BLOCKCHAIN
TÜRKİYE

DİJİTAL KİMLİK SİSTEMLERİ VE SEKTÖREL ETKİLERİ RAPORU

On-Chain
Çalışma Grubu

HAZİRAN 2025

TBV
TÜRKİYE BİLİŞİM VAKFI

BLOCKCHAIN
TÜRKİYE

DİJİTAL KİMLİK SİSTEMLERİ VE SEKTÖREL ETKİLERİ RAPORU

On-Chain
Çalışma Grubu

HAZİRAN 2025

TBV
TÜRKİYE BİLİŞİM VAKFI

DİJİTAL KİMLİK SİSTEMLERİ VE SEKTÖREL ETKİLERI RAPORU

HAZİRAN 2025

SORUMSUZLUK BEYANI

Türkiye Bilişim Vakfı altında çalışmakta olan Blockchain Türkiye Platformu'nun "On-Chain Çalışma Grubu" tarafından hazırlanan işbu rapor blokzincir teknolojisinin mevcut kişisel verilerin korunması mevzuatı ve uygulamaları bakımından incelenmesinden ibaret olup; teknik kapsam ilgili teknolojinin hukuki açıdan özümsenebilmesi amacıyla yayımlanmıştır. Kişi ve kurumları bağlayıcı tavsiye veya görüş niteliği taşımaz. İşbu rapor kamuya açık kaynaklardan yararlanılmış bilgileri içermekte olup, söz konusu bilgilerin güncel ve eksiksiz olduğu taahhüt edilmemektedir. İşbu raporda verilen tüm bilgi ve görüşler zamanla değişkenlik gösterebilir. Bu bağlamda işbu raporun içeriğini okuyan kişilere veya herhangi bir üçüncü kişiye karşı sorumluluğu ve yükümlülüğü bulunmamaktadır.

On-Chain
Çalışma Grubu

ÖNSÖZ

Dijital kimlik, 21. yüzyılın yalnızca teknik bir dönüşüm alanı değil, aynı zamanda bireysel egemenliğin, veri güvenliğinin ve dijital hakların yeniden tanımlandığı küresel bir paradigma değişimidir. Elinizdeki bu çalışma, dijital kimlik sistemlerini sadece teknik bir perspektiften değil; çok boyutlu ve disiplinler arası bir yaklaşımla bakılmıştır. Kimlik yönetim modellerinden W3C ve ISO standartlarına, blokzincir tabanlı altyapılardan güvenlik konularına, kullanıcı deneyimi tasarımlarından donanım bileşenlerine, yasal düzenlemelerden uluslararası örneklere kadar geniş bir yelpazede konu başlıklarına yer verilmiştir. Finans, kamu hizmetleri, sağlık, eğitim gibi çeşitli sektörlerde dijital kimlik senaryoları detaylı biçimde ele alınmış; hem kurumsal aktörler hem de bireyler açısından sistemin işleyişine dair kapsamlı bir değerlendirme sunulmuştur.

Merkezi yapılardan kullanıcı egemen sistemlere uzanan evrim, dijital dünyada kimliğin kontrolünü bireyin eline bırakma vaadiyle yeni bir çağın kapılarını aralıyor. Blokzincir tabanlı mimariler, zero-knowledge proof teknolojileri ve merkeziyetsiz tanımlayıcılarla birlikte artık sınırlar ötesi güvenin tesis edilmesi mümkün hale geliyor. Bu, yalnızca hizmetlerin dijitalleşmesi değil, aynı zamanda kimlik üzerinden yeniden inşa edilen dijital vatandaşlık ve dijital ekonomiler anlamına geliyor.

Türkiye Cumhuriyet Merkez Bankası'nın Dijital Türk Lirası (Dijital TL) projesi kapsamında yayımlanan raporda da Dijital Kimlik altyapısının önemi açık biçimde ortaya konmaktadır. Dijital TL'nin dijital cüzdanlar, ödeme sistemleri ve kimlik doğrulama mekanizmalarıyla entegre çalışabilmesi için, güvenilir ve birlikte çalışabilir dijital kimlik sistemlerine ihtiyaç duyulmaktadır. Bu bağlamda, dijital kimlik çözümleri, Dijital TL'nin mimarisinde güven oluşturma, doğrulama sağlama ve kullanıcı mahremiyetini koruma açısından kritik bir temel bileşen olarak değerlendirilmektedir.

Önümüzdeki yıllarda dijital kimlik çözümleri sadece finansal sistemlerin değil, sağlık platformlarının, eğitim erişiminin ve hatta yapay zeka temelli otonom sistemlerin temel yapı taşı olacak. Yeni nesil iş modelleri; kimlik doğrulamanın anlık, güvenli ve kullanıcı merkezli yapılabildiği bu altyapılar üzerinde inşa edilecek. Bu dönüşüm, sadece bireylerin değil, devletlerin ve şirketlerin de birbirine güvenme şeklini kökten değiştirecek. Türkiye açısından bakıldığında, dijital kimlik sistemlerinin benimsenmesi sadece teknolojik bir ilerleme değil; kamu hizmetlerinin şeffaflığı, özel sektörün verimliliği ve bireylerin mahremiyet hakları açısından bir dönüşüm fırsatıdır. Türkiye'nin güçlü kamu altyapısı, genç nüfusu ve hızla dijitalleşen sektörleri, bu alanda küresel ölçekte örnek gösterilebilecek çözümler üretmesi için büyük bir potansiyel barındırmaktadır.

Bu rapor, mevzuat uyumundan uluslararası standartlara, güvenlik tehditlerinden kullanıcı deneyimine kadar birçok kritik başlığı ele alırken, aynı zamanda dijital kimlik alanında Türkiye'nin küresel rekabette yerini alması için stratejik bir vizyon da ortaya koymaktadır. Kapsayıcı, güvenli ve sürdürülebilir dijital kimlik sistemlerinin yalnızca bugünün sorunlarını çözmekle kalmayıp, geleceğin dijital ekonomisinin temel altyapısını oluşturacağına inanıyoruz.

Son olarak, dijital kimlik ekosisteminin sağlıklı işlemesi için kamu ve özel sektör arasındaki işbirliğini daha da güçlendirecek bir yönetişim modeli gerekmektedir. Mevcut düzenlemelerin dijital çağın ihtiyaçlarını karşılaması, yeni güvenlik tehditlerine karşı önleyici mevzuatların geliştirilmesi ve dijital kimliğin tüm sektörlerde birlikte çalışabilir bir standart olarak kabul görmesi, ekosistemin sürdürülebilirliği için elzemdir. Bu rapor, sadece bugünü anlamak için değil; geleceği şekillendirmek için bir yol haritası olarak kaleme alınmıştır.

Dr. Gökhan Özdinç
Yapı Kredi Teknoloji
Genel Müdürü

İÇİNDEKİLER

1. GİRİŞ 10

2. DİJİTAL KİMLİK KAVRAMI 10

2.1. Dijital Kimlik Yönetim Modelleri 10
2.1.1. Merkezi Kimlik Yönetimi (Centralized Identity Management) 10
2.1.2. Federe Kimlik Yönetimi (Federated Identity Management) 10
2.1.3. Kullanıcı Merkezli Kimlik Yönetimi (User-Centric Identity Management) 11
2.1.4. Kullanıcı Egemen Kimlik Yönetimi (Self-Sovereign Identity Management) 11

3. TEKNOLOJİ VE ALTYAPI STANDARTLARI 12

3.1. Güncel Standartlar 12
3.1.1. World Wide Web Consortium (W3C) 12
3.1.2. OpenWallet 12
3.1.3. ISO Standartları 13
3.1.4. TrustOverIP Standartları 13
3.2. Topluluklar 14
3.3. Dünyadaki Altyapı Örnekleri 15
3.3.1. Sovrin 15
3.3.2. SSI Türkiye 15
3.3.3. Cheqd 15
3.3.4. uPort 16
3.3.5. Microsoft Entra ID 16
3.3.6. Evernym 16
3.3.7. ID2020 17
3.3.8. IBM Digital Credentials and Blockchain Platform 17
3.3.9. Veres One 18
3.3.10. PrivadoID (PolygonID) 18
3.3.11. WorldID (Worldcoin) 18
3.4. Farklı Kanallardaki Deneyim Tasarımları 19
3.4.1. Mobil Donanımlar 19
3.4.2. Masaüstü ve Laptoplar 19
3.4.3. Donanım Cüzdanlar 20
3.4.4. Diğer Entegrasyonlar 21

4. GÜVENLIK VE GİZLİLİK 21

4.1. Siber Saldırılar 21
4.2. Dolandırıcılığın Önlenmesi ve Vatandaşın Korunması 24
4.2.1. Bilinen Dolandırıcılık Yöntemlerinde Veriler Nasıl Ele Geçer 24
4.2.2. Dijital Kimlik doğrulamasının geleneksel kimlik doğrulama yöntemlerine göre artısı nedir? 24
4.2.3. Dijital kimlik doğrulama kullanımında nelere dikkat edilmeli? 25

5. YASAL UYUM VE DÜZENLEMELER 25

5.1. İhtiyaç Duyulan Hukuki Düzenlemeler ve Mevzuata Uyumun Sağlanması 25
5.1.1. Mevcut Yasal Çerçeve ve Düzenlemeler 28
5.1.2. Dijital Kimliğin Hukuki Çerçevesiyle İlgili Gelişmeler 31

6. FİNANS SEKTÖRÜNE ETKİLERİ VE KULLANIM ALANLARI 34

6.1. Finans Alanında Ulusal Blokzincir Altyapıları ve Dijital Kimliğin Etkileri 34
6.2. Dijitalleşecek Belgeler ve Blokzincir Dünyasına Etkileri 35
6.3. Yeni Hizmetler ve Operasyonel Verimlilik 37
6.3.1. Dijital Kimlik Yaratma ve Doğrulama Platformları 38
6.3.2. Kimlik Erişimi ve Yönetimi (Identity and Access Management, IAM) Gelişmeleri 39

7. DİĞER SEKTÖRLERE ETKİLERİ VE KULLANIM ALANLARI 40
7.1. Kamu Yönetimi 40
7.2. Gayrimenkul 41
7.3. Eğitim 43
7.4. Turizm 45
7.5. Sağlık 46
7.6. Ulaşım 47
7.7. Akıllı Şehirler 48
7.8. Dijital Kimliğin Benimsenmesi İçin Gerekli Olan Eğitim ve Tanıtımlar 50
7.8.1. Toplumsal Etkiler 50
7.8.2. Benimsenme Oranının Arttırılması için Gerekenler 51

8. SONUÇ VE ÖNERİLER 52

9. KAYNAKÇA 53

YÖNETİCİ ÖZETİ

Küresel dijitalleşme süreci, kimlik doğrulama mekanizmalarında da köklü bir dönüşüm ihtiyacını beraberinde getirmiştir. Bu rapor, dijital kimlik kavramını yalnızca bir teknolojik araç olarak değil, aynı zamanda veri güvenliği, kullanıcı mahremiyeti, regülasyon uyumu ve dijital egemenlik gibi boyutlarıyla ele alan çok katmanlı bir çerçeve sunmaktadır. On-chain yani blokzincir temelli dijital kimlik sistemleri, kullanıcıların kimlik bilgileri üzerindeki kontrolünü güçlendirirken, aynı zamanda kurumlara daha sürdürülebilir, güvenli ve esnek kimlik doğrulama altyapıları oluşturma fırsatı vermektedir.

Raporda yer verilen modeller arasında en çok dikkat çeken yapı, kullanıcı egemen dijital kimlik sistemleridir. Kullanıcı, kimliğine dair hangi bilgiyi kiminle paylaşacağına kendisi karar verir; böylece veri minimizasyonu ilkesine dayanan daha mahremiyet dostu çözümler ortaya çıkar. Bu yeni mimarinin temelini ise blokzincir teknolojisinin sağladığı şeffaflık, değiştirilemezlik ve güvenilirlik gibi özellikler oluşturur.

Dijital kimliğin sadece bireyler için değil; kurumlar, cihazlar, hizmet sağlayıcıları ve hatta yapay zeka bileşenleri için de uygulanabilir hale geldiği günümüzde, birlikte çalışabilirlik ve uluslararası geçerlilik kritik birer ihtiyaç halini almıştır.

Raporda ayrıca kamu kurumlarından özel sektöre, bankacılıktan eğitime, sağlıktan gayrimenkul sektörüne kadar dijital kimliğin uygulanabilirliğine dair örnekler incelenmiş; kullanıcı deneyimini doğrudan etkileyen mobil uygulamalar, donanım cüzdanlar ve IoT cihazlarla bütünleşik senaryolar üzerinden sistemin işlevselliği değerlendirilmiştir. Güvenlik boyutu ise, sistemin sürdürülebilirliği açısından hayati bir unsur olarak öne çıkmaktadır. Blokzincir mimarisinin sunduğu güçlü koruma mekanizmalarına rağmen, yeni nesil tehdit türlerine karşı kurumsal farkındalık, teknik yeterlilik ve sürekli güncellenen denetim mekanizmaları şarttır. Rapor bu noktada, siber saldırılardan kullanıcı hatalarına kadar uzanan geniş bir yelpazede, alınması gereken önlemleri somut şekilde ortaya koymaktadır.

Hukuki uyumun önemi vurgulanmakta; Türkiye'deki KVKK ile Avrupa Birliği'nin GDPR ve eIDAS düzenlemeleri arasında köprü kurularak, dijital kimliğin yasal bağlamda nasıl konumlanması gerektiği açıklanmaktadır. Regülasyonlara uyumlu sistem tasarımı ve kullanıcı haklarını temel alan yönetişim modelleri, dijital kimlik ekosisteminin başarısı için vazgeçilmez görülmektedir.

Finans sektörü haricinde de dijital kimliklerin bir çok potansiyel kullanım alanı bulunmaktadır. Kamu hizmetlerinden gerçek dünya varlıklarının tokenizasyonuna, eğitim ve akademik bilgilerin yönetimi ve doğrulanmasından turizm ve seyahat teknolojilerinin kullanımına ve sağlık sektöründe verilere hızlı ve bütünsel erişim gibi bir çok alanda rapor bize örneklerle farklı sektörel kullanımları açıklamaktadır.

Dijital kimlik, yalnızca dijital hizmetlerin kapısını açan bir anahtar değil; dijital çağda bireyin ve kurumun güvenliğini, itibarını ve egemenliğini koruyan stratejik bir varlıktır. Bu nedenle, teknolojik gelişmeler kadar etik, hukuki ve yönetişimsel boyutların da birlikte ele alındığı bütüncül bir yaklaşıma ihtiyaç vardır. Blokzincir tabanlı dijital kimlik sistemleri, güvenli, birlikte çalışabilir ve kullanıcı odaklı yapılarıyla hem kamu hem özel sektör için önemli fırsatlar sunmaktadır. Türkiye'nin bu teknolojileri etkin şekilde benimsemesi, hem vatandaşın veri güvenliğini artıracak hem de dijital ekonomiye geçişi hızlandıracaktır.

Ali Akarçay
Yapı Kredi Teknoloji
Bireysel Müşteri Süreçleri Yönetimi
ve İş Geliştirme Müdürü

1. GİRİŞ

Bu kapsamlı rapor, dijital kimlik sistemlerinin kavramsal altyapısını, teknolojik yapı taşlarını, hukuki düzenlemelerini ve farklı sektörlerdeki uygulama örneklerini detaylı biçimde ele almaktadır. Dijital kimlikler, bireylerin ve kurumların dijital ortamlarda kimliklerini doğrulama süreçlerinin temelini oluşturur.

Bu raporda, merkezi, federe ve kullanıcı egemen sistemlerin karşılaştırmalı analizi yapılmakta, küresel standartlar ve düzenlemeler ışığında hukuki uyum gereksinimleri ortaya konmakta ve kamu, finans, eğitim, gayrimenkul gibi alanlardaki uygulama senaryoları detaylandırılmaktadır.

Dijital kimlik ve belgelerde dijitalleşme, modern toplumların dijital dönüşüm süreçlerinde kilit bir rol oynamaktadır. Bu dönüşüm, bireylerin, kurum ve kuruluşların kimlik doğrulama ve belge yönetimi süreçlerini daha hızlı, güvenli ve verimli hale getirmektedir. Özellikle, bu raporda Türkiye'deki mevcut yasal çerçeve ve uluslararası düzenlemeler ışığında, dijital kimlik uygulamalarının yasal uyumluluğunun değerlendirilmesi ve teknolojinin etkin bir şekilde benimsenmesi için öneriler sunulması hedeflenmektedir.

2. DİJİTAL KİMLİK KAVRAMI

Dijital Kimlik, sanal ortamda bir varlığı tanımlayan ve yazılımlar tarafından yorumlanabilen kimlik bilgileri olarak tanımlanır.

Kimlik Yönetimi Sistemleri (Identity Management System - IdM), kullanıcıların dijital kaynaklara erişimini düzenleyen, kimlik doğrulama, yetkilendirme ve güvenlik sağlayan sistemlerdir. IdM, kullanıcıların kimlik bilgilerini yönetir ve bu kimlikler üzerinden erişim kontrollerini sağlar.

2.1. Dijital Kimlik Yönetim Modelleri

2.1.1. Merkezi Kimlik Yönetimi (Centralized Identity Management)

Merkezi kimlik yönetimi, kullanıcıların tek bir merkezi veri tabanında kayıtlı olduğu, kullanıcıların erişim yetkilerinin merkezi bir sistem tarafından kontrol edildiği modeldir. Bu modelin temelleri, 1990'ların ortalarına kadar gitmektedir ve özellikle aktif dizin (Active Directory) ve LDAP (Lightweight Directory Access Protocol) gibi teknolojilerin gelişmesiyle yaygınlık kazanmıştır.

- Tek Bir Kimlik Kaynağı: Kullanıcıların kimlik bilgileri merkezi veritabanında tutulur.
- Basitleştirilmiş Yönetim: Kullanıcı hesapları ve erişim izinleri merkezi bir noktadan yönetilir.
- Kapsamlı Erişim Denetimi: Sistem yöneticileri, kullanıcı erişim düzeylerini ve yetkilerini merkezi olarak kontrol eder.
- Özelleştirilmiş Kimlik Doğrulama: Kullanıcılar, merkezi bir kimlik doğrulama hizmeti (örneğin Active Directory veya LDAP) aracılığıyla doğrulanır.

2.1.2. Federe Kimlik Yönetimi (Federated Identity Management)

Federe kimlik yönetimi, farklı organizasyonlar veya servis sağlayıcıları arasında kimliklerin paylaşılmasına olanak tanır. Bu model, özellikle bulut hizmetlerinin ve sistem entegrasyonlarının yaygınlaşmasıyla popülerlik kazanmıştır. Tek Oturum Açma (Single Sign-On SSO) teknolojileri ve SAML (Security Assertion Markup Language) protokolleri, federe kimlik yönetiminin temellerini atmıştır.

- Kimlik Paylaşımı: kimlik verilerini kullanıcıların her iki sisteme de aynı kimlik ile erişim izin verir.

• Tek Oturum Açma (SSO): Kullanıcı bir kez giriş yaptıktan sonra farklı sistemler ve servisler arasında tekrar tekrar kimlik doğrulaması yapmadan geçiş yapabilir.

• Dış Kaynaklarla Uyum: Farklı organizasyonlar veya servis sağlayıcıları arasında güvenli kimlik doğrulama süreçleri sağlanır.

• Protokoller: Federe kimlik yönetiminde yaygın olarak kullanılan SAML, OpenID Connect ve OAuth gibi protokoller ile yönetilir.

2.1.3. Kullanıcı Merkezli Kimlik Yönetimi (User-Centric Identity Management)

Kullanıcı merkezli kimlik yönetimi, kullanıcıların kendi kimlik bilgileri üzerinde kontrol sahibi olduğu yaklaşımdır. Bu model, 2010'ların sonlarından itibaren, popüler olmaya başlamıştır.

• Kullanıcı Kontrolü: Kullanıcı, kendi kimlik bilgilerini yönetir ve doğrulama işlemleri üzerinde tam kontrol sahibidir.

• Veri Sahipliği: Kullanıcılar erişim izinlerini saklayan bilgi işlem altyapıları kullanır.

• Özelleştirilebilir Kimlikler: Kullanıcılar, kimlik bilgilerini ve doğrulama süreçlerini özelleştirebilirler.

• Mahremiyet: Kullanıcı, sadece gerekli bilgileri istediği kişilerle paylaşabilir. (Selective Disclosure).

2.1.4. Kullanıcı Egemen Kimlik Yönetimi (Self-Sovereign Identity Management)

Dijital kimlik yönetim modellerin arasında 2015 yılından itibaren gittikçe ön plana çıkmaya başlayan Kullanıcı Egemen Kimlik (Self-Sovereign Identity) modeli KVKK düzenlemeleri ile uyum ve birlikte çalışabilirlik konularında, Üçüncü taraf altyapılarına bağımlılığın kaldırıldığı modeldir.

SSI modelinde kimlik bilgileri ait olduğu kişinin veya kurumun kontrolündedir. Bu model, 2005 yılında ortaya atılmış ve 2015 yılından itibaren hızla gelişim sürecine girmiştir.

Blokzincir tabanlı kimlik yönetim sistemi, kişilerin kimliklerini doğrulamak için merkezi otoritelere ihtiyaç duymaz. Aracıları ortadan kaldırarak bireylerin, kimlikleri üzerinde tam kontrol sahibi olmalarını sağlar. Kimlik sahibi, kimlik bilgilerini istediği miktarda ve detayda paylaşabilir. SSI modelinde, kişinin kimlik bilgileri herhangi bir yazılıma ve sisteme özel olmayıp farklı platformlar ve servisler arasında taşınabilir ve kullanılabilir.

Sistemin; dijital mecralarda kullanılabilen, kriptografik olarak doğrulanabilir ve sahtesi üretilemez dijital kimlik sertifikaları sağlayabilmesi mümkündür.

İnsan müdahalesi ile yürüyen, güvenilir üçüncü taraflara ihtiyaç duyan süreçler yerine daha otonom yürüyen, içinde insan, şirket ve akıllı cihazların taraf olabildiği süreçlerin gerçeklemesi mümkün hale gelir. Hali hazırda, elektronik ortamlarda parola ile erişilen servislerde yürüyen hizmetlerin, dijital cüzdanlar sayesinde daha güvenli olarak ve kurumsal taraflarda insan müdahalesini gerektirmeyecek şekilde otonom yazılımlar tarafından yürütülebilir hale dönüşmesine imkan sağlar.

Bu modelde blokzincir sistemi, üzerinde tuttuğu bilgiler sayesinde bütün taraflar arasında ortak güveni sağlayan kilit role sahip bileşendir. Güvenin herhangi bir merkezi otoriteden kaynaklı olmaması sayesinde, sektörler arası ve sınır ötesi dijital kimlik uygulamaları mümkün olabilmektedir.

3. TEKNOLOJİ VE ALTYAPI STANDARTLARI

3.1. Güncel Standartlar

3.1.1. World Wide Web Consortium (W3C)

W3C (World Wide Web Consortium) tarafından standart hale getirilen bu modelde kimlikler, Decentralized Identifier - DID ismi verilen varlığı tekil olarak tanımlayan numara ve doğrulanabilir kimlik bilgileri (Verifiable Credentials - VCs) adlı iki ana tür veriden oluşurlar. DID, kripto para cüzdan adreslerine benzer olarak bir asimetrik anahtar çifti ile ilişkilendirilir. VC'ler ise bir kimlik sağlayıcı tarafından kriptografik olarak imzalanmış, üretildiği kişi veya kurum hakkında çeşitli kimlik bilgilerini içeren sertifikalardır.

Merkezi Olmayan Tanımlayıcılar - Decentralized Identifiers (DIDs): DID'ler (Merkeziyetsiz Kimlik Belirleyiciler), bir kişiyi ya da dijital varlığı temsil eden kimliklerdir. Bu kimlikler, URI formatında tanımlanır ve ilgili kişinin kimliğini temsil eden bir DID belgesiyle (diddoc) ilişkilidir. DID belgeleri; kriptografik anahtarlar, doğrulama yöntemleri ve bazı hizmet tanımlarını içerebilir. Bu unsurlar kimliği yöneten kişinin (DID kontrolörü) bu kimlik üzerindeki yetkisini ve doğrulamasını sağlar.

Doğrulanabilir Kimlik Bilgileri Veri Modeli - Verifiable Credentials (VCs): Dijital kimlik bilgilerini güvenilir bir şekilde temsil etmek için W3C tarafından önerilen bir standarttır. Günlük hayatımızda kullandığımız kimlik bilgilerini (örneğin, sürücü belgeleri, üniversite diplomaları, pasaportlar) dijital ortamda kriptografik olarak güvenli, gizliliği koruyan ve makine tarafından doğrulanabilir bir şekilde ifade etme mekanizması sağlar. Bu modelde şu roller bulunmaktadır:

1. **Sahip / Holder:** Kendi DID değerlerini üretebilen, ihraççı tarafından edindiği doğrulanabilir kimlik bilgilerine sahip olabilen ve bunları diğer aktörlere ispatlayabilen taraf.
2. **İhraççı / Issuer:** Doğrulanabilir kimlik bilgileri oluşturan taraf.
3. **Konu / Subject:** Üzerinde iddialarda (sahiplik gibi) bulunulan varlık.
4. **Doğrulayıcı / Verifier:** Kimlik sahibinin sunduğu bir veya daha fazla doğrulanabilir kimlik bilgisini doğrulayan taraf.
5. **Doğrulanabilir Veri Deposu / Verifiable Data Registry:** Doğrulanabilir kimlik bilgilerini kullanmak için gerekli tanımlayıcıları ve anahtarları yöneten sistem.

3.1.2. OpenWallet

OpenID4VCI (Verifiable Credential Issuance): OpenID4VCI, dijital kimlik sağlayıcılarının doğrulanabilir kimlik bilgilerini (VC) kullanıcılara iletmesini sağlayan bir API standardıdır. Bu sistemde, kimlik verileri önceden belirlenmiş bir yapıya göre düzenlenir ve sahibine kriptografik yöntemlerle atanır. Bu veriler, OAuth koruması altında güvenli şekilde iletilir.

Kimlik bilgileri, sahibinin doğrudan katılımı olmadan bile son kullanıcı tarafından güvenli ve denetlenebilir biçimde sunulabilir. API'ye erişim, OAuth 2.0 protokolüyle güvenli şekilde yetkilendirilir. Bu sayede, kimlik bilgilerinin oluşturulması ve iletimi, OAuth 2.0'ın sunduğu güvenlik altyapısı ile korunur.

OpenID4VP (Verifiable Presentation): OpenID4VP, kullanıcının sahip olduğu kimlik bilgilerini doğrulanabilir biçimde sunmasını sağlayan bir standarttır. Bu yapı da OAuth 2.0 üzerine kuruludur ve kimlik verisinin kime, ne kadar, ne zaman gösterileceği tamamen kullanıcının kontrolündedir. Geliştirici dostu olması, esnek yapısı ve güvenli sunum katmanı sayesinde dijital kimlik sunumlarında temel protokol olarak kullanılmaktadır.

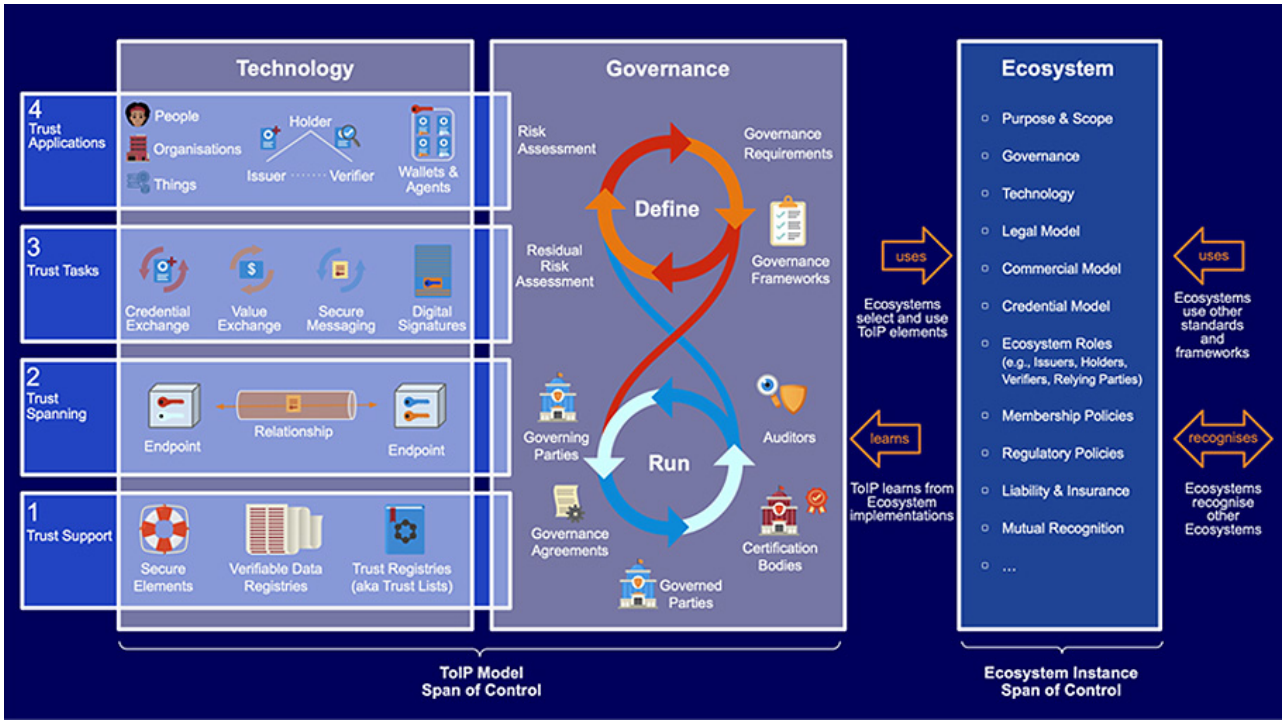
3.1.3. ISO Standartları

• ISO/TR 23244:2020: Bu standart, blokzincir ve defter teknolojileri sistemlerine uygulanan gizlilik ve kişisel olarak tanımlanabilir bilgilerin (personally identifiable information - PII) korunmasına genel bir bakış sağlar.

• ISO/TR 23249:2022: Bu standart, kimlik yönetimi için mevcut DLT sistemlerine genel bir bakış sağlar; örneğin, bir veya daha fazla varlığın bir dizi kimlik niteliğini nasıl oluşturabileceği, alabileceği, değiştirebileceği, kullanabileceği ve iptal edebileceği mekanizmalar açıklanır.

• ISO/TR 23644:2023: Bu standart, kimlik yönetimi için blokzinciri ve defter teknolojilerinden yararlanan sistemlerde güven bağlarının (trust anchors) kullanımına ilişkin kavramlar ve hususlar; örneğin, bir veya daha fazla varlığın bir dizi kimlik niteliğini oluşturma, verme, değiştirme, kullanma ve iptal etme mekanizmaları açıklanmaktadır.

• ISO/IEC 23220-1:2023: Bu standart, mobil eID sistem altyapıları için yapı taşları açısından genel sistem mimarilerini ve yaşam döngüsü aşamalarını belirtir; mobil doğrulama uygulamaları için arayüzleri ve hizmetleri standartlaştırır. Bir mobil eID sistemini kısmen veya tamamen belirleme, mimarisini oluşturma, tasarlama, test etme, sürdürme, yönetme ve işletmeyle ilgili kuruluşlar için geçerlidir.



1 nolu Destek Katmanı, kimlik verilerinin doğrulanmasını sağlayan verilerin güvenli depolanmasını, birbirini bulabilmesini ve doğrulama süreçlerinin işleyişini mümkün kılmaktadır.

2 nolu Haberleşme Katmanı, dijital kimlik cüzdanları arasında güvenli iletişimi sağlarken, güvenli protokoller ve birlikte çalışabilirlik imkânı sunmaktadır.

3 nolu Görev Protokolleri Katmanı, kullanıcının kimlik sertifikalarının oluşturulması, ispatlanması, doğrulanması, iptal edilmesi ve paylaşılması süreçlerini içerir.

4 nolu Uygulamalar Katmanı, sektörlere özel iş süreçlerini içermekte olup, dijital kimliklere dayalı olarak çalışan uygulamaları içerir. Bu katmanda, sektörlerde kimlerin hangi tür kimlik sertifikası yayınlayacağı, bu sertifikaların nasıl doğrulanacağı, nasıl iptal edileceği gibi yönetişim çerçeveleri de tanımlanır.

Bu katmanlı yapı, dijital kimlik sistemlerinin bütün dünyada ortak bir modele dayalı ve çalışabilir olarak geliştirilmesine imkan sağlar. Katmanların birbirinden izole edilmesi sayesinde, her bir katmandaki ürünler diğer katmanlardaki teknolojilerden bağımsız olarak geliştirilebilir.

Bütün katmanları ilgilendiren Yönetişim protokolleri ise politikaları, paydaşları, sözleşmeleri, sertifika verecek otoriteleri, denetleyicileri ve yönetişim çerçevelerini kapsar.

3.2. Topluluklar

Sertifikalandırma Otoriteleri Tarayıcı Forumu (Certification Authority Browser Forum): Bu forum, dijital dünyada güvenli iletişimi sağlayan X.509 v3 dijital sertifikalarının nasıl oluşturulacağı ve yönetileceğine dair kuralları belirleyen küresel bir iş birliği platformudur. X.509 v3 sertifikaları, internet üzerindeki kişi, kurum ve sistemlerin kimliğini doğrulamak amacıyla kullanılan uluslararası bir güvenlik standardıdır. Web sitelerinde HTTPS bağlantısı kurulmasında, yazılım imzalama ve e-posta güvenliğinde sıkça kullanılır.

CA/Browser Forum; sertifika sağlayıcıları (Certificate Authorities - CAs), internet tarayıcı üreticileri, işletim sistemleri geliştiricileri ve diğer güvenlik yazılımı üreticilerinden oluşan gönüllü bir topluluktur. Bu forumun belirlediği yönergeler sayesinde, TLS (Transport Layer Security), kod imzalama ve S/MIME gibi uygulamalarda güvenli ve standarda uygun bir "güven zinciri" oluşması sağlanır.

Bulut İmza Konsorsiyumu (Cloud Signature Consortium - CSC): Bulutta yüksek güvenlikli ve uyumlu dijital imzaların standartlaşmasını sağlamak amacıyla endüstri, hükümet ve akademik kuruluşlardan oluşan küresel bir gruptur. REST / JSON API kullanarak uzak imzaların oluşturulmasına olanak sağlarlar.

Finansal Eylem Görev Gücü (Financial Action Task Force - FATF): 1989 yılında G7 girişimiyle kurulan ve kara para aklamaya karşı mücadele için politikalar geliştirmeye yönelik bir hükümetler arası organizasyondur. Dijital Kimlik Rehberi hükümetler, düzenlemeye tabi kuruluşlar ve diğer ilgili paydaşlara, dijital kimlik sistemlerinin müşteri doğrulama süreçlerinde nasıl kullanılabileceği konusunda yardımcı olmayı amaçlamaktadır.

FIDO: Şubat 2013'te kurulan ve misyonu "dünyanın parolalara aşırı bağımlılığını azaltmaya yardımcı olan kimlik doğrulama standartlarını geliştirmek ve yaymak" olan açık bir endüstri birliğidir.

İnternet Mühendisliği Görev Gücü (IETF): İnternetin gelişimine yön veren teknik standartları belirleyen açık ve gönüllü bir organizasyondur. Elektronik imzalar, PKI (açık anahtar altyapısı) ve güvenli haberleşme gibi alanlarda temel kabul gören teknik belgeleri yayınlar. Bu belgeler, RFC (Request for Comments) adı verilen standart dokümanlardır. RFC'ler; internet protokollerinin nasıl çalıştığını tanımlar, zaman içinde gelişir ve yeni teknolojilere göre güncellenir. Örneğin, TLS (Transport Layer Security) ya da OAuth gibi yaygın güvenlik protokollerinin teknik tanımları da bu belgelerle yapılmıştır.

Yapılandırılmış Bilgi Standartları Geliştirme Organizasyonu (OASIS): OASIS, bilgi güvenliği, dijital kimlik, blokzincir, IoT ve acil durum yönetimi gibi alanlarda açık ve birlikte çalışabilir teknik standartlar geliştiren, kar amacı gütmeyen uluslararası bir konsorsiyumdur. İlk olarak yazılım üreticileri tarafından kurulmuş olsa da, zamanla akademik kuruluşlar, sivil toplum örgütleri ve çeşitli kamu kurumları da üyeleri arasında yer almıştır. Özellikle dijital imza, elektronik belge ve kimlik doğrulama gibi konularda kamu destekli projeler ve regülasyonlarla uyumlu çözümler geliştirilmesini desteklemiştir.

OASIS'in çalışmaları arasında, dijital imzaların teknik temellerini tanımlayan "Dijital İmza Hizmeti Temel Protokolleri, Öğeler ve Bağlantılar" adlı standart paketi de bulunur. Bu belgeler, dijital imza işlemlerinin nasıl yürütüleceğini, hangi veri yapılarının kullanılacağını ve sistemler arası uyumun nasıl sağlanacağını tanımlayarak, güvenli ve standarda uygun dijital imza altyapılarının oluşturulmasına katkı sağlar.

3.3. Dünyadaki Altyapı Örnekleri

Dijital kimlik altyapıları, kullanıcıların kendi kimlik bilgilerini güvenli bir şekilde yönetmelerine, verilerini sadece izin verdikleri kişi ve kuruluşlarla paylaşmalarına olanak tanır. Bu sistemler, kullanıcı verilerini güvence altına alarak, bankacılık, sağlık, eğitim ve devlet hizmetleri gibi pek çok sektörde daha güvenli ve verimli çözümler sunar. Sovrin, SSI Türkiye ve Cheqd gibi projeler, dijital kimlik yönetimi ve doğrulama süreçlerinde önemli rol oynayan altyapı örnekleridir.

3.3.1. Sovrin

Sovrin Vakfı, merkeziyetsiz dijital kimlik sistemleri için bir altyapı sağlayıcısıdır. Blokzincir teknolojisi üzerine inşa edilen Sovrin, kullanıcıların kimlik bilgilerini herhangi bir merkezi otoriteye bağlı kalmadan yönetmelerine olanak tanır. Bu model, bireylerin kimlik bilgilerini tam anlamıyla kontrol etmelerini sağlar.

Öne çıkan özellikleri:

- Self-Sovereign Identity (SSI): Kullanıcılar kimlik bilgilerini kendileri yönetir ve merkezi bir aracıya ihtiyaç duymazlar.
- Altyapısı: Sovrin ağı, blokzincir kullanarak verilerin güvenli ve şeffaf bir şekilde depolanmasını sağlar.
- Veri Güvenliği: Kimlik verileri yalnızca kullanıcıların kontrolünde olur, bu da veri ihlali riskini azaltır.

Sovrin, kullanıcıların dijital kimliklerini koruma altına alarak güvenli bir dijital kimlik doğrulama sistemi sunar. Kimlik bilgilerini üçüncü kişilerle paylaşma süreci tamamen kullanıcı kontrolündedir ve merkezi bir otoriteye ihtiyaç yoktur.

3.3.2. SSI Türkiye

SSI Türkiye, dijital kimlik doğrulama konusunda Türkiye'deki öncü projelerden biridir. Özellikle Türkiye'deki kamu kurumları ve özel sektör tarafından desteklenen bu inisiyatif, vatandaşların ve kullanıcıların kimlik bilgilerini güvenli ve merkeziyetsiz bir şekilde doğrulamalarını sağlar.

Öne çıkan özellikleri:

- Veri Koruma: Kimlik verileri bireylerin dijital cüzdanlarında saklanır ve yalnızca gerekli durumlarda paylaşılır.
- Kamu ve Özel Sektör İş Birliği: Türkiye'deki yasal çerçevelerle uyumlu çalışarak hem devlet hem de özel sektörde güvenli kimlik doğrulama sağlar.
- Yasal Uyum: Türkiye'nin kişisel verileri koruma yasalarıyla uyumlu altyapılar geliştirilmiştir.

SSI Türkiye, özellikle devlet hizmetleri, bankacılık ve sağlık alanlarında dijital kimlik doğrulama süreçlerinde büyük avantajlar sağlamaktadır. Kullanıcıların kimlik bilgilerini güvenli bir şekilde doğrulaması ve verilerini sadece yetkili kişilerle paylaşabilmesi, veri güvenliği ve gizliliği açısından büyük önem taşır.

3.3.3. Cheqd

Cheqd, dijital kimliklerin güvenli bir şekilde yönetilmesine olanak tanıyan bir başka önemli tabanlı projedir. Kullanıcıların verilerini merkeziyetsiz bir şekilde doğrulamalarını sağlayan Cheqd, özellikle Self-Sovereign Identity (SSI) çözümleri konusunda ön plana çıkar.

Öne çıkan özellikleri:

- Veri Sahipliği: Kullanıcılar kimlik bilgilerini kendi dijital cüzdanlarında saklar ve sadece izin verdikleri kişilerle paylaşır.
- Merkeziyetsiz Altyapı: Teknolojisi sayesinde kimlik doğrulama süreçleri hızlı ve güvenilir bir şekilde gerçekleştirilir.
- Gizlilik ve Güvenlik: Cheqd, GDPR gibi veri gizliliği yasalarına tam uyumlu çalışır ve kullanıcı verilerini koruma altına alır.

Cheqd, özellikle Avrupa'da gizlilik düzenlemeleriyle uyumlu dijital kimlik altyapıları sunar ve kullanıcıların verilerinin kontrolünü tamamen kendilerine bırakır. Bu, bireylerin kimlik doğrulama süreçlerini hızlı ve güvenli bir şekilde yönetmelerine olanak tanır.

3.3.4. uPort

uPort, merkeziyetsiz dijital kimliklerin oluşturulması, doğrulanması ve yönetilmesi için Ethereum üzerine inşa edilmiş bir projedir. Kullanıcıların dijital kimliklerini tam anlamıyla kontrol etmesine olanak tanır ve herhangi bir merkezi otoriteye gerek kalmadan kimlik doğrulaması yapılabilir.

Öne çıkan özellikleri:

- Kullanıcı Kontrolü: uPort, kullanıcıların kimlik bilgilerini kendilerinin saklamasını ve kimlik doğrulamalarını merkeziyetsiz bir şekilde gerçekleştirmesini sağlar.
- Entegrasyonu: Ethereum kullanarak, verilerin şifreli ve güvenli bir şekilde depolanmasını sağlar.
- Geniş Uygulama Alanı: uPort, finans, sağlık, eğitim gibi sektörlerde güvenli kimlik doğrulama ve veri paylaşımı için kullanılabilir.

uPort, dijital kimlik yönetiminde özellikle Ethereum tabanlı yaygın olarak kullanılan bir altyapıdır. Kimlik doğrulamanın yanı sıra kullanıcıların dijital hizmetlere erişimlerini güvenli hale getirir.

3.3.5. Microsoft Entra ID

Microsoft Entra, World Wide Web Konsorsiyum'unun kendine egemen kimlik standartları ile uyumlu verifiable credentials ve decentralized identity üretme araçları sunan, kuruluşlara kendi kimlik ve erişim yönetimi yönetişim kural ve süreçlerini oluşturmalarına olanak tanıyan bir altyapıdır. Microsoft'un Decentralized Identity stratejisinin bir sonucu olarak, kurum ve kuruluşların öz egemen kimlik yönetimi sistemlerini kurgulayabilmesi amacıyla ortaya çıkmıştır.

Öne çıkan özellikleri:

- Kurumsal Kimlik Yönetimi: Şirketler ve organizasyonlar için merkeziyetsiz bir kimlik doğrulama sistemi sunar.
- Veri Gizliliği: Kullanıcılar, kimlik bilgilerini kendi kontrolünde tutar ve sadece gerekli olan bilgileri paylaşır.
- Agnostik: Herhangi bir belirli protokolü ile çalışmak üzere tasarlanmamıştır.

Bu sistem, özellikle büyük şirketler ve organizasyonlar için geliştirilmiş olup, veri gizliliği ve güvenliğini ön planda tutan bir çözümdür.

3.3.6. Evernym

Evernym, self-sovereign identity (SSI) standartları ile uyumlu dijital kimlik yönetimi uygulamaları geliştirmeyi sağlayan araçlar üretmektedir. Evernym Verity adında, verifiable credentials düzenlenmesi ve doğrulanması için merkezi olmayan bir protokol sunmaktadır.

Kullanıcıların dijital kimliklerini saklayabilmeleri ve kullanabilmeleri için Connect.Me dijital kimlik cüzdanı ürününü geliştirmiştir.

Evernym, Sovrin Foundation kurucuları ve Hyperledger Indy protokolü geliştiricilerinin kurduğu özel bir şirkettir.

Öne çıkan özellikleri:

- Kurumlar için kullanıma hazır SSI araçları: SSI standartları ile uyumlu kimlik yönetimi uygulamaları geliştirilmesi için Verity protokolü ve Connect.Me cüzdanı sunar.
- ZKP uygulaması: Kimlik bilgilerinin paylaşılması ve doğrulanmasında mahremiyet odaklı zero-knowledge proof yöntemini kullanır.
- Hyperledger Indy: Evernym dijital kimlik uygulamaları ve geliştirme araçları Hyperledger Indy protokolü ile uyumludur.
- Evernym, sağlık, eğitim ve finans sektörlerinde kimlik doğrulama süreçlerinin güvenli ve hızlı bir şekilde yapılmasını sağlayan bir çözüm sunar.

3.3.7. ID2020

2015 yılının sonlarına doğru yayımlanan Birleşmiş Milletler Sürdürülebilir Kalkınma Gündemi kapsamındaki sürdürülebilir kalkınma hedeflerinden biri 2030 yılına kadar herkes için yasal kimlik sağlamak hedefidir. Finansal teknoloji ve dijital kimlik konularında uzmanlaşmış sosyal girişimci olan John Edge, bu hedeften ilham alarak ID2020 birliğinin kuruluşuna öncülük etmiştir.

ID2020, resmi olarak tanınan herhangi bir kimliğe sahip olmayan 1,1 milyar insan için çözümler arayan, kar amacı gütmeyen bir kamu-özel sektör ortaklığıdır. Dünya genelinde kimlik sahibi olmayan bireylere dijital kimlik sağlamayı amaçlamaktadır. Özellikle mülteciler, yerinden edilmiş insanlar ve kimlik belgesi olmayan bireyler için dijital kimlik çözümleri geliştirir.

Blokzincir teknolojisini kullanarak, kişisel bilgilerin güvenli bir şekilde saklanmasını ve doğrulanmasını sağlar.

Öne çıkan özellikleri:

- Yönetişim modeli: ID2020 girişimi, dijital kimlik sistemlerinin gizlilik, kullanıcı kontrolü ve birlikte çalışabilirlik ilkelerine uygun şekilde geliştirilmesini sağlamak üzere yapılandırılmıştır. Bu çerçevede, sistemin işleyişi bir danışma kurulu tarafından yönlendirilir ve kimlik çözümlerinin belirlenen ilkelere uygunluğunu değerlendiren bağımsız bir sertifikasyon programı aracılığıyla denetlenir. Böylece dijital kimlik sağlayıcılarının güvenilir, şeffaf ve standartlara uygun hizmet sunması garanti altına alınır.
- Teknoloji agnostik: ID2020 spesifik olarak bir dijital kimlik teknoloji altyapısı sunmaz. Bununla birlikte SSI standartlarına uygun olacak şekilde blokzinciri ağlarının kullanımını destekler.
- Sosyal Odaklı: Özellikle dezavantajlı grupların kimlik doğrulama sorunlarına çözüm sunar.

ID2020, Birleşmiş Milletler ve büyük teknoloji şirketleri tarafından desteklenmektedir ve dünya genelinde dijital kimlik sistemlerinin yaygınlaştırılmasını hedefler.

3.3.8. IBM Digital Credentials and Blockchain Platform

IBM Digital Credentials and Blockchain Platform, kurumsal organizasyonların kimlik yönetimini merkeziyetsiz bir şekilde dijital kimlik araçları (Digital Credentials) ile yönetmeleri için geliştirilmiş bir altyapı sunar. Kurumların uyum ve genişleme gereksinimlerini gözetecek şekilde Hyperledger Fabric üzerine inşa edilmiş esnek yapıda bir platformdur.

Öne çıkan özellikleri:

- Kontrollerle uyumlu merkeziyetsizlik: IBM Blockchain Platformu merkeziyetsiz teknolojilerin kullanıcı egemen kimlik yönetimi için avantajlarından yararlanırken, kurumların süreç kontrolleri ile uyumlu bir uygulama yapabilmelerini destekler.

- Esnek konsensüs mekanizmaları desteği: Kurumların kendi ihtiyaçlarına yönelik olarak farklı konsensüs mekanizmalarının uygulanmasını destekler.

- Zincirliler arası işleyebilirlik: Dijital kimlik araçları (Digital Credentials) farklı kurumlar ve dijital kimlik yönetim sistemleri ile iletişimi destekleyecek şekilde tasarlanmıştır. Bu, kimlik bilgisi paylaşımını basitleştirir ve cüzdandan cüzdana ve kurumsal sistemlere güven zinciri oluşturur.

3.3.9. Veres One

Veres One, merkezi olmayan tanımlayıcılar (decentralized identifiers - DIDs) için özel olarak Digital Bazaar tarafından inşa edilmiş bir blokzincirdir. Veres One'ın operasyonel modeli şeffaflık sağlar, ağa yönelik saldırıları önler ve ağın güvenliğini sağlamak için yazılım çalıştırmayı seçen kişi ve kuruluşları finansal olarak ödüllendirir. Veres One ağı küreseldir ve kamuya açıktır; herkes katılabilir.

Öne çıkan özellikleri:

- Kişi ve kuruluşların kendi kimliklerini oluşturmaları ve yönetebilmeleri: Veres One projesinin misyonu, dünyadaki herkesin kendi merkezi olmayan tanımlayıcılarını oluşturmasını ve yönetmesini sağlamak için ekosistem yönetişimi sağlamaktır.

- Networkler arası çalışmaya uyumlu: Veres One, hangi cüzdan uygulamasının kullanıldığına bakılmaksızın %100 uyumludur.

- Katılımcı teşvik modeli: Veres One Ağı, ağa katılmak ve ağı korumak için uygun bir ekonomik teşvik dengesi ile kendi kendini idame ettiren küresel bir kamu hizmeti olarak tasarlanmıştır.

Dijital kimlik yönetimi, teknolojisinin sunduğu merkeziyetsiz çözümlerle hızla gelişmektedir. Bu projeler, bireylerin ve kurumların kimlik bilgilerini güvenli ve merkeziyetsiz bir şekilde yönetmelerini sağlarken, veri güvenliği ve gizliliği gibi önemli konularda çözüm sunmaktadır. Sovrin, SSI Türkiye, Cheqd, uPort, Microsoft Decentralized Identity, Evernym, ID2020 ve IBM Blockchain Identity gibi projeler, dijital kimlik teknolojileri alanında öne çıkan önemli altyapı örnekleridir. Bu altyapılar, güvenli dijital kimlik doğrulama süreçlerinin yanı sıra bireylerin dijital dünyada daha fazla söz sahibi olmalarına olanak tanımaktadır.

3.3.10. PrivadoID (PolygonID)

Dijital kimlik doğrulamada sıfır bilgi kanıtı (Zero-Knowledge Proof) teknolojisini kullanarak kişisel verilerin ifşa edilmesini önlemeyi amaçlamaktadır. Bir bilginin doğru olduğunu, bu bilginin kendisini paylaşmadan kanıtlamaya olanak tanıyan bu teknoloji ile kullanıcılar, verilerinin kontrolünü elinde tutarken, doğrulama işlemlerinde onay mekanizmasına yalnızca minimum bilgi sunarlar. Bu yaklaşım, özellikle gizlilik ve veri güvenliği ihtiyacı olan projeler için büyük bir avantaj sunar.

3.3.11. WorldID (Worldcoin)

Biyometrik doğrulama yöntemi ile insan doğrulamasına odaklanır. Yapay zeka ile insan ayrımının gelecekte güçleşeceğini vurgulayan proje, bireylerin kimliklerini benzersiz bir şekilde doğrulamak amacıyla iris tarama teknolojisini kullanır.

İris taramaları, her kullanıcının benzersiz biyometrik verilerini hash değerleri üzerinden şifreleyerek merkeziyetsiz yapılarda doğrulama sağlar. Bu çözüm, sahte hesap ve bot saldırılarına karşı etkili bir güvenlik mekanizması oluşturur.

3.4. Farklı Kanallardaki Deneyim Tasarımları

Blokzincir tabanlı dijital kimlik yönetimi sistemleri farklı senaryolarda farklı mantıklarda çalışabilir. İhtiyaca göre en uygun senaryonun belirlenmesi ancak uygun donanım ile mümkündür. Bu donanımların üzerinde yer alan bileşenler uygulamanın kapasitesi ve akışı üzerinde doğrudan etkilidir. Bu sebeple, deneyim tasarımları 4 farklı grupta incelenecektir.

3.4.1. Mobil Donanımlar

Akıllı telefonlar, saatler ve tabletler gibi taşınabilir cihazlar bu gruba girmektedir. Bu cihazların avantajları taşınabilirlik, kolay kullanım ve diğer uygulamalarla entegrasyon kolaylığı olarak sıralanabilirken, sınırlı işlem gücü, bağlantı ve güvenlik sorunları da dezavantajları arasında gösterilebilir.

Mobil donanımlara yüklenen cüzdan uygulaması ile birlikte etkileşime girilen ortama göre farklı deneyimler tasarlanabilmektedir.

- Mobil: Genel olarak bu kategori aynı cihaz üzerindeki senaryolar ve farklı mobil cihazlar üzerindeki senaryolar olarak ikiye ayrılabilir. Farklı mobil cihaz ortamındaki senaryolar bir sonraki başlıkta anlatılan web senaryolarına benzer işletilmekle beraber, aynı cihaz üzerinde gerçekleşen senaryolarda uygulamadan uygulamaya çağrım (app-to-app deep linking) öne çıkar.

- Web: Mobil donanımlar ile birlikte kullanılan en popüler kanallardan bir tanesidir. Çoğunlukla karekod ya da barkod gibi teknolojilerden faydalanılır. Laptop, masaüstü bilgisayar gibi ikinci bir cihaza ihtiyaç duyar. Kimlik yaratma ve doğrulama işlemlerinde ikinci cihaz üzerinde oluşturulan kodlar mobil donanım kamerası ile sağlanan etkileşimle işlemler tamamlanır. Bununla birlikte her iki cihazda uygun bileşenler bulunduğu takdirde Bluetooth, NFC gibi teknolojilerden yaralanmak da mümkündür.

- Diğer Entegrasyonlar: Bilgisayar, laptop, tablet ve mobil donanımlar dışındaki etkileşimler bu kategoriye düşmektedir. Çeşitli güvenlik noktaları, IoT donanımları vb. cihazlar örnek olarak gösterilebilir. Etkileşime giren her iki cihazdaki bileşenlere göre karekod, barkod, Bluetooth, NFC ve diğer teknolojiler ile akış yürütülebilir.

Tüm bu işlemler sırasında mobil donanımlar üzerinde yer alan bileşenler sayesinde ekstra güvenlik katmanları eklenebilmektedir. 2FA, MFA, biyometrik (parmak izi, yüz tanıma vb.), pin kodları gibi yöntemler bunlara örnek olarak verilebilir. Ancak, bu cihazlardaki sınırlı işlem gücü karmaşık şifreleme işlemleri sırasında yetersiz kalarak işlemlerin uzun sürmesiyle sonuçlanabilir. Ayrıca, bu cihazların bozulması, çalınması, pilinin tükenmesi gibi durumlarda sistem çalışmaz hale gelmektedir.

3.4.2. Masaüstü ve Laptoplar

Masaüstü bilgisayarlar ve laptopların başlıca dezavantajı mobil cihazlar ile karşılaştırıldığında kolay taşınabilir ve kullanılabilir olmamalarıdır. Ancak, işlem gücü açısından mobil cihazların sunmadığı bir takım avantajlar sunabilirler. Öte yandan, cihazların kullanıma elverişli olduğu durumlarda bluetooth, NFC gibi teknolojilerden de yararlanılabilir.

Bu tip cihazlar genellikle dijital kimlik oluşturma süreçlerinde ikincil cihaz olarak kullanılır.

Servis sağlayıcılar üzerinden laptopta oluşturulan kimlikler, karekodlar aracılığıyla mobil cihazlara çekilir ve dijital kimliğin günlük işlemlerde kullanımı mobilden sağlanır. Henüz yaygın olmamakla beraber, geliştirilebilecek internet erişimine sahip masaüstü uygulamalar veya browser cüzdanları aracılığıyla dijital kimlik sahipleri, ellerinde bulundurdukları kimlik verilerini harici cihazlar ve mobil ile etkileşime girmek için laptoplarından da kullanabilirler. Yine bu esnada kimlik bilgilerinin laptopa çekilmesi için bluetooth vb. bir çözüme açık ikincil bir cihaza ihtiyaç duyulacaktır. Taşınabilirlik dezavantajı göz önüne alındığında bu durum pek cezbedici olmasa da mobil cihazlara kıyasla daha güvenli ve hızlı bir işlem süreci sunabilir. Masaüstü bilgisayarlar ve laptopların değerlendirildiği bu kategoride web ortamındaki uygulamalar ve masaüstü uygulamalar ele alınabilir.

- Masaüstü Uygulamaları: Masaüstü bilgisayarlar ve laptoplar için tasarlanan bu tip uygulamalar, genellikle yüksek işlem gücü ve gelişmiş güvenlik özelliklerinin yanı sıra kaliteli bir kullanıcı arayüzü sunar. Çevrimdışı ortamda veri çalınması riskini azaltır. Ancak taşınabilirlik açısından sınırlı olarak yorumlanabilir ve yalnızca belirli tip bilgisayarlarda kullanılabilir.

- Tarayıcı Uygulamaları: Web tarayıcıları üzerinden erişilen bu uygulamalar daha geniş cihaz uyumluluğu sunar. Hızlı kullanım ve erişilebilirlik avantajlarını beraberinde getirirken, genellikle kullanıcı arayüzü limitli gelişmişliğe sahiptir. Anahtarların tarayıcı yerel depolama alanında tutulması, potansiyel güvenlik riskleri oluşturur.

3.4.3.Donanım Cüzdanlar

Her bir kullanıcıya ait özel anahtarların DID değerinin üretilmesi, şifreleme ve imzalama gibi kritik işlevleri mevcuttur. Donanım cüzdanları ise dijital kimlik altyapısında kullanıcının eşsiz tanımlayıcıya sahip olmasını sağlayan bu anahtarların güvenle saklanabilmesi için kullanılabilir. Donanım cüzdanları kullanılabilirlik ve erişim farklılıklarına göre pasif ve aktif olmak üzere ikiye ayrılır.

Pasif donanım cüzdanları genellikle internet erişiminden uzak ya da sınırlı bir bağlantıya sahip cihazlardır. Bu donanım cüzdanları kullanıcının dijital kimliğinin güvenliği için özel anahtarı barındıracak şekilde tasarlanmıştır. İzole bir donanım ve yazılım ortamı içerisinde kullanılan özel anahtar ile şifreleme ve imzalama işlemleri dijital kimliğin deneyim kanalları içerisinde yer bulacaktır. Kullanıcının sahip olduğu birden fazla kimliği güvenli bir şekilde barındırma özelliğini sağlayabilse de kullanım ve entegrasyon kolaylığı konusunda problemler ortaya çıkabilir. Mobil ve bilgisayar gibi diğer cihazlarla olan etkileşimi USB, kamera, NFC gibi yollarla sağlanabilir fakat diğer cihazlara ve internete erişimi sınırlı olacağından kullanım senaryoları diğer yöntemlere göre daha sınırlı kalabilir. Ayrıca her ne kadar daha güvenli bir çözüm üretmiş olsa da kullanıcı için taşıma zorluğu yaratırken aynı zamanda yüksek maliyete sebep olabileceğinden dolayı tercih edilmeyebilir. Öbür yandan, pasif olmalarından ötürü bu donanımlar kendi üzerlerinde bir enerji kaynağına (örneğin pil, batarya vb.) ihtiyaç duymazlar ve aktif cihazlar gibi şarj edilmelerine gerek yoktur.

Aktif donanım cüzdanları ise internet bağlantısı aracılığıyla doğrudan ağa erişebilen aynı zamanda mobil cihaz veya bilgisayar ile etkileşime (Bluetooth, Wi-Fi üzerinden) girebilen cihazlardır. Dijital kimlik cüzdanlarının PKI tabanlı olmasından dolayı yine imzalama ve şifreleme işlemleri aktif donanım cüzdanı içerisinde güvenli bir şekilde tutulan özel anahtarın kullanılması ile olacaktır.

Kullanıcılar mobil cihazları veya bilgisayarları içerisinde yer alan uygulamaları kullanarak dijital kimliğin sunduğu olanakları deneyimlerken donanım cüzdanları ile daha güvenli bir akış içerisinde olacaklardır. Pasif donanım cüzdanlarına göre diğer deneyim kanallarında da olduğu gibi akış içerisinde güvenlik zafiyetlerine dikkat edilmelidir.

3.4.4. Diğer Entegrasyonlar

Daha önce bahsedilenler dışında otomobil, ev sistemleri, üretimde kullanılan makineler gibi IoT kapsamına girebilecek cihazlar bu grupta yer almaktadır. Buradaki vizyon; standartlaştırılmış, kağıtsız ve hatasız olacak şekilde farklı aktörlerin yer alacağı merkeziyetsiz ve güvenilir bir sürecin gerçekleştirilmesidir. Enerji, tedarik zinciri gibi sektörel olarak çözümlerin üretileceği senaryolarda IoT cihazlar üzerinde kurulan dijital kimlik yönetimi ile entegrasyon kolaylığı, güvenli veri transferi ve doğrulanabilirliği kazanımları sağlanabilecektir. Bu cihazların avantajları kolay kullanım ve sürecin hızlanması iken kısıtlı kullanım örnekleri, bağlantı ve güvenlik sorunları dezavantajları arasında gösterilebilir. Bahsedilen IoT cihazlarında yer alacak olan dijital kimlik cüzdanı ile farklı kullanım alanlarında birçok deneyim akışı tasarlanabilmektedir.

Dijital kimlik sahibinin (holder) tüm aksiyonlar üzerinde son karar alıcı unsur olduğunu belirtmekle birlikte diğer entegrasyonlarda kastedilen IoT cihazları düzenleyici (issuer) veya doğrulayıcı (verifier) gibi otonom davranabilir. Etkileşime giren cihazlar arasındaki bağlantı; karekod, NFC, bluetooth, veya kablosuz ağ üzerinden cihazın yeterliliklerine bağlı olarak sağlanabilir. Güvenilir ve doğrulanabilir veri akışının sağlanması ile birlikte kullanım kolaylığı sağlanacaktır.

4. GÜVENLİK VE GİZLİLİK

Dağıtık defter teknolojilerinin (distributed ledger technology) gerçekleme yöntemi olarak evrimleşen blockzincir teknolojileri, kayıtlar/işlemleri bir uzlaşma mekanizması yardımıyla dağıtık olarak birçok noktada tutabilmektedir. Böylelikle tüm kayıtlar, yüksek güvenlik gerektiren merkezi veri tabanlarında tutulmak yerine dağıtık bir ağ üzerinde üyelerin katılımıyla aracısız olarak tutulur. Kriptografik mekanizmalar kullanılarak işlem kayıtlarının tutulduğu veri blokları zincir şeklinde birbirine bağlanır. Blokların her biri bir önceki bloğa ait benzersiz kriptografik özet (hash) bilgisine sahip olduğu için içerisinde kayıtlı işlemler geri dönülemez ve değiştirilemez şekilde merkeziyetsiz defterlerde kayıt altına alınır. Bloklar, her kullanıcının inceleyebileceği neredeyse değiştirilemez bir zincir oluşturur. Bloklardaki tüm işlemler, doğru ve geçerli olduğundan emin olmak için bir mutabakat mekanizması ile doğrulanır ve onaylanır. Bu sistemde single point of failure yoktur ve tek bir kullanıcı, işlem kayıtlarını değiştiremez. Ancak, blokzincir teknolojilerine özel güvenlik tehditler bulunmaktadır ve public/private çözümlerini benimseyen şirketler, bu güvenlik tehditlerini ve açıklarını dikkatlice değerlendirmelidir.

4.1. Siber Saldırılar

2023 yılında CACI firması tarafından yapılan bir araştırmada, teknolojilerinde en çok karşılaşılan üç siber saldırı türü açıklanmıştır. Bunlar;
Borsa Saldırıları: Kripto para borsaları, akıllı sözleşmelerdeki ve zincirler arası köprülerdeki (IBC) açıklar nedeniyle sık sık saldırıya uğrar. 2012 yılından beri, en az 46 kripto para borsası saldırılardan etkilenmiştir ve yaklaşık 10 milyar USD değerinde kripto varlık çalınmıştır. Bybit, 2025 Şubat ayında, dünya tarihinin en yüksek maliyetli kayba sebep olan kripto saldırısına uğramıştır ve yaklaşık 1.5 milyar USD'lık kayıp yaşanmıştır.

DeFi Saldırıları: Merkeziyetsiz finans platformları, özellikle doğrulayıcı düğümler ve anahtar yönetim sistemlerindeki güvenlik zafiyetlerinden yararlanan saldırganların hedefi olur.

Fidye Yazılımı: Kritik sistemleri kilitleyerek fidye talep eden bu saldırılar birçok sektörü etkiler.

Bu saldırı türleri dışında, bir araştırma grubu, 2009 ve 2017 yılları arasında blokzincir sistemlerindeki güvenlik açıklarını inceleyip yaklaşık dokuz kategoride blokzincir güvenlik risklerini listelemiştir. Bu kaynağa göre en önemli tehditler ve saldırı tipleri aşağıda sıralanmıştır.

Oltalama(Phishing) atakları: Geleneksel olarak, tüm oltalama saldırıları iki türe ayrılabilir: sosyal mühendislik yöntemleri ve teknik yöntemler. Sosyal mühendislik yöntemleri, kurbanın aldatılmasına ve ardından kendi kendine yanlış eylemler yapmasına dayanır. Sosyal mühendislik teknikleri kullanan saldırgan kullanıcıların kimlik bilgilerini ele geçirebilir, kullanıcı cihazlarına kötü amaçlı yazılım yükleyebilir ve özel anahtarlar ile kripto cüzdanlarının kurulum sırasında oluşturulan kurtarma ifadelerini elde edilebilir. Bu kurtarma ifadeleri, kullanıcıların şifrelerini unuttuklarında veya cihazlarını kaybettiklerinde cüzdanlarına erişimlerini sağlar. Teknik yöntemler daha çok altyapıların veya akıllı kontratların yazılım açıklıklarından yararlanır. Örnek olarak DNS tabanlı oltalama saldırıları, cookie ele geçirme, keylogger kullanımı, vb. verilebilir.

Sybil atakları: Bu saldırı, bir ağda birden fazla sahte kimlik oluşturarak ağa zarar verme girişimidir. Bu tür saldırılarda, saldırgan çok sayıda sahte düğüm yaratır ve böylece ağı kontrol etmeye ve blok doğrulama süreçlerini manipüle etmeye çalışır. Blokzincir sistemlerinde bu tür saldırılar, dağıtık defterin güvenilirliğini tehdit ederek sistemde güvenlik açıkları yaratır ve konsensüs mekanizmalarını zayıflatabilir. Blok bekleme sürelerindeki gecikme çifte harcamaya sebep olabilir.

51% atakları: Bu saldırı, bir blokzincir ağının çoğunluğunun azınlığa karşı komplo kurması anlamına gelir. Bu tür saldırılar, Ethereum Classic, Verge Currency ve ZenCash (şimdi Horizen) gibi platformlarda yaşanan olaylarda görülmüştür. Bir 51% saldırısında, kötü niyetli bir madenci veya madenci grubu, ağın işlem gücünün %51'inden fazlasını kontrol altına alarak blokzincir üzerinde değişiklik yapabilir. Kontrolü ele geçiren taraf, işlemleri engelleyebilir, ödemeleri durdurabilir, işlemleri geri çevirebilir veya çift harcama yapabilir. Çift harcama, aynı kripto paranın birden fazla işlemde kullanılmasıyla gerçekleşen bir tür dolandırıcılıktır.

Routing atakları: Yönlendirme saldırısı, internet servis sağlayıcıları (ISP) seviyesinde gerçekleştirilen ve web tabanlı sistemlerin çalışma süresini veya katılımını etkileyen bir siber saldırı türüdür. Bu saldırıda, saldırganlar ağı iki veya daha fazla ayrı bileşene böler ve belirli düğümler arasındaki iletişimi engelleyerek paralel blok zincirleri oluştururlar. Saldırı sona erdiğinde, daha küçük zincirde üretilen tüm bloklar ve ilgili işlemler geçersiz sayılır; bu da madencilerin kazançlarının kaybına yol açar. Bitcoin ağı, hem yönlendirici hem de madencilik açısından yüksek derecede merkezileşmiştir. Dünya genelindeki Bitcoin düğümlerinin çoğu, az sayıda ISP üzerinde bulunmaktadır; Toplamda onüç ISP, tüm Bitcoin ağının %30'unu barındırmaktadır. Ayrıca, Bitcoin düğümleri arasındaki trafiğin %60'ı sadece üç ISP üzerinden geçmektedir, bu durum ISP'lerin dünya çapındaki Bitcoin bağlantılarının yarısından fazlasını görebildiği anlamına gelir. Bu yoğunlaşma, saldırganlar için merkezi bir hedef oluşturur.

Saldırgan iki farklı şekilde saldırısını gerçekleştirebilir:

• Bölme Saldırıları: Ağı iki veya daha fazla parçaya ayırarak paralel blok zincirleri oluşturur. Saldırı bittiğinde, küçük zincirdeki bloklar geçersiz olur.

• Gecikme Saldırıları: Blok iletimini geciktirerek çift harcama ve madencilik kayıplarına neden olur.

Bu saldırılar, yönlendirme farkındalıklı eş seçimleri, bağlantı çeşitliliği ve trafik şifrelemesi ile hafifletilebilir. Önlem amacıyla bağlantı davranışlarının daha bilinçli hale getirilmesi, eş seçimlerinin yönlendirme farkındalığına göre yapılması ve trafiğin şifrelenmesinin iyileştirilmesi gerekmektedir. Erken tespit, daha çeşitli bağlantı seçimlerini tetikleyerek blokzincirin güvenliğini artırabilir.

Man-in-the-middle (MitM) atakları: MitM saldırıları, saldırganların ağlarında üçüncü taraflar ile düğüm arasına girerek gönderilen veri veya mesajları değiştirdiği ve tarafları taklit ederek manipüle edebildiği bir saldırı türüdür. Bu saldırılar, akıllı sözleşme parametrelerinin değiştirilmesi, sahte düğümlerle işlemlerin yönlendirilmesi, aynı fonların birden fazla kez harcanması (çift harcama) ve blokların geciktirilmesi gibi farklı yöntemlerle gerçekleşebilir. Saldırıların etkisini azaltmak için şifreli iletişim protokolleri (SSL/TLS), düğüm kimlik doğrulama, konsensüs mekanizmaları (Proof of Work, Proof of Stake) ve merkeziyetsiz yapılar kullanılmalıdır. MitM saldırıları blokzincir güvenliği için ciddi bir tehdit oluştursa da, uygun güvenlik önlemleriyle bu riskler büyük ölçüde azaltılabilir.

Endpoint zafiyetleri: Endpoint açıklıkları, kullanıcı arayüzünde veya sistemin etkileşim noktalarında oluşan zayıflıklar ve potansiyel açıklık noktalarıdır. Cüzdan güvenlik açıklıkları, bozuk kimlik doğrulama, kriptografik hatalar, özel anahtarların güvensiz depolanması, phishing saldırılarına yatkınlık, kripto jacking ve yetersiz şifreleme önlemleri gibi çeşitli şekillerde ortaya çıkabilir ve kullanıcıların dijital varlıklarını tehlikeye atabilir.

Bu güvenlik açıklıklarını kapatmak için farklı yöntemler kullanılabilir. Özellikle kriptografik işlemlerin güvenliği için Güvenli Yürütme Ortamı (TEE) eklenebilir ve steganografi kullanımı önerilebilir. Bu yöntemlerle, hassas verinin saklanmasına, bozuk kimlik doğrulamaya, güvenlik konfigürasyon hatasına veya web güvenliği açıklıklarına karşı önlem alınabilir.

Double Spending tehditi: Çift harcama tehditi, aynı kripto para biriminin birden fazla kez harcanmaya çalışılması durumunda ortaya çıkar ve merkezi olmayan sistemlerin güvenilirliği ile şeffaflığını tehdit eder. Bu sorun, ağ gecikmesi, kötü niyetli aktörler ve kullanılan fikir birliği mekanizmalarının zayıflıkları gibi nedenlerden kaynaklanabilir. Sorunun çözümü için mevcut yaklaşımlar arasında iş kanıtı (Proof-of-Work, PoW) ve hisse kanıtı (Proof-of-Stake, PoS) gibi mekanizmalar öne çıkmaktadır. Ayrıca, çok taraflı hesaplama ve sıfır bilgi kanıtları gibi yenilikçi teknolojiler de araştırılmaktadır.

Güvenilir Yürütme Ortamı (TEE) Kullanımı kaynaklı riskler: SSI model tasarımı, doğrulanabilir kimlik bilgilerini depolamak için cihazlardaki güvenilir yürütme ortamına (TEE) (telefonlar, tabletler, bilgisayarlar) güvenmektedir. TEE, işlem, bellek ve depolama yetenekleri sağlayan izole edilmiş güvenli bir ortamdır. Güvenliği ve bütünlüğü, sağlayıcının donanım ve yazılım bileşenlerini koruma yeteneğine bağlıdır. Güvenilir bir ortam olarak tasarlanmış olsa da, TEE'ler güvenlik açıklarına ve saldırılara karşı tamamen bağışık değildir. Tehdit aktörleri, TEE'leri hedef almak için yan kanal saldırıları, donanım açıkları ve yazılım güvenlik açıkları gibi yeni teknikler geliştirmektedir. Bu tehditlerin önüne geçebilmek için sürekli araştırma, geliştirme ve dikkatli bir izleme gereklidir. Böylece TEE'lerin evrilen güvenlik zorluklarına karşı korunaklı kalması sağlanabilir.

4.2. Dolandırıcılığın Önlenmesi ve Vatandaşın Korunması

Kurumların ve müşterilerinin hassas verilerine merkezi veri tabanları aracılığı ile erişilmektedir. Bu durum, dışarıdan bu veri tabanlarına olası saldırılarda toplu olarak kurumun verilerinin sızması riskini ortaya çıkarabilmektedir. Bu veriler üzerinden dolandırıcılar sosyal mühendislik, oltalama gibi geleneksel dolandırıcılık yöntemleri ile kişilerin varlıklarını hedef alabilmektedir. Veri saklamanın merkezileştirilmeden uzaklaştırılması bu açıdan bir gereklilik olarak ortaya çıkmaktadır.

Dijital Kimlik çözümleri güvenli ve doğrulanabilir bir kimlik tespit aracı olduğu için dolandırıcılık faaliyetlerini önemli ölçüde azaltarak daha sağlam ve güvenilir bir finansal ekosistem oluşturabilir. Dijitalleşmenin ve sosyal medya kullanımının artması ile birlikte özellikle kimlik hırsızlığı vakalarında yaşanan artışa bir önlem olarak dijital kimlik doğrulama yöntemleri kurumlara önemli bir koruma kalkanı sağlamaktadır.

4.2.1. Bilinen Dolandırıcılık Yöntemlerinde Veriler Nasıl Ele Geçer

Sosyal mühendislik, zararlı yazılım, oltalama gibi en sık bilinen dolandırıcılık yöntemlerinde kullanıcılar ya şifre paylaşır, ya bir zararlı/sahte site linkine tıklar, ya da doğrudan kendisi işlem yapmak üzere manipüle edilir. Ayrıca en sık karşılaşılan yöntemlerden olan kimlik sahteciliklerinde kullanıcının hiç işin içinde olmadığı, kimliğinin kopyalanarak o kullanıcı gibi davranılması söz konusudur. Tüm yöntemlerin ortak özelliği, dolandırıcıların bir atak yapmadan önce hedef aldığı kitle için bir takım verilere sahip olduğu gerçeğidir.

Mobil uygulamalar, sosyal medya uygulamaları, bankacılık uygulamaları başta olmak üzere internet tabanlı birçok ortama kullanıcılar şifreleri ile birlikte erişebilmekte, erişilen her hangi bir ortamda yaşanan veri sızıntısı kullanıcının hem o ortamdaki hem de aynı şifreyi kullandığı diğer ortamlardaki verilerinin ortaya çıkmasına sebebiyet vermektedir. Toplu olarak erişilen bu bilgiler sosyal mühendislik başta olmak üzere çeşitli dolandırıcılık yöntemleri ile müşterilerin finansal varlıklarına erişim ya da tehdit unsuru olarak kullanılabilmektedir.

Kurumlar müşterilerinin verilerini korumak amacıyla çeşitli ve maliyetli güvenlik önlemlerine yatırım yapmakta, kimi zaman bu önlemlere rağmen veri sızıntısı saldırıları başarılı olabildiği gibi kurum içi suistimal yoluyla bilgilerin sızması mümkün olabilmektedir. Verilerin geleneksel merkezi sistemlerce saklanması, bilinen kimlik doğrulama yöntemlerinin kullanıcıları korumada yetersiz kalmasına sebebiyet vermektedir.

4.2.2. Dijital Kimlik doğrulamasının geleneksel kimlik doğrulama yöntemlerine göre artısı nedir?

Farklı sektörlerde özellikle uzaktan hizmet verme süreçlerinde müşterilerin yapmış olduğu işlemler çeşitlense de belirli geleneksel kimlik doğrulama yöntemleri kullanılmaktadır. Bu kimlik doğrulama yöntemleri için müşterilerin manipüle edilememesi ve kimliklerinin kopyalanamaması kritiktir. Dijital Kimlik çözümleri ile verilerin merkezileştirilmeden kurtarılarak veri sızıntısı riski minimize edilirken, bir yandan şifrelenmiş veriler üzerinden gerçekleştirilen kimlik doğrulama ile kullanıcıların daha güvenli bir şekilde hizmet alabilmeleri sağlanmaktadır. Dijital kimlik doğrulamada üçüncü tarafların doğrulama süreçlerine dahil olmasına rağmen hassas verinin tamamına sahip olamayacağı için, saklanan verilerin yetkisiz kişilerce kullanılması riski minimize edilmiştir.

Geleneksel kimlik doğrulama yöntemlerinde daha fazla araç, manuel süreç ve insan kaynağı desteğine ihtiyaç duyulabilmekte, blokzincir tabanlı dijital kimlik doğrulama yöntemlerinde bu tür ihtiyaçlar azaldığı için doğrulama süreci daha az sürede ve maliyetli gerçekleştirilmektedir.

4.2.3. Dijital kimlik doğrulama kullanımında nelere dikkat edilmeli?

Diğer kimlik doğrulama yöntemlerindeki gibi dijital kimlik doğrulamanın uygulamasında da mahremiyet ve deneyim açısından dengeli kullanım en az bilgi ve kullanıcı güvenliği kadar önemlidir. Tüm uygulama risklerine yönelik kapsayıcı bakış açısıyla sağlam bir ekosistem dizayn edilmeli, dijital kimlik doğrulama sistemlerinin gücünden optimum düzeyde faydalanılmalıdır. Dijital kimlik doğrulama çözümleri blokzincir teknolojisinin sunduğu ileri düzey güvenlikle veri sızıntısı ve kimlik sahteciliğinin azaltılması için kurumlara güç vermekle birlikte, uygulamada hem kurumlara hem de kullanıcılara düşen sorumluluklar bulunmaktadır.

Bir bilgi blokzincire eklendiğinde asla silinmez ve değiştirilemez. Eklenen kişisel verilerin zamanla unutulması söz konusu olabilir, zamanla kullanımdan vazgeçilmiş bir blokzincir bileşeni için içerideki verilerin ele geçirilme riski her zaman olacaktır. Bu nedenle, kişisel veri içermeyen dijital kimlik ID 'leri kullanılabilir, bu ID'lerle doğrulanabilir kimlik bilgileri blok zincir yerine kullanıcının cüzdanında saklanabilir.

En sık görülen dolandırıcılık yöntemlerinden sosyal mühendislik vakalarında kullanıcıların manipüle edilerek tamamen dolandırıcıların yönlendirmesi ile hareket etmesi, sahip olduğu bilgileri, parolaları, doğrulama bileşenlerini paylaşması, insan faktörünün her zaman önemli bir risk faktörü olarak ele alınması zorunluluğunu getirmektedir.

Bu açıdan, veri güvenliği anlamında dijital kimliği manipüle etmek zor olsa da, dataya erişim için kullanılan anahtar bilgisi için kullanıcının yeterli düzeyde bilinçli olmaması risk teşkil etmektedir. Kurumların hem çalışanları hem de müşterilerini bu yönde eğitmesi, güncel dolandırıcılık trendlerine yönelik düzenli olarak bilinçlendirme/bilgilendirme faaliyetleri yürütmesi standart ve sürekli hale getirilmelidir.

Sonuç olarak, gerek kurum çalışanlarının gerekse de müşterilerin kullanımına sunulan dijital kimlik doğrulama çözümlerinde, insan faktörü göz önüne alınarak, mevcut geleneksel kimlik doğrulama yöntemlerinden çok daha güvenli ve akıcı süreçler dizayn edilebilir. Bu tür yenilikçi yöntemlerin gelişmesi için, sektörlerin blokzincir dünyasını daha iyi anlamasını sağlayacak bilinçlendirme faaliyetlerinin yapılması, buna paralel yapılacak mevzuatsal değişikliklere kurumların hızlı uyum sağlaması önemli olacaktır.

5. YASAL UYUM VE DÜZENLEMELER

5.1. İhtiyaç Duyulan Hukuki Düzenlemeler ve Mevzuata Uyumun Sağlanması

Raporun bu kısmında amacımız, dijital kimlik sistemlerinin benimsenmesini desteklemek için gerekli düzenlemeleri ve kişisel verilerin korunması mevzuatlarına uyumun nasıl sağlanacağını incelemektir.

Türkiye'deki duruma geçmeden önce, karşılaştırmalı hukukta dijital kimlik ve mahremiyetin sağlanması ve uyumun geliştirilmesi konusunda atılan adımlara değinilmesinin yararlı olacağı kanaatindeyiz.

Uluslararası kurum ve kuruluşların da, dijital kimlik ve veri koruma alanında hukuki çerçevenin oluşturulması konusunda çeşitli çalışmalar yürüttüğü ve bu konunun önemine dikkat çektikleri bilinmektedir.

Dünya Ekonomik Forumu (World Economic Forum- WEF), dijital kimliklerin ekonomik ve sosyal etkilerini ele alan raporlar yayınlamakta ve bu alanda küresel iş birliğini teşvik etmektedir. Özellikle "Reimagining Digital ID Insight Report (June 2023)" başlıklı raporunda, merkezi olmayan kimlik (decentralized ID) sistemlerinin doğru bir şekilde uygulandığında gizlilik, kontrol, verimlilik ve etkinliği artırabileceğini belirtmektedir. Merkezi olmayan kimlik sistemlerinin hayata geçirilmesi için doğrulanabilir kimlik bilgileri, merkezi olmayan tanımlayıcılar, ilkeler ve yönetişim çerçeveleri gibi çeşitli teknolojiler, standartlar ve öneriler bulunduğu, ancak, bu yaklaşımın da birtakım riskler taşıdığı belirtilmektedir. Merkezi olmayan kimliklerin ölçeklendirilmesi için çabalar devam etse de, uygulamada birçok engel bulunduğuna dikkat çekilmektedir. Rapor, endüstri temsilcilerine teknolojik yeniliklerin geliştirilmesi, standartların uyumlaştırılması ve yetenek geliştirme çalışmalarına yatırım yapılması konularında tavsiyelerde bulunmaktadır. Ayrıca, kamu sektörüne yönelik olarak da destekleyici düzenlemelerin geliştirilmesi, işbirliklerinin teşvik edilmesi, birlikte çalışabilirlik ve taşınabilirlik gerekliliklerinin belirlenmesi yönünde öncelikler belirlenmiştir. Ancak, bu sistemlerin geniş ölçekte benimsenmesi için ortaklaşa kabul edilmiş teknolojiler, standartlar ve önerilerin eksikliği önemli bir sınırlama oluşturmaktadır. Destekleyici politika ve düzenlemelerin olmamasının, merkezi olmayan kimliklerin etkinliğini azaltabileceği ve ayrıca, yönetişim, iletişim ve işlevsellik gibi konularda da zorluklar çıkarabileceği belirtilmektedir.

OECD ve FATF tarafından, kara para aklama ve terörizmin finansmanıyla mücadele (AML/CFT) kapsamında düzenlemelere tabi olan kuruluşlar için güvenilir, bağımsız dijital kimlik sistemlerinin uygun ve risk temelli bir yaklaşımla kullanımına izin veren net kılavuzların veya düzenlemelerin geliştirilmesi önerilmektedir (Guidance on Digital Identity). Bu çerçevede, ilgili yargı alanında mevcut dijital kimlik sistemlerinin anlaşılması ve bu sistemlerin müşteri tanımlama ve doğrulama, sürekli durum tespiti, kayıt tutma ve üçüncü taraflara dayalı süreçlere ilişkin mevcut gereklilikler veya kılavuzlarla nasıl uyum sağladığının değerlendirilmesi bir başlangıç noktası olarak görülmektedir. OECD ve FATF tarafından ayrıca, müşteri durumu tespiti (CDD) amacıyla resmi kimliğin kanıtlanmasına yönelik gerekli nitelikler, kanıtlar ve süreçlerin belirlenmesinde ilkelere, performansa ve/veya sonuçlara dayalı kriterlerin benimsenmesi önerilmektedir. Dijital kimlik teknolojilerinin hızlı evrimi göz önünde bulundurulduğunda, bu yaklaşım hem sorumlu yenilikçiliği teşvik edecek hem de düzenleyici gerekliliklerin gelecekteki teknolojik gelişmelere uyumlu olmasını sağlayacaktır. Ayrıca, dijital kimlik sistemlerinin finansal kapsayıcılığı destekleme potansiyeli de vurgulanmaktadır. Dijital kimlik ile ilgili fırsat ve riskleri anlamak, bu riskleri azaltmaya yönelik düzenlemeler ve kılavuzlar geliştirmek amacıyla entegre ve çok paydaşlı bir yaklaşım benimsenmesi önerilmektedir. Bu kapsamda, kimlik, siber güvenlik/veri koruma ve gizlilikten sorumlu otoriteler tarafından benimsenen mevcut dijital kimlik doğrulama çerçevelerinin ve teknik standartların değerlendirilmesi ve uygun olduğu durumlarda bunlardan yararlanılması gerekmektedir. Bu süreçte, dijital kimlik sistemlerinin müşteri durumu tespiti (CDD) amacıyla güven seviyelerinin değerlendirilmesi için teknoloji, güvenlik, yönetişim ve kaynak yönetimi gibi hususlar göz önünde bulundurulmalıdır.

Ayrıca, dijital kimlik ekosistemindeki riskleri anlamak ve ele almak için ilgili otoriteler arasında iş birliği ve eş güdüm sağlanması gerektiği belirtilmektedir.

Bu yaklaşım, dijital kimlik sistemleri üzerindeki AML/CFT (kara para aklama ve terörizmin finansmanı) gerekliliklerinin veri koruma ve gizlilik kurallarıyla uyumunu güvence altına almak açısından kritik bir öneme sahiptir. Böylece, dijital kimliklerin hem güvenli hem de düzenleyici gerekliliklere uyumlu bir şekilde kullanımı desteklenebilir.

OECD'nin "Dijital Kimliğin Yönetişimine İlişkin Konsey Tavsiyesi" (Recommendation of the Council on the Governance of Digital Identity), dijital kimlik sistemlerinin güvenilir, kapsayıcı ve kullanıcı odaklı bir şekilde geliştirilmesi ve uygulanması için üye ülkelere kapsamlı bir çerçeve sunmaktadır. Bu tavsiye, bireylerin hak ve özgürlüklerini koruyarak dijital kimliklerin güvenli ve etkili bir şekilde kullanılmasını hedeflemektedir.

Dijital kimlik sistemlerinin oluşturulmasında güvenilirlik ve veri güvenliği en temel unsurlar olarak öne çıkmaktadır. Bu sistemlerin, kullanıcıların kimliklerini doğru şekilde doğrulayabilmesi ve kişisel verilerin güvenliğini sağlayabilmesi gerekmektedir. Aynı zamanda, dijital kimliklerin herkes tarafından erişilebilir olması, sistemlerin kapsayıcılığı açısından kritik önem taşımaktadır. OECD, dijital kimlik sistemlerinin kullanıcıların ihtiyaçlarına uygun olarak tasarlanmasını ve bireylerin kişisel verileri üzerinde kontrol sahibi olmasını önermektedir. Bunun yanı sıra, gizlilik ve veri koruma ilkelerine sıkı sıkıya bağlı kalınması gerektiği vurgulanmaktadır.

Dijital kimliklerin etkin ve güvenilir bir şekilde uygulanabilmesi için sağlam bir yasal ve düzenleyici çerçeveye ihtiyaç duyulduğuna dikkat çekilmektedir. Bu bağlamda OECD, üye ülkelerin dijital kimliklerin tanınması ve kullanımıyla ilgili mevcut kurallarını gözden geçirmelerini ve gerekli güncellemeleri yapmalarını önermektedir. Ayrıca, dijital kimlik sistemlerinin birlikte çalışabilirliğini ve güvenilirliğini artırmak için ulusal ve uluslararası standartların belirlenmesi gerektiği de ifade edilmektedir.

Etkin denetim ve uygulama mekanizmalarının geliştirilmesi, bu sistemlerin yasal çerçevelere uygunluğunu sağlamak açısından önemlidir. Ülkelerin mevcut yasal gerekliliklerini ve güven çerçevelerini değerlendirmeleri ve dijital kimlik sistemlerinin uyumunu sağlamaları önerilmektedir. Ayrıca, teknik standartların uyumlaştırılması, sistemlerin birlikte çalışabilirliğini artıracak önemli bir adımdır. Ülkeler arasında bilgi paylaşımı ve iş birliğinin artırılması, dijital kimlik ekosisteminin güçlendirilmesine katkı sağlayacaktır.

Belgede dijital kimlik ekosisteminin başarısının, kamu ve özel sektör arasındaki etkin iş birliğine de bağlı olduğu belirtilmektedir. OECD, kamu ve özel sektörün politika geliştirme, standart belirleme ve teknolojik yeniliklerin teşvik edilmesi gibi konularda ortak çalışmasını önermektedir. Özel sektörün inovasyon kapasitesi ile kamu sektörünün düzenleyici desteğinin birleşmesi, dijital kimlik çözümlerinin gelişimini hızlandırabilir. Ayrıca, kullanıcıların dijital kimlik sistemlerini etkin ve güvenli bir şekilde kullanabilmesi için eğitim ve farkındalık kampanyalarına ihtiyaç duyulmaktadır. Raporda vurgulanan diğer bir nokta, dijital kimlik sistemlerinin başarısının, kullanıcıların güvenine ve katılımına bağlı olduğudur. Kullanıcıların sisteme duyduğu güvenin artırılması için şeffaflık ve hesap verebilirlik sağlanmalı, kullanıcı geri bildirimleri dikkate alınarak sistemler sürekli iyileştirilmesi gerekmektedir. Bireylerin kişisel verilerinin güvenliği ve gizliliği konusunda garantiler verilmesi, sistemlere olan güveni artıracaktır.

The World Bank Group bünyesinde oluşturulan ID4D (Identity for Development) girişimi, dijital kimlik sistemlerinin Dönüşüm Potansiyelini desteklemek için küresel bilgi ve uzmanlığı kullanarak ülkelerin Sürdürülebilir Kalkınma Amaçlarını gerçekleştirmelerine yardımcı olmayı hedeflemektedir. Bu girişim, ülkelerdeki teşhis çalışmaları temelinde hükümet taleplerine yanıt

verir ve dijital kimlik sistemlerinin tasarımına yönelik küresel iyi uygulamalara dayalı teknik destek sağlamaktadır. Bu kapsamda, evrensel erişim, çok işlevli kullanım, birlikte çalışabilirlik, güçlü ve benzersiz yapılar gibi ilkelerin yanı sıra güven ve hesap verebilirliğe dayalı yasal ve operasyonel temeller geliştirilmesini teşvik etmektedir. Bu kapsamda, veri koruma ve gizlilik gereksinimlerini kapsayan sağlam bir yasal ve düzenleyici çerçeve oluşturulması noktasında hükümetlere destek sağlamaktadır.

Avrupa Birliği'nin 2024/1183 sayılı Tüzüğü, Avrupa Parlamentosu ve Konsey tarafından 11 Nisan 2024'te kabul edilmiş ve 21 Mayıs 2024'te yürürlüğe girmiştir. Bu tüzük, 910/2014 sayılı Tüzüğü (eIDAS) dijital kimlikler ve elektronik işlemlerle ilgili hükümler açısından değiştirmekte ve Avrupa Dijital Kimlik Çerçevesini oluşturmaktadır. 2021 yılında Avrupa Komisyonu, tüm AB vatandaşları, sakinleri ve işletmeleri için birlikte çalışabilir Avrupa dijital kimlik cüzdanları aracılığıyla erişilebilecek bir Avrupa dijital kimlik çerçevesi önerisinde bulunmuştu. 26 Mart 2024'te Avrupa Parlamentosu ve Konsey, bu öneriyi revize ederek kabul etmiştir. Yeni düzenlemeye göre, üye devletler 2026 sonu veya 2027 başına kadar vatandaşlar ve işletmeler için ulusal dijital kimliklerini diğer kişisel niteliklerle (örneğin sürücü belgesi, akademik yeterlilikler, banka hesap bilgileri) ilişkilendirebilecek dijital cüzdanlar sunmaları gerekmektedir.

Birleşik Krallık, dijital kimliklerin güvenli ve etkili kullanımını teşvik etmek amacıyla çeşitli hukuki düzenlemeler ve standartlar geliştirmiştir. Bu çerçevede, Dijital Kimlikler ve Nitelikler Ofisi (OfDIA), dijital kimlik hizmetlerinin güvenilirliğini sağlamak için standartlar belirlemektedir. Bu standartlar, bireylerin kimliklerini dijital ortamda güvenli bir şekilde doğrulamalarına olanak tanırken, mahremiyet ve kişisel verilerin korunmasını da gözetmektedir.

Hükümet ayrıca, dijital kimlik doğrulama hizmetlerine yasal bir temel oluşturmak amacıyla Veri (Kullanım ve Erişim) Yasa Tasarısı'nı Parlamento'ya sunmuştur. Bu tasarı, zorunlu bir dijital kimlik sistemi veya kimlik kartları gerekmeksizin dijital doğrulama hizmetlerinin yasal zeminini oluşturmayı hedeflemektedir.

Mahremiyet ve kişisel verilerin korunması alanında, Birleşik Krallık hükümeti Mart 2023'te Veri Koruma ve Dijital Bilgi (No. 2) Yasa Tasarısı'nı Avam Kamarası'na sunmuştur. Bu tasarı, yüksek veri koruma standartlarını korurken, kuruluşların üzerindeki yükleri azaltmayı ve veri koruma çerçevesini güncellemeyi amaçlamaktadır. Ayrıca, Bilgi Komiserliği Ofisi'nin (ICO) yapısında reformlar öngörmekte ve dijital kimliklerin güvenilir kullanımını sağlamak için bir çerçeve sunmaktadır.

Türkiye'de ise e-Devlet platformu üzerinden blokzincir tabanlı dijital kimlik uygulamalarının hayata geçirilmesi planlanmaktadır. Cumhurbaşkanlığından yapılan açıklamada, e-cüzdan uygulamasıyla vatandaşların blokzincir ağına entegre dijital kimliklerle e-Devlet'e giriş yapabileceklerini duyurmuştur. Bu adım, Türkiye'nin dijitalleşme sürecinde önemli bir dönüm noktası olarak görülmektedir.

5.1.1. Mevcut Yasal Çerçeve ve Düzenlemeler

Dijital kimlik ve belge dijitalleşmesi, kişisel verilerin korunması, güvenliğin sağlanması ve yasal uyumluluk açısından titizlikle ele alınması gereken bir alandır. Bu bağlamda, Türkiye'de ve uluslararası alanda geçerli olan düzenlemeler, bireylerin mahremiyetini koruma ve veri işleme süreçlerinde şeffaflık sağlama amacı taşır. Bu bölümde, KVKK, GDPR ve diğer ilgili düzenlemeler ışığında, dijital kimliğin mevcut yasal çerçevesi değerlendirilmektedir.

KVKK ve GDPR Kapsamında Kişisel Verilerin Korunmasına Yönelik Temel İlkeler

Hem Türkiye'de uygulanan KVKK hem de Avrupa Birliği'ndeki GDPR, kişisel verilerin işlenmesine yönelik temel ilkeleri belirlemiştir. Bu ilkeler, dijital kimlik ve dijital belgelerin yasal olarak korunmasını sağlamak için yol göstericidir. Temel ilkeler şu şekilde özetlenebilir:

- Hukuka ve dürüstlük kurallarına uygun işleme: Veriler, ilgili düzenlemelere uygun ve şeffaf bir şekilde işlenmelidir.
- Belirli, açık ve meşru amaçlar için işleme: Kişisel veriler, yalnızca belirli ve meşru bir amaç doğrultusunda toplanabilir.
- Veri minimizasyonu: İşlenen veriler, amaç için gerekli olanlarla sınırlı tutulmalıdır.
- Doğruluk ve güncellik: İşlenen veriler doğru olmalı ve gerektiğinde güncellenmelidir.
- Saklama süresiyle sınırlı işleme: Veriler, işleme amaçlarına uygun bir süre boyunca saklanmalı, bu süre sona erdiğinde ise silinmelidir.
- Gizlilik ve güvenlik: Veriler, yetkisiz erişime ve zarara karşı uygun güvenlik önlemleriyle korunmalıdır.

KVKK (Kişisel Verilerin Korunması Kanunu)

Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin işlenmesi ve korunması konularında temel hukuki çerçeveyi oluşturur. Kanunun öne çıkan yönleri şunlardır:

- Veri İşleme Şartları: KVKK, verilerin işlenmesi için açık rızayı veya kanunda belirtilen diğer işleme şartlarını zorunlu kılar.
- Veri Sahibi Hakları: Veri sahipleri, verilerinin işlenip işlenmediğini öğrenme, işlenme amacını sorgulama, düzeltilmesini veya silinmesini talep etme gibi haklara sahiptir.
- Veri Sorumlusunun Yükümlülükleri: Veri sorumluları, veri güvenliğini sağlamak, veri ihlallerini bildirmek ve VERBİS'e kayıt olmak gibi yükümlülükler taşır.

KVKK, özellikle bankacılık gibi dijital kimliğin kullanım alanlarının yoğun olduğu sektörlerde sıkı bir denetimi şart koşmaktadır. Kimlik doğrulama, müşteri bilgisi toplama ve bu bilgilerin saklanması süreçlerinde veri güvenliğine yönelik düzenlemeler oldukça detaylıdır.

GDPR (General Data Protection Regulation)

Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), küresel ölçekte dijital kimlik düzenlemelerinde standart oluşturmuş bir mevzuattır. Türkiye'de faaliyet gösteren ve AB vatandaşlarının verilerini işleyen kuruluşlar, GDPR'a uyum sağlamak zorundadır. Tüzüğün Türkiye üzerindeki etkileri şu başlıklarda öne çıkmaktadır:

GDPR, AB sınırlarının ötesine uzanan bir etki alanına sahiptir. Türkiye'deki dijital hizmet sağlayıcıları, AB vatandaşlarının verilerini işlediklerinde bu düzenlemelere uymak zorundadır. GDPR, açık rızayı net bir şekilde tanımlar ve veri işleme süreçlerinde şeffaflık şartı getirir. GDPR, uyumsuzluk durumlarında ciddi cezalar öngörmektedir. Bu, Türk şirketlerinin de GDPR'a uyum konusunda dikkatli olmasını gerektirmektedir.

Diğer İlgili Mevzuatlar

Dijital kimlik ve belge dijitalleşmesi, yalnızca KVKK ve GDPR kapsamında değil, aynı zamanda sektörlere özel düzenlemeler ışığında da değerlendirilmektedir. Özellikle bankacılık sektörü, dijital kimlik doğrulama ve veri işleme süreçlerinde sıkı düzenlemelere tabidir:

Uluslararası Standartlar: FATF (Mali Eylem Görev Gücü) gibi uluslararası kuruluşların belirlediği standartlar, kara para aklama ve terörizmin finansmanını önlemek için dijital kimlik doğrulama süreçlerine doğrudan etki eder.

Dijital kimlik alanında mevzuata uyum, bireylerin haklarını korumanın yanı sıra işletmelerin güvenilirliğini artıran ve cezai yaptırımlardan korunmalarını sağlayan kritik bir unsurdur. Bu nedenle, hem ulusal hem de uluslararası düzenlemelere uygun altyapıların geliştirilmesi önem taşımaktadır.

Bankacılık Düzenlemeleri: Bankacılık Düzenleme ve Denetleme Kurumu (BDDK), dijital kimlik doğrulama süreçleri ve müşteri bilgisi saklama konularında detaylı kurallar belirlemiştir. Elektronik kimlik doğrulama ve uzaktan müşteri edinimi gibi işlemler, bu düzenlemeler kapsamında değerlendirilmektedir.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik Kapsamında Dijital Kimlik

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, bankacılık sektöründe dijital kimlik doğrulama ve bilgi güvenliği süreçlerini düzenleyen temel mevzuatlardan biridir. Yönetmelik, müşteri bilgilerinin korunması, dijital işlemlerin güvenliği ve uzaktan kimlik doğrulama süreçlerinde uyulması gereken standartları belirler.

Bu yönetmelik, dijital kimlik doğrulama ve elektronik bankacılık hizmetlerine yönelik aşağıdaki önemli unsurları içermektedir:

Uzaktan Kimlik Doğrulama: Yönetmelik, uzaktan müşteri edinimi ve kimlik doğrulama süreçlerinde, güvenilir elektronik imza ve biyometrik kimlik doğrulama gibi teknolojilerin kullanılmasını öngörmektedir. Bu süreçlerde KVKK'ya uygun hareket edilmesi zorunludur.

Bilgi Güvenliği: Bankaların, müşterilere ait dijital kimlik ve diğer kişisel verileri korumak için bilgi güvenliği yönetim sistemlerini uygulaması gerekmektedir. Yönetmelik, bu sistemlerin düzenli olarak denetlenmesini ve güvenlik açıklarının zamanında giderilmesini şart koşmaktadır.

- Erişim Yetkilendirme: Dijital kimlik doğrulama süreçlerinde, yalnızca yetkilendirilmiş personelin müşteri bilgilerine erişebilmesi sağlanmalıdır. Yetkilendirme politikaları, verilerin gizliliği ve bütünlüğünü korumaya yönelik tasarlanır.

- Risk Yönetimi: Elektronik bankacılık hizmetlerinde dijital kimlik doğrulama ile ilişkili risklerin tespiti ve yönetimi, bankaların sorumluluğundadır. Yönetmelik, risklerin minimize edilmesi için düzenli sızma testleri ve bilgi güvenliği eğitimlerini zorunlu kılmaktadır.

- Veri İşleme ve Saklama: Yönetmelik, müşteri bilgilerini içeren dijital verilerin, yalnızca belirtilen süre boyunca saklanması gerektiğini ve bu sürenin sonunda verilerin silinmesini ya da anonim hale getirilmesini şart koşar. Bu gereklilik, KVKK ile paralellik taşımaktadır.

- Şeffaflık ve Bilgilendirme Yükümlülüğü: Bankaların, dijital kimlik doğrulama süreçlerinde müşterilerine açık ve anlaşılır bilgilendirme yapması zorunludur. Özellikle uzaktan kimlik doğrulama sırasında kullanılan teknolojiler ve verilerin hangi amaçlarla işleneceği konusunda bilgilendirme yapılmalıdır.

- Denetim ve Uyumluluk: Yönetmelik kapsamında bankalar, bilgi sistemleri ve dijital kimlik doğrulama süreçlerini BDDK tarafından belirlenen standartlara uygun şekilde yürütmekle yükümlüdür. Uyumsuzluk durumunda, idari yaptırımlar ve cezai sorumluluklar doğabilir.

Bu düzenlemeler, bankacılık sektöründe dijital kimlik doğrulama işlemlerinin güvenliğini artırırken, müşteri bilgilerinin gizliliğini sağlama ve yasal uyumluluğu temin etme açısından kritik rol oynamaktadır.

5.1.2. Dijital Kimliğin Hukuki Çerçevesiyle İlgili Gelişmeler

Dijital Kimlik Hukuki Tanımları ve Standartları

Elektronik hizmetlerin güvenli bir ortamda sunulmasını amaçlayan 2014/910 sayılı Elektronik Kimlik Belirleme ve Güven Hizmetleri Tüzüğü'nü (eiDas) güncelleyen Avrupa Birliği'nin yeni düzenlemesi Avrupa Dijital Kimlik Tüzüğü'nde dijital kimlik "bir gerçek veya tüzel kişiyi ya da başka bir gerçek veya tüzel kişiyi temsil eden bir gerçek kişiyi benzersiz bir şekilde temsil eden elektronik formdaki kişi kimlik verilerini kullanma süreci" olarak tanımlanmıştır.

Dijital kimliklerin güvenli, verimli ve uyumlu bir şekilde kullanılabilmesi için belirlenen teknik ve hukuki kurallar, standardizasyondur. Dijital kimliklerin yani kişilerin kimliklerini doğrulamak amacıyla kullanılan dijital araçların, farklı platformlarda, hizmetlerde ve ülkelerde tutarlı ve sistematik bir şekilde çalışabilmesi için belirli standartların oluşturulması gerekmektedir. Standartlar, dijital kimliklerin güvenliğini, gizliliğini, birlikte çalışabilirliğini ve kullanım kolaylığını sağlamaya yöneliktir.

Dijital Kimlik Standardizasyonunun Önemi

- Güvenlik: Dijital kimliklerin korunması, kimlik hırsızlığını ve dolandırıcılığı önlemek için kritik önem taşır. Standartlar, güçlü şifreleme, biyometrik verilerin korunması gibi güvenlik önlemlerini belirler.
- Uyum: Dijital kimlikler farklı hizmet sağlayıcıları ve devlet sistemleri arasında tutarlı bir şekilde kullanılabilmelidir. Standartlar, kimliklerin birden fazla platformda uyumlu çalışmasını sağlar.
- Erişilebilirlik: Kullanıcılar dijital kimliklerini kolayca ve güvenli bir şekilde yönetebilmelidir. Standartlar, dijital kimliklerin herkes için erişilebilir olmasını sağlar.
- Veri Koruma ve Gizlilik: Dijital kimliklerin içereceği kişisel verilerin güvenliği önemlidir. Standartlar, veri minimizasyonu ve kullanıcıların verilerini kontrol etme haklarını sağlamaya yönelik kurallar içerir.

Avrupa'da Dijital Kimlik Standardizasyonu

Avrupa Birliği, dijital kimliklerin standardizasyonu konusunda önemli adımlar atmıştır. Avrupa Dijital Kimlik Yönetmeliği (EU Digital Identity Regulation) ve eIDAS (electronic IDentification, Authentication and trust Services) gibi düzenlemeler, dijital kimliklerin ortak bir çerçevede kullanılmasını sağlamaktadır.

eIDAS Yönetmeliği (2014/910/AB)

eIDAS, Avrupa'da dijital kimliklerin ve dijital imza hizmetlerinin standartlaşmasını sağlayan bir düzenlemedir ve üye ülkelerin dijital kimliklerini birbirleriyle uyumlu hale getirmelerini sağlar. Bu sayede, bir ülkede oluşturulmuş dijital kimlikler başka bir AB ülkesinde de geçerli olabilir. Kimlik doğrulama ve dijital imza gibi güvenlik önlemlerini standardize eder. Elektronik belgelerin yasal geçerliliğini sağlar ve dijital imzaların uluslararası geçerliliğini garanti eder.

Avrupa Dijital Kimlik Tüzüğü (2024):

Avrupa Dijital Kimlik Yönetmeliği, AB genelinde tek bir dijital kimlik standardı oluşturmayı hedeflemektedir. Bu düzenleme, üye devlet vatandaşlarının dijital kimliklerini kendilerinin, güvenli bir şekilde yönetebilmesini amaçlamaktadır. Ayrıca, dijital kimliklerin devlet ve özel sektör hizmetlerinde kullanılabilmesine imkan sağlamaktadır. Dijital kimlik, kullanıcılara sadece kimliklerini doğrulama imkânı sağlamakla kalmaz, aynı zamanda kişisel verilerin kontrolünü de sağlar. Kullanıcılar dijital kimliklerini yalnızca gerektiğinde paylaşarak gizliliklerini koruyabilirler.

Yeni düzenlemeler, 910/2014 sayılı Tüzük kapsamındaki mevcut uygulama kurallarını değiştirecek veya yerine yenilerini koyacak uygulama mevzuatlarının hazırlanmasını öngörmektedir. Revize edilen tüzüğün kabul edilmesinden itibaren 12 aylık bir süre içinde bu uygulama mevzuatlarının geliştirilmesi planlanmaktadır.

Yeni düzenleme, dijital kimlik sistemlerinin güvenli, kullanıcı dostu ve birlikte çalışabilir bir şekilde işleyişini sağlamayı amaçlamaktadır. Avrupa dijital kimlik cüzdanları, kullanıcıların yalnızca kimlik bilgilerini değil, aynı zamanda belirli hizmetlere erişim için gerekli diğer kişisel nitelikleri güvenli bir şekilde yönetmelerini ve paylaşmalarını mümkün kılacaktır. Bu, hem bireysel kullanıcılar hem de işletmeler için işlemleri kolaylaştırarak dijital dönüşümü hızlandırmayı hedeflemektedir.

E-İmza ve E-Mühür Düzenlemeleri

Elektronik imza ve mühürlerin yasal geçerliliği ve kullanılabilirliği ile ilgili düzenlemelerin gözden geçirilmesi de önem taşımaktadır.

E-imza (elektronik imza) ve e-mühür (elektronik mühür), dijital ortamda kimlik doğrulama ve belgelerin güvenliğini sağlamak için kullanılan iki farklı teknolojidir. Her iki kavram da her ne kadar farklı teknolojilere sahip olsa da, dijital işlemlerde, belgelerin doğruluğunu, bütünlüğünü ve güvenliğini garanti altına almak amacıyla kullanılır.

E-imza

E-imza, basit bir ifade ile bir kişinin dijital ortamda yaptığı işlemleri yasal olarak bağlayıcı hale getiren bir güvenlik aracıdır. Elektronik imza, el yazısıyla atılan imzaya benzer şekilde, bir dijital dosyanın üzerinde imza atma işlevi görür. Bu imza, özellikle dijital belgelerin yasal geçerliliğini sağlamak için kullanılır. Elektronik İmza Kanunu'nda ise elektronik imza "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmaktadır.

E-imza, imzalayan kişinin kimliğini doğrulamak için kullanılır. Bu sayede, belgeyi imzalayan kişinin gerçekten o kişi olup olmadığı belirlenebilir. E-imza, imzalanan belgelerin sonradan değişmediğini garanti eder. Belgeye müdahale edilmesi durumunda imza geçersiz olur.

Hem ülkemizde hem Avrupa Birliği'nde elektronik imza, el yazısıyla atılan imza ile aynı yasal geçerliliğe sahiptir. Ülkemizde 5070 sayılı Elektronik İmza Kanunu, e-imzayı hem tanımlamakta ve düzenlemekte hem geçerliliğini yasal olarak tanımaktadır.

Türkiye'de ıslak imza ile aynı yasal geçerliliğe sahip olan elektronik imza; e-fatura, e-reçete ve elektronik yazışma paketi gibi çeşitli alanlarda yaygım olarak kullanılmaktadır. Ayrıca belirtmek gerekir ki, Türkiye'de sürdürülen dijital dönüşüm çalışmalarına paralel olarak elektronik imzanın önemi giderek artmaktadır.

Bu kapsamda elektronik imza oluşturulmasında kullanılan standartların da oldukça önem kazandığına dikkat çekmek gerekmektedir.

Bu konuda önem arz eden noktalardan biri, Avrupa Birliği'ndeki ilgili elektronik imza standartlarının takip edilmesi ve yapılan güncellemelerin analiz edilerek Türkiye'de elektronik imza mevzuatına kazandırılması önemlidir. 1999/93/EC sayılı Elektronik İmza Direktifine uygun olarak Türkiye'de benimsenen elektronik imza standartları, Avrupa Birliği içerisinde zamanla eIDAS düzenlemeleriyle güncellenmiş ve uygulanmaya başlamıştır. Bununla birlikte Türkiye'de henüz eIDAS'ın getirdiği güncel standartlara uyum bulunmamaktadır. Avrupa Birliği ile Türkiye arasındaki dijital ticaretin ve iletişimin güvenliği ve etkinliğini sağlamak adına elektronik imza ve güven hizmetleri kapsamında Avrupa Birliği ve Türkiye arasındaki ortak altyapının sağlanması önemli bir ihtiyaç olduğu belirtilmektedir.

E-mühür (Elektronik Mühür)

E-mühür, genellikle tüzel kişilikler tarafından kullanılan bir dijital güvenlik aracıdır. E-mühür, bir kurumun veya kuruluşun dijital ortamda yaptığı işlemlerin güvenliğini ve geçerliliğini sağlamak için kullanılır. E-mühür, genellikle bir şirketin ya da devlet kurumunun dijital belgelerinin imzalanmasında kullanılır. E-mühür, Elektronik İmza Kanunu'nda, Elektronik Mühre İlişkin Usul ve Esaslar Hakkında Yönetmelik'te ve Kamu Kurum Ve Kuruluşlari Arasinda Elektronik Ortamdaki Belge Paylaşiminda Kullanilan Kurumsal Şifreleme ve Elektronik Mühür Sertifikalarina İlişkin Usul Ve Esaslar'da ise "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve elektronik mühür sahibinin bilgilerini doğrulama amacıyla kullanılan elektronik veri" olarak tanımlanmıştır.

E-mühür, bireylerden ziyade tüzel kişilikler için tasarlanmış bir güvenlik aracıdır. Şirketler veya kamu kurumları, e-mühür ile dijital belgeleri imzalayarak, işlemlerinin geçerliliğini ve güvenliğini sağlar.

Elektronik mühür, elektronik belgenin veya verinin mühür sahibi tarafından oluşturulduğunu, belgenin veya verinin kaynağını ve bütünlüğünü garanti eden delil kaydıdır. Elektronik mühür, resmî mühür dâhil her türlü fiziki mühür ile aynı hukuki niteliği haizdir.

E-imza, bireylerin kimlik doğrulamasını sağlarken, e-mühür, bir kuruluşun veya kurumun dijital kimliğini doğrular. Yani, e-imza bireysel işlemler için, e-mühür ise kurumsal işlemler için kullanılır.

Dijital Kimlik Teknolojisinin Benimsenmesi İçin Gereken Düzenlemeler

Ülkemizde, henüz dijital kimliğe ilişkin özel bir düzenleme bulunmuyor olsa da dijital kimliğe ilişkin temeller 23 Temmuz 2004 tarihinde yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu ("E-İmza Kanunu") ile atılmıştır. E-İmza Kanunu aynı zamanda güvenli elektronik imza ile elektronik imza arasındaki ayrıma ve zaman damgası, elektronik veri, elektronik sertifika gibi kavramların tanımları ile düzenlemelerine de yer vermektedir. E-İmza Kanunu'nun akabinde mobil elektronik imza konusunun da hukuki alt yapısı Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile oluşturulmuştur.

Türkiye'deki elektronik imza sistemlerinin güncel teknolojilere ve standartlara ve AB'deki duruma uyum sağlaması için geliştirilen bazı önerileri şu şekilde sıralayabiliriz:

- Türkiye'de yürürlükte olan elektronik imza mevzuatı ve ikincil düzenlemelerin güncel standartları referans alacak şekilde düzenlenmesi,

- Elektronik imza yazılım kütüphanesi (API) sağlayan geliştiricilerin, güncel standartlara uyum sağlamak adına yazılım güncellemelerini sağlamaları gerekmektedir.

Eski (mevcut) standartlarla oluşturulan imzalı dosyaların, güncel standartlara uygun oluşturulan dosyalarla birlikte çalışabilirliğinin sağlanması önem arz etmektedir. Böylece geçmişte oluşturulan veriler ve dosyalar güncel teknolojilerle uyumlu hâle gelecektir. Bu sayede elektronik imza teknolojilerinin daha geniş bir kullanım ve kabul görmesine olanak tanıyacaktır.

Ülkemizde dijital kimlik sistemine uygulanabilecek genel ve kimlik özelinde yasal düzenlemeler arasında 4721 sayılı Türk Medeni Kanunu, 5490 sayılı Nüfus Hizmetleri Kanunu, 5682 sayılı Pasaport Kanunu, 5901 sayılı Türk Vatandaşlığı Kanunu bulunmaktadır.

Bu düzenlemelerin yanı sıra, bir kimlik sisteminin çerçevesini oluşturan önemli bir dayanak noktası kişisel verilerin korunması ve gizliliğidir. Ülkemizde kişisel verilerin korunması 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemeleri kapsamında düzenlenmektedir.

Elbette bunun dışında gelişen teknoloji ve kişilerin alışkanlığının değişmesi ile birlikte gerek bankacılık gerek her türlü finansal işlemlerin dijital kimlik, akıllı sözleşme ya da daha genel tabir ile dijitalleşerek verilebilmesi için de yasal zeminin oluşturulması önem arz etmekte, düzenleyici kurumların mevzuat çalışmaları devam etmektedir.

Bununla birlikte, bugüne kadar yapılan mevzuat değişikliklerinin tam olarak uygulanabilmesini ve beklenen faydanın sağlanabilmesini teminen aşağıda yer alan mevzuat değişikliklerinin de yapılmasının önem taşımaktadır.

- 5070 Sayılı Elektronik İmza Kanunu
- 6100 Sayılı Hukuk Muhakemeleri Kanunu
- 6098 Sayılı Türk Borçlar Kanunu
- 6102 Sayılı Türk Ticaret Kanunu
- 4721 Sayılı Türk Medeni Kanunu
- 2004 Sayılı İcra ve İflas Kanunu
- 6750 Sayılı Ticari İşlemlerde Taşınır Rehni Kanunu
- Konut Hesabı ve Devlet Katkısına Dair Yönetmelik
- Çeyiz Hesabı ve Devlet Katkısına Dair Yönetmelik
- 5941 Sayılı Çek Kanunu
- Finansal Hizmetlere İlişkin Mesafeli Sözleşmeler Yönetmeliği
- Konut Finansmanı Sözleşmeleri Yönetmeliği

6. FİNANS SEKTÖRÜNE ETKİLERİ VE KULLANIM ALANLARI

6.1. Finans Alanında Ulusal Blokzincir Altyapıları ve Dijital Kimliğin Etkileri

Müşteri Kabulü, KYC Süreçleri ve CBDC Sistemlerinde Kullanımı

KYC (Know Your Customer – Müşterini Tanı), bankalar, sigorta şirketleri, fintech vb. finansal kurumların suç gelirlerinin aklanması ve terörizmin finansmanı gibi yasadışı faaliyetlerin engellenmesi ve müşterilerin finansal durumları, gelir kaynakları ve risk profilleri hakkında bilgi sahibi olmalarını sağlayan bir süreçtir. Geleneksel finansta KYC süreçleri insan ve sistemlerin birlikte dahil olduğu şekilde ilerlemektedir. Aynı zamanda KYC, finansal kurumlar için müşterilerinin kimliklerinin doğrulanmasında hayati bir rol oynamaktadır.

Her bankanın kendine özgü KYC süreci vardır ve müşterilerden her banka aynı bilgi ve belgeleri ayrı ayrı sunmaları ister. Bu da KYC süreçlerini günümüzde hem kurum hem de müşteri açısından maliyetli, zaman alan, verimsiz süreçler haline getirmektedir. Ayrıca müşteri verilerinin merkezi veri tabanlarında saklanıyor olması siber saldırılara hedef haline gelmektedir.

Blokzincir teknolojisi KYC süreçlerinde ve dijital ID kullanımında devrim yaratacak bir yeniliktir.

Bu teknoloji yalnızca kimlik doğrulama ve KYC süreçlerini yeniden tanımlamayı değil, aynı zamanda dijital çağda bankacılığın geleceğini şekillendirmeyi de vaat etmektedir. Blokzincir alt yapısı kullanılarak dijital kimlik doğrulama yapılmasının da bir çok faydası ortaya çıkmaktadır.

Şeffaflık: Blockzincir kullanılarak KYC verileri değişmez bir şekilde saklanabilir ve yetkilendirilmiş kişi ve kuruluşlar tarafından erişilebilir, doğrulanabilir şeffaf bir sistem sağlar.

Güvenlik: Blokzincirin merkezi olmayan yapısı, işlemlerin ağda birden fazla kaydının tutulmasını sağlayarak değişiklikleri, sahteciliği ve siber güvenlik risklerini neredeyse imkansız hale getirir.

Dijitalleşme: Kullanıcıların kimlik verilerine elektronik olarak erişmelerini sağlayarak süreçleri hızlandırır ve bankacılık hizmetlerinde kesintiye uğramadan pürüzsüz bir şekilde ilerlemesini sağlar. Mevcut teknolojiler ile mesafeli olarak sözleşme ilişkisi kurulması risk içeren belgelerin dijital ortamda imzalanması mümkün olmaktadır. Dijital kimlik, finansal kuruluşların şube ve acentelerine fiziksel ziyaret ihtiyacını ortadan kaldırır, bekleme sürelerini azaltır ve anında doğrulama sağlayarak kullanıcı dostu bir deneyim sunar.

Kimlik Verilerinin Kontrolü ve Müşteri Rızası: Mevkut kimlik sistemlerinin merkezi doğası, veri sahipliği, kontrolü paylaşımı hakkında sorunlar müşterilerin kişisel bilgilerinin önemi ve değeri konusunda daha fazla bilinçlenmesiyle, gizlilik endişeleri arttırmaktadır. Dijital kimlik, merkeziyetsiz ve kullanıcı kontrollü yapısıyla müşterilere kişisel bilgileri üzerinde kontrol sağlama, paylaşacakları verileri seçebilme ve rıza paylaşma olanağı sağlamaktadır.

Erişim, Kullanabilirlik ve Birlikte Çalışılabilirlik: Dijital kimlik doğrulama sayesinde müşteriler verileri üzerinde daha fazla kontrol sahibi olduğunda finansal kurumların müşterilerin bireysel ihtiyaç ve tercihlerine göre uygun özel ürünler ve hizmetler sunmaktadır. Birlikte çalışabilirlik standartlarının ortaya konmasıyla finansal kurumlar hizmetlerini küresel anlamda genişletebilmekte ve fiziksel varlığa ihtiyaç duymadan dünya çapında müşterileri bünyelerine katıp kapsayıcılıklarını arttırmaktadırlar.

6.2. Dijitalleşecek Belgeler ve Blokzincir Dünyasına Etkileri

Finans Dünyasında Mesafeli Sözleşme Kurulması ve Blokzincir Teknolojisinin Yaratacağı Avantajlar

Blockchain teknolojisi geleneksel sözleşmelerin güvenilirliğini ve şeffaflığını artırarak dijital dünyada yeni bir çağ açtı. Akıllı sözleşmeler olarak adlandırılan bu dijital anlaşmalar, belirli koşullar yerine getirildiğinde otomatik olarak yürütülebilen kod parçacıklarından oluşuyor.

Kurum ve kuruluşların müşterilerine sunduğu mesafeli hizmetlerde sözleşme ilişkisinin de mesafeli olarak kurulabilmesi hizmetlerin kesintisiz bir şekilde verilebilmesi ve sürdürülebilirlik açısından kritik önem taşıyor. Sözleşmelerin mesafeli olarak kurulabilmesi noktasında düzenleyici kurumların kurum ve müşteri arasında oluşabilecek uyuşmazlıkların önüne geçmek amacıyla üzerinde durduğu en önemli kriterler kimlik doğrulama ve işlem güvenliğidir.

Bankacılıkta mesafeli sözleşme kurulması bankalar ile müşteri arasındaki ürün başvuru ve kullandırımları esnasında zaman ve mekan kısıtlaması olmadan iletişim araçları üzerinden gerçekleşmektedir. Son yıllarda artan işlem hızı, dijitalleşme trendi ve içerdiği finansal riskler nedeniyle bankacılık en çok regülasyona tabi tutulan sektörlerin başında geliyor. Müşteriye sunulan ürün ve hizmetler karşılığında sözleşmelerin mesafeli olarak kurulabilmesi ilk olarak 31 Ocak 2015 yılında Gümrük ve Ticaret Bakanlığı tarafından yayımlanan Finansal Hizmetlere İlişkin Mesafeli Sözleşmeler Yönetmeliği ile düzenlenmiş oldu.

Bu yönetmelik sonrasında bankacılık işlemleri dijitalleşmeye başladı. Özellikle pandemi döneminde uzaktan hizmet modellerinin ön plana çıkmaya başlaması ile dijitalleşme trendi çok daha büyük bir ivme kazandı.

Bankacılık Düzenleme ve Denetleme Kurulu; 15/03/2020 tarihli ve 31069 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmeliği ve 27/03/2023 tarihli Elektronik Bankacılık Hizmetlerinde ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasında Kimlik Doğrulama ve İşlem Güvenliği için Sağlanması Gereken Kriterler Hk. Genelgesi ile elektronik bankacılık hizmet kanallarında kimlik doğrulama ve işlem güvenliğinin nasıl gerçekleştirilmesi gerektiği ve bu kanallar üzerinden gerçekleştirilecek işlemlerde hem banka hem de müşteriler için inkâr edilemezliği ve sorumluluk atamayı mümkün kılacak teknikler kullanılması gerektiğini düzenlemiştir.

Diğer taraftan, ilk defa 01/04/2021 tarihli ve 31441 sayılı Resmi Gazete'de yayımlanan Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmeliği ile gerçek kişi müşteriler ve banka arasında kurulacak ve yazılı şeklin yerine geçecek nitelikte mesafeli sözleşme ilişkisi kurulabilmesi için gereken kriterleri belirlemiştir. 25/05/2023 tarihli 32201 sayılı Resmi Gazete'de yayımlanan güncelleme ile aynı yönetmeliğin kapsamı genişletilerek; gerçek kişilere ilave olarak tüzel müşteriler ile mesafeli sözleşme kurulabilmesine yönelik kriterler belirlenmiştir.

BDDK tarafından yürürlüğe konan düzenlemeler sayesinde uzaktan hesap açılışı ve birçok bankacılık ürününe ilişkin sözleşme ilişkisinin mesafeli olarak kurulabilmesi mümkün hale gelmiştir. Ancak burada bankaların uzaktan sunduğu ürün ve hizmetlerin kapsamını genişletebilmesi için çözüm bekleyen bazı yasal düzenlemeler bulunuyor. Çeşitli kanun maddelerinde "yazılı şekle tabi" olarak kurulması gereken sözleşmeler, halen daha mesafeli olarak kurulamıyor. BDDK'nın yönetmelik ile düzenlemiş olduğu kriterler yazılı şekle tabi olmayan sözleşmelerin kurulabilmesi için hukuki bir dayanak oluştururken, aşağıda belirtilen sözleşme tiplerinde kanun maddelerinden dolayı bankalara hukuki anlamda bir güvence teşkil edemiyor.

Blokzincir, dağıtık bir ağ üzerinde sakladığı verilerin değiştirilemezliğini, güvenilirliğini ve şeffaflığını garanti etmesi bakımından finans dünyasının yaşadığı bu problemi kökünden çözebilecek fırsatlar sunabilir. Özellikle dijital kimlik yönetimi alanında blockchain teknolojisinin kullanımı işlem güvenliği ve kimlik doğrulama süreçlerinde tüm sektöre büyük avantajlar sağlayabilir. Bu nedenle, belgelerin blockchain teknolojisi ile dijitalleştirilmesi, gelecekte daha güvenli ve etkili belge yönetim sistemlerinin oluşturulmasına, uzaktan yapılan işlemlerin artmasına, kağıt ve zaman tasarrufu sağlayarak sürdürülebilirliğe katkı sunmasına olanak tanıyacaktır.

Sözleşme Adı	İlgili Kanun/Yönetmelik	Yasal Alınma Şekli	Kullanıldığı Ürünler
Cari Hesap Hükümleri	• 6102 Sayılı Türk Ticaret Kanunu	Yazılı Şekle Tabi	• Esnek Ticari Hesap • Borçlu Cari Hesap
Temlik Sözleşmesi	• 6098 Sayılı Türk Borçlar Kanunu	Yazılı Şekle Tabi	• Temlik Teminatlı Kredi
Çek Karnesi Beyannamesi	• 5941 Sayılı Çek Kanunu	Yazılı Şekle Tabi	• Çek Karnesi
Alacak ve Haklar Üzerine Rehin Sözleşmesi	• 4721 Sayılı Türk Medeni Kanunu	Yazılı Şekle Tabi	• Vadeli ve Vadesiz Mevduat Rehni • Hisse Senedi ve Menkul Kıymet Rehni • Motorlu Araç Rehni
Kefalet Sözleşmesi	• 6098 Sayılı Türk Borçlar Kanunu	Resmi Şekle Tabi	• Ticari Kredi (GKTS)
Ticari İşletmelerde Taşınır Rehni Sözleşmesi	• 6750 Ticari İşletmelerde Taşınır Rehni Kanunu	Resmi Şekle Tabi	• Ticari Taşıt Rehni
İpotek Sözleşmesi	• 4721 Sayılı Türk Medeni Kanunu	Resmi Şekle Tabi	• İpotekli Ticari Söz
Konut Finansmanı Sözleşmesi	• 6502 Sayılı Tüketicinin Korunması Hakkında Kanun - 31 Ekim 2024'te güncellendi. • Konut Finansmanı Sözleşmeleri Yönetmeliği – 31 Aralık 2024'te güncellendi. • 2644 Sayılı Tapu Kanunu	Resmi Şekle Tabi	• Konut Kredisi

6.3. Yeni Hizmetler ve Operasyonel Verimlilik

Dünya çapında dijital kimlikler, her türden kuruluş - özel şirketler, hükümet organları, sivil toplum kuruluşları ve bunların hizmet verdiği insanlar ve kuruluşlar için giderek daha vazgeçilmez hale gelmektedir. Dijital teknoloji kullanımının artması ve yapay zekanın gelişimi, dijital kimliğin oluşturulmasını daha da önemli hale getiriyor. Gelecek dönemde dijital kimlik çalışmalarının yaygınlaşması ile birçok sektör ve iş kolu köklü bir değişime uğraması beklenmektedir. Bu yeni teknolojiler değişime öncülük ederken, yeni hizmet ve servisleri de beraberinde getirmekte ve hali hazırdaki sistemlerde operasyonel verimliliği artırmaktadır.

Bu kimlik özelinde gelecek dönemde ortaya çıkması beklenen yeni hizmet alanları ve operasyonel verimlilik süreçlerini 6 kategoride sınıflandırabiliriz. Bunlar;

- Dijital Kimlik Doğrulama Platformları
- Biyometrik Kimlik Doğrulama Sistemleri
- Kimlik ve Erişim Yönetimi (Identity and Access Management, IAM) Gelişmeleri
- Otomatik Kredi Değerlendirme ve Risk Yönetimi
- Dış Ticaret Alanı ve Dijital Varlık Yönetimi
- Güvenli Erişim Çözümleri

6.3.1. Dijital Kimlik Yaratma ve Doğrulama Platformları

Dijital kimlik teknolojisinin gelişmesi ile dijital kimliklerin doğrulanması ve bu hizmetin mikro işlem düzeyinde ölçeklenebilmesi, teknolojinin yaygınlaşmasındaki önemli basamaklardan birisini oluşturmaktadır. Bu doğrultuda, dijital kimlik sistemleri, üç ana rolü birbirine bağlayan bir güven üçgeni oluşturur: vericiler, sahipler ve doğrulayıcılar.

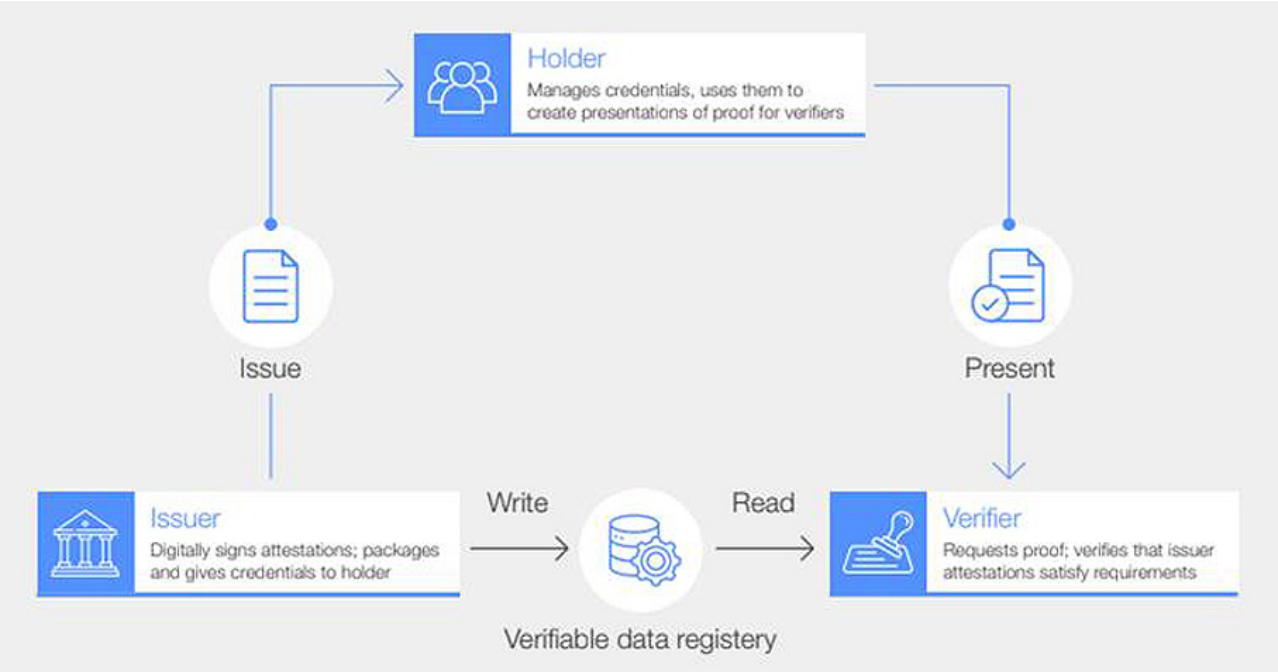
Dijital Kimlik Yaratıcıları, dijital olarak onaylanmış belgeleri oluşturan ve bunları sahiplerine sağlayan kurum ya da kuruluşlardır. Kimlik bilgilerini oluşturma ve doğrulama sorumluluğuna sahiptirler.

Dijital Kimlik Sahipleri, bireyler gibi, kendi kimlik bilgilerini yönetir ve bunları verilerinin veya kimliğinin doğruluğunu kanıtlamak için kullanır. Bilgilerinin nasıl ve kiminle paylaşıldığı üzerinde kontrol sahibi olurlar.

Doğrulayıcılar, bu belgeleri değerlendirerek belirli gereklilikleri karşılayıp karşılamadığını belirlerler. Sahipler tarafından sunulan kimlik bilgilerin geçerliliğini kontrol ederler.

Bu sistem, bireylerin kimliklerini yönetmelerine olanak tanırken, kriptografik doğrulama yoluyla süreçteki güveni artırarak gizliliği ve güvenliği geliştirmektedir.

Bu kapsamda ilk olarak dijital kimlik yaratma platformları yeni bir hizmet ve servis türü olarak karşımıza çıkmaktadır. Dijital kimlik yaratma adımlarında yasal otoritelerinde sürece dâhil olması ve dijital kimlik içerisinde yer alacak olan verilerin kaynağı olarak yer alması gerekmektedir. Dijital kimlik yaratma sürecine paralel olarak dijital kimlik doğrulama platformları da yeni bir hizmet ve servis türü olarak ortaya çıkması beklenmektedir.



Şekil 1 Doğrulanabilir Kimlik Bilgisi Güven Üçgeni (WEF, 2023)

Dijital kimlik doğrulama platformları ile kullanıcılar, kimlik doğrulama ihtiyacı olan süreçlerinde tek seferlik kimlik doğrulama, çok faktörlü kimlik doğrulama gibi metotları kullanarak, kendilerini kolayca doğrulayabilirler. Bu süreçte kimliğin yaratılması ile zincir üzerine doğrulayıcı olacak olan kurum/kuruluşlar için ilgili verinin okunması hizmeti, bilgi talep eden şirketlere sağlanabilir.

Örneğin; bir vatandaş herhangi bir finansal kuruluşun hesap açma adımlarındaki kimlik doğrulama sürecinde cüzdan uygulaması ile sakladığı dijital kimliğin içerisinde yer alan hesap açılışı için gerekli olan bilgileri, cüzdan uygulamasından onay vererek finansal kuruluşa hızlı ve kolay bir şekilde hesap açılışı gerçekleştirebilir.

Yapay zekâ alanındaki gelişmeler, dijital kimliğin önemini de da artırmıştır. Yapay zekânın görsel işleme teknolojisinin gelişmesi ile kimlik doğrulama mekanizmalarını aşma potansiyeli de paralel olarak gelişmiştir. Bu doğrultuda KYC süreçlerinde kullanıcının gerçek bir insan olduğunu doğruladığı ve gerekli bilgi/belgeleri yönetebildiği dijital kimlik sistemlerinin önemi giderek artmaktadır.

6.3.2. Kimlik Erişimi ve Yönetimi (Identity and Access Management, IAM) Gelişmeleri

Dijital kimliklerin yaygınlaşması ile kimlik erişimi ve yönetimi yeni bir hizmet ve servis olarak ortaya çıkması beklenmektedir. Kimlik erişimi ve yönetiminin uygulanma metotları ve bu alanda geliştirilmekte olan teknolojiler bu fonksiyon setinin yeni bir hizmet ve servis biçimi olarak ön plana çıkmasını sağlamaktadır.

Bulut Tabanlı IAM Çözümleri

Son yıllarda bulut teknolojilerinin yaygınlaşmasıyla birlikte bulut tabanlı IAM çözümleri öne çıkmaya başladı.

Geleneksel IAM sistemleri genellikle yerel sunuculara dayanırken, bulut tabanlı sistemler, esneklik ve ölçeklenebilirlik sunarak işletmelere maliyet tasarrufu sağlar. Bu sistemler, kullanıcıların herhangi bir yerden güvenli bir şekilde erişim sağlamasına olanak tanırken, organizasyonların kimlik ve erişim yönetimini merkezi bir platformda toplamasına yardımcı olur.

Çok Faktörlü Kimlik Doğrulama (MFA)

Gelişen siber tehditler karşısında, çok faktörlü kimlik doğrulama (MFA) giderek daha fazla önem kazandı. MFA, kullanıcıların kimliklerini doğrulamak için birden fazla kanıt sunmalarını gerektirir. Bu, yalnızca şifreye dayanarak güvenlik sağlamaktan çok daha güvenli bir yöntemdir. Örneğin, bir kullanıcı şifresini girdikten sonra, cep telefonuna gönderilen bir kodu da girmesi gerekebilir. Bu, kötü niyetli kişilerin hesaplara erişimini büyük ölçüde zorlaştırır.

Yapay Zeka ve Makine Öğrenimi

Yapay zeka (AI) ve makine öğrenimi (ML) teknolojileri, IAM süreçlerini daha etkili hale getirmekte önemli bir rol oynamaktadır. Bu teknolojiler, kullanıcı davranışlarını analiz ederek olağan dışı aktiviteleri tespit edebilir. Örneğin, bir kullanıcının alışılmadık bir saat veya yerden giriş yapması durumunda, sistem anormal bir durum olduğunu algılayabilir ve gerekli önlemleri alabilir. Bu tür proaktif yaklaşımlar, siber saldırılara karşı koruma sağlamakta büyük avantaj sunar.

Kimlik ve Erişim Yönetimi Standartları

IAM alanında standartlar ve uyumluluk gereksinimleri de önem kazanmaktadır. Örneğin, Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği (GDPR) ve diğer benzer düzenlemeler, organizasyonların kullanıcı verilerini nasıl yöneteceklerine dair kurallar koymaktadır. Bu nedenle, IAM sistemlerinin bu standartlara uygun şekilde yapılandırılması, hem yasal zorunluluklar hem de güvenlik açısından kritik bir konudur.

Sıfır Güven (Zero Trust) Yaklaşımı

Sıfır güven modeli, modern IAM uygulamalarında önemli bir trend haline geldi. Bu yaklaşım, "hiçbir kullanıcıya güvenme" ilkesine dayanır. Kullanıcıların iç veya dış olup olmalarına bakılmaksızın, her erişim isteği için kimlik doğrulama ve yetkilendirme gereklidir. Bu, organizasyonların daha iyi bir güvenlik seviyesi sağlamasına yardımcı olurken, kullanıcı deneyimini de iyileştirebilir.

Sonuç olarak, kimlik erişimi ve yönetimi alanındaki gelişmeler, dijital dönüşümle birlikte hızla devam etmektedir. Bulut tabanlı çözümler, çok faktörlü kimlik doğrulama, yapay zeka, standartlar ve sıfır güven yaklaşımları, organizasyonların güvenliğini artırmak ve verimliliği sağlamak için kritik öneme sahiptir. IAM, gelecekte de siber güvenliğin en önemli bileşenlerinden biri olmaya devam edecektir.

7. DİĞER SEKTÖRLERE ETKİLERİ VE KULLANIM ALANLARI

Blokzincir teknolojisi, dijital kimlik doğrulama süreçlerinde güvenlik, şeffaflık ve verimlilik sağlayarak devrim niteliğinde yenilikler sunmaktadır. Raporun bu kısmında, dijital kimliğin farklı sektörlerde nasıl kullanıldığını özellikle blokzincir teknolojisiyle desteklenen uygulama örnekleriyle birlikte inceleyeceğiz.

7.1. Kamu Yönetimi

Dijital kimliklerin kullanımı özellikle kamu sektöründe büyük önem taşır. Kimlik doğrulama süreçlerinde hata ve sahtekarlık riskini minimize ederken, aynı zamanda kullanıcıların hizmetlere hızlı ve güvenli bir şekilde erişimini sağlar. Blokzincir teknolojisi, veri manipülasyonuna karşı korunmamızda, bu süreçlerin şeffaflığını ve güvenilirliğini artırmamızda bize destek olabilir.

Aşağıda devletler tarafından kullanılan dijital kimlik örnek ve uygulamalarına yer verilmiştir; varsa blokzincir teknolojisinin kullanımı vurgulanmıştır.

1 milyardan fazla insanın biyometrik bilgisini toplamayı, depolamayı ve kullanmayı amaçlayan ve Hindistan Kimlik Tanılama Kurulu (Unique Identification Authority of India, UIDAI) tarafından vatandaşlara verilen 12 haneli bir numara olan Aadhaar, 2009 senesinde Hindistan hükümeti tarafından hayata geçirilmiştir. Hindistan vatandaşları için eşsiz bir kimlik olması için tasarlanan Aadhaar'ın amacı, yanlış kimlik problemini ve bunun sonucunda finansal hareketlerde oluşabilecek dolandırıcılıkları engellemektir. Bu biyometrik verilerle desteklenen en büyük dijital kimlik projesinde blokzincir teknolojisi, Aadhaar sisteminin daha güvenli ve şeffaf hale getirilmesi için potansiyel olarak görülmektedir. Blokzincir teknolojisinin güvenlik ve oylama sistemi gibi kullanım senaryoları için potansiyel oluşturulduğu kabul edilmektedir.

Singapur'da her ay 5 milyon kullanıcı tarafından 41 milyondan fazla işlem gerçekleştiren Singpass, vatandaşların hükümet ve işletme hizmetlerine online olarak erişmesini sağlayan güvenilir bir dijital kimliktir. 800 kamu kurumu ve 2700'den fazla işletmede hizmetlere güvenli ve kolay erişim sağlar. GovTech tarafından geliştirilen Singpass uygulaması sayesinde biyometri (parmak izi, yüz Doğrulama) veya SMS İki Faktörlü Kimlik Doğrulama (2FA) ile giriş yapılarak kimlik doğrulamadan belge imzalamaya günlük birçok işlem gerçekleştirilebilir. Dijital kimlik sistemini kullanarak sözleşmeleri, anlaşmaları ve diğer yasal belgeleri elektronik olarak imzalama imkanı sunan hizmet blokzincir teknolojisine dayanır. İmzacıya kriptografik olarak atama ve imza anında otomatik doğrulama sayesinde elektronik bir belge kolayca dijital olarak imzalanabilir.

AB Dijital Kimlik Cüzdanı uygulaması ile AB vatandaşları, AB'de ikamet eden kişiler ve AB Üye Ülkelerinde faaliyet gösteren işletmeler yeni elektronik kimliklerini kullanarak çevrimiçi sunulan tüm hizmetlere ulaşabilecek, çevrimiçi olarak kimliklerini kanıtlayabilecek ve ayrıca sisteme entegre uygulamalar aracılığıyla dijital kimliklerinde yer alan bir belgeyi çevrimiçi olarak paylaşabileceklerdir. Bu uygulama sayesinde vatandaşlar ulusal dijital kimliklere bağlanarak diplomalarını, ehliyetlerini, banka hesaplarını ekleyebilecekleri güvenli ve bütünlüklü bir hesaba sahip olacaklardır. Kullanıcılar; banka hesabı açmak, yaş uygunluklarını kanıtlamak, tıbbi reçeteleri yenilemek, araç kiralamak ve uçak biletlerini görüntülemek için cüzdanı kullanabilirler. İtalya, AB Dijital Kimlik Cüzdanı şemasının yeni versiyonu olan IT-Wallet'ın lansmanını yaparak vatandaşların kimlik belgelerini tek bir uygulama üzerinden dijitalleştirmelerine olanak tanımıştır.

Estonya, E-Residency programı ile güvenli bir dijital kimlik uygulaması sunarak online olarak devlet hizmetlerinden yararlanmaya olanak tanır. Blokzincir teknolojisi, devlet tarafından hizmeti kullanacak kişilerin kimliklerinin doğrulanması ve alınan kimlik bilgilerinin güvenliğinin sağlanmasında kritik bir rol oynamaktadır.

Dubai, "Dubai Blockchain Strategy 2020" programı kapsamında blokzincir tabanlı dijital kimlik sistemlerini belediye hizmetlerine entegre etmeyi planlamaktadır. Bu sayede, vatandaşlar belediye hizmetlerine dijital kimlikleriyle erişebilecektir. Aynı zamanda blokzincir tabanlı dijital kimlik doğrulama sistemlerini kullanarak kamu süreçlerini hızlandırmayı ve şeffaflığı artırmayı hedefleyen ülke pilot projelerde çeşitli hukuki belgelerin doğrulanması için de çalışmaktadır.

Sierra Leone, blokzincir teknolojisini kullanarak seçim sonuçlarının doğruluğunu ve şeffaflığını artırmak için pilot bir proje gerçekleştirmiştir.

Bu proje kapsamında dijital kimlikler, seçmen kimlik doğrulama süreçlerinde kullanılmıştır. Rusya'da yapılan yerel seçimlerde ise blokzincir tabanlı bir oylama sistemi kullanılarak seçmen kimlik doğrulama ve oy güvenliği sağlanmıştır.

Brezilya, dijital kimlik doğrulama gerektiren noterlik hizmetlerinde blokzincir teknolojisini kullanarak belgelerin doğruluğunu ve güvenliğini sağlamak için pilot projeler yürütmektedir.

Kanada'da Toronto, dijital kimlik ve blokzincir teknolojilerini bir araya getirerek vatandaşlarının belediye hizmetlerine daha hızlı ve güvenli erişimini sağlamak için projeler yürütmektedir.

İsveç'te SEB bankası ve Nasdaq, blokzincir tabanlı dijital kimlik sistemlerini şirket kimlik doğrulama süreçlerinde kullanmaktadır. Bu sistemler, şirketler arası işlemlerin daha güvenli ve şeffaf bir şekilde gerçekleştirilmesini sağlamaktadır.

7.2. Gayrimenkul

Gayrimenkul doğası gereği hareketsiz, bölünemez ve likit değildir. Likit olmayan gayrimenkullerin likit, alınıp satılabilir menkul kıymetlere dönüştürülmesi-menkul kıymetleştirme olarak bilinen bir süreç-1960'lara kadar uzanmaktadır.

Gayrimenkul sektöründe dijital kimlik ve blokzincir teknolojisi kullanımını mümkün hale getirmek için öncelikle gayrimenkulleri blokzincir üzerinde dijital olarak temsil edilebilmesi yani tokenizaysonu gerekmektedir. Tokenizasyon, bir varlığın dijital bir temsilini oluşturma sürecini ifade eder; bu da bir blokzincirde bu gerçek varlıkların kısmi sahipliğini, dijital transferini ve yönetimini sağlar. Gayrimenkul tokenizasyonunun çeşitli sonuçları vardır:

- mülkiyeti parçalara ayırır,
- operasyonel verimliliğe katkıda bulunur,
- ödeme sürelerini azaltır,
- veri şeffaflığını sağlar ve
- likiditeyi arttırır.

Bu alanda umut vaat eden detaylardan biri, arazi tapuları ve diğer mülkiyet haklarıyla ilgili eşler arası (P2P) işlemlerin yapılabilecek olmasıdır.

Birçok ülke yıllardır elektronik kadastro sistemlerini kullanıyor, ancak aynı zamanda hala büyük ölçüde kâğıt işlemlere güveniyorlar. Aslına bakılırsa, henüz hiçbir ülke tapu haklarıyla ilgili elektronik eşler arası işlemleri etkinleştirmemiştir. Bu tür sicillerde tapu hakları ve mülkiyet hakları elektronik ortamda kaydedilse de bu kayıtlar kâğıt ortamında gerçekleşen işlemlere göre ikincil ve ardıl niteliktedir. Birleşik Krallık, Avustralya, Kanada ve Yeni Zelanda gibi birkaç ülke elektronik işlemlerde daha fazla yol katetmiş olup elektronik kayıt ve başvuru sistemlerini aktif olarak kullanmaktadırlar.

Gayrimenkul tokenizasyonu, tek bir mülkün veya bir mülk portföyünün mülkiyetini veya haklarını dağıtık bir defterde temsil etmeyi içeren yeni bir eğilimdir. Gayrimenkul tokenizasyonu, 2018 yılında Elevated Returns tarafından St. Regis Aspen Resort'un tokenizasyonu ile dünyanın dikkatini çekmiştir. Bunu 2019 yılında RealToken olarak bilinen benzer bir gayrimenkul tokenleştirme projesi izlemiştir. '9943 Marlowe' mülkünün tokenizasyonu dünya çapında ilk tokenize mülklerden birisi olup, token daha sonra halka açık ve izinsiz Ethereum blokzincirinde 7/24 alınıp satılabilir hale getirilmiştir.

Fakat birçok farklı ülke, mülkiyet haklarının tokenizasyonunu mümkün kılacak düzenleyici, yasal ve teknik çerçevelerden yoksundur. Günümüzde mevcut yöntemlerle gayrimenkul tokenizasyonu mümkün kılınabilmektedir:

- Varlık Seçimi: Tokenlaştırılacak gayrimenkul seçilir. Bu, tek bir mülk veya bir mülk portföyü olabilir.
- Yasal Çerçeve: Tokenlaştırmanın yerel düzenlemelere uygun olmasını sağlamak için yasal bir yapı oluşturulur. Bu genellikle mülkü elinde tutmak için bir Özel Amaçlı Şirket (SPV) oluşturmayı içerir.
- Token Oluşturma: Bir blokzincir platformu üzerinde dijital tokenlar geliştirilir. Bu tokenlar mülkün kısmi sahipliğini temsil eder. Hedefe bağlı olarak, bunlar benzersiz mülkler için değiştirilemez tokenlar (NFT'ler) veya kısmi mülkiyet için değiştirilebilir tokenlar olabilir.
- Akıllı Sözleşmeler: Tokenların yönetimini ve transferini otomatikleştirmek için akıllı sözleşmeler uygulanır. Bu sözleşmeler, işlemlere ilişkin kuralları ve koşulları tanımlayarak şeffaflık ve güvenlik sağlar.
- Token Arzı: Tokenlar, yatırımcılara sunulur. Örneğin, Menkul Kıymet Token Arzı (STO) olarak yatırımcılar bu tokenları alabilir, satabilir, takas edebilir veya gayrimenkul piyasasına likidite sağlayabilir.
- Yönetim ve Uyumluluk: Mülkün sürekli olarak yönetilmesi ve yasal gerekliliklere uygunluğun sağlanması için kira geliri veya kâr akıllı sözleşme şartlarına göre token sahiplerine dağıtılır.

Tokenları ihraç eden platform, düzenleyici yükümlülüklerin (KYC - Müşterini Tanı - süreci dahil) yerine getirilmesini ve hedef yatırımcılara dayalı olarak STO'lara ilişkin özel düzenlemenin gerektirdiği bilgileri sağlama görevine sahiptir. Bu aşamada Dijital Kimlikler, gayrimenkulün blokzincirde tokenleştirilmesinde çok önemli bir rol oynamaktadır.

- Kimlik Doğrulama: Dijital kimlikler, tokenizasyon sürecindeki tüm katılımcıların doğrulanmasını sağlayarak dolandırıcılık riskini azaltır ve Müşterini Tanı (KYC) ve Kara Para Aklamayı Önleme (AML) düzenlemelerine uyumluluk sağlar.

• Şeffaflık ve Güven: Dijital kimliklerin işlemlerle ilişkilendirilmesi sayesinde tüm faaliyetler doğrulanmış kişi veya kuruluşlara kadar takip edilebilir. Bu, şeffaflığı artırır ve yatırımcılar ile paydaşlar arasında güven oluşturur.

• Verimli İşlemler: Dijital kimlikler gayrimenkul tokenlarının alım, satım ve ticaret sürecini kolaylaştırır. Kimliklerin hızlı ve güvenli bir şekilde doğrulanmasını sağlayarak işlemleri hızlandırır ve idari yükü azaltır.

• Erişim Kontrolü: Dijital kimlikler, hassas bilgilere erişimi yönetmek ve yalnızca yetkili kişilerin belirli işlemlere katılabilmesini veya belirli verilere erişebilmesini sağlamak için kullanılabilir.

• Düzenleyici Uyumluluk: Tüm katılımcıların doğrulanmış dijital kimliklere sahip olmasını sağlamak, tokenize edilmiş gayrimenkulün meşruiyeti ve kabulü için çok önemli olan çeşitli yasal gerekliliklerle uyumluluğun sürdürülmesine yardımcı olur.

• Gelişmiş Güvenlik: Dijital kimlikler, yalnızca doğrulanmış kişilerin işlem başlatabilmesini sağlayarak yetkisiz erişim ve dolandırıcılık riskini azaltarak ek bir güvenlik katmanı sağlar.

Birçok platform, gayrimenkul tokenizasyonunda Dijital Kimliklerin kullanımını başarıyla uygulamıştır.

RedSwan, ticari gayrimenkul tokenizasyonunda uzmanlaşmıştır. Yatırımcı kimliklerini doğrulamak için dijital kimlikleri kullanır, KYC ve AML düzenlemelerine uygunluğu sağlar.

Securitize, varlıkları tokenize etmek için çeşitli gayrimenkul firmalarıyla ortaklık kurar. Yatırımcı doğrulama sürecini kolaylaştırmak için dijital kimlikleri kullanarak mevzuata uygunluğu sağlar ve işlem güvenliğini artırır.

Kasa Korea, Güney Kore'deki gayrimenkul varlıklarını tokenlaştırmaya odaklanır. Katılımcıları doğrulamak ve güvenli bir işlem ortamı sağlamak için dijital kimlikler kullanır. Uluslararası düzenlemelere uyum sağlayarak sınır ötesi yatırımları kolaylaştırır.

Polymath, gayrimenkul de dahil olmak üzere çeşitli varlıkların tokenlaştırılması için bir platform sağlar. Yalnızca doğrulanmış yatırımcıların token tekliflerine katılabilmesini sağlamak için dijital kimlikleri entegre eder. Sağlam kimlik doğrulama süreçleri sayesinde güvenlik ve uyumluluğu artırır. Bu platformlar, dijital kimliklerin gayrimenkul tokenizasyonuna entegre edilmesinin etkinliğini göstermekte ve güvenli, şeffaf ve verimli işlem ortamları sağlamaktadır.

7.3. Eğitim

Blokzincir tabanlı dijital kimlik sistemleri, eğitim kurumlarının akademik kimlik bilgilerini oluşturma, yönetme ve doğrulama yöntemlerini değiştirmektedir. Bu sistemler, diploma, transkript ve sertifikalar gibi akademik belgelerin güvenli, değiştirilemez ve kolayca doğrulanabilir bir formatta sunulmasını sağlamayı amaçlamaktadır.

Bu tür kimlik bilgileri, akademik başarıların doğruluğunu artırarak öğrenci, işveren ve kurumlar arasında manuel işlemleri azaltarak süreci kolaylaştırmaktadır. Ayrıca, bireylerin kimlik bilgilerini güncellemelerini kolaylaştırarak sürekli eğitim ve kariyer gelişimine katkıda bulunma potansiyeli taşımaktadır. Blokzincir tabanlı kimlik sistemlerinin yaygınlaşmasıyla, eğitim alanında daha şeffaf, güvenilir ve verimli bir kimlik doğrulama ekosistemi oluşturulması beklenmektedir.

Akademik Kimlik Bilgilerinin Saklanması ve Doğrulanması

Blokzincir; diploma, sertifika ve transkript gibi akademik kimlik bilgilerini güvenli bir şekilde saklama ve doğrulama imkanı sunar.

Bu kimlik bilgilerini blokzincir üzerinde oluşturarak kurumlar, bu bilgilerin değiştirilemez ve işverenler veya diğer eğitim kurumları tarafından anında doğrulanabilir olmasını sağlar.

Massachusetts Teknoloji Enstitüsü (MIT), 2017 yılında blockchain tabanlı diplomalar vererek bu teknolojiyi erken benimseyen kurumlardan biri olmuştur. 2023 yılında da Lille Üniversitesi Dem-Attest projesini tamamen canlıya alarak tüm dünyada doğrulanabilir dijital diplomalar vermeye başlamıştır.

Eğitim Verilerinin Sahipliği ve Taşınabilirliği

Blokzincir tabanlı dijital kimlikler, öğrencilerin kendi akademik kayıtları üzerinde tam kontrole sahip olmasını sağlar. SSI (Self-Sovereign Identity) sayesinde öğrenciler, eğitim kimlik bilgilerini sahiplenebilir, yönetebilir ve aracı kurumlara ihtiyaç duymadan paylaşabilir. Kullanıcılar orijinal belgeleri kaybolsa bile eğitim geçmişlerini kanıtlayabilir.

Avrupa Birliği'nin "EBSI" (European Blockchain Services Infrastructure) projesi, Avrupa genelinde akademik yeterliliklerin sınır ötesi tanınmasını sağlamak ve doğrulama giderlerini azaltmak için SSI çözümlerini araştırmaktadır.

Merkeziyetsiz Transkript Sistemleri

Blokzincir ve dijital kimlik kullanarak, kurumlar akademik transkriptlerin saklanması ve paylaşılması için merkeziyetsiz sistemler oluşturabilmektedir. Bu sistemler, veri bütünlüğünü artırır ve öğrencilerin okullar arasında geçiş yapması veya iş başvuruları sırasında süreci kolaylaştırır. Transkriptler öğrencilere anında erişilebilir olurken, üçüncü taraflarca doğrulanabilir hale gelir.

Japonya'da Tokyo Üniversitesi ve Sony Global Education, transkript yönetimi ve kurumlar arası kredi transferini kolaylaştırmak için blokzincir tabanlı bir platform geliştirmek üzere iş birliği yapmıştır.

Merkeziyetsiz Öğrenme ve Sosyalleşme Platformları

Merkeziyetsiz öğrenme sistemleri, öğrencilere daha fazla kontrol ve şeffaflık sunarak, öğrenme süreçlerini ve içeriklerini kendilerinin belirlemesine olanak tanır. Bu yaklaşım, geleneksel eğitim sistemlerinin sınırlamalarını aşmaya ve öğrenme deneyimlerini daha erişilebilir hale getirmeye yardımcı olabilir. Geleneksel eğitim sistemleri genellikle eğitim kurumları, yayıncılar ve içerik dağıtıcıları gibi birçok aracıyı içerir. Blokzincir, doğrudan eşler arası (peer-to-peer) etkileşimleri mümkün kılarak maliyetleri düşürmeyi ve erişilebilirliği artırmayı amaçlar.

T.C. Sanayi ve Teknoloji Bakanlığı tarafından gerçekleştirilen Dijital Rozet projesi; sertifika sağlayan kurumların kullanıcı haline getirilerek kazanımların dijital bir platform üzerine taşınmasına olanak verilmesi ve bu sayede özgeçmiş ve diplomalarla anlatılamayan yetkinliklerin dijital sertifika ve rozetlerin avantajları ile birlikte paylaşılmasına imkân vermektedir. Dijital Rozetler bireylerin elde ettiği başarıları sergileyen veya bireyin belirli bir bilgi, beceri ve yeteneği kazandığını gösteren doğrulanabilir dijital sembollerdir. Kurumlar, sertifika ve rozetleri bireylere gönderebilir, bireyler ise sahip olduğu sertifika ve rozetleri dijital ortamda paylaşabilirler. Bireyler ve kurumlar, sertifika ve rozetleri e-posta adresi veya Sertifika/Rozet ID' sini kullanarak doğrulayabilirler.

Online kurslar ve mikro-kredilendirme programlarının büyümesiyle birlikte blokzincir, tamamlanan kurslar için dijital rozetler ve sertifikalar güvenli bir şekilde vermek için değerli hale gelmiştir. Bu doğrulanabilir dijital sertifikalar, dijital kimlikte saklanabilir ve potansiyel işverenlerle paylaşılabilir.

IBM, çevrimiçi kursları için blokzincir destekli sertifikalar sunmak üzere çeşitli eğitim kurumlarıyla iş birliği yapmıştır. Bu sertifikalar, öğrencilerin dijital kimliklerinde saklanmalarına olanak tanır.

7.4. Turizm

Seyahat esnasında yolcuların kendilerini tanıtmak için harcadıkları zaman "uçuş rezervasyonu yapmak, havaalanında bagaj vermek, güvenlikten geçmek, uçağa binmek, uçak içi hizmetlerden yararlanmak ve varış noktasına ulaşarak gerekli kontrollerden geçmek" şeklinde özetlenebilir.

Havayolu sektörü dijital kimlik uygulamalarından yararlanmak için büyük bir potansiyel barındırıyor Havaalanlarında uçuştan önce oluşan bekleme yoğunluklarının azaltılması, bilet alımından uçuşun sonlanmasına kadar olan sürecin hızlı ve güvenilir şekilde yönetilmesi, maliyetlerin azaltılması ve yolcuların memnuniyetinin arttırılması konularında yeniliklere ihtiyaç bulunmaktadır. Bu nedenle turizm sektörü teknolojideki gelişmelere paralel olarak biyometri ve dijital kimlik kullanımları ile çözümler üretmeye çalışmaktadır.

Havacılık sektöründe biyometrik ve dijital kimlik teknolojilerinin kullanımının önemli bir yere sahip olacağı görülmektedir. Denenmeye başlanılan çözümlerin havayolları, havalimanları ve yolcular üzerindeki olumlu yansımaları görüldükçe bu alana daha çok yatırım yapılması ve yaygınlaşması beklenmektedir.

Günümüzde mevcut uygulamalarda yolcu rezervasyon işlemi sırasında akıllı telefonunu kullanarak kimlik kartı veya pasaport belgelerini yüklemekte, daha sonra yüz tarama ile güvenlik kontrollerinden geçebilmektedir. ABD'de Gümrük ve Sınır Koruma (CBP) 'Biyometrik Çıkış' programının bir parçası olarak Orlando, Los Angeles ve Miami Uluslararası Havaalanı gibi bazı büyük havaalanlarında biyometrik tarama programlarını başlatmıştır. Birleşik Krallık yolcu taşıma sürecini hızlandırmak için Heathrow Biyometri projesi kapsamında birçok havaalanında uygulamayı test etmektedir. Birleşik Arap Emirlikleri de check-in, güvenlik taraması ve biniş sürecinde biyometrik tarama uygulayan ilk ülkelerdendir.

Yakın gelecekte ise biyometri verileri de dahil olmak üzere elektronik kimlik bilgilerinin tek bir yerde güvenli ve şeffaf bir şekilde saklanması ve yönetilmesini sağlayacak Avrupa Dijital Kimlik Cüzdanı'nın (EUDIW) kullanıma sunulması beklenmektedir.

Uluslararası Hava Taşımacılığı Birliği (IATA), British Airways ile Londra Heathrow'dan (LHR) Roma Fiumicino'ya (FCO) yapılan seçilmiş uçuşlarda uçak bileti alımından seyahat edilen lokasyona varışa kadarki tüm süreçlere tamamen entegre çalışan dijital kimlikli seyahat deneyimini başarıyla test etti. Proje, seyahat zincirindeki paydaşları bir araya getirerek çözümler üretmek amacıyla faaliyet gösteren IATA Inovasyon Laboratuvarı'nda geliştirilen bir PoC (Kavram Kanıtı) çalışması olarak yapıldı. Seyahat deneyimini iyileştirmek üzere dijital kimlikle entegre çalışan cüzdanlar sayesinde kişilerin gerekli bilgi ve sadakat programı detaylarını saklamaları ve süreçlerden hızlıca geçmeleri mümkün kılınmıştır.

Anında kimlik doğrulama ile işlemlerin daha hızlı ve verimli hale gelmesini hedefleyen IDNOW kullanıcılarına yasal imza yerine geçen dijital kimlik uygulamasını sunmaktadır. Cüzdana dijital kimliğin bir kez yüklenmesi yeterli olup birçok yerde kullanılmaktadır. Aynı zamanda doğrulanmış Avrupa kimlik havuzuna entegre olması nedeniyle de müşterilerine kolaylık sağlar.

iProov ve Eurostar iş birliği ile geliştirilen SmartCheck, kimlik doğrulaması için yüz

biyometrisini kullanarak bilet ve pasaport kontrollerinde işlemleri kolaylaştıran bir dijital kimlik çözümüdür. SmartCheck, biyometrik yüz tanıma ve uzaktan kimlik doğrulama teknolojisini kullanarak temassız seyahati mümkün kılar. Yolcular bilet yerine yüzlerini kullanarak kontrollerden geçebilirler. Londra St.Parncras Uluslararası Tren İstasyonunda kullanılmaktadır. Uygulama, tren istasyonundaki yoğunluk ve beklemelerden kurtararak zaman kazandırır, manuel kontrol süreçlerini azaltarak işlem sürelerini kısaltır, personel verimliliğini artırır, son kullanıcıya hızlı ve güvenli bir çözüm sunar.

7.5. Sağlık

Sağlık sektöründe dijital kimlik kullanımı, hem hastalar hem de sağlık hizmeti sağlayıcıları için birçok avantaj sunar. Dijital kimlik sistemleri, hastaların kimlik bilgilerinin hızlı ve doğru bir şekilde doğrulanmasını sağlar. Bu sayede, hasta kayıt işlemleri hızlanır ve hata oranı azalır. Hastaların tıbbi geçmişi, mevcut tedavileri ve ilaç kullanım bilgileri dijital kimlikleri ile entegre edilerek, sağlık hizmeti sağlayıcılarına anında erişim imkanı sunar.

Blokzincir tabanlı dijital kimliğin sağlık sektöründe kullanıldığı bazı örnekler aşağıdaki gibidir:

Estonya'daki hasta kayıtları blokzincir tarafından dijitalleştirilip güvence altına alınarak sağlık profesyonelleri için tek bir değişmez veri kaynağı sağlamaktadır. Ülkenin e-Health sistemi, hasta verilerini güvenli bir şekilde saklamak ve sağlık hizmet sağlayıcıları arasında veri paylaşımını kolaylaştırmak için blokzincir kullanmaktadır. Bu sistem sayesinde, hastalar kendi sağlık verilerine erişebilir ve bu verilerin kimler tarafından görüntülendiğini görebilirler.

MIT Medya Laboratuvarı Konsorsiyumu tarafından desteklenen bir çalışma kapsamında oluşturulan MedRec projesi blokzincir teknolojisini kullanarak elektronik sağlık kayıtlarını işlemek için merkezi olmayan bir kayıt yönetim sistemi kullanmaktadır. Sistem tasarımı hastaların kapsamlı ve değiştirilemez kayıtlara ve sağlık kuruluşlarındaki bilgilerine erişim imkanı sağlamaktadır. MedRec, kimlik doğrulama, veri girişi, güncelleme ve paylaşımı süreçlerini yönetmektedir. Sağlık sektörü paydaşları ise blokzincir "madencileri" olarak ağa katılmaya teşvik edilmektedir. Bu katılım karşılığında madencilik ödülü olarak anonimleştirilmiş verilere erişim sağlanmaktadır.

Bunun dışında blokzincir teknolojisi kullanılmasa da ülkemizde birçok farklı örnek görmek mümkündür. E-Nabız dışında Türkiye'deki e-Devlet, MHRS, HES, AHBS gibi diğer uygulamalar dijital kimliğin sağlık alanındaki kullanımını desteklemektedir.

- e-Devlet Kapısı: Türkiye'de dijital kimlik doğrulama ve sağlık hizmetlerine erişim, e-Devlet Kapısı üzerinden sağlanmaktadır. Vatandaşlar, e-Devlet üzerinden sağlık raporlarına, ilaç reçetelerine ve tıbbi geçmişlerine ulaşabilirler.

- E-Nabız: Hastaların sağlık verilerini güvenli bir şekilde saklamayı ve paylaşmayı hedeflemektedir. Bu sistem sayesinde, hastalar kendi sağlık verilerine erişebilir ve verilerin kimler tarafından görüntülendiğini izleyebilir.

- Merkezi Hekim Randevu Sistemi (MHRS): MHRS, Türkiye'de hastaların hastanelerdeki doktorlardan randevu almasını kolaylaştıran bir sistemdir. Dijital kimlik doğrulama sayesinde, hastalar güvenli bir şekilde randevu alabilir ve yönetebilirler. Bu sistem, sağlık hizmetlerine erişimi hızlandırır ve hastaların zamanını verimli bir şekilde kullanmasını sağlar.

• Aile Hekimliği Bilgi Sistemi (AHBS): AHBS, aile hekimlerinin hastaların sağlık bilgilerini dijital ortamda tutmalarını sağlayan bir sistemdir. Dijital kimlik doğrulama ile hastaların sağlık geçmişi, muayene sonuçları ve reçeteleri güvenli bir şekilde saklanır ve yönetilir.

Ayrıca bireysel olarak sıklıkla kullandığımız Apple Health ve Google Health de güzel bir örnek olarak karşımıza çıkar. Apple Health uygulaması, kullanıcıların sağlık verilerini güvenli bir şekilde toplar ve saklar. Kullanıcılar, kimlik doğrulama yöntemleriyle bu verilere erişebilir ve paylaşabilirler. Benzer şekilde, Google Health de sağlık verilerinin yönetiminde dijital kimlik doğrulama sistemleri kullanmaktadır. IATA da benzer bir şekilde Travel Pass ile, yolcuların COVID-19 test sonuçlarını ve aşı kayıtlarını güvenli bir şekilde saklamasını ve paylaşmasını sağlayan dijital bir sağlık pasaportu sunmaktadır. Bu kimlik, Emirates ve Qantas gibi büyük havayolları tarafından benimsenmiş ve birçok kıtada kullanılmaktadır.

7.6. Ulaşım

Dijital kimlik ve blokzincir teknolojileri, modern ulaşım sektöründe önemli bir dönüşüm yaratmaktadır. Bu teknolojiler, kimlik doğrulama, veri güvenliği ve işlem verimliliği gibi konularda büyük avantajlar sunmaktadır. Aşağıda, bu teknolojilerin ulaşım sektöründeki çeşitli uygulama alanları ve örnekleri yer almaktadır.

• Dijital İkiz ve Grafik Teknolojisi: Londra'da dijital ikiz ve grafik teknolojisi, ulaşım altyapısının dijital olarak modellenmesi ve yönetilmesi için kullanılmaktadır. Bu teknoloji, çeşitli senaryoların simülasyonunu yaparak trafik sıkışıklığı, yol bakımı ve acil durum müdahaleleri gibi durumları önceden tespit eder ve en iyi müdahale çözümlerini belirler. Bu uygulama, Londra Ulaşım Kurumu tarafından geliştirilmektedir.

• Küresel Dijital Kimlik Çalışmaları: Dijital kimlik teknolojileri, uluslararası seyahatlerde ve sınır geçişlerinde kullanılarak kimlik doğrulama süreçlerini hızlandırır ve güvenliği artırır. Örneğin, Kanada ve Hollanda arasındaki kağıtsız uçuş projesi, yolcuların dijital kimlikleri ile uçuşlarını gerçekleştirmelerini sağlar. Bu proje, Kanadalı ve Hollandalı hava yolları iş birliği ile gerçekleştirilmiştir.

• Lojistik: Blokzincir teknolojisi, lojistik ve ulaştırma sektöründe malzeme hareketlerini ve teslimat süreçlerini izlemek için kullanılmaktadır. Bu sayede tedarik zincirinde şeffaflık ve izlenebilirlik sağlanırken, kayıplar ve hatalar minimize edilir. Örneğin, Maersk firması blokzincir tabanlı dijital kimlikler kullanarak ürünlerin takibini sağlamaktadır.

• Akıllı Sözleşmeler ve IoT: Blokzincir tabanlı akıllı sözleşmeler, ulaşım sektöründe IoT cihazları ile entegrasyon sağlayarak veri paylaşımını ve işlem otomasyonunu geliştirir. Örneğin, Fr8 adlı lojistik firması, akıllı sözleşmeleri kullanarak tedarik zinciri süreçlerini şeffaf ve hatasız hale getirir.

• Otomotiv ve Otonom Araçlar: Blokzincir teknolojisi, otonom araçların veri güvenliği ve kimlik doğrulama süreçlerinde kullanılır. Örneğin, araçların sahiplik bilgileri, bakım kayıtları ve kullanım geçmişi blockchain üzerinde saklanarak, araç güvenliği ve izlenebilirliği artırılır. Bu teknolojiyi kullanan firmalar arasında Tesla ve BMW bulunmaktadır.

• Deniz Taşımacılığı ve Gemi Sigortası: Dünya genelinde deniz taşımacılığı yapan firmalar, blokzincir tabanlı sistemleri kullanarak gemi sigortası işlemlerini hızlandırmakta ve güvence altına almaktadır. Bu sayede deniz taşımacılığı operasyonları daha verimli ve güvenli hale gelir. Bu teknolojiyi kullanan firmalar arasında Maersk ve IBM bulunmaktadır.

Helium People's Network, dünyadaki en büyük LoRaWAN ağı olup, IoT cihazları arasında bilgi transferini sağlamakatdır. Bu ağ, akıllı şehirler ve lojistik için gerçek zamanlı varlık verilerini izleme ve yönetme yeteneğine sahiptir. Bu sistem, taşımacılık sektöründe kullanılan cihazların güvenli ve verimli bir şekilde iletişim kurmasını sağlar ve veri bütünlüğünü garanti eder.

İstanbul Büyükşehir Belediyesi, şehirdeki ulaşım sistemlerini blokzincir teknolojisi ile entegre etmeye yönelik projeler geliştirmektedir. Bu projeler, şehir içi ulaşımda kullanılan araçların ve kullanıcıların kimlik doğrulama süreçlerini güvenli hale getirerek, toplu taşıma hizmetlerinin verimliliğini artırmayı hedeflemektedir.

Maersk ve IBM tarafından geliştirilen TradeLens platformu, deniz taşımacılığı sektöründe blokzincir teknolojisini kullanarak tedarik zinciri boyunca ürünlerin izlenebilirliğini sağlar. Bu platform, konteyner nakliyesinde şeffaflığı artırmak ve verimliliği artırmak için kullanılır. TradeLens, tüm tedarik zinciri boyunca çeşitli paydaşların gerçek zamanlı veri paylaşımını ve iş birliğini destekler. Bu sayede, deniz taşımacılığı operasyonlarının daha güvenli, hızlı ve verimli bir şekilde gerçekleştirilmesi sağlanır.

7.7. Akıllı Şehirler

Günümüzün hızla dijitalleşen dünyasında, dijital kimlikler, bireylerin ve kurumların kimlik doğrulama ve güvenlik süreçlerini yönetmede hayati bir rol oynamaktadır. Özellikle akıllı şehirlerde, dijital kimlikler, şehir yönetimi ve hizmetlerinin daha verimli, güvenli ve kullanıcı dostu hale gelmesinde kritik bir bileşen olarak öne çıkmaktadır. Dijital kimlikler, kullanıcıların çevrimiçi işlemlerini güvenli bir şekilde gerçekleştirmelerine olanak tanır.

Akıllı şehirlerde, dijital kimlikler vatandaşların kamu hizmetlerine erişimini kolaylaştırır, toplu taşıma sistemlerinde biletleme süreçlerini ve kullanıcı deneyimini iyileştirir, şehirdeki güvenlik önlemlerinin ve acil durum müdahalelerinin etkinliğini artırır, e-devlet uygulamaları ile vatandaşların devlet ile olan işlemlerini dijital ortamda yapabilmelerini sağlar. Blokzincir tabanlı dijital kimlikler, akıllı şehirlerin daha etkin, şeffaf ve kullanıcı odaklı hale gelmesine katkıda bulunabilir. Akıllı şehirler, bu teknolojiyi kullanarak vatandaşların kimlik doğrulama işlemlerini, veri yönetimini ve hizmet entegrasyonunu daha güvenli ve verimli hale getirebilir.

Estonya'da e-Identity, Singapur'da SingPass, Hindistan'da Aadhar, Hollanda'da DigiD, Türkiye'de e-Devlet olduğu gibi devlet destekli dijital kimlik tabanlı uygulamalar akıllı şehirlerin yaratılmasında ve dijital toplumların yaratılmasında önemli rol oynamaktadır.

Türkiye'de biyometrik verilerle birlikte kimlik bilgilerini içeren çipli kimlik kartları; sürücü bilgilerini ve içeren çipli ehliyetler ve seyahat belgelerini içeren çipli pasaportların kullanılmaktadır. Elektronik imza (e-İmza) ise, dijital kimlik doğrulaması için kullanılan bir başka önemli araçtır. E-İmza, kullanıcıların dijital belgeleri güvenli bir şekilde imzalamalarına ve kimlik doğrulaması yapmalarına olanak tanır. Türkiye'de e-İmza, özellikle kamu kurumları ve bankacılık sektörü gibi alanlarda yaygın olarak kullanılmaktadır.

Birleşik Arap Emirlikleri'nde (BAE), UAE Pass adı verilen akıllı şehir projelerinin bir parçası olarak entegre edilmiş bir dijital kimlik platformu bulunmaktadır. UAE Pass, BAE'deki devlet kurumları ve özel şirketler için çeşitli web sitelerine ve uygulamalara güvenli bir giriş mekanizması vererek kullanıcıların 130'dan fazla kuruluş tarafından sağlanan 6.000'den fazla hizmete erişmesini sağlar.

UAE Pass, kullanıcıların fiziksel kimlik kartları veya belgeler taşıma zorunluluğunu ortadan kaldırarak işlemleri dijital ortamda yapabilme imkanı tanır. Dubai Blockchain Strategy ile şehrin tüm devlet işlemlerinin blokzincir üzerine taşınması hedeflenmektedir. UAE Pass için de Consensys ile birlikte çalışılmıştır.

Enerji sektörü, dijitalleşme ve yenilikçi teknolojilerin entegrasyonu ile hızla dönüşmektedir. Bu dönüşümün önemli bileşenlerinden biri olan blokzincir teknolojisi, enerji ticareti ve yönetimi süreçlerinde şeffaflık, güvenlik ve verimlilik sağlamaktadır. Blokzincir teknolojisinin enerji sektöründe sunduğu en büyük avantajlardan biri, dijital kimlik kavramı ile olan entegrasyonudur. Dijital kimlikler, bireylerin ve kurumların dijital ortamda kimliklerinin doğrulanmasını ve güvenli bir şekilde yönetilmesini sağlar. Enerji sektöründe dijital kimlikler, enerji tüketicileri ve üreticilerinin kimlik doğrulama süreçlerini kolaylaştırmakta ve işlemlerini güvence altına almaktadır.

Blokzincir ayrıca, yenilenebilir enerji sertifikaları (I-REC), karbon kredileri ve Guarantees of Origin (Go) gibi sistemlerle de uyumlu çalışmaktadır. Bu sistemler, enerji üreticilerinin yeşil enerji üretimlerini sertifikalandırmalarını ve karbon emisyonlarını dengelemelerini sağlamaktadır. Blokzincir teknolojisi, bu sertifikaların ve kredilerin güvenli, şeffaf ve izlenebilir olmasını temin ederek sahtecilik riskini azaltmakta ve sürdürülebilirlik hedeflerine ulaşmayı kolaylaştırmaktadır. Dijital kimlikler, bu sertifikalar ve kredilerle ilgili tüm işlemlerin doğrulanmasında ve izlenmesinde kritik bir rol oynamaktadır. Örneğin, bir enerji üreticisinin ürettiği yeşil enerjiyi I-REC sistemi ile sertifikalandırması, bu üreticinin dijital kimliği ile ilişkilendirilmektedir. Bu sayede, enerji üreticisinin kimliği ve ürettiği enerjinin kaynağı, blokzincir üzerinde güvenli bir şekilde kaydedilmekte ve izlenebilmektedir.

Aynı şekilde, karbon kredileri ve Guarantees of Origin (Go) sistemlerinde de dijital kimlikler, işlemlerin doğruluğunu ve şeffaflığını sağlamak için kullanılmaktadır.

Elia Group ve Energy Web, enerji sektöründe dijital kimlik uygulamalarını destekleyen bir çözüm geliştirmiştir. Bu uygulama, enerji tüketicilerinin ve üreticilerinin kimlik doğrulama süreçlerini dijitalleştirerek daha güvenli ve verimli bir sistem sunmaktadır. Dijital kimlikler, enerji alışverişlerinde ve tüketim takibinde şeffaflığı artırmaktadır. Elia Group, bu teknoloji ile enerji sistemlerini daha akıllı ve esnek hale getirerek kullanıcıların enerji tüketimlerini daha etkin bir şekilde yönetmelerini sağlamaktadır. Energy Web'in blokzincir altyapısı ile desteklenen bu dijital kimlik uygulaması, kullanıcıların enerji işlemlerini güvence altına almakta ve enerji piyasasında yeni iş modellerinin ortaya çıkmasına olanak tanımaktadır. Bu çözüm, enerji sektöründe dijitalleşmenin önünü açarken, aynı zamanda güvenli ve şeffaf bir enerji ticareti ortamı sunmaktadır.

Elia, Energy Web ve BMW iş birliği ile yapılan projede, elektrikli araç (EV) şarj istasyonlarının şebeke operatörleri tarafından görünür hale getirilmesi başarıyla gösterilmiştir. Bu proje, elektrikli araç şarj altyapısının yönetimini ve şeffaflığını artırarak enerji sistemlerine entegrasyonunu kolaylaştırmaktadır. Proje kapsamında, elektrikli araçların şarj işlemleri blokzincir tabanlı dijital kimlikler kullanılarak izlenmekte ve yönetilmektedir. Bu sayede, enerji talebi ve arzı daha iyi dengelenmekte, şarj işlemleri sırasında enerji verimliliği artırılmakta ve kullanıcı deneyimi iyileştirilmektedir. Ayrıca, bu teknoloji sayesinde şarj istasyonlarının doluluk durumu ve kullanılabilirliği gerçek zamanlı olarak takip edilebilmektedir. Bu proje, elektrikli araç şarj altyapısının güvenli ve şeffaf bir şekilde yönetilmesine katkı sağlamaktadır.

Shell, tedarik zincirinin verimliliğini artırmak amacıyla merkezi olmayan dijital pasaportlar geliştirmiştir. Bu dijital pasaportlar, tedarik zincirindeki her bir bileşenin kimliğini doğrulamak ve izlemek için kullanılmaktadır. Blokzincir teknolojisiyle desteklenen bu sistem, tedarik zincirindeki işlemlerin güvenli ve şeffaf olmasını sağlamaktadır. Dijital pasaportlar, ürünlerin üretim aşamasından son kullanıcıya ulaşana kadar tüm süreçlerini izlemekte ve her bir adımda doğrulama sağlamaktadır. Bu sayede, tedarik zincirindeki sahtecilik ve usulsüzlükler önlenmekte, ürünlerin kalitesi ve güvenilirliği artırılmaktadır. Ayrıca, bu sistem sayesinde Shell, tedarik zincirinde daha hızlı ve etkin bir yönetim sağlayarak operasyonel maliyetleri düşürmektedir.

Energinet, Danimarka'nın enerji şebekesi operatörü, Microsoft ile iş birliği yaparak blokzincir tabanlı bir enerji veri yönetim sistemi geliştirmiştir. Bu proje, enerji üretim verilerini blokzincir üzerinde güvenli bir şekilde kaydetmekte ve paylaşmaktadır. Dijital kimlikler, enerji üreticilerinin kimliklerini doğrulamak ve enerji verilerini izlemek için kullanılmaktadır. Bu sistem, enerji piyasasında şeffaflığı artırmakta ve veri güvenliğini sağlamaktadır. Energinet ve Microsoft'un bu iş birliği, enerji veri yönetiminde blokzincir teknolojisinin potansiyelini göstermekte ve enerji sektöründe yenilikçi çözümler sunmaktadır.

Energie Steiermark ve Power Ledger iş birliği ile Avusturya'da başlatılan SmartCommunity projesi, yerel enerji toplulukları arasında enerji paylaşımını ve ticaretini kolaylaştırmak amacıyla blokzincir teknolojisini kullanmaktadır. Proje kapsamında, kullanıcılar kendi ürettikleri fazla enerjiyi blokzincir tabanlı bir platform aracılığıyla diğer kullanıcılarla paylaşabilmekte ve ticaretini yapabilmektedir.

Bu süreçte dijital kimlikler, kullanıcıların kimlik doğrulama ve enerji işlemlerini güvenli bir şekilde gerçekleştirme süreçlerinde kritik bir rol oynamaktadır. Dijital kimlikler, her enerji kullanıcısının kimliğini doğrulamakta, enerji işlemlerini güvence altına almakta ve tüm işlemlerin şeffaf bir şekilde kaydedilmesini sağlamaktadır. Bu sayede, yerel enerji üretimi teşvik edilmekte, çevresel sürdürülebilirlik desteklenmekte ve enerji toplulukları arasında güçlü bir iş birliği sağlanmaktadır.

Yeni bir uygulama, merkezi olmayan enerji kaynakları ile şebeke arasındaki dijital kimlik trafiğini yönlendirmektedir. Bu uygulama, biyometrik veriler ve dijital kimlik teknolojilerini kullanarak enerji tüketicilerinin kimliklerini doğrulamakta ve enerji akışını optimize etmektedir. Biyometrik dijital kimlikler, kullanıcıların enerji tüketim profillerini güvenli bir şekilde kaydederek, kişiselleştirilmiş enerji çözümleri sunmaktadır. Bu sayede, enerji yönetimi daha verimli hale gelmekte ve kullanıcıların enerji maliyetleri düşmektedir. Ayrıca, biyometrik verilerin kullanılması, kimlik doğrulama süreçlerinde güvenliği artırmakta ve kullanıcıların enerji işlemlerini daha hızlı ve kolay bir şekilde gerçekleştirmelerini sağlamaktadır. Bu teknolojiler, enerji sektöründe verimlilik ve güvenliği artırmakta önemli bir rol oynamaktadır.

7.8. Dijital Kimliğin Benimsenmesi İçin Gerekli Olan Eğitim ve Tanıtımlar

7.8.1. Toplumsal Etkiler

Kapsayıcılık Artışı

- Herkesi Sistem Dahilinde Tutma: Dijital kimlik, özellikle kırsal kesimde yaşayan, fiziksel kimlik ofislerine erişimi zor olan ya da geleneksel yöntemlerle kimlik doğrulama yapamayan insanlar için önemli bir çözüm sunar. Örneğin, mobil cihazlarla erişilebilen dijital kimlik çözümleri sayesinde, herkes sosyal hizmetlerden yararlanabilir.

• Dijital Eşitsizliği Azaltma: Birçok ülkede dijitalleşme, teknolojiye erişimi olmayan bireyler için ciddi bir bariyer yaratabilir. Ancak dijital kimlik çözümleri, düşük maliyetli entegrasyon ve basitleştirilmiş erişim yöntemleriyle bu eşitsizliği azaltabilir. Kullanıcı odaklı tasarım, yaş ve teknolojik tecrübe fark etmeksizin herkesin bu hizmetlere erişimini kolaylaştırır.

Kolaylık ve Erişilebilirlik

• Hızlı İşlem Yapma İmkanı: Online işlemler sırasında sürekli belge yükleme, kimlik gösterme gibi adımların getirdiği zaman kayıplarını düşünün. Dijital kimlik; e-ticaret, sağlıklı işlemler ve devlet hizmetleri gibi birçok alanda süreçleri hızlandırır.

• 7/24 Erişim Sağlama: Kimlik doğrulama için geleneksel kurumların mesai saatleri sınırlı olabilir, ancak dijital kimlikler günün 24 saati kullanılabilir. Bu sayede bireyler, fiziksel kısıtlamaları aşarak istedikleri zaman ihtiyaç duydukları işlemleri gerçekleştirebilir.

Güvenlik ve Veri Yönetimi

• Fraud ve Kimlik Hırsızlığını Önleme: Güçlü şifreleme ve iki faktörlü kimlik doğrulama gibi önlemlerle dijital kimlikler, fiziksel kimliklere kıyasla daha güvenlidir. Veri ihlali ya da kimlik hırsızlığı gibi durumları minimuma indirir. Örneğin, Hindistan'daki Aadhaar sistemi, biyometrik veriyi kullandığı için kimlik doğrulama işlemlerinde yüksek güvenlik sağlar.

• Merkezi Olmayan Veri Depolama: Kullanıcıların kendi verilerini kontrol ettikleri ve sadece gerektiğinde paylaştıkları bir sistem, kişisel mahremiyeti artırır. Merkezi olmayan dijital kimlik çözümleri, bu konuda mükemmel bir örnek oluşturmaktadır.

7.8.2. Benimsenme Oranının Arttırılması için Gerekenler

Eğitici Kampanyalar Düzenlemek

• Farkındalık Yaratmak: Toplumun dijital kimliğin faydalarını anlaması, adaptasyonu kolaylaştırır. Sosyal medya, televizyon ve internet gibi kitle iletişim araçları kullanılarak bilgilendirici kampanyalar düzenlenebilir.

• Kullanıcı Deneyimini Gösterme: Basit adım adım kılavuzlar veya kullanıcı hikayeleri, dijital kimliğin nasıl kolaylık sağladığını açık bir şekilde göstermenin etkili yollarıdır.

• Güvenlik Konusundaki Endişeleri Gidermek: Kullanıcıların "Verilerim güvende mi?" veya "Bu teknoloji güvenli mi?" gibi soruları olabilir. Bu nedenle, dijital kimliğin arkasındaki güvenlik altyapısını sade ve anlaşılır bir dille anlatmak önemlidir.

Daha Erişilebilir Platformlar Tasarlamak

• Mobil Entegrasyonu Artırmak: Günümüzde çoğu kişinin ilk tercihi mobil cihazlar oluyor. Bu nedenle, dijital kimlik uygulamalarının mobil uyumluluğu kritik önem taşımaktadır.

• Teşvik Sağlama: Devletler, dijital kimlik kullanımı için teşvik edici avantajlar sunabilir. Örneğin, dijital kimlik kullananlara işlem harcı indirimi yapılarak daha fazla kişinin bu sisteme katılması sağlanabilir.

• Kullanımı Basitleştirmek: Dijital kimlik uygulamaları, karmaşık olursa kullanıcılar sisteme adaptasyon sağlayamaz. "Kullanıcı Dostu" bir arayüz ve adım adım rehberler sunarak adaptasyon hızlandırılabilir.

8. SONUÇ VE ÖNERİLER

Dijital kimlik ve belgelerde dijitalleşme, bireylerin, kurumların ve devletlerin dijital dönüşüm süreçlerinde kritik bir yere sahiptir. Ancak bu dönüşüm, kişisel verilerin korunması amacının gerçekleştirilmesi ve mahremiyetin sağlanması için sağlam bir hukuki ve teknik altyapıya ihtiyaç duymaktadır. Özellikle, dijital kimlik sistemlerinin güvenli, erişilebilir, kullanıcı dostu ve hukuk kurallarına uygun olması gerekmektedir. Uluslararası uygulamalar ve araştırmalar ışığında, dijitalleşme süreçlerinin sürdürülebilirliği için belirli adımlar atılması zorunludur.

Dijital kimliklerin başarılı bir şekilde hayata geçirilmesi için hukuki ve düzenleyici çerçevelerin gözden geçirilmesi güçlendirilmesi gerekmektedir. Türkiye'de mevcut düzenlemeler, mahremiyetin korunmasını hedeflese de, dijital kimlik ve belgeler konusunda teknolojinin hızlı gelişimine uyum sağlamak için sürekli güncellenmeye ihtiyaç duyabilecektir. Özellikle, Avrupa Birliği'nin eIDAS ve 2024/1183 sayılı düzenlemelerinden alınacak örneklerle, birlikte çalışabilirlik standartlarının geliştirilmesi ve ulusal mevzuatın uluslararası standartlarla uyumlu hale getirilmesi önemlidir.

Kişisel verilerin korunması açısından, KVKK ve GDPR çerçeveleri temel referans noktaları olarak kalmalıdır. Ancak, bu çerçevelerin uygulamadaki etkinliği artırılmalı ve denetim mekanizmaları daha kapsamlı hale getirilmelidir. Örneğin, dijital kimlik sistemlerinde veri minimizasyonu, şeffaflık ve veri sahibinin kontrol hakları eksiksiz şekilde uygulanmalıdır. Ayrıca, KVKK kapsamında biyometrik veriler gibi hassas kişisel verilerin işlenmesine ilişkin özel düzenlemeler yapılmalı ve uygulamada yaşanan zorluklar giderilmelidir.

Dijital kimlik sistemlerinin güvenilirliğini artırmak için, siber güvenlik önlemleri ön planda tutulmalıdır. Sistemlerin güvenlik açıkları veya kötüye kullanım riskini minimize etmek için güçlü şifreleme yöntemleri, çok katmanlı güvenlik mekanizmaları ve düzenli sızma testleri yapılmalıdır. Ayrıca, blokzincir gibi yenilikçi teknolojilerden faydalanarak, kimlik doğrulama süreçlerinin güvenliği ve şeffaflığı artırılabilir.

Kullanıcı farkındalığının artırılması, dijital kimliklerin benimsenmesinde kritik bir diğer unsurdur. Vatandaşlar, dijital kimlik sistemlerinin nasıl çalıştığı, kişisel verilerinin nasıl korunduğu ve bu sistemleri güvenli bir şekilde nasıl kullanabilecekleri konusunda bilgilendirilmelidir. Kamu ve özel sektörün ortaklaşa düzenleyeceği eğitim programları ve farkındalık kampanyaları, bu süreçte büyük bir rol oynayacaktır.

Son olarak, çok paydaşlı bir iş birliği mekanizması oluşturulmalıdır. Kamu kurumları, özel sektör, akademi ve uluslararası kuruluşlar, dijital kimlik ekosisteminin geliştirilmesi için koordinasyon içinde çalışmalıdır. FATF ve OECD'nin vurguladığı gibi, AML/CFT gereklilikleri ile veri koruma ve gizlilik standartlarının uyumlu hale getirilmesi, bu sistemlerin güvenilirliğini artıracak ve daha geniş bir kullanıcı kitlesi tarafından benimsenmesini sağlayacaktır.

Dijital kimlik ve belgelerde dijitalleşmenin sağladığı fırsatlar, bireylerin mahremiyetine ve verilerinin güvenliğine olan hassasiyetle dengelenmelidir. Bu doğrultuda, Türkiye'nin dijital dönüşüm hedeflerine ulaşabilmesi için, hukuki ve teknik altyapının güçlendirilmesi, kullanıcıların güveninin sağlanması ve uluslararası iyi uygulamalardan faydalanılması kritik önem taşımaktadır. Bu yaklaşım, yalnızca ulusal düzeyde değil, küresel dijital ekosistemde de Türkiye'yi önemli bir konuma taşıyacaktır.

9. KAYNAKÇA

Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Ap- plication Platform. 2014. URL: https://github.com/ethereum/wiki/wiki/White-Paper.

Daniel Macrinici, Cristian Cartofeanu, and Shang Gao. “Smart contract applications within blockchain technology: A systematic mapping study”. In: Telematics and Informatics 35.8 (2018), pp. 2337–2354. DOI: https://doi.org/10.1016/j.tele.2018.10.004.

J. Frankenfield, “51% attack,” Investopedia, 2019.

J. L. Zhao, S. Fan, and J. Yan, “Overview of business innovations and research opportunities in blockchain and introduction to the special issue,” Financial Innov., vol. 2, no. 1, pp. 1–7, Dec. 2016.

Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. Future Gener. Comput. Syst. 2020, 107, 841–853.

Alajlan, R.; Alhumam, N.; Frikha, M. Cybersecurity for Blockchain-Based IoT Systems: A Review. Appl. Sci. 2023, 13, 7432.

Andryukhin, A.A.. (2019). Phishing Attacks and Preventions in Blockchain Based Projects. 15-19. 10.1109/EnT.2019.00008.

Shijie Zhang and Jong Hyouk Lee. “Double-Spending with a Sybil Attack in the Bitcoin Decentralized Network”. In: IEEE Transactions on Industrial Informatics 15.10 (2019), pp. 5715–5722. DOI: 10.1109/TII. 2019.2921566.

I. Riadi, R. Umar, I. Busthomi and A. W. Muhammad, "Block-hash of blockchain framework against man-in-the-middle attacks", Register: Jurnal Ilmiah Teknologi Sistem Informasi, vol. 8, no. 1, pp. 1-9, 2022.

P. Ekparinya, V. Gramoli and G. Jourjon, "Impact of man-in-the-middle attacks on ethereum", 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS), pp. 11-20, 2018.

Faizi, Azeem & Mustafa, Khurram. (2024). Mitigating Blockchain Endpoint Vulnerabilities: Conceptual Frameworks. International Journal of Computer Networks and Applications. 11. 933-953. 10.22247/ijcna/2024/56.

A. Kumar, B. Kumar Sah, T. Mehrotra and G. K. Rajput, "A Review on Double Spending Problem in Blockchain," 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2023, pp. 881-889, doi: 10.1109/CISES58720.2023.10183579.

X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen A survey on the security of blockchain systems, Future Generat. Comput. Syst., 107 (June 2020), pp. 841-853 [accessed Jul 09 2024].

BCTR Dijital Kimlik Raporu, Erişim Tarihi:Nisan 2019

Decentralized Identifiers (DIDs) v1.0, Erişim Tarihi: Temmuz 2024

Verifiable Credentials Data Model v1.1, Erişim Tarihi: Temmuz 2024

OpenID4VCI, Erişim Tarihi: Temmuz 2024

OpenID4VP, Erişim Tarihi: Temmuz 2024

DIGITAL IDENTITY STANDARDS, Analysis of standardization requirements in support of cybersecurity policy, ENISA, July 2023

European Data Protection Supervisor, Where are we heading with digital identities,

Konstantin Schaarschmidt, Data protection and data security in the context of digital identities

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2).

Nikhil Ghadge. (2024). Digital Identity in the Age of Cybersecurity: Challenges and Solutions. London Journal of Research In Computer Science and Technology, 24(1), 1–10. Retrieved from https://journalspress.uk/index.php/LJRCST/article/view/1023

Mary-Jane Sule, Marco Zennaro, Godwin Thomas, Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends, Technology in Society,Volume 67, 2021, https://doi.org/10.1016/j.techsoc.2021.101734.

The security and privacy features of the EU Digital Identity Wallet,

UNDP, Drafting Data Protection Legislation, Global Frameworks, Reimagining Digital ID INSIGHT REPORT JUNE 2023,

World Bank, DIGITAL ID AND THE DATA PROTECTION CHALLENGE2 October 2019,

OECD, Recommendation of the Council on OECD Legal Instruments the Governance of Digital Identity,

WEF, Digital Identity Module, https://widgets.weforum.org/blockchain-toolkit/digital-identity/index.html

31 Ocak 2015 Cumartesi Resmî Gazete Sayı : 29253

T.C. Resmî Gazete, 15 Mart 2020, Sayı : 31069

Elektronik Bankacılık Hizmetlerinde ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasında Kimlik Doğrulama ve İşlem Güvenliği için Sağlanması Gereken Kriterler Hakkında Genelge Sayı: 77574904-010.06.02

T.C. Resmî Gazete, 1 Nisan 2021, Sayı : 31441

T.C. Resmî Gazete, 25 Mayıs 2023, Sayı : 32201

e-Residency of Estonia. (n.d.). Retrieved from

Marr, B. (2019, January 21). Estonia's e-Residency: Redefining Citizenship in a Digital Age. Forbes. Retrieved from Forbes

UIDAI (Unique Identification Authority of India). (n.d.). Retrieved from

How Blockchain Could Improve India's Aadhaar System. (2018, September 22). The Economic Times. Retrieved from Economic Times

Blockchain Can Transform Notary Services in Brazil. (n.d.). Cointelegraph. Retrieved from Cointelegraph

Dubai Courts and Blockchain: A New Era of Legal Transparency. (2019, November 17). Zawya. Retrieved from Zawya

Blockchain Used in Sierra Leone's Election for the First Time Ever. (2018, March 15). TechCrunch. Retrieved from TechCrunch

Moscow's Blockchain Voting Platform Fails, Attracts Just 1,500 Users. (2019, September 11). CoinDesk. Retrieved from CoinDesk

Dubai Aims to Be the World's First Blockchain-Powered Government. (2017, April 25). World Economic Forum. Retrieved from WEF

Toronto Explores Blockchain Technology for Municipal Services. (2019, March 28). The Globe and Mail. Retrieved from The Globe and Mail

Nasdaq and SEB Partner on Blockchain for Mutual Funds. (2017, September 27). Finextra. Retrieved from Finextra

IBM and SecureKey Partner for Blockchain-Based Digital Identity System. (2017, March 20). IBM. Retrieved from

Think Digital Partners. (2024). How Digital Twin Powered Graph Technology Keeps London Moving. Retrieved from https://www.thinkdigitalpartners.com/news/2024/05/09/how-digital-twin-powered-graph-technology-keeps-london-moving/

Think Digital Partners. (2023). Digital Identity Global Roundup. Retrieved from https://www.thinkdigitalpartners.com/news/2023/01/23/digital-identity-global-roundup-99/

Think Digital Partners. (2019). Now You Can Fly Paperless Between Canada and the Netherlands. Retrieved from https://www.thinkdigitalpartners.com/news/2019/07/03/now-you-can-fly-paperless-between-canada-and-the-netherlands/

Think Digital Partners. (2023). Digital Identity Global Roundup. Retrieved from https://www.thinkdigitalpartners.com/news/2023/05/30/digital-identity-global-roundup-117/

Google Drive. Blockchain in Logistics and Transportation. (11. Madde, Sayfa 81-88). Retrieved from https://drive.google.com/file/d/1reY0wxfMIfrDPsOP-sPIrnbgt5DReHuP/view

Astarita, V., Giofrè, V. P., Mirabelli, G., & Solina, V. (2020). A Review of Blockchain-Based Systems in Transportation. Information, 11(1), 21. doi:10.3390/info11010021

Subramanian, N., Chaudhuri, A., & Kayıkcı, Y. (2020). Blockchain Applications and Future Opportunities in Transportation. In: Blockchain and Supply Chain Logistics. Palgrave Pivot, Cham. doi:10.1007/978-3-030-47531-4_5

Stanford Online. Blockchain use cases in the supply chain. Retrieved from https://online.stanford.edu

Built In. (2024). 37 Top Blockchain Applications to Know for 2024. Retrieved from https://builtin.com/blockchain/blockchain-applications

Dock.io. (2024). Blockchain Identity Management: Complete Guide 2024. Retrieved from https://www.dock.io/blog/blockchain-identity-management

Deloitte Insights. (2024). Blockchain trends. Retrieved from https://www2.deloitte.com/insights/us/en/focus/tech-trends.html

IBM. (2024). Blockchain for Digital Identity and Credentials. Retrieved from https://www.ibm.com/blockchain-identity

Faizi, Azeem & Mustafa, Khurram. (2024). Mitigating Blockchain Endpoint Vulnerabilities: Conceptual Frameworks. International Journal of Computer Networks and Applications. 11. 933-953. 10.22247/ijcna/2024/56.

A. Kumar, B. Kumar Sah, T. Mehrotra and G. K. Rajput, "A Review on Double Spending Problem in Blockchain," 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES), Greater Noida, India, 2023, pp. 881-889, doi: 10.1109/CISES58720.2023.10183579.

X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen A survey on the security of blockchain systems, Future Generat. Comput. Syst., 107 (June 2020), pp. 841-853 [accessed Jul 09 2024].

BCTR Dijital Kimlik Raporu, Erişim Tarihi:Nisan 2019

Decentralized Identifiers (DIDs) v1.0, Erişim Tarihi: Temmuz 2024

Verifiable Credentials Data Model v1.1, Erişim Tarihi: Temmuz 2024

OpenID4VCI, Erişim Tarihi: Temmuz 2024

OpenID4VP, Erişim Tarihi: Temmuz 2024

DIGITAL IDENTITY STANDARDS, Analysis of standardization requirements in support of cybersecurity policy, ENISA, July 2023

European Data Protection Supervisor, Where are we heading with digital identities,

Konstantin Schaarschmidt, Data protection and data security in the context of digital identities

Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2).

Nikhil Ghadge. (2024). Digital Identity in the Age of Cybersecurity: Challenges and Solutions. London Journal of Research In Computer Science and Technology, 24(1), 1–10. Retrieved from https://journalspress.uk/index.php/LJRCST/article/view/1023

9. KATKI SAĞLAYANLAR

Alev Orbay
Ali Akarçay
Alican Şahin
Arda Ata
Aykut Şahin
Ayşe Keleş
Barbaros Büyükyılmaz
Belamir İrem Acar
Bengisu Özgehan
Berkay Doğan
Berke Bayhoca
Berke Sohtaoğlu
Berna Elyıldırım
Burcu Sakız
Burcu Tümer
Burçin Bozkurt Günay
Cansu Yaşar
Cemal Enis Ös
Erhan Yılmaz
Erman Mutlu
Erol Alkan
Ersin Yılmaz
Esra Özdemir
Gökhan Polat
Göksel Doğan
İlayda Aydın
İskender Kalkan
Macit Mete Oğuz
Mahir Kubilay Dağlı
Mehmet Yasin Akpınar
Meltem Erdem
Merve Akgün Sarı
Murat Güç
Mustafa Öztürk
Mustafa Serdaroğlu
Dr. Mustafa Takaoğlu
Naz Büke Bolluk
Necati Keskin
Nesrin İlker Peker
Ogün Sarıer
Oktay Adalıer
Onur Çakır
Onur Köse
Ozan Eğe
Özlem Aydın Bulut
Pınar Çağlayan Aksoy
Sadettin Kerim
Selin Pekmezci
Taner Dursun
Tolga Ünal
Umut Can Erten
Vedat Güven
Yalçıncan İkin
Yiğit Akkoyunlu

BLOCKCHAIN
TÜRKİYE

DİJİTAL KİMLİK SİSTEMLERİ VE SEKTÖREL ETKİLERİ RAPORU

On-Chain
Çalışma Grubu

HAZİRAN 2025

TBV
TÜRKİYE BİLİŞİM VAKFI