BLOCKCHAIN
TÜRKİYE

BLOCKCHAIN İÇİN KAVRAMSAL MİMARİ

Blockchain Türkiye Platformu Teknoloji Çalışma Grubu Raporu

MAYIS 2019

TBV
TÜRKİYE BİLİŞİM VAKFI

BLOCKCHAIN TÜRKİYE

BLOCKHAIN İÇİN KAVRAMSAL MİMARİ

Blockchain Türkiye Platformu
Teknoloji Çalışma Grubu Raporu

MAYIS 2019

***

Tasarım ve Grafik Uygulama
TERMİNAL MEDYA LTD. ŞTİ.
Maslak Mah. Bilim Sokak No:5 SUN Plaza Kat:13 Sarıyer/İSTANBUL
0(212) 367 4988 ve 0(532)643 6959

Editör
ÖZLEM ÖZKAN

Grafik Uygulama
GÜLİSTAN ŞENOL

Baskı
RUMİ MATBAACILIK
Maltepe Mah. Fazılpaşa Cad. No:8 Topkapı/İSTANBUL
0(212) 612 7172

Teknoloji

İÇİNDEKİLER

TÜRKİYE BİLİŞİM VAKFI

Türkiye Bilişim Vakfı, *Türkiye'nin bilgi toplumuna dönüşebilmesi için altyapının oluşturulabilmesine katkıda bulunmak ve bilişim sektörünün ekonomideki payının arttırılması için, bilimsel araştırma ve geliştirme etkinliklerinde bulunarak ekonomik ve sosyal çalışmalar yapmak, projeler üretmek ve uygulamalarını sağlamak amacıyla kurulmuştur.*

BLOCKCHAIN TÜRKİYE

Blockchain Türkiye Platformu, *Türkiye Bilişim Vakfı (TBV) liderliğinde Türkiye'de sürdürülebilir blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapış biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu oluşturmak amacıyla kurulmuştur.*

SUNUŞ

Faruk Eczacıbaşı
Blockchain Türkiye
Yürütme Kurulu Başkanı
Türkiye Bilişim Vakfı
Yönetim Kurulu Başkanı

Türkiye Bilişim Vakfı'nı Mayıs 1995'te kurduğumuzda, kendine çok basit bir misyon belirlemişti; bilgi ve iletişim teknolojilerinin ülkenin verimliliğine katkıda bulunmasını sağlamak. Bugün ister Dördüncü Endüstri Devrimi diyelim, ister bilgi toplumu, gerçek şu ki dünya gittikçe hızlanan bir aşamaya girdi ve bizi de yeni bir düşünme biçimine zorluyor.

Blokzincir, bu yeni düşünce kalıbının en devrimsel sonuçları olacak ürünlerinden biri ve bu teknolojinin anlaşılabilmesi, uygulanabilmesi için, deneyimin kazanılması beklenmeli. Her yeni teknolojide olduğu gibi, blokzincirde de konseptlerle başlayan deneysel süreçlerin pilot aşamalarına, bunların da nihai ürüne dönüşmesi gerekiyor.

Blokzinciri diğer teknolojilerden ayıran en temel özellik ise beraberinde getirdiği sektörler arası konsorsiyumlar, platformlar gibi ortamlarda "birlikte çalışma" ihtiyacı. Yeni bir düşünce kalıbı olarak blokzincir, ekosistemlerin önemini artırırken, teker teker şirketler ve onların ürünlerinden ziyade, bir arada değer yaratmayı başarabilen ekosistemleri ön plana çıkarıyor.

Bu sebepten, Türkiye Bilişim Vakfı olarak 8 Haziran 2018 tarihinde bir adım attık. Blokzincir teknolojisinin Türkiye'de yaygınlaşması, bilinirliği ve kullanımının artırılması, faydalarının araştırılması ve stratejik önceliklerinin saptanması gibi temel hedeflerle, Blockchain Türkiye Platformu'nu (BCTR'yi) hayata geçirdik. Blockchain Türkiye Platformu (BCTR), Türkiye'de sürdürülebilir blokzincir ekosistemi oluşturarak, bu teknoloji ile yeni dönem iş yapış biçimlerinin önündeki zorlukların giderilmesine yönelik bir paylaşım platformu.

Umuyorum ki dünya, buhar makinesinin icadından bu yana alıştığımız "önce üret, sonra sat" iş modelinden, "birlikte üret, sat ve tüket" (Co-create & Prosume) kavramlarına doğru yolculuğa çıkarken, bu platformun ve ürettiği çalışmaların ülkemize bir faydası dokunsun.

KATKI SAĞLAYAN KURUMLAR

BANKALARARASI KART MERKEZİ A.Ş.

Bankalarının ortaklığıyla kurulan Bankalararası Kart Merkezi A.Ş.'nin (BKM) faaliyetleri, ödeme sistemleri içerisinde; nakit kullanımı gerekmeksizin her türlü ödemeyi veya para transferini sağlayan veya destekleyen sistem, platform ve altyapıları oluşturmak, işletmek ve geliştirmektir. BKM, nakit dışı ödemeleri kolaylaştıran güvenli çözümler sunmak misyonu çerçevesinde yeni teknolojileri takip etmektedir. Bu kapsamda Türkiye'nin ilk blokzincir projesi olan ve bir sadakat programı konseptiyle geliştirilen BBN, BKM bünyesinde geliştirilmiştir. BKM, bu projenin ardından blokzincir teknolojisi üzerine çalışmalarını eğitim sertifikalarının dijital dünyada saklanmasını ve paylaşılmasını sağlayan belgem.io projesiyle sürdürmektedir.

GARANTİ BANKASI

1946 yılında Ankara'da kurulan Garanti Bankası, 30 Haziran 2018 tarihi itibarıyla 385 milyar Türk Lirası'na yaklaşan konsolide aktif büyüklüğü ile Türkiye'nin en büyük ikinci özel bankası konumundadır. Kurumsal, ticari, KOBİ, bireysel, özel ve yatırım bankacılığı, ödeme sistemleri dahil olmak üzere bankacılık sektörünün tüm iş kollarında faaliyet gösteren Garanti, Hollanda ve Romanya'daki uluslararası iştiraklerinin yanı sıra bireysel emeklilik ve hayat sigortası, finansal kiralama, faktoring, yatırım ve portföy yönetimi alanlarındaki finansal iştirakleri ile entegre bir finansal hizmetler grubudur. Banka'nın vazgeçilmez değerlerini destekleyen ileri bir kurumsal yönetişim modeli uygulayan Garanti Bankası'nın hakim ortağı, hisselerinin %49.85'ine sahip olan Banco Bilbao Vizcaya Argentaria S.A. (BBVA)'dır. Hisseleri Türkiye'de, depo sertifikaları İngiltere ve ABD'de işlem gören Garanti'nin Borsa İstanbul'daki halka açıklık fiili dolaşım oranı 30 Haziran 2018 itibarıyla %50.06'dır.

SOFTTECH

Softtech, 2006 yılından bu yana İstanbul, Ankara, San Francisco ve Şanghay'da bulunan ofisleriyle toplam 8 farklı lokasyonda 1000'i aşkın profesyonel kadroyla Türkiye'nin en büyük yerel sermayeli yazılım şirketidir. Dünyadaki teknoloji merkezlerini de yakından takip ederek, bankacılık ve finans sektöründeki tecrübesini ve deneyimli insan kaynağı ile farklı alanlarda faaliyet gösteren iş ortaklarına, müşteri odaklı çözümler geliştirmektedir. Yaratıcı ve inovatif çözümler sunarak farklı alanlardaki ürünlerle uluslararası pazarda da güçlü ve global bir oyuncu olma yolunda hızlı bir şekilde ilerlemektedir. Bu hedef doğrultusunda da Softtech, birçok yenilikçi girişimi desteklemekte ve dünyaya açılmalarına yardımcı olmaktadır. Softtech bünyesinde birer ürün olarak doğarak 2 ayrı şirket haline dönüşen Livewell ve En İyi Kurumiçi Girişimcilik Ödülüne sahip olan Gullseye firmaları yer almaktadır. Türkiye'nin en büyük yazılım teknoloji şirketlerinden biri olma iddiasını istatistiklere de yansıtan Softtech, Türkiye'nin İlk 500 Bilişim Şirketi Araştırması kapsamında gerçekleşen Bilişim500 Ödül Töreni'nde "Türkiye Ekonomisine Katkı Özel Ödülleri" kategorisi altında "Türkiye Merkezli Üretici Yazılım Birincisi" ödülünün sahibi olmuştur.

TÜBİTAK - BİLGEM

TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM), 40 yılı aşkın bilgi birikimi ve % 85'i ar-ge personeli olmak üzere 1.700 kişiyi aşan nitelikli insan kaynağı ile bilişim, bilgi güvenliği ve elektronik harp alanlarında Türkiye'nin en yetkin Ar–Ge merkezi olma niteliğini taşımaktadır. Kamu ve özel kurum/kuruluşların ihtiyaçlarına istinaden, blokzincir teknolojilerinin altyapısı, kurulumu, güvenlik ve mahremiyet analizi, iş modelleri, kitle fonlama yaklaşımları ve muhtelif teknik detayları üzerine Ar-Ge faaliyetlerini icra etmek üzere, BİLGEM UEKAE Matematiksel ve Hesaplamalı Bilimler Biriminin altında kurulan Blokzincir Araştırma Laboratuvarı'nda bu konudaki faaliyetlerini yürütmektedir.

ÖNSÖZ

Barış Özistek
Boğaziçi Ventures
Yönetim Kurulu Başkanı

Blockchain'in en belirgin karakteristiklerinden birisi çoklu katılımcıların olması gereğidir. Bu nitelik farklı yönlerden hem avantajlara hem de dezavantajlara sahiptir. Raporun içeriğini de okuduğunuzda blockchain teknolojisini etkin kullanarak problemler çözmek için ne kadar farklı yetkinlik ve teknolojinin bir araya gelmesi gerektiğini göreceksiniz. Önemli olanın avantajlardan maksimum faydayı sağlamak ve dezavantajları da mümkün olduğunca bertaraf etmek olduğuna inanıyoruz. Tam bu noktada Blockchain Türkiye Platformu (BCTR) çok kritik bir boşluğu doldurmuş, Türkiye için farklı sektörlerden ve ilgi alanlarından çok sayıda kurum ve kişiyi bir araya getirerek Blockchain'in doğasındaki birlikte-çalışma ihtiyacı için çok verimli bir ortam oluşturmuştur.

Doğru kazanımları elde edebilmek adına BCTR platformu, çalışmalarını Blockchain teknolojisini ve onun etkisiyle oluşan paradigma değişimini hem dikeyde hem de yatayda oluşturulmuş çalışma alanları vasıtasıyla çok boyutlu ele alarak gerçekleştirmektedir. Dikeyde sektörel değer alanları değerlendirilirken, yatayda ise farklı boyutları ile bu teknoloji ve paradigma değişimi çalışılmaktadır.

Yataydaki çalışma gruplarından birisi olan Teknoloji çalışma grubu Blockchain'i teknik perspektiften ele arak bu teknolojinin tanımına, gelişimine, ve yaygınlaştırılmasına katkı sunmayı amaçlamıştır. Bu kapsamda da çalışmalarına Blockchain için teknik bir tanım yaparak başlamış ve ilk çıktısı olarak ta bu rapordaki kavramsal mimariyi oluşturmuştur. Her yeni gelişen ve anlaşılan teknolojide olduğu gibi, gerek kapsam gerekse de bileşen alternatifleri noktalarında bir kargaşa mevcuttur. Blockchain'i bir çözüm olarak görüp, tanımını mevcut kullanım alanlarından bağımsız ve tarafsız bir şekilde, yalnızca kavramsal bir sistematik ile yapmak bu karmaşayı hafifletmekte yardımcı olacaktır. Bu kazanımın yanı sıra Blockchain ekosistemi içerisindeki tüm paydaşlar için ortak bir dil oluşturulması ve gerek strateji belirleme gerekse de alternatif seçimlerinde ortak bir değerlendirme enstrümanı yaratılması noktalarında da fayda sağlayacaktır.

Geleneksel sektörlerden farklı olarak teknoloji dünyası bizlere sürekli yeni fırsat ve imkanlar sunmaktadır. Blockchain teknolojisi ile birlikte yaşanacak değişimi Türkiye yakalayabilir ve hatta liderliğini yapabilir. Bu anlamda tüm okuyucular için çok büyük fayda sağlayacağına inandığım bu raporu oluşturan BCTR Teknoloji çalışma grubunu kutlar, emeği geçen tüm çalışma grubu paydaşlarına, bu imkanı veren değerli şirketlere ve BCTR platformuna teşekkürlerimi sunarım.

Saygılarımla.

YÖNETİCİ ÖZETİ

Blockchain temelli kullanım senaryolarının daha fazla yaygınlaşmasındaki en önemli engeller arasında bu yeni teknolojinin gerek olgusal karakteristiklerinin yeterince anlaşılamaması ve gerekse de gündeme gelişinin bu teknolojinin bir uygulaması ile oluşunun yarattığı karmaşa gösterilebilir. Bu sorunu aşmada öncelikle Blockchain'i bir çözüm olarak görmek ve sonrasında da bu çözüm için stratejileri ve alternatifleri ortak bir çerçeve üzerinden değerlendirebiliyor olmak faydalı olacaktır. Bu amaçla Blockchain için bir referans mimari tanımı yapmak oluşturmak yoluna gidilmiştir. Böylece şu konularda fayda sağlanacağını beklenilmektedir: "Blockchain kapsamında oluşacak farklı çözüm seçeneklerin kıyaslanabilmesi içi ortak zemin olması", "Her bir seçeneğin tanımının ve kapsam alanının net belirlenebilmesi", "Gerçek dünya problemlerinin çözümü için Blockchain'in uygunluğunun değerlendirilmesinde kullanılacak bir çerçeve olması", ve "Bu sistem/çözüm kapsamda çalışacak farklı ilgi ve bilgi seviyelerindeki tüm paydaşlar için ortak bir dil oluşturulması". Mimari tanım, bir sistemin temel bileşenlerinin organizasyonunu tanımlamada kullanılan bir pratiktir. Sistemlerin karmaşıklığına bağlı olarak farklı detay seviyelerinde bu organizasyonlar tanımlanabilir, ki raporun bu versiyonu kapsamında en üst detay seviyesi olan kavramsal mimari tanımı ile yetinilecektir. Kavramsal seviyede tanımlama, sistemin bileşenlerinin belirli alanlar (raporda seçilen alanlar; vizyon/strateji ve gereksinimler, iş, veri, uygulama, ve altyapı olarak belirlenmiştir) bazında oluşturulmuş bir sınıflandırmaya tabi tutulmasından oluşmaktadır. Burada, belirlenecek sistem bileşenlerinin özel bir kullanıma, teknolojiye, veya gerçeklemeye özgü terminolojiden bağımsız olarak, yalnızca kavramsal bir terminoloji ile ifadesi önemlidir. Benzer şekilde bileşenler arasında belirlenecek dikey hiyerarşiler de özel kullanım veya tasarımlardan bağımsız olarak genel geçerdir. Mimari tanımlamanın bir başka boyutu da perspektiflerdir. Kavramsal seviyede özel olarak belirli perspektiflere ihtiyaç duyulmayacağını ön görerek, bütünsel bir bakış açısı ile ilerlenilmiştir.

1. GİRİŞ

Özellikle kripto paralara olan ilgide yaşanan patlamadan sonra, altındaki teknoloji olarak Blockchain de her sektörde merak ve gündem oluşturmuştur. Buna rağmen Blockhain'i, hala hem iş hem teknoloji alanlarından pek çok karar vericinin bile doğru yorumlamakta zorluk yaşadığı bir kavram ve çözüm olarak nitelemek çok haksız olmaz. Bu zorlukların temelinde, Blockchain'in olgusal karakteristiklerinin bir teknolojik buluştan farklı oluşunun yeterince anlaşılamamasına ek olarak, gündeme gelişinin kendisinin bir uygulaması vasıtasıyla olması sebebiyle yaşanan karmaşayı da göstermek mümkündür. Sebep ne olursa olsun, Blockchain'i bir çözüm olarak görüp, tanımını mevcut gerçeklemelerinden ve uygulamalarından bağımsız (nötr) bir şekilde, yalnızca kavramsal bir sistematik ile gerçekleştirerek yapmak bu zorlukları hafifletmekte yardımcı olacaktır.

Bu amacı gerçekleştirebilmek için Blockchain özelinde kavramsal mimari oluşturmak yoluna gidilecektir. Mimari tanım, bir sistemin temel bileşenlerinin organizasyonunu tanımlamada kullanılan bir pratiktir. Sistemlerin karmaşıklığına bağlı olarak farklı detay seviyelerinde bu organizasyonlar tanımlanabilir, ki raporun bu versiyonu kapsamında en üst detay seviyesi olan kavramsal mimari tanımı ile yetinilecektir. Ancak, ileriki dönemdeki çalışmalarda bu kavramsal tanımın detaylandırılması planlanmaktadır.

Kavramsal seviyede tanımlama, sistemin bileşenlerinin belirli alanlar (örneğin veri, uygulama, altyapı, strateji, vb.) bazında oluşturulmuş bir sınıflandırmaya tabi tutulmasından oluşmaktadır. Burada, belirlenecek sistem bileşenlerinin özel bir kullanıma, teknolojiye, veya gerçeklemeye özgü terminolojiden bağımsız olarak, yalnızca kavramsal bir terminoloji ile ifadesi önemlidir. Benzer şekilde bileşenler arasında belirlenecek dikey hiyerarşiler de özel kullanım veya tasarımlardan bağımsız olarak genel geçer olacaktır. Mimari tanımlamanın bir başka boyutu da perspektiflerdir. Yine kavramsal seviyede özel olarak belirli perspektiflere ihtiyaç duyulmayacağını ön görerek, bütünsel bir bakış açısı ile ilerlenecektir. Ancak, elbette detay seviyesi arttıkça özel olarak farklı perspektiflerde (uygulama, veri, altyapı, vb.) bu tanımlamayı yapma ihtiyacı olacaktır.

Bir sistem (veya çözüm) için mimari tanımlama yapmak şu konularda fayda sağlayacaktır: bu sistem kapsamında oluşacak farklı çözüm seçeneklerin kıyaslanabilmesi içi ortak zemin olması, her bir seçeneğin tanımının ve kapsam alanının net belirlenebilmesi, problemler için çözümün uygunluğunun değerlendirilmesinde kullanılacak bir çerçeve olması, ve bu sistem/çözüm kapsamda çalışacak farklı ilgi ve bilgi seviyelerindeki tüm paydaşlar için ortak bir dil oluşturulması. İşte bu raporda Blockchain özelinde bir kavramsal çerçeve ve terminoloji tanımlamayı amaçlamaktadır.

Dağıtık kayıt defteri (DLT) kavramı ve Blockchain genellikle birbirlerinin yerine kullanılsa da, Blockchain'i özelleşmiş bir DLT olarak nitelemek doğru olacaktır. Blockchain'i diğer DLT'lerden farklılaştıran temel unsur, işlem kayıtlarının bloklar halinde organize edildiği ve bu bloklarında kriptografik olarak birbirine bağlanması ile oluşturulan bir veri yapısının kullanılmasıdır.

İleride de değinileceği üzere Blockchain kavramının değer önerimleri birbirleriyle çelişen gereksinimler ve kısıtlar üzerinde şekillendirilmiştir. Bu nedenle tüm önerimleri tek bir çözümde sunabilmek mümkün olamamaktadır ve alternatifler arasında bir ödünleşme yapmak gerekmektedir. İşte yapılan bu tercihlere göre şekillenmiş çok farklı türde Blockchain gerçeklemesi ortaya çıkmıştır. Bu raporda yapılacak mimari tanım bu farklı çözümlerin kapsamlarının ortak bir çerçeve üzerinden mukayeseli olarak yapılabilmesine olanak sağlayacaktır.

Bir problem için Blockchain kullanımı değerlendirilirken, genellikle çeşitlenmiş Blockchain seçenekleri arasından bir tanesine odaklanılır ve siyah-beyaz şeklinde bir karar ile ilerlenir. Ancak problemin bütünsel olarak Blockchain ile çözümünün yerine, alt problemlere odaklanılarak birden fazla Blockchain yaklaşımının kullanımı ile çözüme gitmek çoğu zaman daha etkin bir kullanım sağlamaktadır (örneğin private network şeklinde temel bir senaryoya, public network kullanımı dahil edilerek noter/denetleme fonksiyonu gerçeklenebilir). İşte bu noktada da tüm alternatiflerin değer önerimlerinin ortak bir çerçeve üzerinden kıyaslanabilmesi önemli olacaktır.

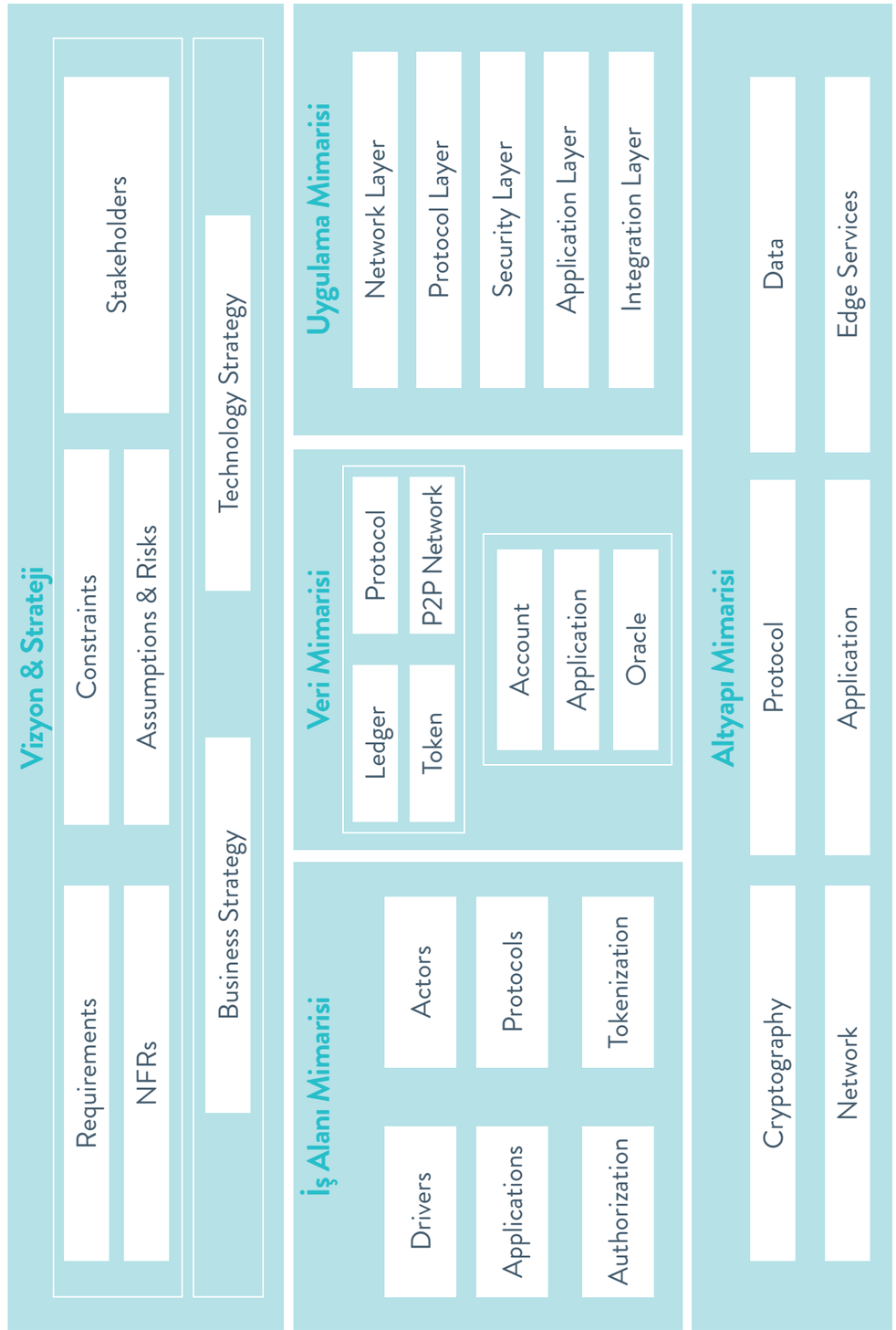
Blockchain'in problemler için çözüm olarak değerlendirilmesinde izlenecek strateji pek çok fonksiyonel olmayan gereksinimin de dikkate alınmasını içermelidir. Elbette Blockchain kullanımından maksimum değer sağlamak temel amaçtır, ancak bu türden bazı gereksinimlerin yaratacağı kısıtlar nedeniyle evrimsel bir kullanım ve benimseme stratejisi izlemek çoğu zaman daha gerçekçi olacaktır. Bitcoin örneğinde olduğu gibi public network kurgusundaki kullanımlar sarsıcı değer önerimleri sunmaktadır, ancak mevcut koşullara uyumu ve yaygınlaşması hala pek çok belirsizliğin ve alt problemin çözülmesini gerektirmektedir. Bu evrimsel süreci baştan itibaren net kapsamlarla tariflemek yine ortak bir çerçeveyi gerektirecektir.

İnterneti dönüştürme potansiyeline sahip olan Blockchain teknolojisi, kurumsal seviyedeki iş yapış şeklini değiştirerek yeni kullanım senaryolarını sunuyor. Günümüzde bir çok şirket ve konsorsiyum, yeniden kurguladıkları kullanım senaryolarıyla ilgili Ar-Ge süreçlerini ve pilot çalışmalarını sürdürüyor. Blockchain teknolojisi, ortaya çıkan protokoller ve uygulamalarla kendi ekosistemini genişletmeye ve daha giderek büyüyen kitleler tarafından benimsenmeye devam etmektedir. Günümüzde Blockchain platformları, sahip oldukları teknolojiyi daha ileriye taşımak için ölçeklenebilirlik, birlikte çalışabilirlik ve gizlilik olarak sıralayabileceğimiz üç önemli öğeye yoğunlaşmaktadır. Kullanılan araçlar, servisler ve alt yapılar ile platformların üzerine inşa edilen kullanım senaryoları ve uygulamalarını, sektörlere

göre dağılımı günümüzde B2C alanında sosyal medya, mesajlaşma, içerik yönetimi, reklam ve e-ticaret sektörlerine yoğunlaşmıştır. B2C alanında karşılaştığımız ve genellikle halka açık (public) zincirlerin kullanıldığı dağıtık uygulamaların, günümüzde verinin sahipleri olarak nitelendirebileceğimiz platformların yerine geçmesi olasıdır. B2B alanında ise kurumlar arasındaki ilişkilerin yönetildiği, özel zincirlerde (private) akıllı sözleşmelerin desteğiyle kurgulanmış, takip, doğrulama ve kanıtlama uygulamalarını görüyoruz. Finans sektöründe ise günümüz hizmetlerinin yerini alması için tasarlanmış ve yeni değer kavramını da yapısına eklemiş uygulamaları görebiliriz. Blockchain teknolojisi, güvenilir bilgilerin yönetimini kolaylaştırabilir ve devlet kurumlarının bu bilgilerin güvenliğini korurken kritik kamu sektörü verilerine erişimini ve kullanımını kolaylaştırır. Bir halka açık veya özel bir Blockchain'de depolanan veriler tek bir oyuncu tarafından değiştirilemez veya silinemez; bunun yerine, otomasyon ve yönetişim protokolleri kullanılarak doğrulanır ve yönetilir. Bu özellikler çerçevesinde yeniden şekillenen veri sektöründe, kişisel verilerin farklı bir bakış açısıyla değerlendirildiği, yapay zeka teknolojisinin de dahil edildiği Blockchain uygulamalarıyla karşılaşmaktayız.

Raporun geri kalan kısmında oluşturulan kavramsal mimari tanım anlatılmaktadır. Bu tanımı betimler taslak Şekil 1'de gösterilmektedir. Bu taslaktan da görüleceği üzere sistem tanımı genel mimari pratiğine paralel olarak 5 temel alan üzerinde bir sınıflandırma yapılarak oluşturulmuştur ve ileride her biri için detay tarifler sunulmaktadır.

Şekil 1. **Yüksek Seviye Blockchain Kavramsal Mimarisi**



2. MİMARİ VİZYON VE STRATEJİ

Blockchain merkezi olmayan dijital kayıt defteri kavramının özel bir türüdür. Kayıtların peer-to-peer (P2P) ağ içerisindeki bilgisayarlarda eş kopyalar şeklinde ve eş güdüm ile onaylanıp saklanmasını sağlayarak, bu kayıtların değiştirilemezliklerini garanti altına alan bir teknoloji ile gerçeklenir. Böylece güvenli, değiştirilemez, şeffaf, demokratik ve denetlenebilir şekilde işlem yapmak vizyonunu yerine getirir.

Bu vizyon bir takım gereksinimlerin karşılanması amacıyla ortaya çıkmıştır ve bu gereksinimler tüm Blockchain protokolleri için ortak bazı prensipler ile adreslenir. Bunlar; ortak ve tutarlı durum (veri) saklama ortamına birden fazla paydaşın kayıt yazabilmesinin gerekmesi, tüm bu kayıt ekleyebilen aktörler arasında bir güven veya hiyerarşi eksikliğinin olması, bir aracı veya merkezi kontrol otoritesinin istenilmemesi veya gerek duyulmaması, kayıtların bilerek veya bilmeyerek değiştirilmesinin istenilmemesi, ve ekosistem içerisindeki katılımcıların kurguya bağlı olarak belirlenecek seviyede anonimliğe sahip olmasıdır.

Bu fonksiyonel gereksinimlerin yanı sıra fonksiyonel olmayan gereksinimlerde Blockchain çözümlerinin başarımını etkileyen önemli karar noktaları olarak değerlendirilmektedir. Teknik bağlamda bunlar ölçeklenebilirlik, işlem hızı ve hacmi, sistemin güvenilirliği (çatallaşma-fork problemi, ortak karar alma mekanizmalarındaki açıklar, vb.), diğer sistemler ile entegrasyon ve ortak çalışabilme, teknik ve süreç olgunluk/standardizasyon düzeyi, ve verimlilik (enerji ve zaman gibi maliyetler, vb.) şeklinde sıralanabilir. Ancak, fonksiyonel olmayan gereksinimleri yalnızca teknik bağlamda ele almak kısıtlayıcı olur ve bu da gerçekçi kararlar vermeyi zorlaştırır. Bu nedenle, Blockchain kavram olgusu içerisinde politik, ekonomik, kültürel ve sosyolojik yönlerden de bazı gereksinimleri çözüm tasarımında değerlendirmek önemlidir; regülasyonlar ve yönetimsel düzenlemeler (politikalar) ile uyum derecesi, kültürel ve sosyal davranış ile ilgili risk faktörleri (güven, sosyopati, değişiklik ihtiyacı, vb.), ve işbirliği gereksinimi bu türden gereksinimler arasında gösterilebilir.

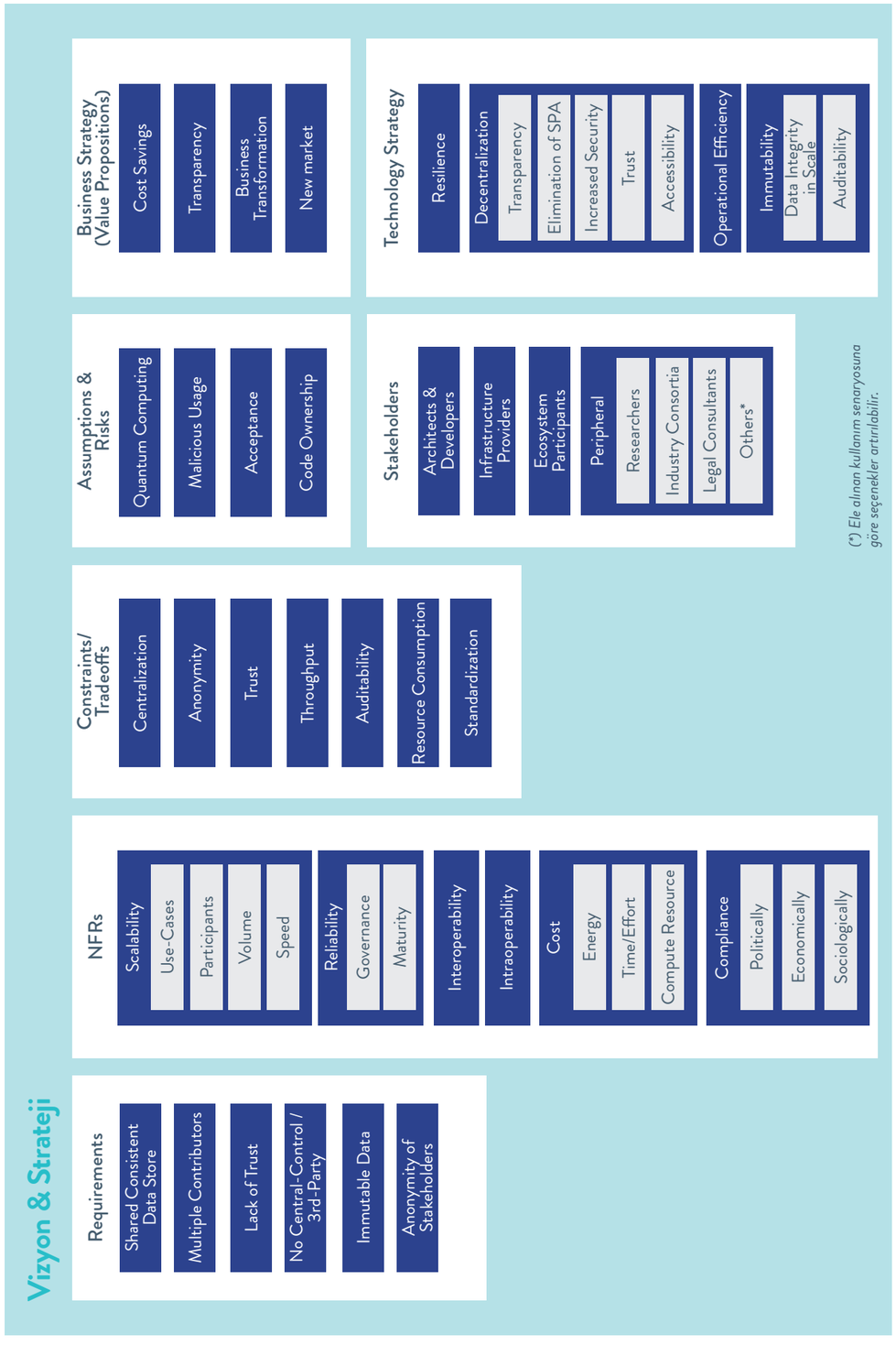
Görüldüğü üzere Blockchain kullanım kararı pek çok değerlendirme gerektirmektedir. Bir başka deyişle Blockchain'in sihirli bir değnek gibi düşünmek yanlıştır. Zira bu gereksinimlere ek olarak, çözüm bazı riskleri ve kabulleri de barındırır. Dolayısı ile risk değerlendirmesinde kuantum hesaplamadaki beklenen gelişmeler, kötü niyetli kullanıcılar ve kullanımlar, yazılımın yönetişimi, değişimlere kullanıcıların göstereceği adaptasyon gibi faktörlerde göz önünde bulundurulmalıdır.

Çözüm olarak Blockchain kullanımında karar kılındığı durumlar genellikle kurumlar ve organizasyonlar için maliyet tasarrufu, denetlenebilirliği artırmak, mevcut bir iş kolunun/sürecinin dönüştürülmesi veya tamamen yeni bir iş kolunun ve pazarının yaratılması gibi stratejilerin gerçekleştirilmesi

içindir. Bu ticari stratejilerin yanı sıra teknoloji stratejisi özelinde de şu kazanımlar amacıyla kullanımları mevcuttur: kırılma noktasını yayarak direnç sağlama (resilience), merkezi otoritenin kaldırılması ile şeffaflık, güvenlik, güven, operasyonel verimlilik, veri değiştirilemezliğinin garanti altına alınması sayesinde artırılmış denetlenebilirlik ve uyum, veri bütünlüğü, ve erişilebilirlik.

Blockchain kavramı daha önce bahsi geçen mimari yapılar ve bileşenlerin konfigürasyonlarına göre farklı karakteristiklere sahip olacak şekilde gerçeklenebilir. Ancak karakteristikleri farklı olsa da, tüm gerçeklemelerde yer alan temel paydaşlar genel olarak ortaktır ve bunlar mimarlar ve yazılımcılardan, altyapı sağlayıcılarından, ekosistem (ağ) katılımcılarından, araştırmacılardan, ve diğer çevresel paydaşlardan oluşur.

Şekil 2. **Mimari Vizyon ve Gereksinimler Alanı.**



3. İŞ MİMARİSİ ALANI

Teknolojik gelişmeler ve inovasyonlar, sürekli olarak gelişmekte ve büyümektedir. Kişiler ve kurumların bu gelişmeler ve yeniliklerden haberdar olmaları gerekmektedir. Blockchain'in getirdiği paradigma değişikliği bu evrimi farklı bir perspektif doğrultusunda sürdürmektedir. Blockchain'in arkasındaki teknoloji, konsept olarak veri tabanına benzese de, teknolojinin doğru yorumlanabilmesi için anlaşılması gereken temel kavramlar bulunmaktadır. Akıllı sözleşmeler, merkezi olmayan bir fikir birliği(mutabakat), kriptografik kanıt, değiştirilemez zincir yapısı ve değerin evrimi bu kavramların başında gelmektedir. Bu heyecan verici bilgi işlem paradigması dağıtık uygulamaların geliştirilmesinde kritik rol oynamaktadır. Bu bölüm, Blockchain teknolojisiyle gelen paradigma değişimini iş mimarisi perspektifinden ele alacaktır.

Yaşanan teknolojik gelişmeler zamanla insanların hayatına farklı noktalarda dokunmaya devam ederken, sunduğu yeni paradigmalarla değişimi de beraberinde getirmiştir. Hızla dijitalleşen dünyada, veri, işlenebilen değerli bir madene dönüşürken, iletişim araçları mesafeleri kısaltarak, insanların birbirleriyle olan etkileşimlerini anlık hale getirmiştir. Bu bağlamda bireysel haklar da evrimleşerek kapsamını artırmış ve artık dijital belirteçleri de kapsayan bir yapıya kavuşmuştur. Bu paradigma değişimini sağlıklı bir şekilde yorumlamak ve anlamlandırmak için Blockchain teknolojisinin eşsiz bir araç olduğu görülmektedir. Blockchain teknolojisi, dijital değerlerin hakim olduğu, merkeziyetsiz ve tam güvenilir bir ortam sunarak geleceğin şekillenmesindeki potansiyelini günümüzdeki farklı uygulamalarıyla bizlere kanıtlamaktadır.

Asırlardır insanların en çok kullandığı araçlardan biri olan paranın, bugüne kadar gelinen noktada yaşadığı değişimler, bir çok kavram için ilham kaynağı olmuştur. Sanat, hukuk ve daha nice alanda evrimleşen değer, her gün daha çok dijitalleşmiştir. Blockchain teknolojisi perspektifinden bu konuyu değerlendirdiğimizde, değerlerin kripto para birimleri, tokenlar ve dijital kayıtlara evrimleştiğini görüyoruz.

Güven Makinası olarak da adlandırılan Blockchain teknolojisi, bu olguyu yeniden tesis ederken gizlilik, şeffaflık ve refah kavramlarına da dokunuyor. Blockchain, gücünü matematikten alan kriptografi bilimi sayesinde değiştirilemez, doğrulanabilir ve sürdürülebilir bir yapıya sahiptir. Blockchain, dünyasında rol oynayan aktörler, kendilerini ifade etmek için anahtar çiftlerini kullanılmaktadırlar. Kullanıcılar, özel anahtar (private key) ile gizliliklerini korurken, genel anahtarlarıyla (public key) ağda etkileşimde bulunabilirler. Bunlara ek olarak, kullanıcıların cüzdanlarında kimlik verilerini temsil eden token'lar da bulunabilir. Blockchain felsefesinin temsil ettiği bir başka kavram merkeziyetsizlikten doğan eşitliktir. Merkeziyetsiz demokratik bir ortam oluşturmak için mutabakat algoritmalarından faydalanan Blockchain teknolojisi, tüm ağın eşit olmasını sağlamaktadır.

Bu eşitliğin kişi/kurumlardan bağımsızlaşarak otonom yönetim, denetim ve hukuk sistemlerine evirildiği aşamada ise akıllı sözleşmelerin gücünden faydalanılacaktır.

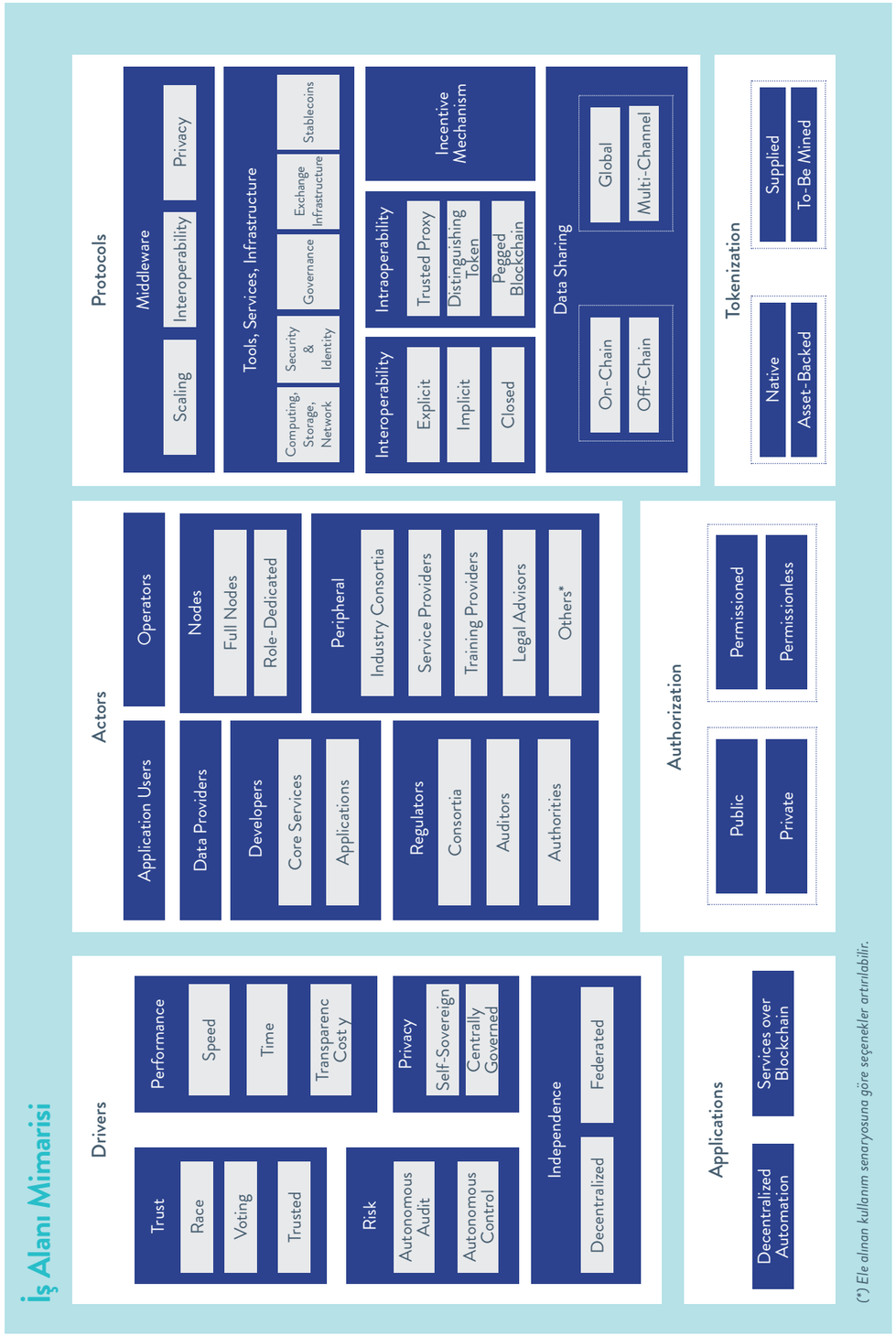
Koda dökülmüş kurallar bütünü olan akıllı sözleşmeler, günümüzdeki birçok süreci hızlandırarak, maliyetlerin ve insan kaynaklı hataların azalmasını sağlamaktadır.

Bir ekosistem işi olan Blockchain, gelişmeye devam eden protokollerle kullanım alanını genişletmektedir. Büyüyen kullanım alanı, teknolojiye hizmet eden çekirdek rollerin sayısını gün geçtikçe artırmaktadır. Kullanıcı ve yatırımcıların yanı sıra, mevcut platformların sürdürülebilmesi için işlem yükünü üstlenen madenciler, daha gelişmiş bir deneyim sunmak için çalışan geliştirici toplulukları, kripto paraların takasında görev alan borsalar, değerlerin güvenli bir şekilde saklanmasını sağlayan cüzdanlar, teknolojinin hayatımıza girişini ve devamındaki süreci denetleyen düzenleyiciler/hukuk birimleri ve Blockchain'in son kullanıcı tarafından daha iyi benimsenmesini sağlamak amacıyla güçlerini birleştiren organizasyonlar, günümüzdeki Blockchain teknolojisini oluşturan ekosistemin çekirdek rolleri olarak gösterilebilirler.

Blockchain teknolojisini, günümüz kullanım alanlarında daha verimli kullanılması için önündeki bazı kısıtlamalara çözüm bulunmalıdır. Bir Blockchain ağının işleyebileceği işlem kapasitesine ölçeklenebilirlik denir. Ölçeklenebilir bir sistem, ağ stresinden etkilenmeden ağdaki tüm işlemleri işleyebilmelidir. Mevcut Blockchain protokolleri için ölçeklenebilirlik önem derecesi en yüksek problemlerden biridir ve farklı katmanlardaki çözümler karşımıza çıkmaya devam etmektedir. On-chain, çözümler Blockchain'in birincil katmanındaki kod tabanında değişiklik yapılmasını gerektirir. Örnek olarak, blok büyüklüğü sınırının 1 MB'tan 10 MB'a yükseltilmesi veya blok oluşturma süresinin 10 dakikadan 5 dakikaya indirgenmesi verilebilir. Blockchain'in yapısal özelliklerinde yapılan bu kapsamdaki değişikliklerin hard-fork gerektirebileceği gözden kaçırılmamalıdır. İkincil katman ölçeklenebilirlik çözümleri ise yer tasarrufu sağlamak ve ağ tıkanıklığını azaltma konusunda yoğunlaşmaktadır. Off-chain olarak adlandırılan bu çözümler, Blockchain protokollerinin üzerine inşa edilmiş ikincil katmanları ifade eder ve genellikle yan zincirler ve kanallar olarak karşımıza çıkmaktadır. Daha fazla ölçeklenebilirlik ve işlem işleyebilmek için consensus sürecini kolaylaştıran mekanizmalar vardır. Ölçeklenebilirlik sorununa uygulanabilir bir çözüm olabilecek bu consensus mekanizmalarını, çeşitli projeler geliştirmiş ve yönetmiştir. Ölçekleyebilecek ana fikir birliği modellerini Delegated Proof-of-Stake, Byzantine Fault Tolerance (BFT) ve Proof of Authority olarak belirtebiliriz. Blockchain teknolojisi, dağıtık mimarisi nedeniyle genel DLT altında bir altkümedir. Bilginin (işlemlerin) organize edilmesiyle, aynı veri yapısını zincirleme ve ardışık bloklar halinde kullanmayan başka dağıtılmış defterler de vardır. Bu gibi dağıtık defterlerin

en popüler şekli Yönlendirilmiş Asiklik Grafikler (DAG) adı verilen bir teknolojidir. Birlikte çalışabilirlik, Blockchain ekositemi için tamamen yeni bir yapı sunuyor. Blockchain sistemleri arasındaki birlikte çalışabilirlik sorunu, protokollerin birbirleriyle aynı dilleri konuşmamalarından kaynaklanmaktadır. Akıllı sözleşme işlevsellik yetkinlikleri, işlem planları ve mutabakat algoritmalarının farklılıkları bu dili ayrıştıran bazı etmenlerdendir. Bu sorunun üstesinden gelebilmek için her bir Blockchain sistemi arasında evrensel iletişimi kolaylaştıran açık protokol çözümü gerekmektedir. Multi-channel frameworkler, daha kapsamlı bir ağın üzerinde birden fazla Blockchain arasında hem değerlerin hem de verilerin açık iletişimini ve transferini kolaylaştırmaya yardımcı olan ortamlardır. Her bir Blockchain'in daha büyük sistemin bir parçası olduğu standart bir ekosistem, bu yapılarla oluşturulabilir. Blockchain'lerin İnterneti konseptini sağlayacak yetkinlikteki frameworkler için günümüzde çalışmalar sürdürülmektedir.

Şekil 3. **İş Mimarisi Alanı**



4. VERİ MİMARİSİ ALANI

Farklı ihtiyaçlara cevaben farklı karakteristiklere sahip Blockchain çözümleri var olmasına karşın, pek çok Blockchain ağı için veri modelinde yer alacak temel varlıklar ortaktır.

DLT kavramı içerisinde özel bir dağıtık kayıt defteri (Ledger) kavramı olan Blockchain'in doğal olarak en temel bileşeni bu ortak kullanımdaki ve paylaşımdaki Ledger'dır. Ledger Blockchain'e özgü olarak zincir veri yapısı içerisinde tutulan bloklardan oluşur. Bloklar ise yine ismi ile bağlantılı olarak belirli sayıdaki işlemleri (Transaction) birlikte tutmak için kullanılan veri yapılarıdır. Zincir veri yapısının ilk halkası diğer halkalardan oluşturuluş şekli itibariyle özel bir yapıya sahiptir ve Genesis blok olarak tanımlanır.

Transaction, temelde tanımlanmış bir varlığın (asset) oluşturulması ve statüsü ile ilgili güncellemeleri içerir. Bu varlık her Blockchain çözümüne özgü olarak tanımlanır ve Token adı verilir. Token gerçek dünyada karşılığı olan bir varlığı temsil edebileceği gibi tamamen kurgusal olarak Blockchain içerisindeki işleyişi sağlayabilmek amacıyla da oluşturulmuş olabilir. Bu detaylar Token tanımı içerisinde tariflenir. Bunun yanı sıra Token temsil ettiği varlığın tanımına bağlı olarak farklı seviyelerde veriye de işaret eder, ki bu verinin büyüklüğü arttıkça veya erişimi ile ilgili kısıtlar oluştukça bu veriler zincir üzerinde (on-chain) tutulmak yerine harici (off-chain) olarak ta tutulabilirler.

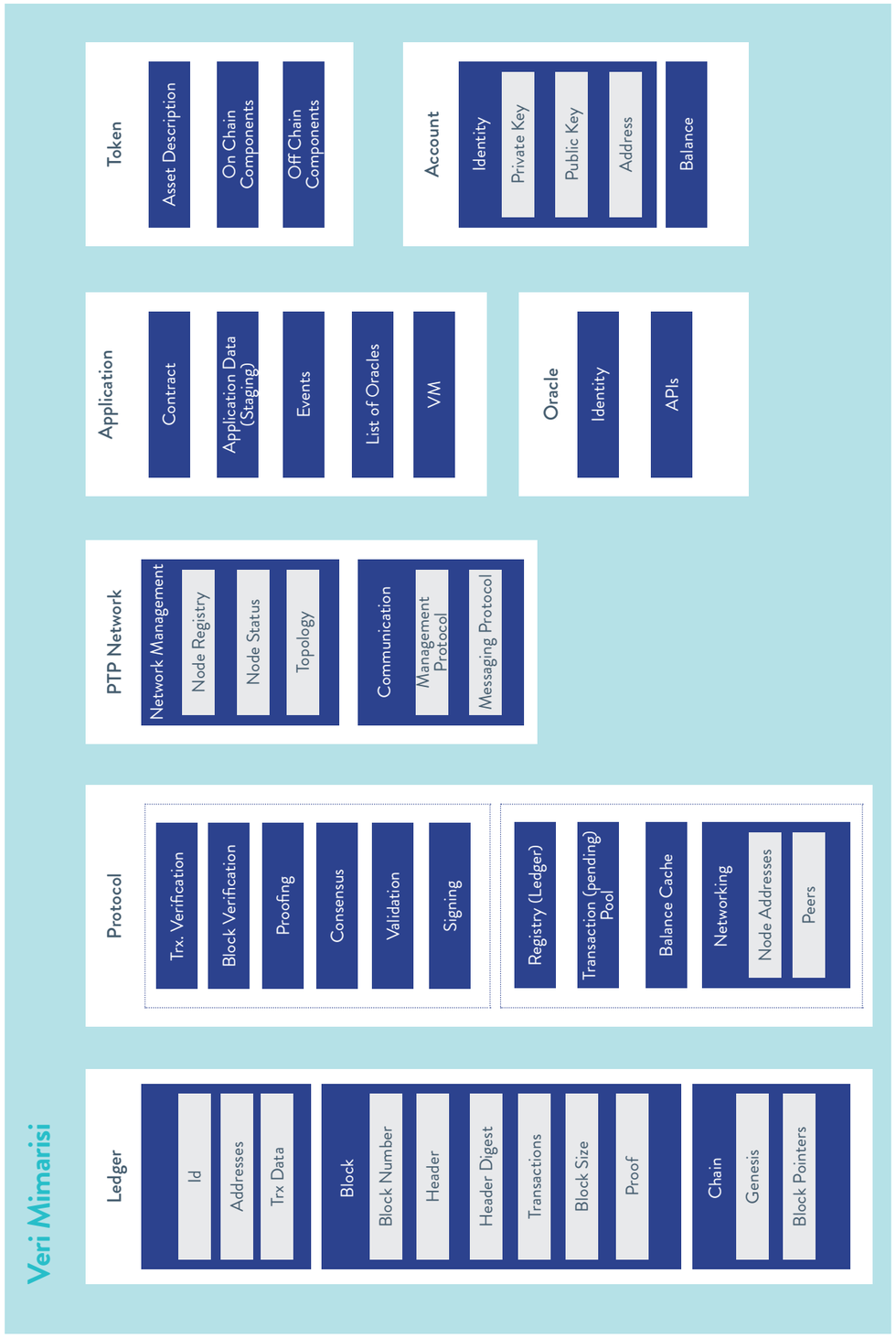
Blockchain'in kavram olarak vaat ettiği kazanımları sağlayacak süreçler Protokol diye adlandırılan sistem mimarisinde tanımlanır. Zaten Blockchain çözümlerini farklılaştıran temel varlıkta Protokoldür; yani oyunun kurallarını tanımlar. Farklılıklarına rağmen tüm protokoller ortak bazı süreçleri içerir; işlem talebi (transaction submission), işlem geçerliliği kontrolü (validation) ve konsensüs. Bu süreçler içerisinde özellikle konsensüs'a hem karmaşıklığı hem de yüksek etki faktörü sebebiyle daha fazla değinmek gerekir. Konsensus(mutabakat) temel olarak iki alt temel süreç içerir; türüne göre madencilik veya oylama, ve sağlama (verification). Her iki alt süreçte çok fazla kriptografik iş yerine getirir ve bu işlere ilişkin veri yapılarını gerektirir. Protokol tanımladığı süreçleri işletirken üzerinde çalışacağı veri kümelerini de tanımlar. Tahmin edilebileceği gibi ilk veri bileşeni Ledger'dır. Fiziksel olarak aynı olsa da, kavramsal olarak bu Ledger sürecin işletileceği yerdeki yerel kopyası olarak ayırt edilebilir. Bir diğer veri yapısı ise süreçlerin yeni bir kayıt oluşturmakta kullanacağı işlem listesidir. Bunun yanı sıra özellikle doğrulama sürecinde faydalanılacak sistemdeki varlıkların durum bilgileri (Balance) de hızlıca erişilebilecek bir önbellek tarzı ortamda tutulur.

Protokolde tariflenen süreçlerin işletileceği temel altyapı dağıtık bir ağ olacaktır, ancak Blockchain'in tasarım prensibinin gereği olarak bu ağ peer-to-peer (P2P) türünde olacaktır. P2P ağ hem kendi ağ altyapısı ile ilgili fonksiyonları işletebilmek için veri yapılarına ihtiyaç duyar, hem de sunduğu

haberleşme hizmetlerini yerine getirmek için ayrı veri yapıları kullanır.

Blockchain bir teknolojik çözüm olarak gerçek dünya problemlerini adreslemede kullanılır. Bu problemlere istinaden oluşturulan uygulamalar ve bunların kullanıcıları da ayrı veri yapıları ile ekosistemde yer alırlar. Kullanıcılar en temelde bir kimlik ve sahip oldukları varlıklar ile tanımlanır. Öte yandan uygulamalar ise pek çok türüne istinaden farklı veri yapılarına gereksinim duyar. Kontrat gibi göreceli olarak daha basit uygulamalarda durum ve fonksiyon tanımları yeterli olurken, dağıtık uygulama bileşenleri daha fazla kaynağa ihtiyaç duyar. Hatta bu kaynakların bazıları ekosistem dışındaki sistemlerle etkileşimden de sağlanıyor olabilir, ki bunlar özel olarak Oracle şeklinde ifade edilir. Yalnızca veri yapısı bağlamında karmaşıklığın yanı sıra uygulamalar hesaplama gereksinimleri bağlamında da daha fazla kaynak gerektirir ve bunlar arasında hesaplamalar sırasında kullanılacak geçici veri kümeleri de vardır.

Şekil 4. **Veri Mimarisi Alanı**



5. UYGULAMA MİMARİSİ ALANI

Blockchain uygulama mimari yığını özelleştirilmiş olanlarda farklı kurgular içermekle birlikte genellikle altı ana katmandan oluşur. Temel katmanları şöyle sıralayabiliriz: Ağ katmanı, Blokzincir çekirdek katmanı, mahremiyet ve seviyelendirme katmanı, araçlar katmanı, uygulamalar katmanı, entegrasyon katmanı.

Ağ katmanı, Blockchain düğümlerinin birbirleriyle iletişim kurmasına izin veren eşler arası (P2P) bir ağ protokolü uygulamasından oluşur. Bağlantı mutabakatı ve izinsiz bağlantı önleyici mekanizmalar bu katman içinde yer alır. Eşler arası Blockchain ağı, herhangi bir katılımcının temel alt yapıyı kontrol etmesini veya tüm sistemi etkisiz hale getirmesini önler. Ağdaki katılımcıların tümü aynı protokollere bağlıdır. Bu nedenle protokoller ağı yöneten kurallar kümesidir. Blockchain protokolleri genellikle fikir birliği, işlem geçerliliği ve ağ katılımı ile ilgili kurallar içerir. Temel ağ fonksiyonlarının yanı sıra private blockchain uygulamalarında kurumsal hizmetler için ek özelliklerde sunulur. Bu ek özelliklerin yanı sıra pek çok ağ katmanı çözümü yan fonksiyonlarla desteklenirler; Anti-spam filtreleme ve güvenli mesajlaşma atlyapısı gibi.

Çekirdek (core) fonksiyonlar, yeni blokların kabulü için Blockchain düğümleri arasında mutabakat (fikir birliği) mekanizmasından oluşur. Yürütme veya işletim alt katmanı komut kümesini ve hesaplama yeteneklerini barındıran bir sanal makinedir. Depolama ve defter alt katmanı akıllı sözleşmeler ve Blockchain'in durumunu saklamak için kullanılır. Dijital varlıkları tanımlamak, işlem göndermek, geçerli işlemleri işlemek, blok doğrulamak, blok oluşturmak, blok yayınlamak ve blok imzalamak, Blockchain protokollerinin ortak çekirdek katmanı servisleri olarak değerlendirilir.

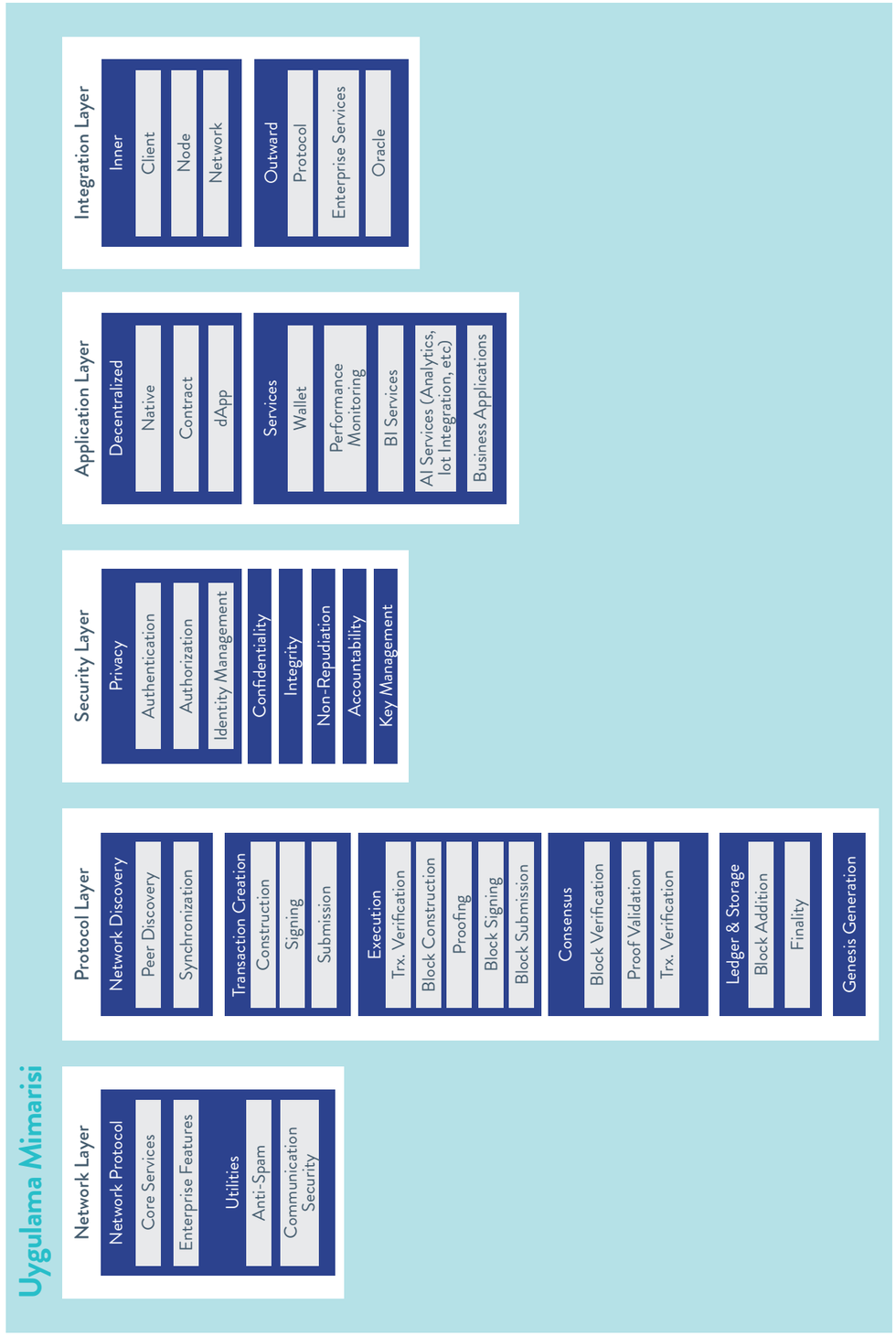
Kurumsal seviyede kullanılan Blockchain teknolojileri, açık Blockchain protokollerinde bulunmayan iki önemli kavram üzerinde yoğunlaşır; izin gerektiren yapılar ve gizli işlemler. İzin gerektiren bir Blockchain, düğümlerin yalnızca "güvenilir" katılımcılar tarafından çalıştırıldığı ve yalnızca yetkili kullanıcıların işlemlere katılabileceği bir ağdan oluşur. Gizli işlemlerin amacı ise genellikle iş mantığının yetkili olamayan kullanıcıların erişimini engellemektir. Bu nedenle mahremiyet ve seviyelendirme katmanı, blokların dağıtımı için gerekli gizlilik ve yetki seviyesi kurallarını uygular. Hesap yönetimi, rol bazlı yetki ve izin yönetimi bu katmanda gerçekleştirilir.

Uygulamaların güvenlik katmanları Blockchain'in yapısına göre değişkenlik gösterebilir. Tüm zincirlerde doğrulama, gizlilik, bütünlük, hesap verebilirlik ve inkar edilemezlik şartlarının sağlanması hedeflenmektedir. İzin gerektiren zincir yapılarında ise mevcut güvenlik bileşenlerine yetkilendirme ve kimlik yönetimi kavramları da eklenmektedir.

Uygulamalar katmanı, protokol ve ağ katmanlarının üstünde yer alan birincil kullanıcı ara-yüzdür. Akıllı sözleşmelerdeki yönergeleri sıralı bir şekilde çalıştıracak, mantıksal operasyonları ve talimat operasyonlarını gerçekleştirecek bir sanal makine de bu katmanda bulunur. Bu katmanda, uygulama operatörler ve uygulama kullanıcıları olarak iki aktörden söz edilebilir. Uygulama operatörleri, bir veya birden fazla Blockchain'e bağlanarak, kullanıcılara belirli hizmetler sunan uygulamaları yöneten kişilerdir. Bu uygulamalara örnek olarak düğüm izleme uygulamaları, Blockchain durum görselleştiricileri, cüzdan ve diğer ekosistem uygulamaları gibi üst seviye hizmetleri örnek verebiliriz. Uygulama kullanıcıları ise, bir uygulamanın ara-yüzü üzerinden dolaylı olarak ağ ile etkileşime giren kişilerdir.

Entegrasyon katmanı temel olarak 2 kapsamda fonksiyonları yerine getirir; Blockchain içerisindeki bileşenlerin birbirleri ile olan etkileşimlerini ve Blockchain'in dış dünya ile olan işbirlikleri için gereken etkileşimleri. Bu etkileşimler sağlamlık (robustness) prensibi gereği mümkün olduğunca etkileşilen sistemin detaylarından bağımsız genel geçer gereksinimlere ve standartlara uygun olarak gerçeklenirler.

Şekil 5. **Uygulama Mimarisi Alanı**



6. TEKNOLOJİ MİMARİSİ ALANI

Blockchain sistemlerinin altyapı incelemesi, Ağ, Protokol, Güvenlik/Kripto, Ledger, Data, Application ve Edge Servisleri başlıkları altında yapılabilir. Bu bölümde, günümüz Blockchain sistemlerinin geliştirilmesinde ve işletmesinde kullanılan teknolojiler, bu başlıklar altına ayrıştırılarak tanıtılacaktır. Her bir teknolojiye, donanım, sistem yazılımları ve üçüncü parti yazılımlar tipinden olan alt bileşenleri açısından bakılabilir.

Ağ teknolojisi (P2P network) açısından bakıldığında, Blockchain sistemlerinin üç alt protokolün birleşiminden oluştuğu değerlendirilebilir:

›› **Transaction Protocol,** madencilik ile kripto paranın üretilmesi, yokedilmesi, işlemlerin doğrulanması, dijital verilerin yönetilmesi gibi iş katmanı aktiviteleri kapsar.

›› **Consensus Protocol,** Blockchain düğümlerinin, kendi aralarında, ledger'a, doğru ve tutarlı veri yazılmasını garanti altına almak üzere işlettikleri protokoldür. Blockchain'in değiştirelemezliğini sağlayan, kuraldışı transferleri engelleyen hayati bileşendir. Bu konudaki alternatif teknolojilerin çalışma prensibi, genelde çeşitli yetkinliklerine veya özniteliklerine göre (işlem gücü, kriptopara miktarı, kimliği, depolama alanı vb.) ortak kararların alınmasında farklı seviyede söz hakkı olan düğümlerin faaliyetlerini kapsar. Başlıcaları: PoW, PoS, DPoS, PoC, PoE, PoET, PoA, PoB, PoI, BFT, PBFT, DBFT'dir. Özellikle mutabakat işlemleri için çok çekirdekli bilgisayarlar, GPU, FPGA ve ASIC tabanlı donanımlar kullanılır.

›› **Network Protocol,** yaygın olarak Gossip protokolleri kullanılır. İşlemlerin, Blockchain düğümleri arasında hızlıca yayılması, peer düğümlerin bulunması, Blockchain verisinin indirilmesi, blokların ağda yayımlanması işlemlerini yerine getirir.

Güvenlik ve Kripto Teknolojileri kapsamında, Blockchain'in en önemli vizyonu olan güvenlik fonksiyonunu sağlamak için çeşitli bileşenler kullanılır. Özellikle kriptografinin çeşitli bileşenleri, bu amaçla farklı kombinasyonlarda kullanılır. Bitcoin ile tanıştığımız örnekteki Özet (Hash) ve Dijital imza (signature) bileşenleri, neredeyse bütün Blockchain gerçeklemelerinde kullanılan yapıtaşlarıdır. Özet, blokların değiştirilemezliğini sağlamak, blok oluşturma işleminde konsensüs sağlamak için kullanılır. Dijital imza ise, en temel olarak işlemlerin kaynağının doğrulanması için kullanılır. Özet ve Dijital imzanın çeşitli versiyonları, hedeflenen güvenlik ve performans seviyelerine göre tercih edilmektedir. Çoğunluğu Eliptik Eğri Kriptografi (ECC) teknolojisini kullanır. Bunun yanında kuantum kriptoya dayanıklı olduğu bilinen Hash Tabanlı imza teknolojisi de kullanılmaktadır.

Blockchainde mahremiyet sağlama kapsamında, işlemlerin kaynaklarının

ve hedeflerinin gerçek kimliklerle bağdaştırılamaması ve birbiri ile ilişkilendirilememesi (anonymity ve untraceability), işlemlerdeki içeriklerin gizlenmesi, durum verilerinin gizlenmesi hedefleri, farklı seviyelerde karşılanmaya çalışılır. Blockchain'in doğası gereği, verilerin bütün düğümlerde kopyasının bulunduğu ve işlenmesi gerektiği göz önüne alındığında, mahremiyet hedeflerinin sağlamanın güçlüğü de anlaşılabilir. Bu temel bileşenlerin yanında, mahremiyet konusunda da yetenekler eklenmesi hedeflendiğinde, kullanılabilecek yapıtaşlarının sayısı ve kullanım kombinasyonları artmaktadır.

Sıfır Bilgi İspatları (SNARKS, Bulletproof vb.), taahhütler (Commitments), akümülatörler, simetrik şifreleme ve homomorfik şifreleme teknolojileri, işlemlerin (karşılaştırma, doğrulama, toplama, çıkarma vb.) verinin kendisi yerine gizlenmiş halleri ile yapılmasını sağlamak amacıyla kullanılır. Özel imzalama (Ring-signature ve türevleri, Multi-signature, Blind Signature vb.) teknolojiler ise işlemi başlatan kişilerin kimliklerinin gizlenmesi, imzalanan verinin gizlenmesi vb. mahremiyeti artırıcı amaçlarla kullanılır. Threshold Signature veya Threshold Cryptography teknolojisi ise işlemleri birden fazla kişinin başlatabilmesine olanak vermek amacıyla kullanılır. Blockchain'in güvenliği (bütünlüğü ve işlemlerin orijinini doğrulama) amaçlı yapıtaşları, ön tanımlı olarak on-chain olarak yerleşmişken, mahremiyet amaçlı olanlar, off-chain olarak da kullanılan bileşenler olarak karşımıza çıkmaktadır.

İzinli tipteki Blockchain'lerde kullanıcıların sisteme kaydı ve işlemler için kimlik doğrulanması işlemleri, Membership Service adı verilen bileşenlerce yerine getirilir. Genelde PKI teknolojileri kullanılır ve izinli kullanıcılara/düğümlere sertifikalar üretilir. Hyperledger platformu içinde kullanılan IDEMIX teknolojisi bu tür servislere örnek olarak verilebilir.

Bu sınıfta yaygın kullanılan donanım bileşenleri, HSM (Hardware Security Module) ve SGX (Software Guard Extensions) modülleridir. SGX, özellikle Blockchain düğümlerinde, hassas veriler işleyen kodların korumalı ortamda çalıştırılması gerektiği durumda kullanılır. HSM ise Blockchain düğümlerinde, anahtar gibi hassas verilerin saklanması ve kullanılması gerektiği durumlarda, güvenliği sağlamak için kullanılır (Bkz. Quorum paltformu). Cüzdan olarak genelde USB tabanlı donanımsal modüller kullanılır.

Ledger ve Data kapsamında, Blockchain içinde verilerin organizasyonu ve işlenmesi ile ilgili teknolojiler ele alınır.

Smart Contract, Blockchain içinde veri işleme için kullanılan bileşendir. Blockchain içinde akıllı kontratı kullanabilir kılan, Virtual Machine adı verilen teknolojidir.

Önceki bölümlerde açıklandığı gibi, veriler Blockchain içinde ve dışında depolanır. Blockchain içinde iki farklı türde veri depolanır. Birisi işlemler diğeri işlemler ile yönetilen state bilgisidir. İşlemlerin içine yayılmış verilerin kullanıldığı (UTXO modeli) verilerle çalışan Blockchain sistemlerinin yanında, işlemlerle kümülatif olarak güncellenen (Account Model) state verilerine

dayalı çalışan sistemler vardır. Bir NoSQL database türü olan Key-Value database, smart contract içinde (on-chain) state verisi depolamada en çok kullanılan teknolojidir.

Blockchain içinde, madencilerin ürettiği ve/veya işlemlerin ücretlerinin ödendiği natif token'lara ek olarak daha üst seviyede modellenen ve smart contract içinde depolanan token'lar bulunur. Bu üst seviye token'lar için de kullanılabilecek teknolojiler gelişmektedir. Ethereum Blockchain üzerinde çalışan ERC-20 ve ERC-721 tipli token'lar, bu alanda en çok kullanılan standartlardır. Kodlar token'in nasıl çalışacağını tarif ederken veritabanları temel olarak kimin kaç token'i olduğunu takip eden, satır ve sütunlardan oluşan tablolardır.

Ledger ölçeklenebilirliğini sağlamaya yönelik teknolojiler konusunda karşımıza sharding, sidechain, state channel ve channel teknolojileri çıkmaktadır. Sharding, veritabanını parçalara ayıran ve her parçayı farklı bir sunucuya koyan, geleneksel bir veritbanı ölçekleme teknolojisidir. Amacı, ağın tam durumunu ve gerçekleşen her işlemi saklayan "full node" gereksinimini ortadan kaldırmaktır. Bunun yerine, her düğüm bu verilerin bir alt kümesini saklar ve yalnızca bu işlemleri doğrular. Bir düğümün saklamadığı işlemler veya bloklar hakkında bilgi sahibi olması gerekiyorsa, ihtiyaç duyduğu bilgilere sahip başka bir düğüm bulur. PoS mutabakat kullanan Blockchain sistemlerinde uygulanabilir. Sidechain, Blockchain'ler arasında dijital varlıkların geçişmesine izin vermeye dayalı bir ölçeklenebilirlik artırma teknolojisidir. Channel kavramı ise aynı Blockchain platformunda, sanal alt Blockchain'ler oluşturmaya karşı düşer. Channel üyelikleri ile hem erişim denetimi sağlanır hem de farklı veri setleri üzerinde aynı Blockchain ortamında işlenmesi sağlanır. State channel ölçeklenebilirlik teknolojisi, channel kavramı ile veya sidechain kavramı ile karıştırılabilen bir terimdir. State channel, ölçeklenebilirlik, düşük maliyet, yüksek hız, mahremiyet ve başka blockchain entegrasyonu hedefleri ile işlemlerin bir kısmının off-chain olarak sürdürülmesi ve sonuçlarının blockchain'e yansıtılmasını ifade eder. Bitcoin için Lightning Network, Ethereum için SpankChain vb. örnekleri kullanılır.

Blockchain sistemlerinin fiziksel dünya ile veri alış verişi için Oracle teknolojileri kullanılır. Görevleri, akıllı kontratlar içinde kullanmak üzere gerçek dünyaya ilişkin verileri (para kur bilgisi, hava durumu, bir maç sonucu, uçuş bilgisi vb.), bulmak, doğrulamak ve Blockchain içine sağlamaktır. Bu bileşenler, dış dünya ile olan arayüze göre, yazılım ve donanım oracle olarak gerçeklenmiş olabilir. Yazılım bileşenler, genelde Internet ortamında ve API'ler ile sunulan verileri kullanırlar. Donanım oracle bileşenleri ise RFID sensör, barkod okuyucu vb fiziksel veri alınmasını sağlayabilirler. Oracle bileşenleri genelde Blockchain içine dış dünya verisi sağlama amaçlı (inbound oracle) kullanılsa da Blockchain'de oluşan duruma göre dış dünyaya bir veriyi sağlamak (outbound oracle) amacıyla da kullanılabilirler (Örneğin, kişinin

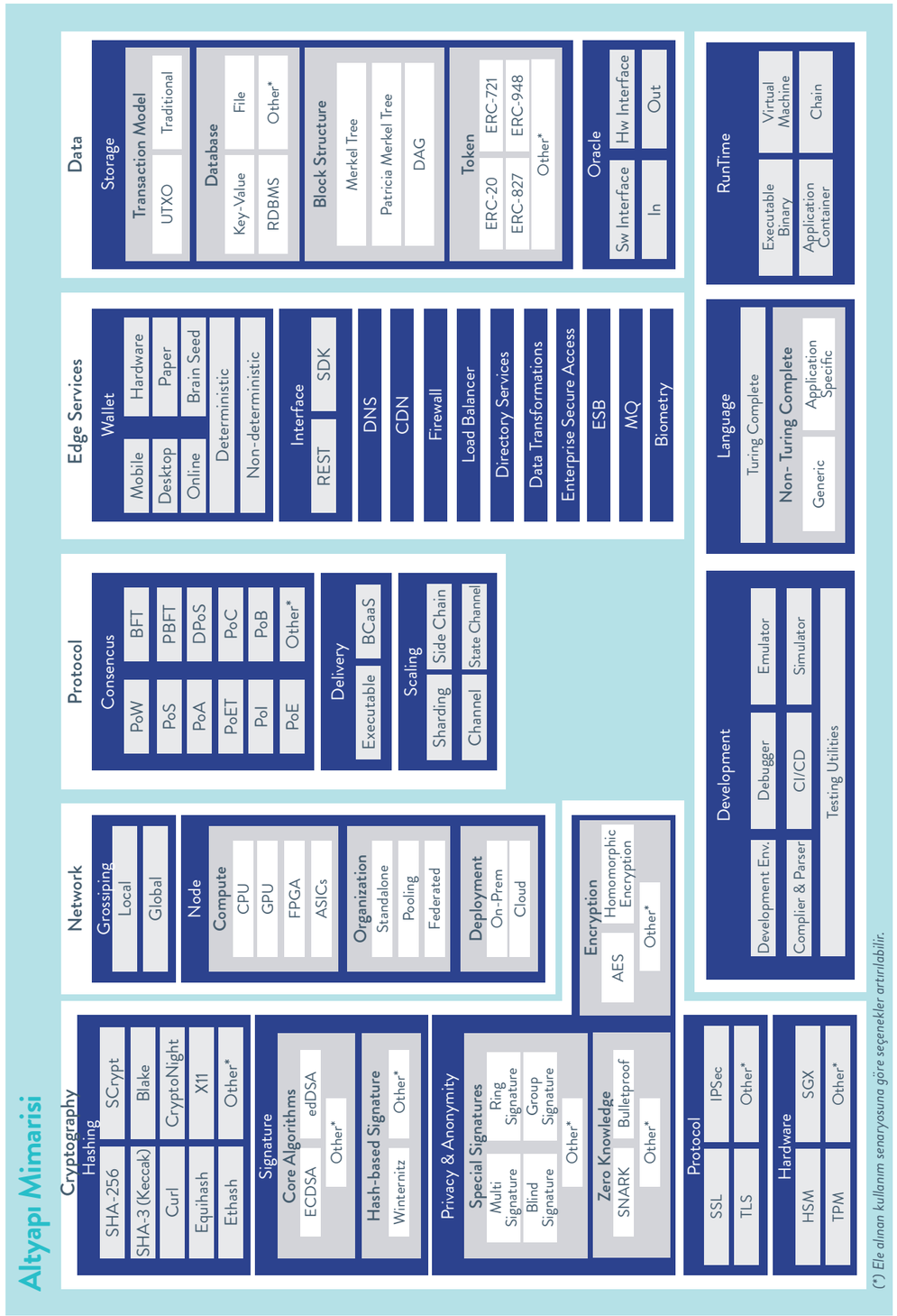
Blockchain hesabında belli bir miktar para birikince, fiziksel dünyadaki bir kilidin açılmasının tetiklenmesi).

Edge Teknolojileri, Blockchain ile etkileşen uygulamalar katmanında yer alan teknolojileri ifade eder. İstemci yazılım olarak cüzdan kavramı, kullanıcının kimlik ve Blockchain erişim bilgilerini tutan ve bazıları Blockchain ile de etkileşebilen bileşenlerdir. Farklı teknolojiler ile gerçeklenebilirler: Online, Mobile, Desktop, Hardware ve Paper cüzdanlar. Cüzdan teknolojileri, kullanım şekline göre Hot ve Cold Wallet tipleri olarak sınıflanır. Deterministic olan ve olmayan cüzdan tipleri sınıflaması ise cüzdanın özel anahtarlarının üretimin bağımsız olup olmamasına göre yapılır.

Blockchain ile etkileşmek için Blockchain tipine göre çeşitli API'ler kullanılır. En çok kullanılan tip ise Rest API'dir. Blockchain içinde ve bu API servislerinde kullanılan JSON formatı, yapıtaşı teknolojilerdendir. Edge servisleri katmanı, güvenlik duvarı, dizin servisi, çeşitli proxy servisleri gibi bileşen teknolojilerini de içerir. Bu katmandaki uygulamaların entegrasyonu için mesaj kuyrukları, ESB, microservice vb. Teknolojiler kullanılır.

Application Teknolojileri, blockchain için uygulamaların geliştirilmesi, test edilmesi ve çalıştırılması ile ilgili sınıflara bölünebilir. Java, Phyton, Javascript, Go, Solidity gibi çeşitli diller ve IDE'ler kullanılarak geliştirilen smart contract ve edge uygulamaları, testnetler veya Blockchain simülatör/emülatörleri kullanılarak doğrulanır. Smart Contract'ların çalıştırılması için Blockchain düğümü üzerinde bulunan Virtual Machine bileşenleri kullanılır.

Şekil 6. **Altyapı Mimarisi Alanı**



KATKI SAĞLAYAN KİŞİLER

Enes Türk

BKM

Aydın Akyol

Garanti Bankası

İbrahim Kara

Softtech

Taner Dursun

Fatih Birinci

Tübitak Bilgem

REFERANSLAR

1. Tasca, Paolo & Thanabalasingham, Thayabaran. (2017). Ontology of Blockchain Technologies. Principles of Identification and Classification. SSRN Electronic Journal. 10.2139/ssrn.2977811.
2. C. Ballandies, Mark & Dapp, Marcus & Pournaras, Evangelos. (2018). Decrypting Distributed Ledger Design - Taxonomy, Classification and Blockchain Community Evaluation.
3. Dylan J. Yaga, Peter M. Mell, Nik Roby, Karen Scarfone (2018). Blockchain Technology Overview. NIST Interagency/Internal Report (NISTIR) – 8202.
4. Andreas Ellervee, Raimundas Matulevicius, Nicolas Mayer (2017). A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology. ER Forum/Demos: 306-319.
5. Xu, Xiwei & Weber, Ingo & Staples, Mark & Zhu, Liming & Bosch, Jan & Bass, Len & Pautasso, Cesare & Rimba, Paul. (2017). A Taxonomy of Blockchain-Based Systems for Architecture Design. 10.1109/ICSA.2017.33.
6. Enterprise Ethereum Alliance - Enterprise Ethereum Client Specification V2 (2018). https://entethalliance.org/technical-documents.
7. Architecture reference (2019). https://hyperledger-fabric.readthedocs.io/en/release-1.4/architecture.html
8. IBM Blockchain developer portal: https://developer.ibm.com/tutorials/category/blockchain/
9. Business Innovation Through Blockchain - The B^3 Perspective - Vincenzo Morabito (2017)
10. Fat Protocols – Joel Monegro (2016): https://www.usv.com/blog/fat-protocols

BLOCKCHAIN

TÜRKİYE

TBV

TÜRKİYE BİLİŞİM VAKFI