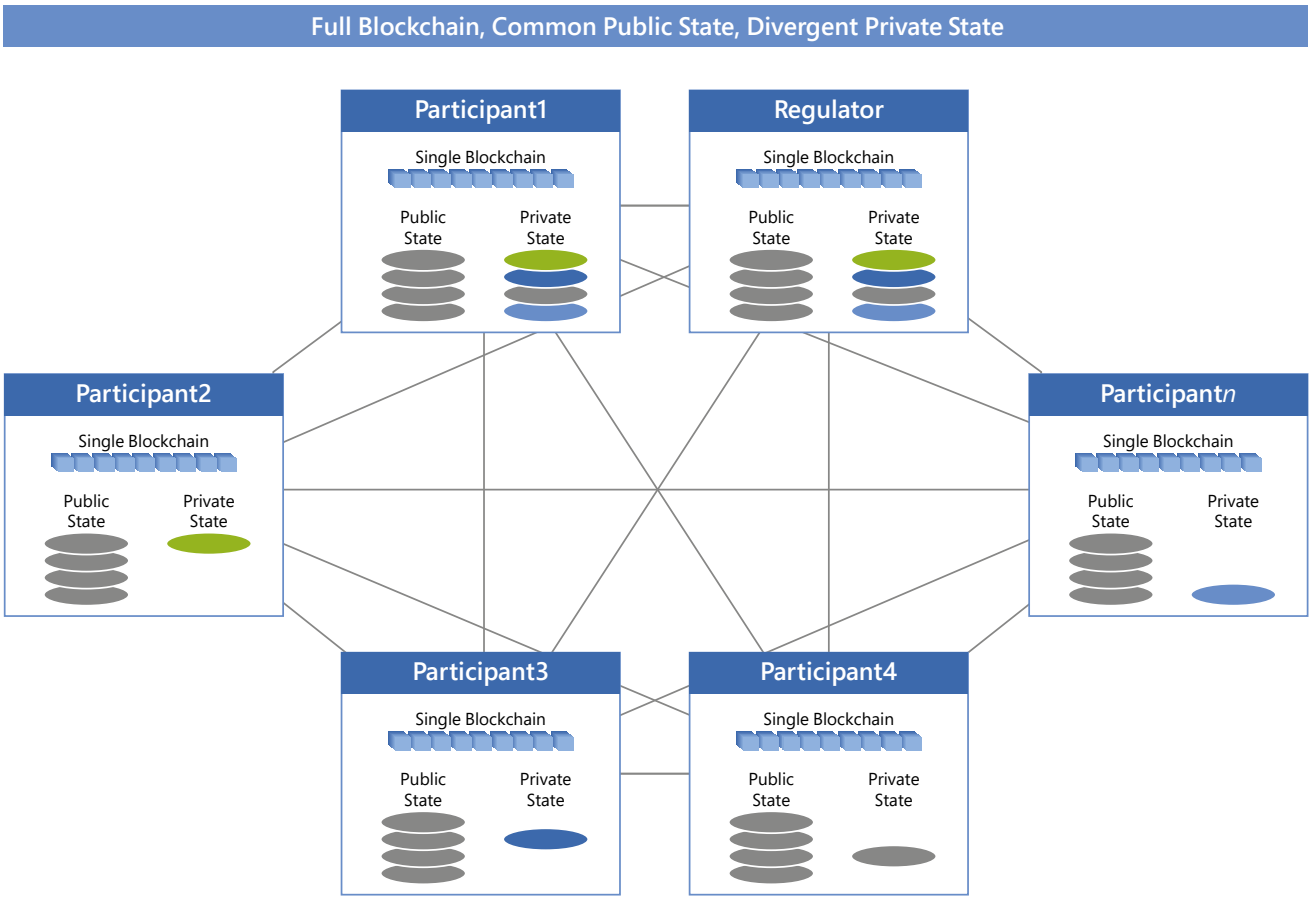
Üyelik servisleri; kimlik, gizlilik gibi konularda hizmet verirken; blokzincir servisleri sahip olduğu P2P protokolü ile birlikte içerdiği blokzincir ve mutabakat yapısını yönetmektedir. Chaincode servisleri, Hyperledger mimarisi içerisinde akıllı sözleşmelerin yönetim ve işletimini sağlamaktadır. Ayrıca alt seviyede bulunan bir haberleşme katmanı ile birlikte servis katmanı içerisinde olay güdümlü (event driven) çift yönlü etkileşim sağlanabilmektedir. Her ne kadar bu kavramlar ve yapılar ilk etapta oldukça karışık gelse de Hyperledger iş dünyasının ihtiyaç duyduğu temel unsurları bünyesinde barındırdığı için pek çok Blokzincir Ar-Ge projesinde test edilmektedir. Hyperledger tek bir blokzincir çerçevesi oluşturmak yerine kendi altında beş farklı projeyi desteklemektedir. Bu projelerden öne çıkanı ise Fabric projesidir. Modüler mimarisi sayesinde ihtiyaca göre modüller tak-çalıştır felsefesiyle değiştirilebilmektedir. Ayrıca Iroha, Sawtooth, Burrow ve Indy Hyperledger projeleri de bulunmaktadır.



Kaynak: https://medium.com/@abhinav.garg_90821/hyperledger-fabric-multi-orgs-multi-nodes-with-kafka-zookeeper-and-swarm-cluster-946a94dade0f

Quorum

Ethereum'un finansal piyasalarda kullanılmasına yönelik olarak yapısının değiştirilmesi sonucunda 2015 yılında J.P. Morgan tarafından piyasaya sürülmüş açık kaynak kodlu bir platformdur. Bu platform iş süreçlerini ve yasal kısıtlamaların aşılmasını kolaylaştırırken temelinde güven, hesap verebilirlik ve şeffaflık barındıran yeni nesil işlem uygulamaları üretmek için kullanılmaktadır. Aynı zamanda Ethereum altyapısına sahip olduğundan bu platformun sağladığı avantajları da içinde barındırmaktadır. İzinli bir yapıda olmasına rağmen kullanmış olduğu konsensus algoritmasının hızlı ve yüksek doğrulukta çalışması, şeffaf ve gizli işlemlere olanak sağlaması en önemli özellikleri olarak görülmektedir. Ethereum altyapısında yapılacak geliştirmeler Quorum altyapısına da kolaylıkla yansıtılmaktadır. Bu platform kullanılarak oluşturulan ağ oldukça hızlı kurulabilmektedir.



Kaynak: Quorumwhitepapper-https://github.com/jpmorganchase/quorumdocs/blob/master/Quorum%20Whitepaper%20v0.1.pdf

Sıfır Bilgi İspatı (Zero Knowledge Proof)

Sıfır Bilgi İspatı, kriptoloji alanında en yaygın sorunlardan birisi olan ispat problemlerini çözmek için üretilen bir modeldir. "Bir bilgiyi bildiğimi, karşı tarafa bu bilgiyi vermeden nasıl bildiğimi ispat ederim?" mottosuyla yola çıkılarak üretilmiş bir ispat yöntemidir. Bilgiyi ispat etmek için arka planda kriptolojik fonksiyonlar çalışır ve bunların varsayımları kullanılır.

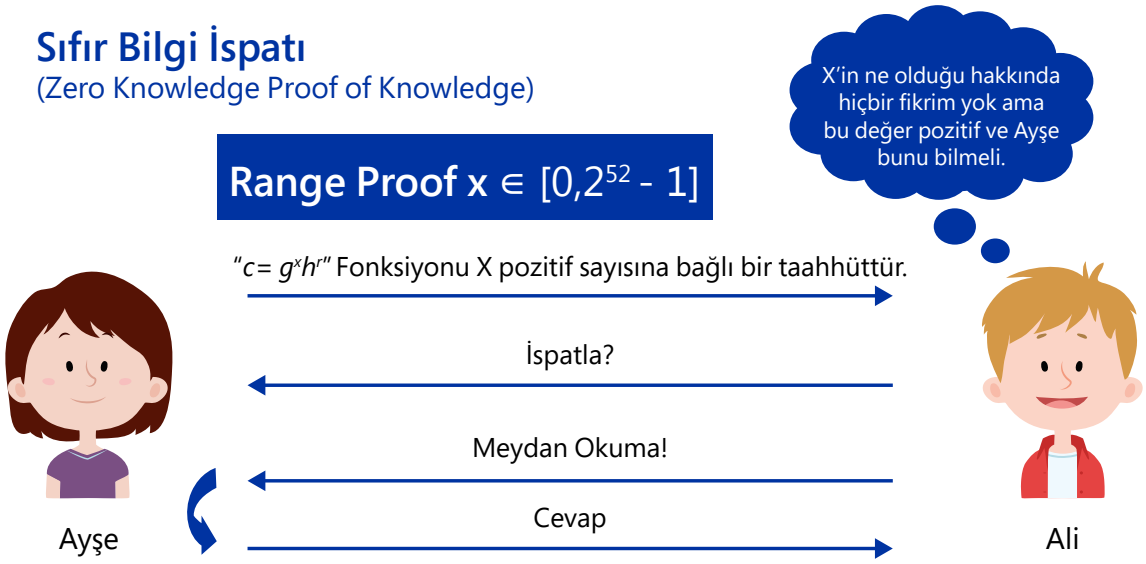
Sıfır bilgi kanıtı şu üç özelliği sağlamalıdır:

- **Tamlık:** Eğer verilen kanıt doğru ve eksiksiz ise alıcı, vericinin bilgiye sahip olduğundan emin olur.
- **Doğruluk:** Eğer kanıt yanlış değil ise sahtekarlık yapmadan verici, alıcıyı ikna eder.
- **Sır Vermemek:** Eğer ifade doğru ise alıcı bunu anlayacaktır. Alıcıya verilen örnek ile vericinin bildiği ispat edilir.

Tamlık ve Doğruluk özellikleri genel anlamda alıcı ile iletişime geçme yöntemidir. Sır vermemek ise kanıtlama yöntemi olarak belirtilebilir.

Sıfır bilgi ispatı matematiksel anlamda bir ispatlama yöntemi değildir. Bu yöntemde bilgi manipüle edilerek alıcıya ispatlama amacıyla çalışır.

Blokzincir teknolojilerinin özellikle finansal alanlarda mevcut haliyle kullanımı regülasyon gerekliliklerinden ötürü oldukça zor olarak değerlendirilmektedir. Verinin bütün düğümlerde sürekli olarak güncel tutulması ve gelen her işlemin düğümler tarafından onaylanıyor olması yapılan işlemlerin kimin tarafından yapıldığı ve miktar bilgilerinin bütün düğümlerde açık olarak bulunması, bu teknolojinin finans alanında kullanımı ve regülasyon gereklerinin sağlanması gibi konularda ciddi engeller teşkil ettiği değerlendirilmektedir. Bu konuların çözümü için Sıfır Bilgi İspatı modeli ile çalışmalar yapılması gerekmektedir.

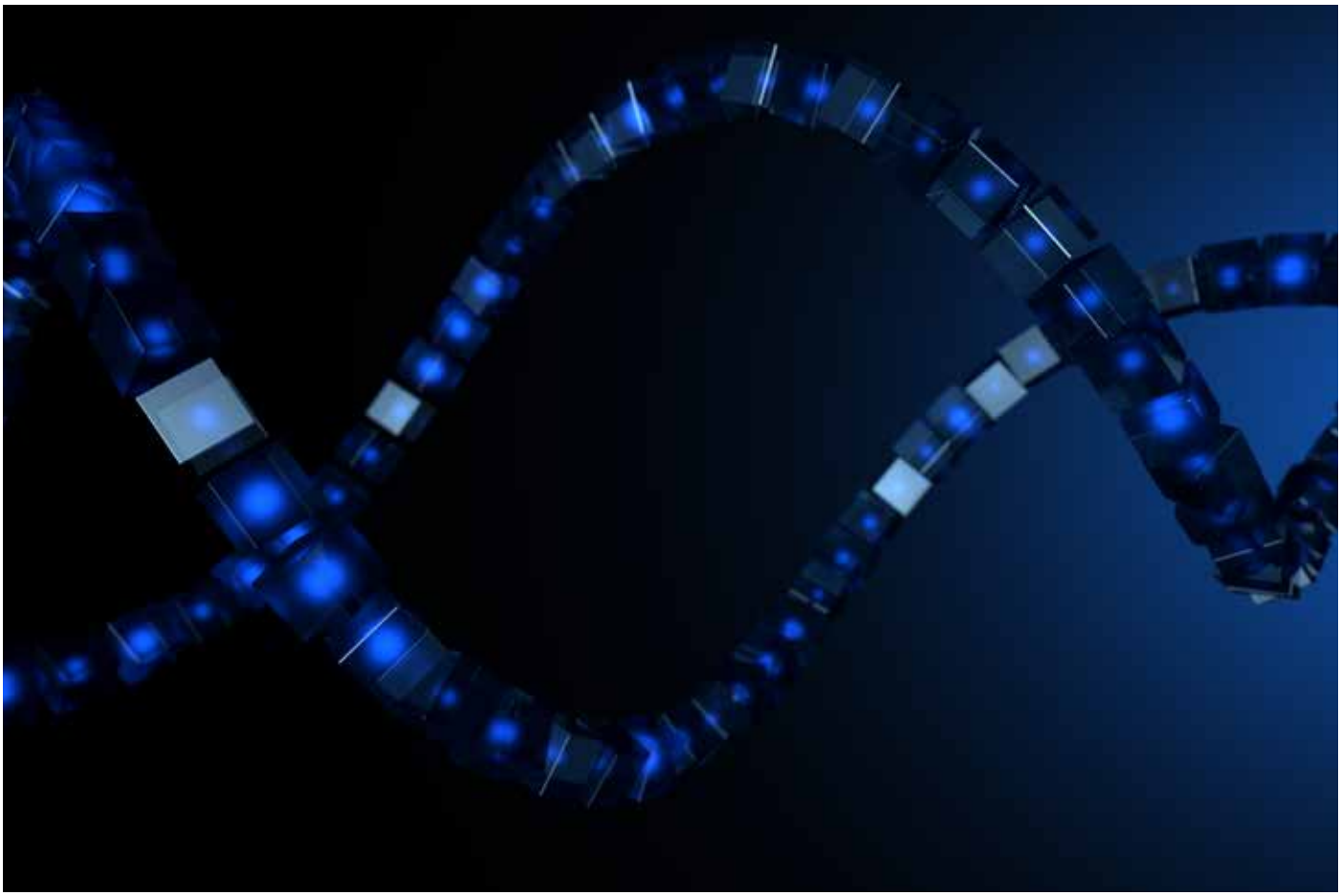


Kaynak: https://hackernoon.com/bulletproofs-the-new-kid-in-blockchain-security-land-e730fc0efe14

Kullanılan Diğer Teknolojiler

Projede blokzincir altyapıları dışında yazılım geliştirme süreçlerini kolaylaştıran yenilikçi teknolojiler kullanılmıştır. Bu teknolojiler aşağıdaki gibidir:

- **Programlama dilleri:** Java, Go, JavaScript, AngularJS, Solidity
- **Destekleyici çözümler:** Quorum Maker
- **Container teknolojisi:** Docker
- **İşletim sistemi:** Linux
- **Uygulama sunucusu:** WildFly
- **Veritabanı:** PostgreSQL, CouchDB



FONKSİYONEL TASARIM

BiGA Projesinde farklı platform ve teknolojiler için çeşitli alternatifler bulunmasına karşın yukarıda belirtilen yetkinlikleri nedeniyle Hyperledger Fabric ve Quorum platformları üzerinde çalışmalar yapılmıştır. Bu kapsamda kapalı devre bir sistem ve sadece platform yöneticisinin yetki vereceği düğümlerin sisteme dahil olabileceği bir yapı planlandığı için izin gerektiren yapıda platformlar seçilmiştir (permissoned blockchain).

İzin gerektiren blokzincirlerde sadece belirlenen düğümler belirli haklarla blok oluşturabilir ve mutabakata katılabilir. İzin gerektirmeyen blokzincirlerde ise tüm düğümler mutabakata ve blok oluşturmaya katkı sağlar. 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 düğümlerin erişimine açıktır. BiGA, izin gerektiren (permissoned) ve özel (private) kategorisinde yer alan bir blokzincir ağına sahiptir.

Projede uygulamada kullanılmak üzere seçilen mevcut blokzincir teknolojilerinin sağladığı altyapılar finansal enstrümanlarda kullanılmak

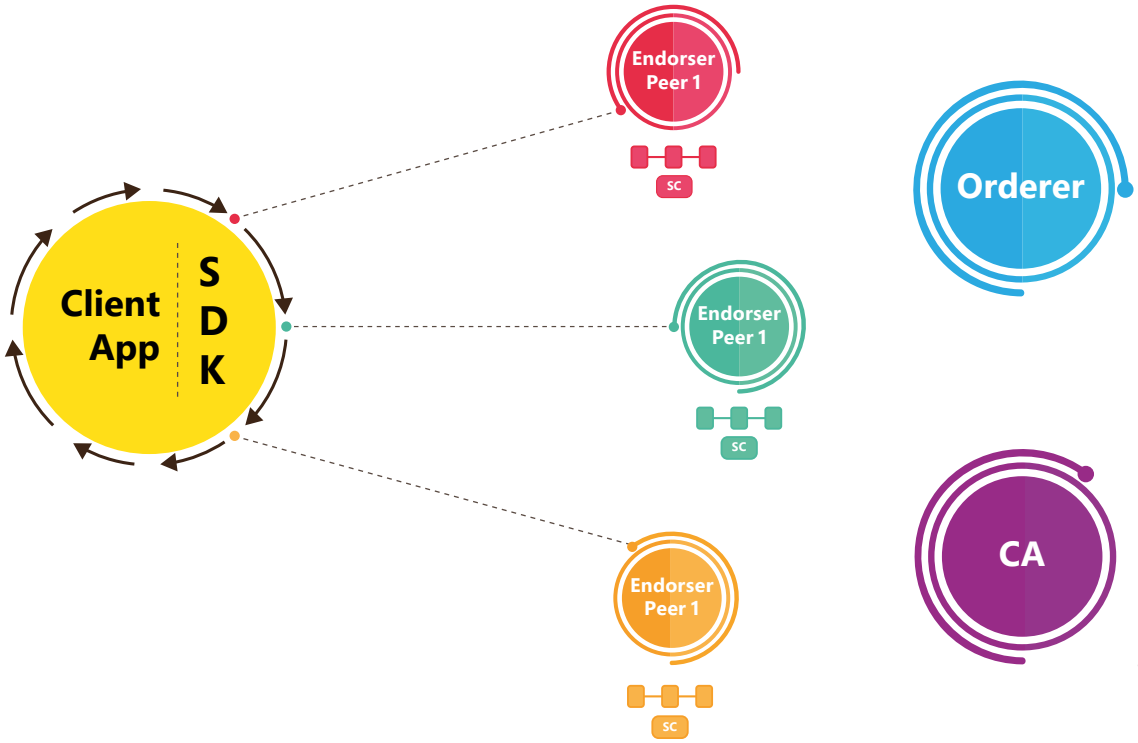
istendiğinde 2 önemli kısıt ön plana çıkmaktadır. Bu kısıtlar, bütün işlemlerin görünür olması durumunda işlem yapan taraflar dışında diğer düğümlerin de bütün işlemleri görebilmesi nedeniyle oluşacak mahremiyet problemi ve işlemlerin kapalı olması durumunda işlemlerin bir otorite kurum tarafından kontrol ve denetiminin sağlanamaması problemi olarak tanımlanmaktadır.

BiGA Projesi bu 2 kısıta da çözüm üreten bir tasarım sunmaktadır. Bu tasarım işlem yapan düğümlerin ilgili işlemleri görebildiği, sistemdeki diğer düğümlerin ise hassas ve kritik verileri göremediği halde yapılan işlemin ve transferin doğruluğunu onayladığı, aynı zamanda otorite düğümün ise istediği zaman istediği işlemleri izleyebildiği çözümü kapsamaktadır. Bu mimari tasarımın teknik olarak sağlanması, mevcut blokzincir platformlarına sıfır bilgi ispat algoritmalarının eklenmesi yöntemini içermektedir.

Hyperledger platformu ile BiGA

Hyperledger platformu ile tasarlanan BiGA Projesinde blokzincir ağında bulunan düğümlerin her biri onaylayıcı (endorser) olarak kurgulanmıştır. BiGA'daki her bir düğümün kendi uygulama sunucusu, veri tabanı ve ilgili servisleri tanımlanmıştır.

BiGA blokzincir yapısında ayrıca bir cüzdan bulunmamaktadır. Kullanıcıların hesap yapıları ve onlarla ilgili işlemler, sunucu üzerinde bulunan REST servisler vasıtasıyla, blokzincir üzerinde ilgili düğüm tarafından gerçekleştirilmektedir. Durum bilgilerini saklamak için veritabanı olarak CouchDB kullanılmaktadır. Hyperledger Fabric ile oluşturulan blokzincir ağında varsayılan olarak en az bir tane kanal (channel) olmaktadır. Bu yapılarla birlikte bir organizasyon, bir CA (Certificate Authority) ve bir orderer kullanılmaktadır.



BiGA için kurgulanan yapıların genel görünümü BiGA Hyperledger Tasarımında belirtilmiştir. Oluşturulan yapıda tek organizasyon ve tek kanal yapısı kullanılmıştır. BiGA Projesi Hyperledger Platformu çalışmaları akıllı sözleşmeler ile geliştirilmiştir. Akıllı sözleşmeler kullanılmasıyla altyapının üzerinde başka değerler tanımlanması sağlanmıştır. Hyperledger Fabric üzerindeki akıllı sözleşmeler Go ile geliştirilmiştir.

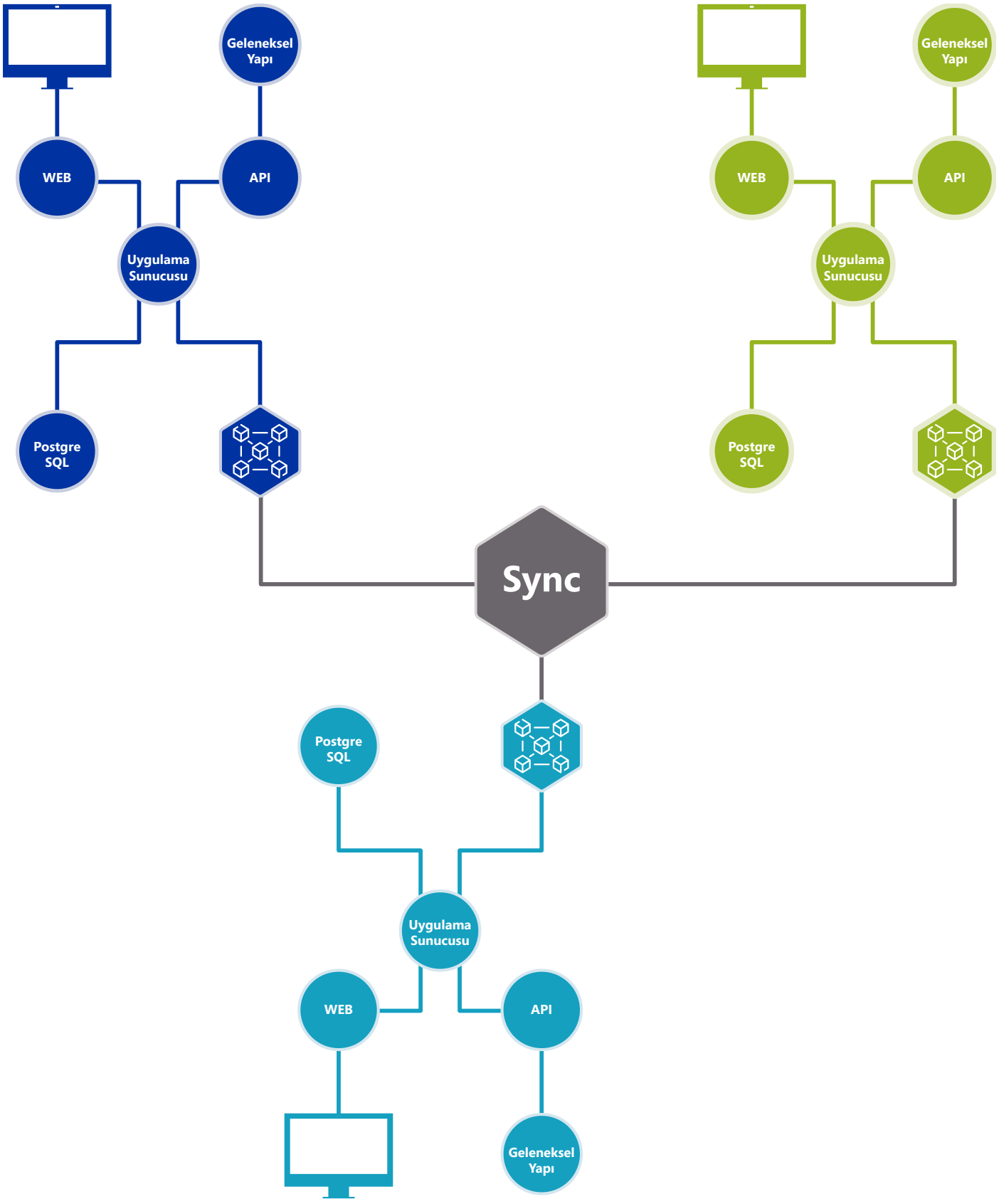
Her düğüm için ayrı bir sunucu kurulmuş ve farklı ortamlarda çalışacak şekilde konfigüre edilmiştir. Düğümler arasında blokzincir ağı dışında herhangi bir entegrasyon yapılmamıştır. Böylelikle gerçek ağ ortamı oluşması sağlanmıştır.

Proje kapalı devre bir kavram kanıtlama projesi olduğu için geliştirme ve test süresini daha etkin kullanmak adına altyapı olarak bulut ortamı tercih edilmiştir. Aynı zamanda blokzincir ağında hiçbir şekilde kişisel veri saklanmamamıştır.

Projenin Hyperledger ile geliştirilmesi aşamasında aşağıdaki işlemler sırasıyla yapılmıştır:

- **Fabric Konfigürasyonu:** Organizasyon, eşler, kanal gibi tanımlamaların yapılması, sertifikaların üretilmesi, docker imajlarının oluşturulması,
- **Akıllı kontrat:** Go dilinde ilgili geliştirmenin yapılması,
- **Chaincode Deploy:** Sunuculara chaincode ve kanal properties yüklemelerinin yapılması,
- Fabric SDK ile istemci java uygulamasının oluşturulması,
- **Kurulum scriptleri:** Cloudformation scriptlerinin düzenlenmesi,
- **API Layer:** Rest API için servis katmanı oluşturulması,
- Kullanım, Raporlama ve İzleme fonksiyonları için web tabanlı geliştirmelerinin yapılması.

BiGA alternatif finansal araçların tek bir blokzincir altyapısıyla yaygınlaşabileceğini ispatlamıştır.

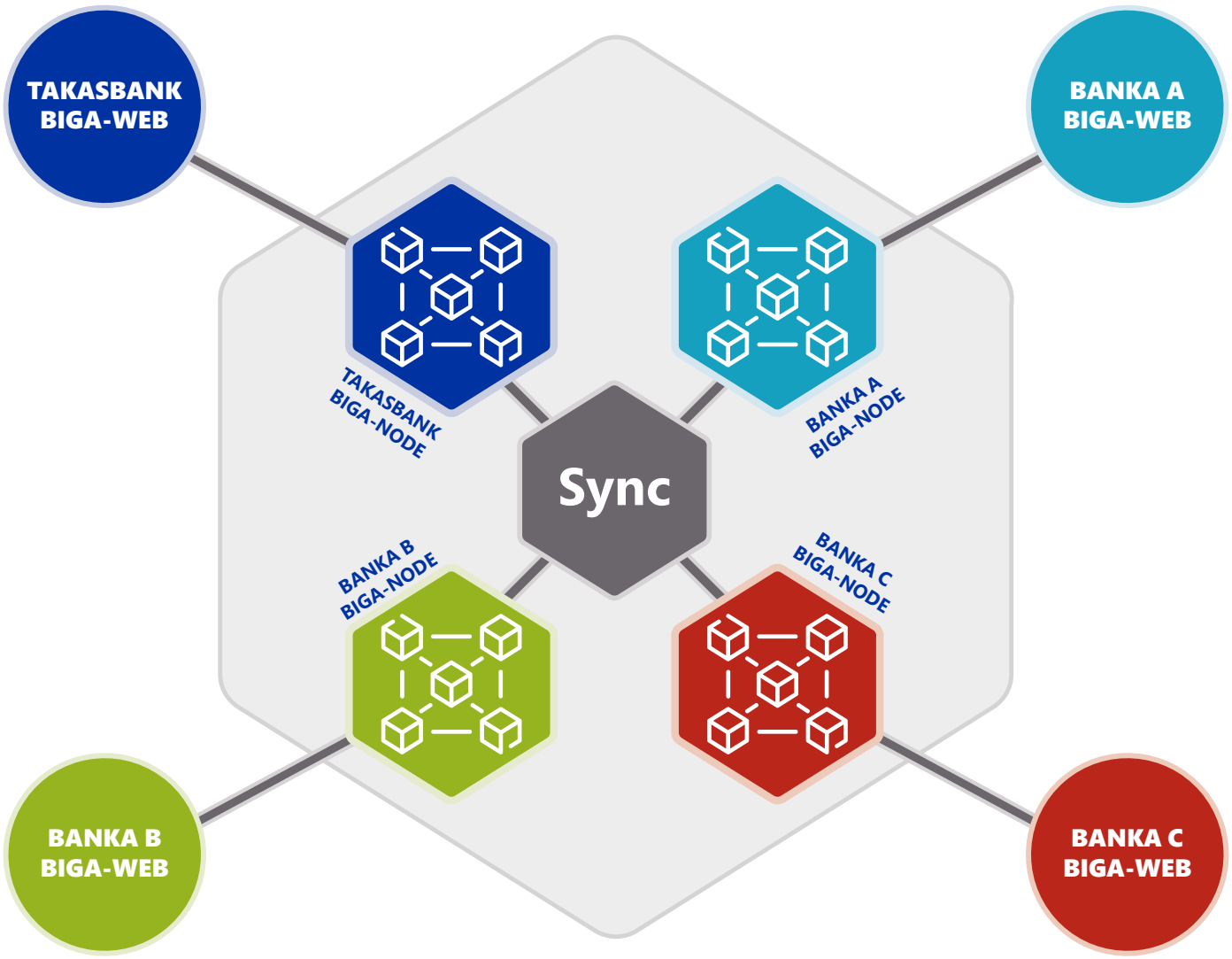


BiGA Hyperledger Tasarımı

Quorum platformu ile BiGA

BiGA Projesi tasarımı yapılırken kullanılabilecek bir diğer blokzincir altyapısı da Ethereum olarak ön plana çıkmıştır. Yapılan incelemelerde yalın ethereum altyapısının kurumsal kullanım için yeterli olmadığı, ve halka açık (public) kullanıma daha uygun olduğu gözlemlenmiştir. Bu bağlamda Ethereum blokzincir altyapısının kurumsal uygulamalar için özelleştirilmiş versiyonu olan ve J.P.Morgan tarafından geliştirilen açık kaynak kodlu, izinli (permissioned) blokzincir altyapısı olan Quorum'un kullanılması uygun görülmüştür. BiGA Projesi için gerekli iş mantığı akıllı kontratlar yardımı ile gerçeklenmiştir. Ethereum tabanlı akıllı kontratların yazılabilmesi için en popüler programlama dili olan Solidity kullanılmıştır. Bu akıllı kontratlar ile iletişime geçmek için Java tabanlı bir entegrasyon uygulaması geliştirilmiş ve bu uygulamada Web3j kütüphanesi kullanılmıştır. Buna ek olarak Quorum blokzincir ağını hızlı

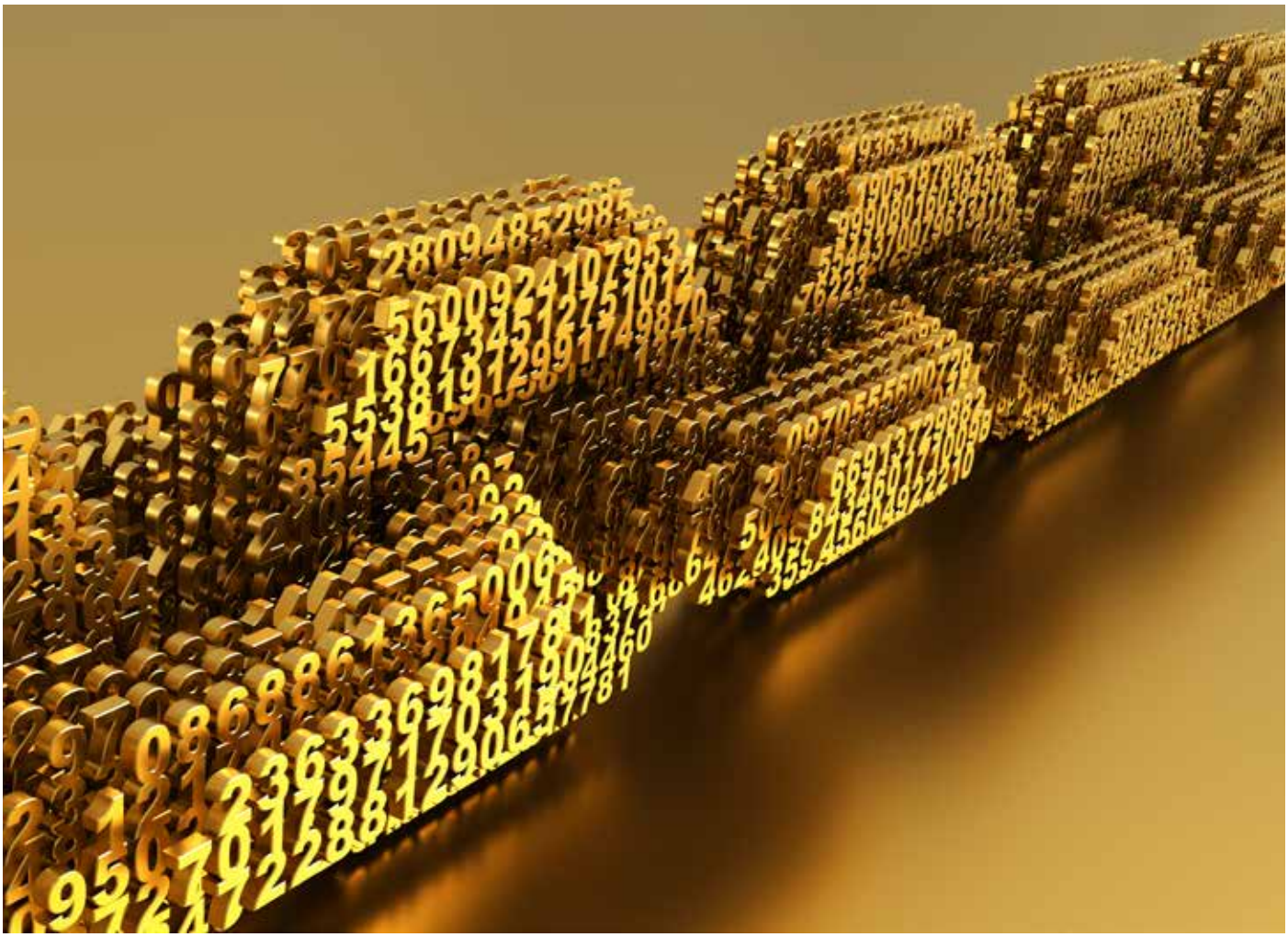
Takasbank BiGA Blokzincir Ağı



bir şekilde ayağa kaldırıp konfigüre edebilmek için Synechrorn-Finlabs tarafından geliştirilen açık kaynak kodlu Quorum-Maker projesi kullanılmıştır. BiGA Projesi geliştirilirken Quorum blokzincir altyapısı ve Quorum-Maker aracının tam olarak proje gereksinimlerini karşılamadığı görülmüştür. Bu gereksinimleri karşılamak üzere Quorum ve Quorum Maker projeleri çatallanarak (fork) bazı özelleştirmeler yapılmış ve BiGA Projesi ile uyumlu hale getirilmiştir.

BiGA Projesinin Ar-Ge odaklarından biri blokzincir üzerinde gerçekleşen işlemlerin gizliliğinin sağlanmasıdır. Hali hazırda transfer gizliliğini sağlayan bazı blokzincir teknolojileri (Zcash, Monero vb.) bulunmaktadır. Ancak bu teknolojiler tam gizlilik ilkesi ile çalışıp, transfere konu taraflar dışında kimse tarafından izlenememektedir. Bu durum, düzenleyici kurumlar tarafından transferlerin incelenmesi ve kontrol edilmesi imkânını ortadan kaldırmaktadır. Bu problemi çözmek için hem transfere konu olmayan taraflar için gizliliğin sağlandığı hem de regülasyona uyumlu bir blokzincir altyapısı geliştirilmesi hedeflenmiştir. Buna göre tüm işlemlerin içeriği bilinmeden sıfır bilgi ispatları ile tüm düğümler tarafından onaylanması ve sadece düzenleyici otoritenin sistemdeki tüm transferleri izleyebilmesi sağlanmıştır.

Bu ihtiyaçları karşılamak için farklı kriptografik ispat algoritmaları test edilmiştir. Quorum ağına işlem yapacak taraf; ilgili işleme ait tüm bilgileri şifrelemek, işleme ait bazı kriptografik ispatları oluşturmak, bu şifrelenmiş bilgi ve ispatları ağa yayınlamak durumundadır. Ağda yayınlanan bu işlemler, tüm düğümlerde akıllı kontratlar aracılığı ile kriptografik olarak doğrulanmak ve bu doğrulama sonucunda işleme alınmak durumundadır. Yüksek performans gerektiren kriptografik doğrulama faaliyetleri düğümler üzerindeki akıllı kontratlar tarafından yapılabilir. Akıllı kontratlar EVM (Ethereum Virtual Machine) katmanında çalıştığı için hem performans hem de ölçekleme açısından yüksek maliyetler oluşturmaktadır. Bu nedenle gereksinimi karşılayabilmek için bu faaliyetler EVM dışında çalışan, Go programlama dili ile yazılmış, Ethereum Pre-Compiled akıllı kontratlara eklenmiştir. EVM üzerinde çalışan bu akıllı kontratlar, Pre-Compiled kontratlar yardımı ile kriptografik ispatları doğrulama işlemlerini yapmaktadır. İşlemin sonucuna göre blokzincir üzerinde ilgili blok oluşturulmaktadır. Bahsi geçen kriptografik ispat doğrulama mekanizmasının Quorum altyapısında gerçekleşebilmesi için Quorum ve Quorum Maker aracı özelleştirilip çatallanmıştır. Projenin ilk fazında konsensus algoritması olarak RAFT kullanılmaktadır. Projenin ilerleyen fazlarında başka konsensus algoritmaları ile değiştirilmesi planlanmaktadır.



BiGA PROJESİ TEST SONUÇLARI

BiGA Projesi çok partili test süreci, blokzincir ve ATS entegrasyon geliştirmelerinin tamamlanması ile başlamıştır. Bu süreçte ilk olarak hali hazırda Takasbank ATS sistemini kullanan bankalara BiGA Projesinin tanıtımı ve bilgi paylaşımı sağlanmıştır. Albaraka Türk Katılım Bankası, Garanti BBVA, Kuveyt Türk Katılım Bankası, VakıfBank ve Ziraat Bankası olmak üzere beş banka testlere katılım sağlamıştır.

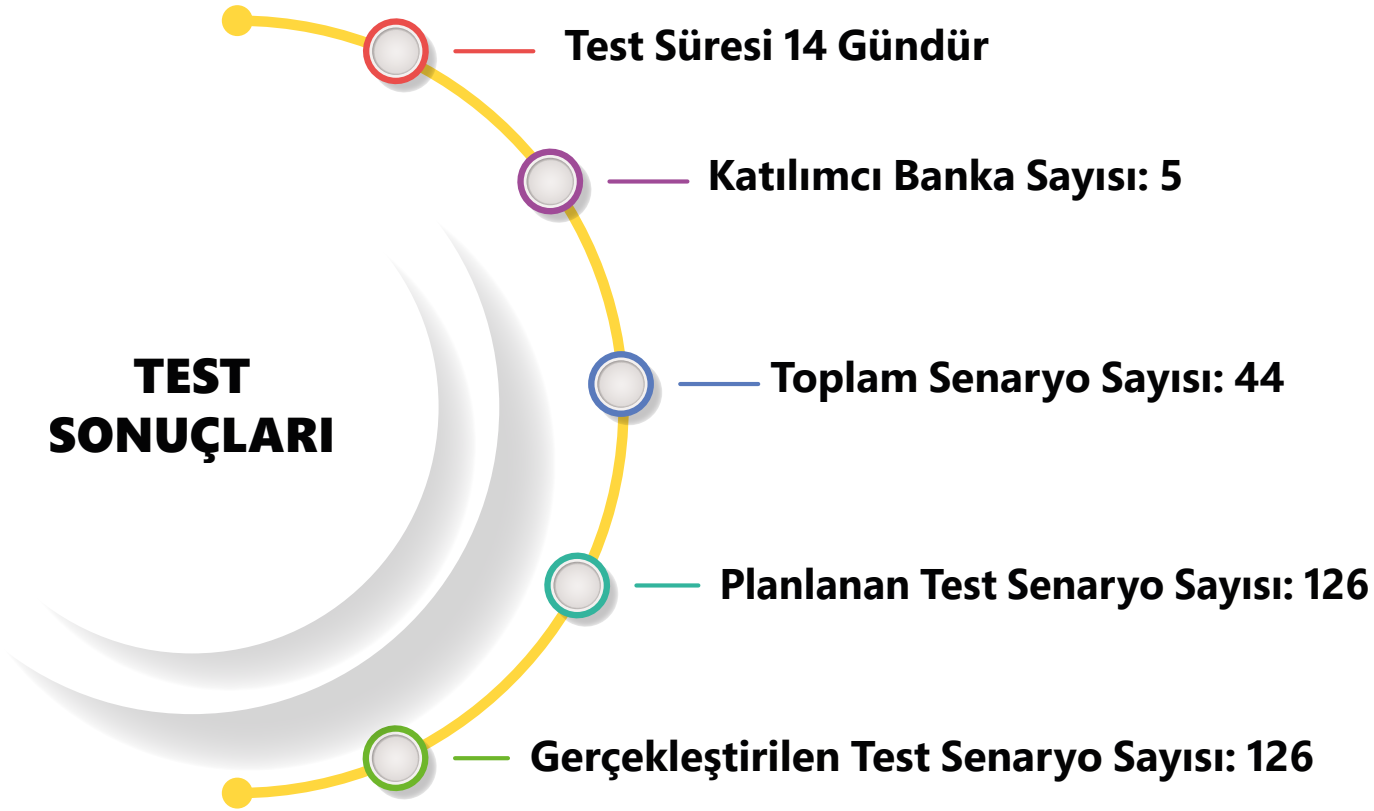
Test edilen geliştirmeler

Test kapsamında aşağıdaki maddeler test edilmiştir.

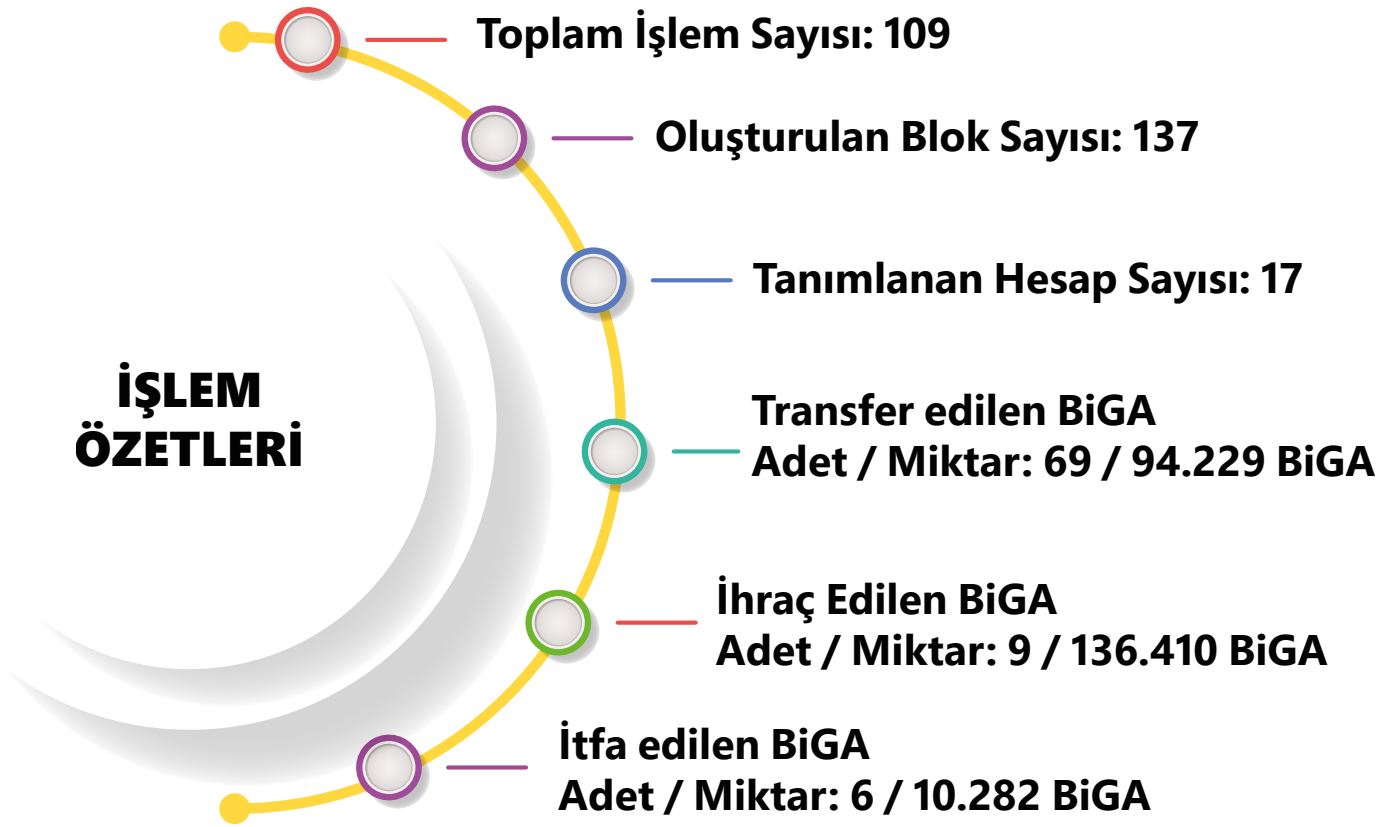
- Blockchain node kurulum scripti
- Blockchain ağının kurulması ve blockchain ağına katılma
- Blockchain web kurulum scripti
- Blockchain cüzdan işlemleri
- Blockchain üzerinde transaction oluşturma ve blokların izlenmesi
- Smart kontratlar
- Zero Knowledge kapsamında sadece ilgili tarafların bakiyeleri görebilmesi
- Takasbank Altın Transfer Ekranları ve Entegrasyonları

Test sonuçları

Test sonuçları aşağıdaki tabloda özetlenmiştir.



Test süresince gerçekleştirilen işlemlerin özeti aşağıdaki tabloda yer almaktadır.



BiGA Fonksiyonları Test Sonuçları

BiGA Projesi testi kapsamında test edilen fonksiyonlar aşağıdaki tabloda belirtilmiştir. Fonksiyonların testi tüm katılımcılar tarafından başarılı bir şekilde tamamlanmıştır.

BiGA Fonksiyonları Test Değerlendirmesi	Albaraka Türk Katılım Bankası	Garanti BBVA	Kuveyt Türk Katılım Bankası	VakıfBank	Ziraat Bankası
Node kurulumları ve blockchain ağına katılma	✓	✓	✓	✓	✓
Web uygulamasının kurulumu	✓	✓	✓	✓	✓
BiGA Platformu Portföy Hesabının ATS üzerinden Tanımlanması	✓	✓	✓	✓	✓
BiGA Platformu Yeni Kullanıcı Tanımlama	✓	✓	✓	✓	✓
BiGA Platformu Yeni Hesap Oluşturma	✓	✓	✓	✓	✓
Kaydi Altın - BiGA Çevrim İşlemi	✓	✓	✓	✓	✓
BiGA İhraç İşlemi	✓	✓	✓	✓	✓
Üye içi BiGA Transferi (Portföy- Müşteri, Müşteri-Müşteri)	✓	✓	✓	✓	✓
Üyeler arası BiGA Transferi (Portföy - Müşteri, Müşteri-Müşteri)	✓	✓	✓	✓	✓
BiGA İtfa İşlemi	✓	✓	✓	✓	✓
BiGA - Kaydi Altın Çevrim İşlemi	✓	✓	✓	✓	✓

BiGA tasarımı itibariyle herhangi bir dijital değerin transferine mümkün kılan parametrik bir altyapıya sahiptir.

Dolayısıyla oluşturulan bu varlık transfer altyapısı altın dışında herhangi bir kıymetin dijitalleştirilip transfer edilmesine de imkan vermektedir.

TEKNİK KAZANIMLAR

Bu dokümanın amacı, BiGA projesi ile elde edilen tecrübelerin paylaşılarak, Türkiye'de ve Dünya'da yapılacak yeni çalışmalara yol göstermesi, konu hakkında fikir sahibi olan ve proje alternatiflerini değerlendiren girişimcilere ve Ar-Ge merkezlerine bakış açısı sunması, bu alanda çalışmaları takip eden kamu otoritelerine somut çıktıların ve faydaların sunulması ve muhtemel iş birliği alternatifleri için ilgililere ulaşılabilmesidir. Bu bölümde proje boyunca elde edilen teknik ve süreçsel deneyimler paylaşılmaktadır.

BiGA Projesinde geleneksel veri işleme, saklama, mutabakat, yöntem ve teknolojilerinden ayrışan blokzincir yaklaşımının temel ilkeleri esas alınarak gerçeklenebilirlik ispat çalışmaları yapılmıştır. Bu bağlamda, projede blokzincir ve kriptografi üzerine edinilen teknik bilgi birikimi aşağıdaki gibidir.

Dağıtık sistemlerin çalışma prensipleri:

Geleneksel yaklaşımlarda verinin merkezi bir yerde saklanması, ihtiyaç duyulan kadarının ilgili diğer paydaşlarla entegrasyon yöntemleriyle paylaşımı sağlanmaktadır. Blokzincir yaklaşımlarında

ise veri ve işlemler eş zamanlı olarak tüm paydaşlarda birebir aynı format ve içerikte saklanmaktadır. Bu durum verinin herhangi bir paydaşa ve zamana bağlı kalmaksızın bütünlüğü, erişilebilirliği, gizliliği ve doğruluğunu garanti altına almaktadır.

Mevcut blokzincir altyapılarının deneyimlenmesi:

Kurumsal bir çözüme ulaşabilmek için izinli blokzincir altyapılarının kullanılması başlangıç için önemli bir kriter olarak değerlendirilmiştir. Bu kapsamda, Hyperledger ve Quorum altyapılarıyla çalışılmıştır. Projede öncelikli olarak kullanılması tercih edilen Hyperledger Fabric 1.0 altyapısının henüz üretim ortamına alınacak bir çözüm için yeterli olgunluk kriterlerini sağlamadığı görülmüştür. Quorum altyapısı ise benzer kısıtları nedeniyle çatallama (fork) yöntemiyle yapısı değiştirilerek kullanılmıştır. Aynı şekilde benzer bir çatallamanın Hyperledger altyapısı ile de yapılabileceği öngörülmektedir. Quorum'un daha fazla ulaşılabilir kaynağa sahip olması ve Quorum Maker ile blokzincir ağının daha hızlı aktif hale getirilmesi sebeplerinden dolayı projeye Quorum ile devam edilmiştir.

Konsensus algoritmaları:

Yapının dağıtık mimariye sahip olmasından dolayı paydaşlarda saklanacak verinin bütünlüğü, erişilebilirliği, gizliliği ve doğruluğunun garanti altına alınması için BFT (Byzantine Fault Tolerance) ve RAFT algoritmaları deneyimlenmiştir. RAFT algoritması Quorum altyapısıyla birlikte gelen bir çözümdür. Mevcut durumda yeterli olduğu düşünülmemektedir.

Kriptografik algoritmalar

Düğümler arasındaki veri transferlerinin, işlemlerin mahremiyetini ve otorite tarafından izlenenebirliğini aynı anda sağlamak üzere kullanılan kriptoloji ve ispat algoritmaları, bu projenin bu alanda yapılacak çalışmalara en önemli katkısı olarak görülmektedir. Zira söz konusu algoritmalar ile hem işlemlerin mahremiyeti sağlanmakta hem de dağıtık olarak saklanan kriptolu verilerin doğruluğu taraflarlarca onaylanabilmektedir. Projede kullanılan ve literatürde yüksek geçerliliği bulunan temel algoritmalar aşağıdaki gibidir:

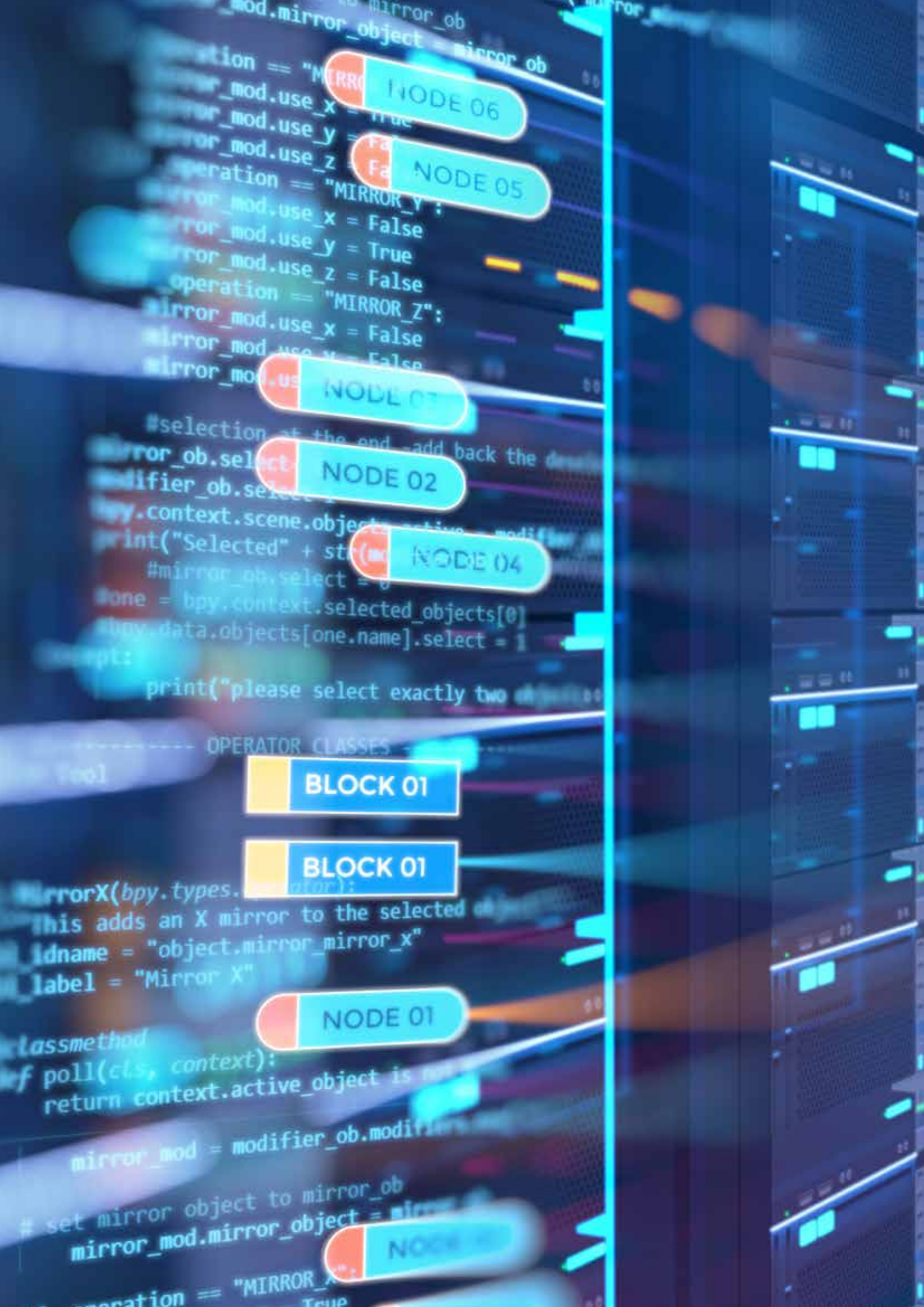
- Homomorphic encryption,
- Range proof ,
- Equality proof,
- Diffie Hellman proof,
- ECDSA (Eliptic Curve Digital Signature Algorithm)

Blokzincir hesap yapıları:

Blokzincir altyapıları, kullanıcıların işlem yapmalarını ve yapılan işlemlerin sonuçlarının gözlemlenebildiği ve varsa bir değer üzerinden işlem yapılıyorsa bu işlemlerin sonucunda oluşan bakiyelerin görüntülenebileceği yapılardır. Genel (Public) ve özel (Private) anahtar çiftleri ile oluşmaktadır. Genel anahtarlar ağ üzerinde işlem yapılmasına imkan verirken gizli anahtarlar hesabın kendisini tanımlamaktadır.

Pre-Compile kontratlar:

Proje kapsamında kullanılan ve yoğun matematiksel işlemler içeren sıfır bilgi ispatı algoritmalarının Quorum üzerinde Solidity diliyle geliştirilmesi performans bakımından mevcut haliyle yeterli gelmemektedir. Performans gerektiren problemleri çözmek için Ethereum ve Quorum altyapılarında pre-compile kontrat yapıları bulunmaktadır. Bu yapılar özellikle yoğun işlem gücü gerektiren işlerin tasarlanmasında kullanılmaktadır. Bu projede de sıfır bilgi ispatı algoritmalarının gerçeklenmesi sıfırdan geliştirilen pre-compile kontratlar ile yapılmıştır. Bu sayede performans kaybı en aza indirilmiş ve Quorum platformunun çatallanması sağlanmıştır. Bu geliştirmeler hem içeriği hem metodolijisi ile literatüre önemli kazanımlar katacaktır.


NODE 06
NODE 05
NODE 02
NODE 04
BLOCK 01
BLOCK 01
NODE 01

İŞ KAZANIMLARI

İş kazanımları aşağıdaki şekilde üç ana başlık altında değerlendirilmektedir. Bu konular; bir varlığın transferinin gerçekleştirilmesi, iş sürekliliğinin sağlanması ve bir ödeme sistemi altyapısını oluşturması olarak aşağıda açıklanmaktadır.

Varlık Transferi

- Altının dijitalleştirilerek blokzincir ağında oluşturulan sisteme katılması, transferinin güvenli bir şekilde yapılması ve sistemden çıkışının sağlanmasıyla birlikte uçtan uca bir dijital varlığın yaşam döngüsü sağlanmaktadır.
- Bilinen blokzincir ağlarında yapılan her bir işlem ya herkes tarafından görülebilmektedir ya da hiçbir şekilde görülememektedir. BiGA Projesinde çalışılan sıfır bilgi algoritmaları ile kriptolu işlem yapısı oluşturulmuştur. Bu yapı; alıcı ve göndericinin işlemleri görebildiği fakat başkalarının göremediği, düğümlerin içeriğini görmemesine rağmen bütün işlemlere onay veya red verebildiği, sistemde otorite olarak bulunan düğümlerin dilediği zaman tüm işlemlerin içeriğini görüntüleyebildiği şekilde tasarlanmıştır. Bu özellik BiGA'yı

bilinen tüm blokzincir çözümlerinden pozitif şekilde ayrıştırmaktadır. Böylelikle blokzincir tabanlı finansal çözümlerin yaygınlaşması için gerekli olan altyapıların yapılabilirliği ispatlanmıştır.

- BiGA tasarımı itibariyle herhangi bir dijital değerin transferine mümkün kılan parametrik bir altyapıya sahiptir. Dolayısıyla oluşturulan bu varlık transfer altyapısı altın dışında herhangi bir kıymetin dijitalleştirilip transfer edilmesine de imkan vermektedir. Bu yönüyle BiGA, alternatif finansal araçların tek bir blokzincir altyapısıyla yaygınlaşabileceğini ispatlamıştır.

İş Sürekliliği

- Blokzincir teknolojisinin getirmiş olduğu en önemli özelliklerden birisi de veri tabanının bütün düğümlerde eş zamanlı olarak aynı olmasıdır. Bu sebeple, oluşturulan sistemde anlık mutabakat yapıldığından sistem kesintisiz 7 gün 24 saat çalışabilmektedir.

- Oluşturulan altyapı sayesinde blokzincir ağında bulunan herhangi bir düğüm erişilemez olsa bile sistem blokzincir ağının diğer düğümleri üzerinde hayatına devam etmektedir. Erişilemeyen düğüm tekrar ağa dahil olduğunda otomatik olarak kendini ağdaki diğer paydaşlarla eş bilgi seviyesine ulaştırmaktadır.

- Veri tabanının bütün düğümlerde eş zamanlı olarak aynı olması single point of failure olma durumunu ortadan kaldırmaktadır. Kurumlar, sistemin yedekli çalışması veya felaket kurtarma gibi senaryoları düşünmeden çalışmalarını yürütebilmektedir. Bu hem iş sürekliliği hem de maliyet açısından ciddi faydalar sağlamaktadır.

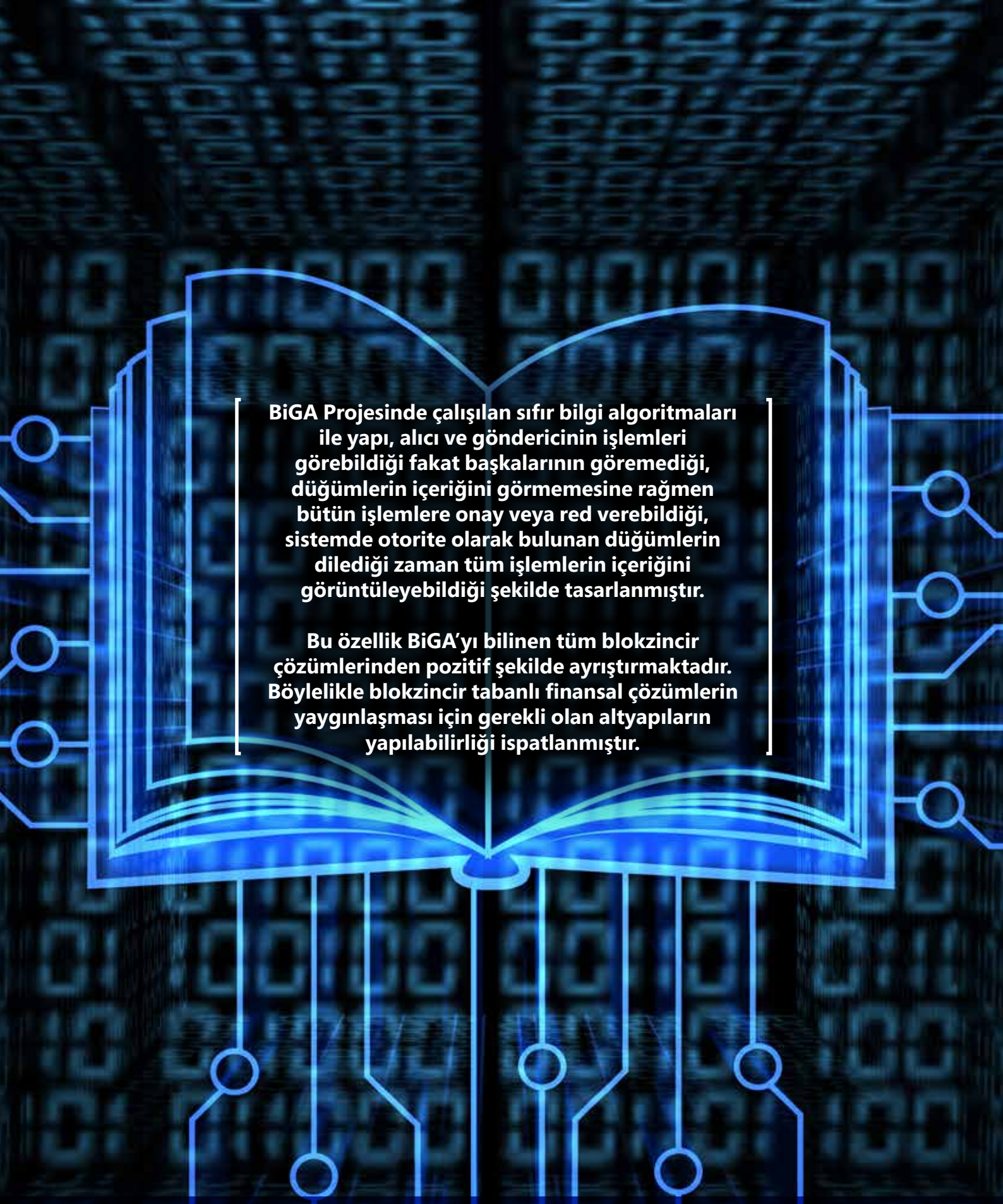
Ödeme Sistemi Altyapısı

- Altın Transfer Sistemi ile oluşturulan kaydi gram altın ve kişiler arası transfer özelliğinin altına mobilizasyon kazandırması beklenmektedir. BiGA ile genişleyecek kullanıcı kitlesi sayesinde altının mobilizasyonunun daha da arttırılması hedeflenmektedir.

- Blokzincir yaklaşımıyla dijital varlık transfer sistemi altyapısı sayesinde altının bir dijital ödeme enstrümanına dönüşmesine olanak sağlamaktadır.

- Sisteme eklenecek düğümler birer finansal kurum olarak düşünülmektedir. Bu kurumların sisteme entegre olması ve sistemden çıkmaları geliştirilen kurulum otomasyonlarıyla çok hızlı bir şekilde yapılabilmektedir.

- Tüm datanın kullanıcıya verilmesinden dolayı istenilen raporların hiçbir kuruma bağlı kalmadan oluşturulması sağlanmaktadır. Bu sayede kurumların raporlama ile ilgili yaşadığı bağımlılıklar en aza indirilmektedir.



BiGA Projesinde çalışılan sıfır bilgi algoritmaları ile yapı, alıcı ve göndericinin işlemleri görebildiği fakat başkalarının göremediği, düğümlerin içeriğini görmemesine rağmen bütün işlemlere onay veya red verebildiği, sistemde otorite olarak bulunan düğümlerin dilediği zaman tüm işlemlerin içeriğini görüntüleyebildiği şekilde tasarlanmıştır.

Bu özellik BiGA'yı bilinen tüm blokzincir çözümlerinden pozitif şekilde ayrıştırmaktadır. Böylelikle blokzincir tabanlı finansal çözümlerin yaygınlaşması için gerekli olan altyapıların yapılabilirliği ispatlanmıştır.

ÖĞRENİLEN DERSLER VE SONRAKİ ÇALIŞMALARA YÖNELİK ÖNERİLER

Blokzincir, mevcut haliyle tüm dünyanın yakından takip ettiği, henüz somut örneklerinin sınırlı olduğu ve etkilerinin tam anlamıyla bilinemediği bir yaklaşımdır. Konu hakkında çalışmalar yapmak isteyen çoğu araştırmacı ve kurum için, blokzincir yaklaşımının yanında çok farklı teknik bilgi ve kabiliyete de ihtiyaç duyulmaktadır. Bu durum ise bireysel çalışmalardan ziyade, disiplinler arası sinerji oluşturmak suretiyle proje grupları kurarak konuya yaklaşmayı zorunlu kılmaktadır. Zira ileri seviye matematik, kodlama, yeni nesil yazılım dilleri, uygulama sanallaştırma gibi farklı konuları aynı projede araştırmak, öğrenmek, geliştirmek gibi bir zorluk da mevcuttur. Bu durum blokzincir yaklaşımının henüz yolun başında olmasına bağlandığında, kaynak olarak okunacak dokümantasyonların yetersizliği, henüz geliştirilen çerçevelerin ve platformların kararlı sürümlere ulaşmamış olması, platformların kullanımını kolaylaştıran ek teknolojilerin henüz istenen seviyede olgunlaşmamış olması, referans olarak alınabilecek proje sayısının ve proje dokümanlarının eksikliği gibi hususlar özellikle ön plana çıkmaktadır.

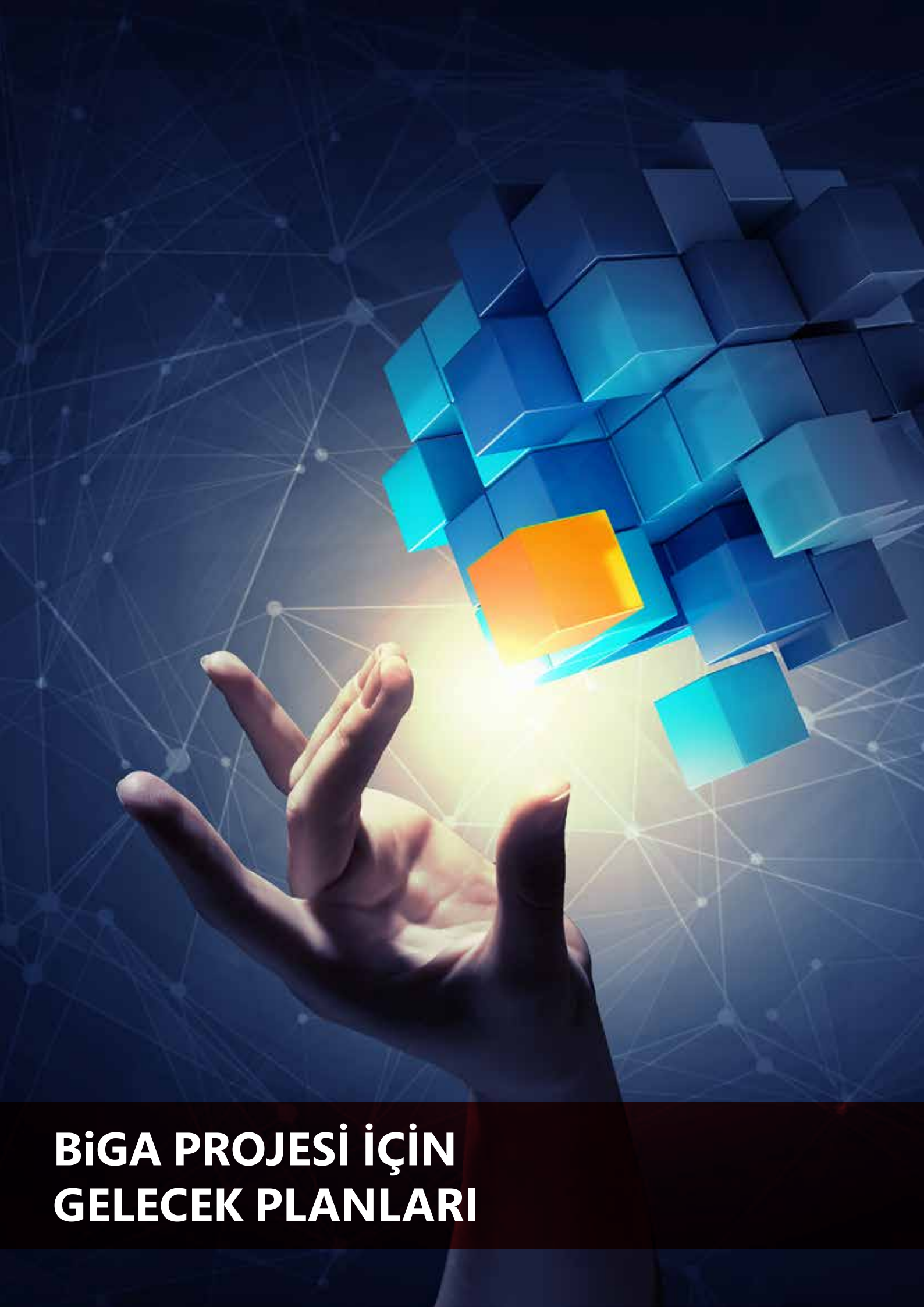
Günümüzde kullanılan tüm yazılım geliştirme ortamları ve araçları geleneksel mimarilerdeki ihtiyaçlar dikkate alınarak geliştirildiği için aynı araçlar ve yöntemler ile geliştirme yapılması, debug ve test yapılmak istenmesi çalışmaları ayrıca zorlaştırmaktadır. Basit bir debug işlemi için bile zahmetli bir ortam kurulumu çalışmasına ihtiyaç duyulmaktadır.

Bu bağlamda, konuya farklı bir noktadan yaklaşmak isteyen girişimciler için bu tür üçüncü parti geliştirme, paketleme, test, debug, yaygınlaştırma araç ve teknolojilerine yönelik çalışmaların yapılması tarafımızdan önerilmektedir.

Ar-Ge özelliği taşıyan, belirsizlikleri çok ve kısıtları olan bir projenin kesinlikle standart kurumsal bilgi işlem altyapılarında kurgulanmaması önemli bir detay olarak öne çıkmaktadır. Zira özellikle bankacılık gibi bilgi güvenliği politikalarının en üst düzeyde uygulandığı bilgi işlem yapılarında geliştirme ve test ortamlarının stabil hale getirilmesi için oldukça fazla efor harcamak gerekmektedir. Bunun yerine geliştirici bilgisayarları dahil tüm geliştirme ortamının tamamen izole bir ortamda sağlanması proje takvimi ve başarısı için mühimdir. Bulut ortamları bu çalışmalar için iyi bir alternatif olarak değerlendirilebilir.

Teknik kısıtlarının yanında blokzincir yaklaşımının geleneksel bakış açılarına alternatifler getirmesi ve bir çeşit yıkıcı etkisinin doğru anlaşılması zaman alacaktır. Zira proje boyunca tüm paydaşlar ve katılımcılar bu işi neden geleneksel yöntemler ile yapmıyoruz sorusunu birbirlerine sorabilmektedirler.

Aynı şekilde projenin üçüncü taraflara anlatımında da benzer sorular ile sıklıkla karşılaşılmaktadır. Kurum olarak, bu yönüyle blokzinciri bir teknoloji olarak görmekten ziyade bir yaklaşım, bir felsefe olarak tanımlamaktayız.



BiGA PROJESİ İÇİN GELECEK PLANLARI

Projenin Faz-1 kısmı, öğrenilen dersler ve sonraki çalışmalara yönelik önerilerle beraber tamamlanmıştır. Projenin Faz-2 kısmında bankalar aracılığı ile son kullanıcıların da BiGA platformunda işlem yapması hedeflenmektedir. Bu kapsamda aşağıda belirtilen başlıklar hakkında çalışmalar yapılması planlanmaktadır.

Sıfır Bilgi İspat Algoritmasının Değiştirilmesi

Mevcutta kullanılan kriptolojik algoritmalar bünyelerinde bazı kısıtlamalar bulundurmaktadır. Özellikle altın transferi için yeterli şartları sağlasa da bu altyapıyı başka varlıklar için kullanmak istediğimizde bu kısıtların iyileştirilmesi gerekmektedir. İşlemin süresi 2^{32}'lik uzayda yaklaşık 3 saniye sürmektedir. Uzayın artırılması sonucu işlem süresi logaritmik olarak artmaktadır. Burada hedef; 2^{64}'lük uzayda 1 saniyede işlemlerin yapılmasını sağlamaktır.

Bir işlemin boyutu mevcut işlem yapısında yaklaşık 30 kB tutmaktadır. Burada kullanılacak kriptolojik algoritmaların iyileştirilmesi sonucunda işlem boyutunun 1 kB olması hedeflenmektedir.

Yine mevcutta uzaya bağlı olarak transfer edilebilecek maksimum miktar 2^{32} boyutunda olabilir. Uzayın 2^{64} yapılmasıyla transfer edilebilecek maksimum miktar artırılmış olacaktır.

Quorum Maker bağımlılığının kaldırılması

Projede oluşturulacak blokzincir ağının hızlı şekilde aktif hale gelebilmesi için destekleyici çözüm olarak kullanılan Quorum Maker aracına olan bağımlılığın ortadan kaldırılması hedeflenmektedir.

Konsensus algoritmasının değiştirilmesi

Projede mevcut durumda kullanılan RAFT algoritmasının tespit edilen eksikliklerini karşılamak adına İBFT (İstanbul Byzantine Fault Tolerance) olarak değiştirilmesi planlanmaktadır. Ayrıca daha efektif olabilecek algoritmalar da araştırılacaktır.

Gizli anahtar kurtarma senaryoları

Blokzincir çözümünün yoğun güvenlik gereksinimleri nedeniyle ilgili tarafların kullanacağı gizli anahtarların kaybolması durumunda kurtarılmasına yönelik bir iş modeli geliştirilecektir. Takasbank'ın saklama bankacılığı konusunda yetkilendirilmiş olması ve bu konuda yeterli iş bilgisine sahip olması iş modelinin oluşturulmasında önemli bir avantaj sağlamaktadır.

Transfere konu olan tarafların gizlenmesi

Mevcut durumda yapılan işlemlerde işlemlerin içeriği kriptoloji algoritmalarıyla gizlenmiş durumdadır. Söz konusu işlemleri gerçekleştiren tarafların kimliklerini temsil eden açık anahtarlar görünür durumdadır. Yapılacak ek bir geliştirme ile açık anahtarlar da gizlenecektir.

Güncellenebilir akıllı kontrat yapısı

Blokzincirin temel çalışma prensipleri gereği, oluşturulan bir bloğun içeriğinin değiştirilmemesi esastır. Ancak muhtemel iş ihtiyaçları göz önünde bulundurularak özellikle akıllı kontratların zaman içinde güncellenebilmesini gerektirmektedir. Bu bağlamda bloklar arasındaki veri tutarlılığı bozulmayacak şekilde akıllı kontratların güncellenebilmesi üzerine çalışmalar yapılacaktır.

Hyperledger Fabric Platformu ile Geliştirme

BiGA Platformu'nun performansını artırmak için alternatif blokzincir platformları ile geliştirmelerin yapılması planlanmaktadır. Bu kapsamda mevcut işlem yapısı ve değiştirilen sıfır bilgili işlem yapısı Hyperledger Fabric platformu ile de geliştirilecektir.

Know Your Customer çalışmaları

Mevcut yapıda blokzincir üzerinde kullanılacak olan hesapların açılışları kurumlar tarafından yapılmaktadır. Bunun sebebi olarak blokzincir platformundaki hesap sahiplerinin gerçekte kim olduğunun bilinmesi gerekliliğidir. Kimlik bilgileri kurumlar üzerinden onaylanarak geldiğinden bu yükümlülük kurumlara bırakılmıştır. İlerleyen zamanlarda platform kullanıcılarının kimlik bilgilerinin

kurumlardan bağımsız olarak onaylandığı bir dijital kimlik platformu geliştirilip, kurumlara bağımlılığın en aza indirilmesi ile bireysel kullanıcıların kendi hesaplarını kurumlardan bağımsız yönetebilmesi planlanmaktadır.

Bireysel kullanım için cüzdan uygulaması

İlerleyen fazlarda bireysel kullanıcıların düğümlerden bağımsız işlem yapabilmelerini sağladıktan sonra bireysel kullanıcıların sistemi daha rahat kullanabilmesi için bir mobil cüzdan uygulaması geliştirilmesi düşünülmektedir.

Bazı uç senaryoların değerlendirilmesi

- Gizli anahtarların kaybolması durumunda alınacak aksiyonlara yönelik iş modeli ve teknik çözümde çalışmalar yapılması,
- Özel yetkiye sahip hesapların kötü niyetli kişiler tarafından ele geçirilmesi senaryosuna yönelik önleyici çözümlerin çalışılması,
- 3n düğümlü bir ağda n düğümün konsensus aleyhine kötü niyetli olarak hareket etmesi durumunda alınacak aksiyonların çalışılması,

başlıkları ilerleyen dönemde yeni projelerde ön planda olacaktır.

SONUÇ

Adını ilk olarak 2008 yılında duyuran blokzincir ancak 2017 yılı itibariyle kripto paralarda meydana gelen aşırı değerlenmeler sonucu popüler bir hale gelmiştir. Blokzincirin kurumsal hayatta kullanımına yönelik çalışmalar da yine aynı dönemde başlamıştır. Takasbank olarak 2016 yılında aktif olarak başladığımız bu araştırma sürecinin somut bir proje ile bu noktaya getirilmiş olması önemli bir dönüm noktası olarak değerlendirilmektedir. Blokzincir üzerine bireylerin ve kurumların bir miktar literatür araştırmaları yapmaları, çıkan haberleri takip etmeleri sonrasında bir proje yapma fikrinin ortaya çıkması doğaldır. Ancak doğru iş senaryosunun belirlenmesi ve proje ekibinin bu işe odaklanmasının sağlanması aynı zamanda üst yönetimlerin bu konularda öncü olması blokzincir çalışmaları için büyük önem arz etmektedir.

Takasbank, blokzincir konusunda takip eden değil, takip edilen olma vizyonu ile harekete geçerek hem iş modeli hem de teknik çözümüyle katma değeri yüksek bir Ar-Ge projesini tamamlamıştır.

Her teknoloji ve inovasyon gibi blokzincirin de Ar-Ge projeleri yapılmadan anlaşılması ve somutlaştırılması yakın vadede mümkün görünmemektedir. Bu noktada değerlendirme aşamasında olan kurum ve girişimciler için bir an önce pilot projeler ile devam etmelerinin önemini vurguluyoruz.
Genel Müdürlük makamından, projede çalışan uzman personellerine, iş birimi çalışanlarına ve dış paydaşlara kadar ekip çalışmasının önemi bu projenin sonuçlanmasında önemli bir unsur olarak öne çıkmaktadır.

Takasbank olarak bu teknolojinin finansal alanlarda kullanılmasının önünde en büyük engel olarak görünen tam mahremiyet ve regülasyona uyumluluk konularında yaptığımız çalışmalarla blokzincir alanında çalışmalar yapan kişi ve kurumlara öncülük etmiş olmaktan gurur duymaktayız.

PROJE EKİBİ

Gökhan ELİBOL
Proje Sponsoru

İlker KUŞCU
BT Yöneticisi

Nesrin ÖZKURT
İş Birimi Yöneticisi

Mustafa ATAHAN
Proje Yöneticisi

Faruk Selman LEKESİZ
BT Mimarı

Mustafa ŞENTÜRK
Yazılım Uzmanı

Muhammet EVİRGEN
Yazılım Uzmanı

Ramazan BARDA
Yazılım Uzmanı

Mustafa KELEŞ
Yazılım Uzmanı

Elvan SAKANCI
Analist

M. Fatih BAYINDIR
Bilgi Güvenliği Uzmanı

Kadir SARI
Altyapı Uzmanı

BiGA Projesine değerli katkılarından dolayı
Bankamız Yönetim Kurulu Başkanı ve **Borsa İstanbul Genel Müdürü**
Sayın Mehmet Hakan Atilla ve **Yönetim Kurulu Üyelerimize**,

Genel Müdür Vekilimiz **Sayın Gökhan Elibol**'a,

Projenin başlangıcından itibaren desteklerini esirgemeyen önceki üst düzey yöneticilerimiz
Sayın Murat Çetinkaya, **Sayın Mahmut Kayacık** ve **Sayın Ekrem Arıkan**'a,

BiGA Proje Ekibi ve tüm **Takasbank çalışma arkadaşlarımıza**,

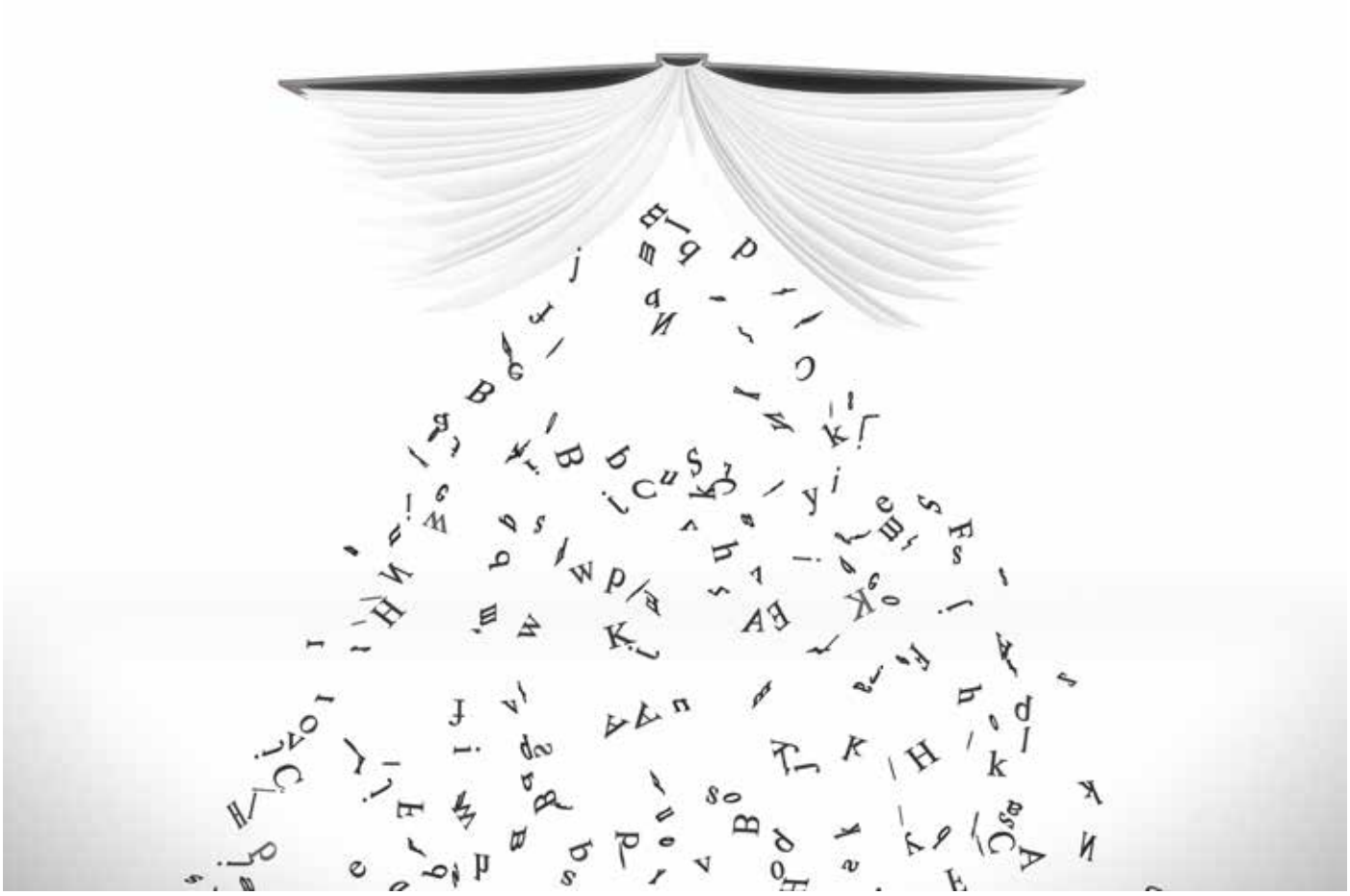
Doç. Dr. Mehmet Sabır Kiraz ve **TÜBİTAK BİLGEM Blokzincir Laboratuvarına**,

Sabancı Üniversitesinden **Doç. Dr. Kamer Kaya**'ya,

BiGA Projesi testlerine katılımlarıyla projenin çıktılarını çok daha anlamlı hale getiren
Albaraka Türk Katılım Bankası, **Garanti BBVA**,
Kuveyt Türk Katılım Bankası, **VakıfBank** ve **Ziraat Bankası**
değerli yönetici ve çalışanlarına,

Projenin farklı aşamalarında fikri ve teknik desteklerini bizlerle paylaşan
fintek ekosistemine ayrı ayrı teşekkürlerimizi sunarız.

İstanbul Takas ve Saklama Bankası A.Ş.



KISALTMALAR / TERİMLER SÖZLÜĞÜ

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

ATS: Altın Transfer Sistemi

BFT (Byzantine Fault Tolerance): BFT, bir sistemin, özellikle bileşenlerin arızalanabileceği ve bir bileşenin arızalı olup olmadığına dair eksik bilgilerin bulunduğu dağıtılmış bilgi işlem sistemlerinin bir durumudur. Terim ismini "Bizans Generalleri Sorunu" adlı bir metafordan alıyor. Bu metafor aktörlerin felakete yol açacak bir sistemin başarısızlığını önlemek için ortak bir strateji üzerinde hemfikir olmaları gerektiği, ancak bazı aktörlerin güvenilmez oldukları durumu ifade ediyor. BFT'de, sunucu gibi bir bileşen, farklı gözlemcilere farklı semptomlar sunarak, hem başarısız hem de arıza tespit sistemlerinde çalışır durumda tutarsız görünebilir. Diğer bileşenlerin tutarsız görünen bileşenin başarısız olduğunu beyan etmeleri ve ağdan çıkarmaları zor, çünkü ilk önce hangi bileşenin başarısız olduğu konusunda bir fikir birliğine varmaları gerekiyor. BFT, hataya dayanıklı bir bilgisayar sisteminin bu gibi koşullara güvenilirliğidir.

BiGA: 995/1000 saflıkta LBMA ici şartlarına uygun bir gr altının Blokzincir platformundaki değeri. Bir gr altın bir BiGA ya tekabül gelmektedir.

BiGA Projesi: BiGA Blokzincir Platformunun geliştirilmesi için yapılan bütün çalışmaları ifade eder.

BİST: Borsa İstanbul

Blokzincir (Blockchain): 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 gelen önce gelen blokların özet değerleriyle bağlanmıştır.

Cüzdan (Wallet): İçinde sahibine ait gizli anahtarı barındıran yapıdır.

Çatallama (Fork): Blockzincir geçmişini korumak, tutarsızları önlemek ya da yeni özellikler eklemek adına blokzincir protokollerinde oluşan farklılıklar olarak tanımlanabilir.

Dağıtık Defter: Farklı sunucularda, ülkelerde veya kurumlarda kopyaları duran bir veritabanı çeşididir. Kayıtlar birbiri arkasına eklenerek sürekli büyür.

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

Dijital Kimlik: Bir kişiyi, organizasyonu ya da elektronik bir cihazı, bir ağ içerisinde tanımlanması sağlayan kimliktir.

Docker: Docker, 'containerization' olarak da bilinen işletim sistemi düzeyinde sanallaştırma gerçekleştiren bir bilgisayar programıdır. İlk olarak 2013 yılında piyasaya sürüldü ve Docker, Inc. tarafından geliştirilmiştir.

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

EFT: Elektronik Fon Transferi

İhraç: ATS sistemindeki kaydi altının BiGA'ya dönüştürülmesi işlemidir.

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

İtfa: Blokzincir sistemi üzerinde var olan BiGA bakiyesinin ATS sisteminde kaydi altın bakiyesine dönüştürülmesi işlemidir.

İzinli Blokzincir (Permissoned Blockhchain): Permission Blockchain kimlerin ağa erişimi olduğunu yönetmek için bir erişim kontrol katmanı kullanır. Public blockchain ağlarının aksine, blockchain ağlarındaki doğrulayıcılar ağ sahibi tarafından incelenir. İşlemleri doğrulamak için adsız düğümlere güvenmezler veya ağ etkisinden de faydalanamazlar.

Kaydileştirme: Fiziksel bir varlığın dijital bir varlığa dönüştürülmesidir.

LBMA: London Bullion Market Association

Konsensus Algoritması: Konsensüs algoritması, bilgisayar bilimi alanındaki bir mutabakat oluşturma problemini çözmek için önerilen protokolleri ifade etmektedir.

Mislen Saklama: Saklanan bir varlığın aynı özelliklerde varlıklarla ortak olarak saklanması ve iadesi durumunda ortak alandan herhangi bir varlığın iadesinin yapıldığı saklama türü

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

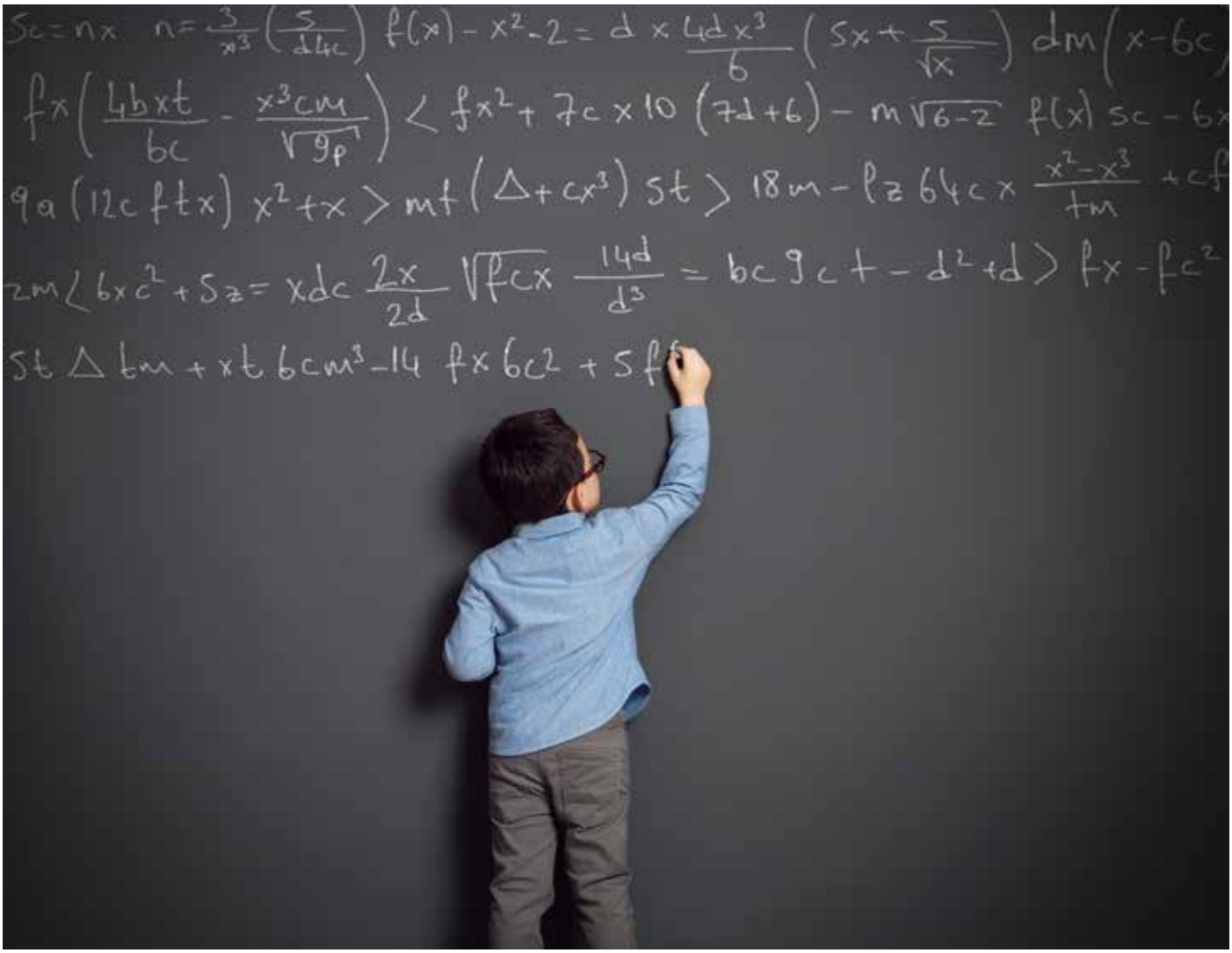
Onaylama: Bir işlemin Blockchain ağı tarafından onaylanmasına denir. Bu işlem bazı Blockchain ağlarında madencilik ile yapılır.

RAFT: RAFT, Paxos'a alternatif olarak tasarlanmış bir konsensus algoritmasıdır. Farklı bir mantık geliştirilerek Paxos'tan daha anlaşılır olması hedeflenmiştir ancak aynı zamanda güvenli olduğu ve bazı ek özellikler sunduğunu da kanıtlamıştır. RAFT, bir durum makinesini bir bilgisayar sistemleri kümesinde dağıtmanın genel bir yolunu sunar ve kümedeki her düğümün aynı durum geçişi serileri üzerinde anlaşmasını sağlar. Go, C ++, Java ve Scala'da geliştirmesi tamamlanmış uygulamalarla birlikte birçok açık kaynaklı referans uygulaması vardır.

Stable Coin: Değeri sabit olan bir varlığa göre endekslenmiş dijital paradır.

Token: Sahiplik özelliği olan dijital varlıklardır.

Quorum Maker: Quorum Maker, kullanıcıların Quorum ağı oluşturmalarını ve yönetmelerini sağlayan bir araçtır. Konfigürasyon dosyalarını manuel düzenleme ve düğüm oluşturma yavaş ve hataya açık bir işlemdir. Quorum Maker, azaltılmış kullanıcı girişi ile dinamik olarak herhangi bir sayıda farklı konfigürasyon düğümü oluşturabilir. Bu tool ile düğüm yaratırken kullanıcıyı yönlendirecek bir dizi soruyla wizard benzeri bir arayüz sağlar.



EKLER

Ek A
Sıfır Bilgi İspatı Sistemleri

$\mathbf{\Sigma} = \{\mathbf{0}, \mathbf{1}\}$. L bir dil olsun. Hatırlarsak $\mathbf{L} \in \mathbf{NP}$ ifadesi, $\mathbf{V} : \mathbf{\Sigma}^* \times \mathbf{\Sigma}^* \to \{\mathbf{0}, \mathbf{1}\}$ 'nin determenistik bir algoritma olduğunu belirtir. $\mathbf{x} \in \mathbf{L}$ ifadesi $\mathbf{P} \in \mathbf{\Sigma}^*$ olduğu anlamına gelir. Öyle ki $\mathbf{V}(\mathbf{x}, \mathbf{P}) = \mathbf{1}$ ve $|\mathbf{P}| < \mathbf{poly}(|\mathbf{x}|)$ 'dir. $\mathbf{P}$'nin $\mathbf{x} \in \mathbf{L}$ olduğuna dair kısa bir kanıt olduğunu söyleyebiliriz.

Eğer $\mathbf{V}$ randomize edilirse MA karmaşıklık sınıfına sahip oluruz. Eğer $\mathbf{V}$, $\mathbf{P}$ ile etkileşime girebilirse, $\mathbf{IP}$' yi (etkileşimli kanıtlar) elde ederiz. Sonuç olarak $\mathbf{IP} = \mathbf{PSPACE}$ olur.

Amacımız bazı $\mathbf{N}$ ve $\mathbf{x}$'ler için ek bilgiler sızdırmadan bir beyanı kanıtlamaktır. $\mathbf{x}$, $\mathbf{Z_N^*}$'da kuadratik bir kalandır.

$\mathbf{L} \subseteq \mathbf{\Sigma}^*$ olsun. $\mathbf{L}$ için sıfır bilgi ispatı sistemi $\mathbf{L}$(P, V) çifti:

1. **(Tamlık)** Tüm $\mathbf{x} \in \mathbf{L}$'ler için, doğrulayıcıdır ve ispatçı ile etkileşime girdikten sonra **"evet"** der.

2. **(Doğruluk)** Tüm $\mathbf{x} \notin \mathbf{L}$ ve tüm $\mathbf{P}^*$ sağlayıcıları için bir doğrulayıcı, $\mathbf{P}^*$ ile en az $\frac{\mathbf{1}}{\mathbf{2}}$ olasılıkla etkileşime girdikten sonra **"hayır"** der.

3. **(Sır Vermemek)** Tüm $\mathbf{V}^*$ doğrulayıcıları için, tüm $\mathbf{x} \in \mathbf{L}$'ler için olduğu gibi rastgele bir polinom zaman algoritması olan bir $\mathbf{S}^*$ simülatörü vardır.

$$\{\mathbf{transcript}((\mathbf{P}, \mathbf{V}^*)(\mathbf{x}))\} = \{\mathbf{S}^*(\mathbf{x})\} \tag{1}$$

+ **(dağılımların eşitliği)** durumlarını sağlar.

Bir simülatörün varlığı durumunda (eğer $\mathbf{x} \in \mathbf{L}$ ise o zaman) $\mathbf{V}^*$'nin $\mathbf{x} \in \mathbf{L}$ durumundan daha fazlasını öğrenemeyeceğini gösterir.

Örnek: $\mathbf{N} = \mathbf{pq}, \mathbf{x} \in \mathbf{Z_N^*}$ olsun. Diyelim ki $\mathbf{x}$'in $\mathbf{Z_N^*}$'de kuadratik bir kalan olduğunu kanıtlamak istiyoruz. $\mathbf{x} = \alpha^{\mathbf{2}}$ **(modulo N)** olsun.

- P: $\mathbf{r} \leftarrow \mathbf{Z_N}$, $\alpha = r^2$' yi gönderir.

- V: $\mathbf{b} \leftarrow \{\mathbf{0}, \mathbf{1}\}$' i gönderir.

- P: $\mathbf{z} = \mathbf{r}\alpha^{\mathbf{b}}$' yi gönderir.

- V: $\mathbf{z^2} = \alpha\mathbf{x^b}$'yi test eder. Eğer eşitse **"evet"** çıktısını değilse **"hayır"** çıktısını üretir.

Bu tasarımın **tamlığı** hemen gözükmektedir. **Sağlamlığa** gelince eğer α kuadratik bir kalan değilse o zaman doğrulayıcı en az $\frac{1}{2}$ olasılıkla **"hayır"** der (yani $\mathbf{b = 0}$ olduğunda). Eğer α kuadratik bir kalansa ama x değilse doğrulayıcı en az $\frac{1}{2}$ olasılık ile **"hayır"** der (örneğin, $\mathbf{b = 1}$ olduğunda).

İddia: Eğer $\mathbf{x}$, $\mathbf{Z_N^*}$'in kuadratik bir kalanı değilse, o zaman tüm $\mathbf{P}^*$ 'ler için, $\mathbf{V}$ en az $\frac{1}{2}$ olasılıkla **"hayır"** der.

Geriye tasarımın mükemmel bir sıfır bilgi olduğunu göstermek kalmıştır. $\mathbf{V}^*$ bir doğrulayıcı olsun ve $\{\mathbf{transcript}(\mathbf{P}, \mathbf{V}^*)(\mathbf{N}, \mathbf{x})\} = \{\mathbf{S}^*(\mathbf{N}, \mathbf{x})\}$ olsun.

Bir kara kutu simülatörü $\mathbf{S}^*$ aşağıdaki gibi oluşturulur:

1. Rastgele bir $\mathbf{z} \leftarrow \mathbf{Z_N^*}$ seçilir ve rastgele bir $\mathbf{b} \leftarrow \{\mathbf{0}, \mathbf{1}\}$ seçilir. $\alpha = \mathbf{z^2}/\mathbf{x^b} \mod \mathbf{N}$ olarak belirlenir.

2. $\mathbf{V}^*(\mathbf{x})$ hesaplanır ve ispatlayıcıdan başlayarak ilk mesaj olarak verilir.

3. $\mathbf{V}^*$, $\{\mathbf{0}, \mathbf{1}\}$'den bir b çıkarır. Eğer $\mathbf{b} \neq \mathbf{b'}$ ise adım 1'e geçilir aksi takdirde transkript olarak $[\mathbf{a}, \mathbf{b}, \mathbf{z}]$ çıktısı verilir. Bu ortalamada iki iterasyonla elde edilir.

İddia: $\{\mathbf{transcript}(\mathbf{P}, \mathbf{V}^*)(\mathbf{N}, \mathbf{x})\} = \{\mathbf{S}^*(\mathbf{N}, \mathbf{x})\}$ **(dağılımların eşitliği)**.

İspat taslağı: $\mathbf{x}$ kuadratik bir kalan olduğu için α da $\mathbf{Z_N^*}$ içinde kuadratik bir kalandır. b, α bilindiğinde $\mathbf{V}^*$ tarafından üretilen aynı dağılıma sahiptir.$\mathbf{z}$,$\mathbf{z^2} = \alpha\mathbf{x^b}$ denklemini sağlar.

Sağlamlık, protokolün tekrarlanmasıyla iyileştirilir. Bu tekrarlama şu şekilde yapılır:

- P: $\mathbf{r_1}, ..., \mathbf{r_n} \leftarrow \mathbf{Z_N}$'yi gönderir, $\alpha_\mathbf{1} = \mathbf{r_1^2}, ..., \alpha_\mathbf{n} = \mathbf{r_n^2}$
- V: $\mathbf{b_1}, ..., \mathbf{b_n} \leftarrow \{\mathbf{0}, \mathbf{1}\}$ 'yi gönderir,
- P: $\mathbf{z_1} = \mathbf{r_1}\alpha_\mathbf{1}^\mathbf{b}, ..., \mathbf{z_n} = \mathbf{r_n}\alpha_\mathbf{n}^\mathbf{b}$ 'yi gönderir,
- V: $\mathbf{i} = \mathbf{1}, ..., \mathbf{n}$ için $\mathbf{z_i^2} = \mathbf{a_i}\mathbf{x_i^b}$ eşitliğini test eder. Eğer öyleyse **"evet"** aksi halde **"hayır"** çıktısı üretilir.

Bu şemanın **"tamlık"** ve **"sağlamlık"** durumlarını gösterdik ancak nasıl bir simülatör oluşturacağı henüz belli değil. (Sadece tüm $\mathbf{b_i}$'lerin sadece $\mathbf{1/2^n}$ olasılık ile doğru olduğunu tahmin edebiliriz.)

Teorem: **L**, ihmal edilebilir hile olasılığıyla üç aşamalı mükemmel bir sıfır bilgi kanıtına sahipse $\mathbf{L} \in \mathbf{BPP}$.

Kuadratik kalanın **BPP**'de olmadığına inanıldığından kuadratik kalan durumunun üç aşamalı güçlü bir mükemmel sıfır bilgi protokolü olmadığı düşünülmektedir.

Dolayısıyla sıfır bilginin daha zayıf bir versiyonunu görüyoruz:

Cebirsel Sıfır Bilgi: Bir dil **L** için $(\mathbf{P}, \mathbf{V})$ bir $(\mathbf{t}, \in)$ - sıfır bilgi kanıtı sistemidir eğer aşağıdaki şartlar sağlanıyorsa:

1. **Sağlamlık**
2. **Tamlık**
3. **Cebirsel SB:** Tüm doğrulayıcı $\mathbf{V}^*$'ler için bütün $\mathbf{x} \in \mathbf{L}$ durumlarında $\mathbf{S}^*$ gibi bir simülatör olsun, $\{\mathbf{transcript}((\mathbf{P}, \mathbf{V}^*)(\mathbf{x}))\}$ dağılımı $\{\mathbf{S}^*(\mathbf{x})\}$'ten $(\mathbf{t}, \in)$ için ayrılamazdır (indistinguishable).

Teorem: Eğer bir $(\mathbf{t}, \in)$ -bit taahhüt(commitment) taslağı mevcutsa, **NP**'deki tüm dillerin hesaplanabilen SB kanıtları vardır.

Tanım: (kesin olmayan tanım) $(\mathbf{t}, \in)$ -bit taahhüt tasarımı aşağıdaki gibi tanımlanır:

1. Taahhüt eden $b \in \{0, 1\}$ taahhüdüne sahiptir ve $commit(b) \in \{0, 1\}$ bitini (b bit'ine taahhüt eden bit) gönderir.
2. Yüklenici taahhüdü b' olarak açabilir ve doğrulayıcı $b = b'$ olduğunu kontrol edebilir.

Bu şema aşağıdaki gibi olmalıdır:

- **Bağlayıcı:** Son derece güçlü bir taahhütçü taahhüdün $b \neq b'$ için bir taahhüt olduğuna doğrulayıcıyı ikna edemez.
- **Sağlam:** $\mathbf{commit(b)}$, b hakkında hiçbir bilgi göstermez. Yani herhangi bir bit $\mathbf{b} \in \{0,1\}$ durumunda $\{\mathbf{commit(b), b}\}$, $\{\mathbf{commit(b), r | r} \leftarrow \{0,1\}\}$ 'dan $(\mathbf{t}, \in)$-ayırt edilemez.

Örnek: Tek yönlü permütasyonlar taahhüt şeması anlamına gelir:

$\mathbf{f} : \{0,1\}^{\mathbf{n}} \rightarrow \{0,1\}^{\mathbf{n}}$ tek yönlü bir permütasyon olsun. $\mathbf{r} \leftarrow \{0,1\}^{\mathbf{n}}$'yi seçin ve $\mathbf{commit(b)} = [\mathbf{f(r)}, \mathbf{B(r)} \oplus \mathbf{b}]$ olsun, buradaki $\mathbf{B}$, $\mathbf{f}$'nin merkezi bir bitidir.

Ek B

Homomorfik Şifreleme

Soyut cebirde homomorfizm, gruplar benzeri iki cebirsel yapı arasındaki yapıyı koruyan bir haritadır.

Grup $\mathbf{G}$, bir başka eleman oluşturmak amacıyla $\mathbf{a}$ ve $\mathbf{b}$ öğelerini birleştiren bir $\circ$ işlemiyle birlikte bir küme olarak tanımlanabilir ve $\mathbf{a} \circ \mathbf{b}$ şeklinde ifade edilebilir. Bir grup olarak nitelemek için, küme ve işlem $(\mathbf{G}, \circ)$, grup aksiyomları olarak bilinen dört gereksinimi karşılamalıdır:

- **Kapalılık:** İşlemin sonucu ve girdileri $\mathbf{G}$ içindedir yani $\mathbf{a}$, $\mathbf{b}$ ve $\mathbf{a} \circ \mathbf{b}$ de $\mathbf{G}$ içindedir.
- **Birleşme:** $\mathbf{G}$'de bulunan bütün $\mathbf{a}$, $\mathbf{b}$ ve $\mathbf{c}$'ler için $(\mathbf{a} \circ \mathbf{b}) \circ \mathbf{c} = \mathbf{a} \circ (\mathbf{b} \circ \mathbf{c})$' dir.
- **Birim eleman:** $\mathbf{G}$'de bir e elemanı vardır, öyle ki $\mathbf{G}$'deki her eleman için, eşitlik $\mathbf{e} \circ \mathbf{a} = \mathbf{a} \circ \mathbf{e} = \mathbf{a}$ ' ya eşitlenir. Her grubun birim elemanı bir tanedir.
- **Ters eleman:** $\mathbf{G}$'deki her a için, $\mathbf{G}$'de öyle bir $\mathbf{b}$ elemanı vardır ki, $\mathbf{a} \circ \mathbf{b} = \mathbf{b} \circ \mathbf{a} = \mathbf{e}$, burada $\mathbf{e}$, birim elemanıdır.

G grubunun birim elemanı genellikle 1 olarak yazılır. Bir işlemin sonucu, işlenenlerin sırasına bağlı olabilir. Başka bir deyişle, eleman **a**'nın eleman **b** ile birleştirilmesinin sonucu, eleman **b**'nin eleman **a** ile birleştirilmesiyle aynı sonucu vermek zorunda değildir; $\mathbf{a} \circ \mathbf{b} = \mathbf{b} \circ \mathbf{a}$ denklemi her zaman doğru olmayabilir.

Bu denklem her zaman tam sayılar grubunda toplama özelliği için sağlanır çünkü herhangi iki tamsayı için $\mathbf{a} + \mathbf{b} = \mathbf{b} + \mathbf{a}$' dır(toplamanın birleşme özelliği). Birleşme özelliği denkleminin her zaman sağlandığı $\mathbf{a} \circ \mathbf{b} = \mathbf{b} \circ \mathbf{a}$ olan gruplara *abelian* gruplar denir.

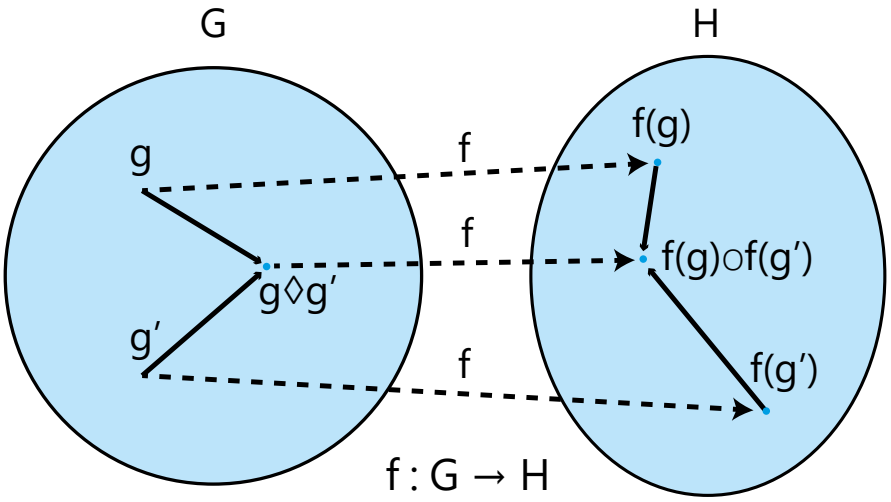


Figure 1: Grup Homomorfizm

İki gruba $(\mathbf{G}, \star)$ ve $(\mathbf{H}, \circ)$ verildiğinde, $(\mathbf{G}, \star)$ 'den $(\mathbf{H}, \circ)$ fonksiyonuna kadar bir grup homomorfizmi $\mathbf{f} : \mathbf{G} \to \mathbf{H}$ öyle ki **G** içindeki tüm $\mathbf{g}'$ ve **g** ler için aşağıdaki denklem sağlanır.

$$f(g \star g') = f(g) \circ f(g')$$

Grup homomorfizmi, Figure 1'deki gibi gösterilebilir.

$(\mathbf{P}, \mathbf{C}, \mathbf{K}, \mathbf{E}, \mathbf{D})$ bir şifreleme şeması olsun; buradaki $\mathbf{P}$; $\mathbf{C}$, düz metin ve şifreli metin alanlarıdır, $\mathbf{K}$, anahtar alandır ve $\mathbf{E}$; $\mathbf{D}$, şifreleme ve şifre çözme algoritmalarıdır. Düz metinlerin bir grup $(\mathbf{P}, \star)$ oluşturduğunu ve şifreli metinlerin bir grup $(\mathbf{C}; \circ)$ oluşturduğunu ve sonra şifreleme algoritmasının $\mathbf{E}$, $\mathbf{P}$ grubundan $\mathbf{C}$ grubuna bir harita olduğunu, yani $\mathbf{E_k} : \mathbf{P} \to \mathbf{C}$ burada $\mathbf{k} \in \mathbf{K}$ bir gizli anahtar (bir gizli anahtar şifreleme sisteminde) veya bir genel anahtar (bir açık anahtar şifreleme sisteminde) 'dır.

Tüm $\mathbf{a}$ ve $\mathbf{b}$'lerde $\mathbf{P}$ ve $\mathbf{k} \in \mathbf{K}$, eğer

KAYNAKÇA

[1] TAKASBANK-TÜBİTAK BİLGEM BiGA Cryptographic Architectural Design Özel çalışma, 2018

[2] NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system, 2008.

[3] NARULA, N. VASQUEZ, W. VIRZA, M. zkLedger: Privacy-Preserving Auditing for Distributed Ledgers, 2018.

[4] Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., and Capkun, S. Evaluating User Privacy in Bitcoin

[5] RON, D. and SHAMIR, A Quantitative Analysis of the Full Bitcoin Transaction Graph, 2012.

[6] REID, F. HARRIGAN, M. An Analysis of Anonymity in the Bitcoin System, 2011 IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing.

[7] ANDROULAKI, E , KARAME, G.O. , ROESCHLIN, M., SCHERER, T., and CAPKUN, S. Evaluating User Privacy in Bitcoin.

[8] SPAGNUOLO, M. Thesis: BitIodine: Extracting Intelligence from the Bitcoin Network, 2013 Politecnico di Milano

[9] MEIKLEJOHN, S., POMAROLE, M., JORDAN, G., LEVCHENKO, K., Mccoy, D., VOELKER, G.M., SAVAGE, S. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, 2013

[10] GARMAN, C., GREEN, M., Ian MIERS, I. Accountable Privacy for Decentralized Anonymous Payments, 2016.

[11] BUNZ, B., BOOTLE, J., BONEH, D., POELSTRA, A., WUILLE, P., and MAXWELL, G. Bulletproofs: Short Proofs for Confidential Transactions and More, 2017.

[12] KOENS, T., RAMAEKERS, C., and van WIJK, C. Efficient Zero-Knowledge Range Proofs in Ethereum ING, 2017

[13] Hearn, M.: Merge avoidance: Privacy enhancing techniques in the bitcoin protocol (2013), http://www.coindesk.com/merge-avoidance-privacy-bitcoin/

[14] Wilcox-O'Hearn, Z.: Zcash begins (2016), zCash Blog Post, https://z.cash/blog/zcash-begins.html. Retrieved 2016-10-31.

[15] MA, S., DENG, Y., HE D., ZHANG J., XIE X., An Efficient NIZK Scheme for Privacy-Preserving Transactions over Account-Model Blockchain, 2017

[16] Certicom Research, SEC 2: Recommended Elliptic Curve Domain, Parameters, Standards for Efficient Cryptopgraphy, 2010

[17] National Institute of Standards and Technology, FIPS PUB 186-4: Digital signature standard, 2013

[18] Schnorr Non-interactive Zero-Knowledge Proof, Newcastle University, 2017 [18] Ian Miers, Christina Garman, Matthew Green, Rubin, A.D., Zerocoin: Anonymous Distributed E-Cash from Bitcoin, 2013

[19] Koens, T.,Ramaekers, C., van Wijk, C., Efficient Zero-Knowledge Range Proofs in Ethereum, ING 2018.

[20] https://crypto.stanford.edu/pbc/notes/crypto/zk.html

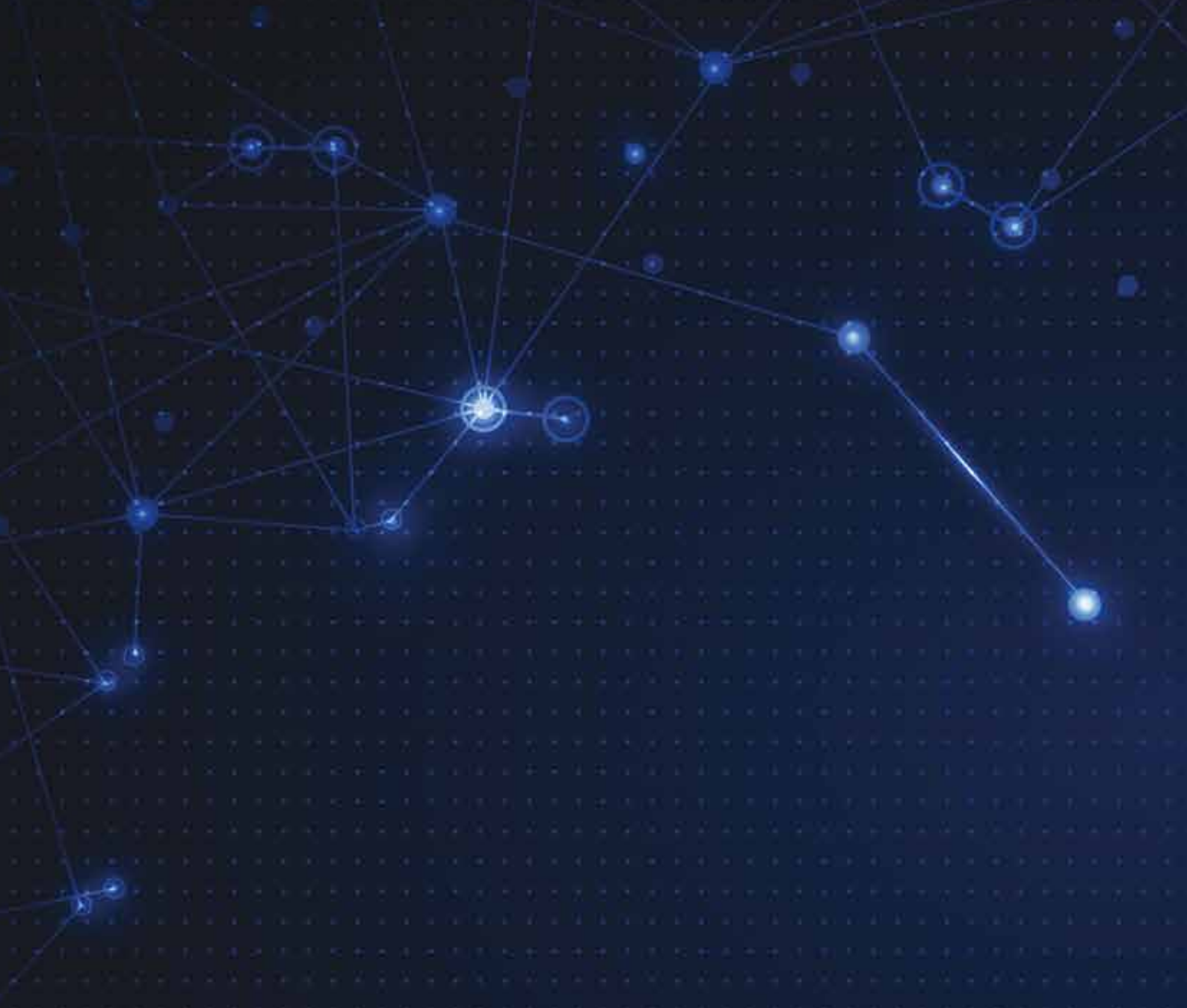
[21] Homomorphic Encryption https://www.springer.com/cda/content/document/cda_downloaddocument/9783319122281-c1.pdf?SGWID=0-0-45-1487904-p177033600

TAKAS İSTANBUL

FinTechHub
TAKAS İSTANBUL

FİZİKSEL DAYANAĞI OLAN, REGÜLASYONLA UYUMLU, MAKSİMUM GİZLİLİK VE GÜVENLİK SAĞLAYAN ALTIN

24h GÜVENLİ TRANSFER



TAKAS İSTANBUL

Takasbank

İstanbul Takas ve Saklama Bankası A.Ş.
Reşitpaşa Mahallesi, Borsa İstanbul Caddesi, No: 4 Sarıyer 34467 İstanbul
T +90 212 315 25 25 F +90 212 315 25 26 ats@takasbank.com.tr
www.takasbank.com.tr