Why Digital ID ?

Taner Dursun

2. Uusal Blokzincir Çalıştayı, İstanbul, 2019

Dijital Kimlik Nedir

Dijital Kimlik (Digital Identity)

- 5490 sayılı Nüfus Hizmetleri Kanunu. Madde 3(r)
  - Kişinin Türk vatandaşı olduğunu ve aile kütüğüne kayıtlı bulunduğunu gösteren TC kimlik kartı,
- Kimlik kartı niteliğinde olmamakla birlikte, bireyi diğer kişilerden ayırma ve tanıtma işlevi sunan ve dijital kimliğinizi oluşturan veriler

- KVKK Madde 3
  - kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
  - yalnızca bireyin adı, soyadı, doğum tarihi ve doğum yeri gibi onun kesin teşhisini sağlayan bilgiler değil, aynı zamanda kişinin fiziki, ailevi, ekonomik, sosyal ve sair özelliklerine ilişkin bilgileri de kapsar

Kişisel veri

- Kişisel veri (personal data) - Kimlik öznitelikleri (identity attributes):
  - Bütün öznitelikler kişisel verilerdir
  - Ama bütün kişisel veriler öznitelik olmayabilir (adres)

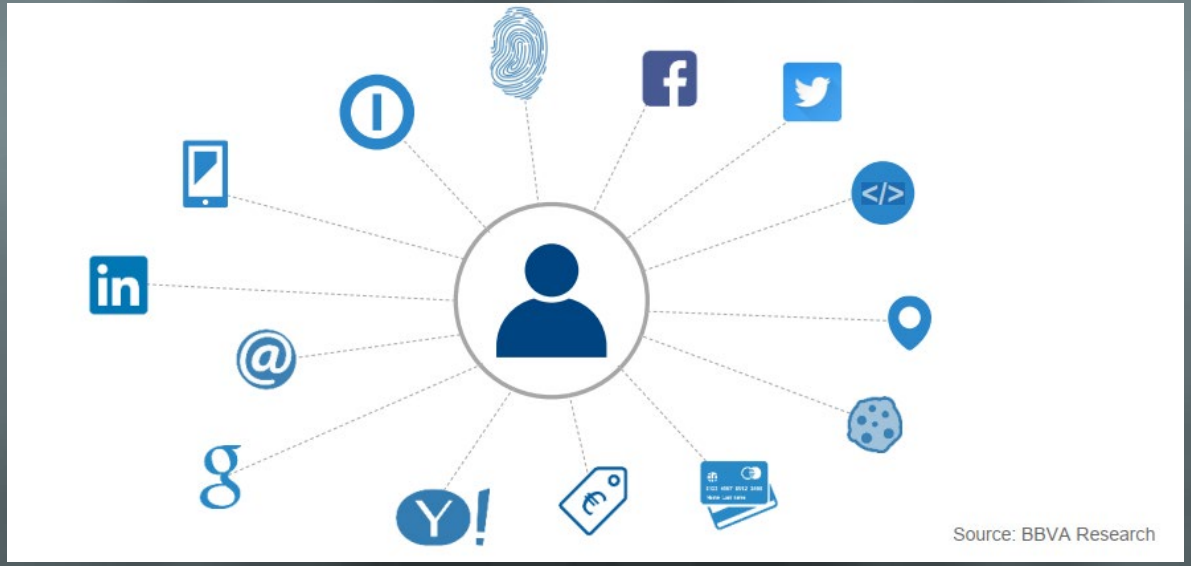
- Kişisel verilerin paylaşımı (güvenli, kontrollü, mahremiyetle) dijital kimlik için kritik bir konudur

Dijital Kimlik

- ITU : “representation of an entity in the form of one or more attributes that allow entity(ies) to be sufficiently distinguished within context.”
- ISO: “item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has a recognizably distinct existence.”
- WEF: “collection of individual attributes that describe an entity and determine the transactions in which that entity can participate”
- WB: kimlik ibraz ve ispatında kullanılabilecek elektronik olarak toplanan, saklanan ve doğrulanabilen, kişiye ait kimlik bilgilerinin tamamı

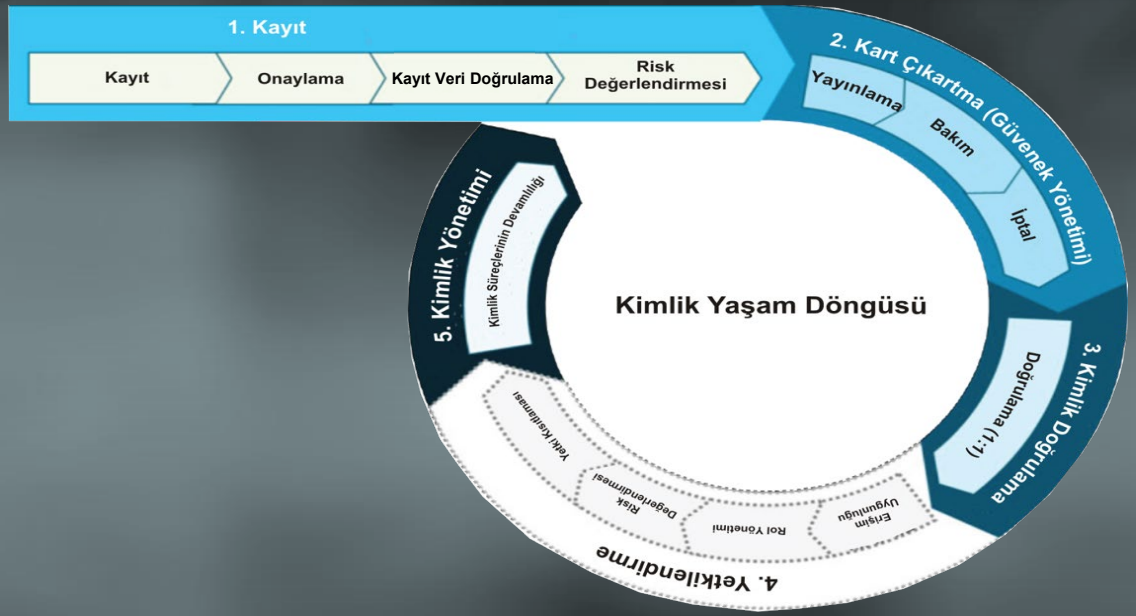
Dijital Kimlik

- Öznitelik tipleri
  - Doğal (age), Kalıtsal (behaviour) ve Atanmış (ID)



Dijital Kimlik Yönetimi Önemi, Faydaları
Değişim tetikleyicileri

Kimlik yönetimi



kişinin yaşam süresini, ölümünden sonraki dönemi kapsayan, kimlik doğrulama süreçlerinde kullanılan kişiye ait öznitelik bilgilerin belirli otoriteler tarafından verilmesi veya atanmasını içeren döngüdür

Technology Landscape for Digital Identification, 2018 - World Bank Group.

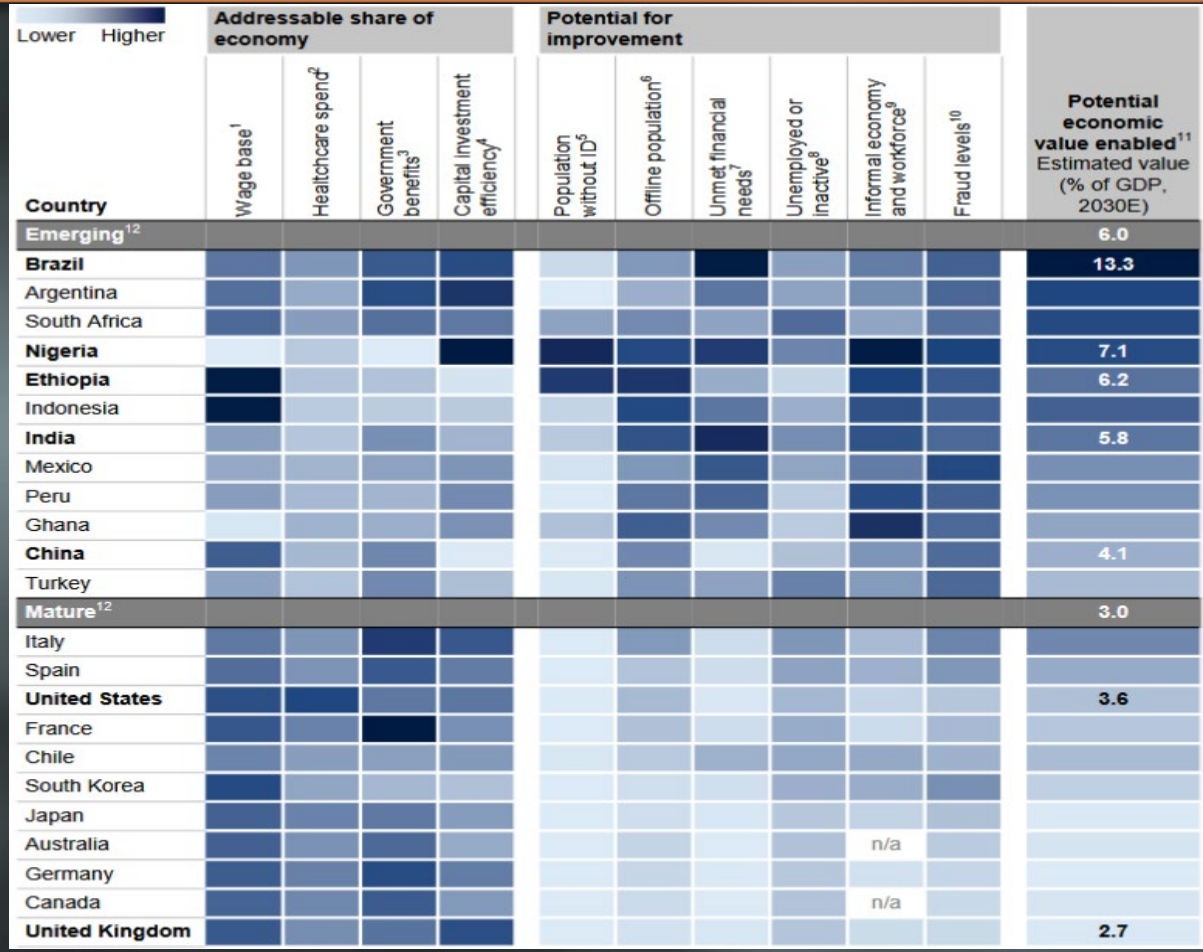
Dijital Kimlik Yönetimi (Identity Management Systems)

- Kullanıcı kimliklerini dijital ortamlarda, sağlamak, doğrulamak (authentication), yetkilendirmek (authorisation) ve veri paylaşımını yönetmek
  - Basit Dijital ID kimlik doğrulamaya izin verir
  - Gelişmiş Digital ID, ID sahibi birey hakkında daha detaylı bilgileri ilişikili depolamaya ve kullanıcı rızasına dayalı gelişmiş veri paylaşımına, yetki kontrolü ile çevrimiçi süreçlere katılıma olanak sağlar

- Geleneksel IDMS yöntemleri ile hayat sürüyor
  - Merkezi ve Federe yapılar
  - Yönetici/Aracı kurumlar

Dijital Kimliğin ve Yönetiminin oluşturacağı değer

- GSYİH'nın %3 - %13 arasında ekonomik değer oluşturma potansiyeli (2030)
  - Ekonomik akışların daha formal hale gelmesi
  - Bireylerin hizmetlerin içine daha fazla dahil edilmesi
  - Yüksek güven gerektiren hassas etkileşimlerin dijitalleşmesi
  - Hız, Maliyet, güvenlik, şeffaflık kazanımları
- Gelişmekte olan ülkelerde daha fazla %6, gelişmişlerde %3
- Ülkeden ülkeye etkisi farklı
  - Mevcut dijital ID altyapısı
  - Ülkenin süreçlerinin karakteristiği
  - Ekonomide dijitalleşmeye müsait alan (addressable share)
  - Süreçlere katma, dijitalleşme ve ID kapsama alanı

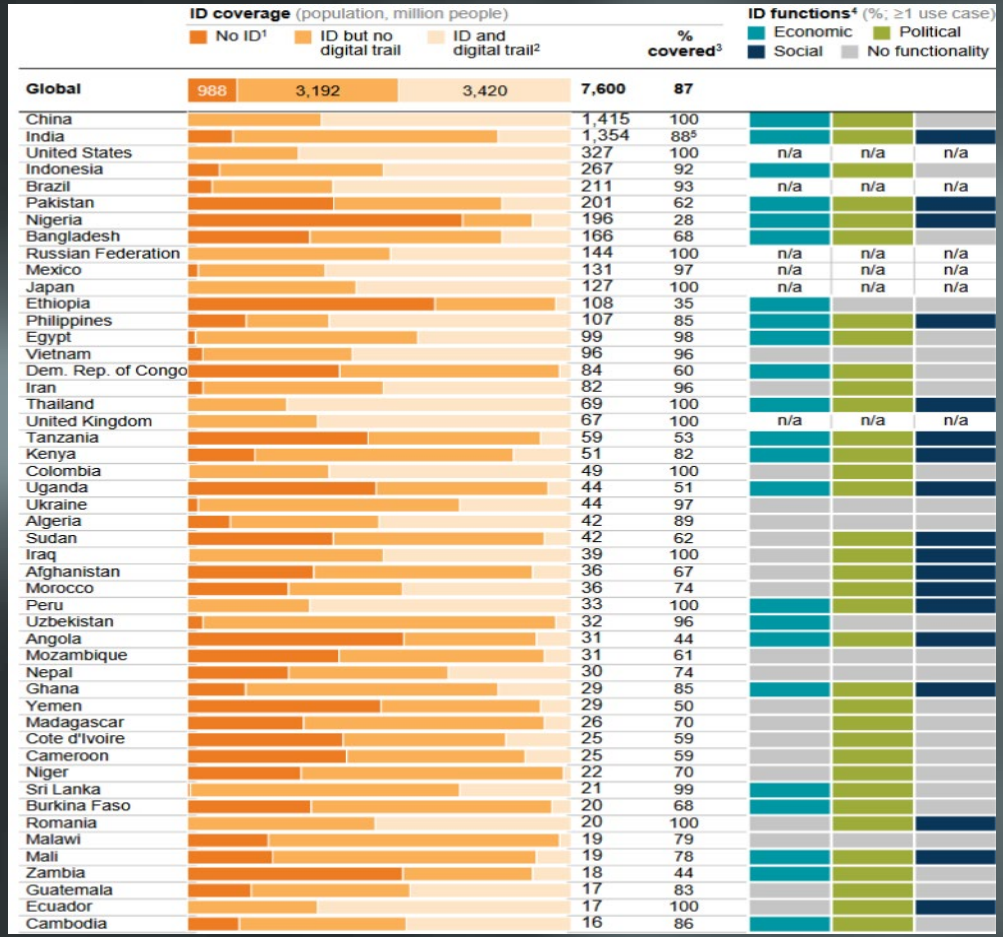


DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH, McKinsey, Jan 2019

- **1 milyar** kimliğini ispat edemiyor
  - digital ID ile kritik devlet ve ekonomik hizmetlere dahil olabilme

- **3.2 milyar için**
  - Zaten dijital ID var
  - Daha detaylı kullanıcı kontrolü, mahremiyet, online servislerde

- **3.4 milyar için (ID and digital trail):**
  - digital ID programların artması
  - DigitalID'nin doğrulamada kullanılabildiği digital altyapı ve uygulamalar oluşturma,
  - Dijital etkileşimlere katılım ve verimlilik
  - e-devlet ve gelişmiş kişisel veri paylaşımı, such as medical data
  - Zaman tasarrufu, Düşük maliyet, Güvenlik, Şeffaflık



Geleneksel IDMS sorunları

- Güvelik ve mahremiyet (bilgileri kontrol edenin ayrıcalıkları nedeniyle)
  - Merkezi veri depoları, siber saldırıları cezbeder, Artan saldırılar
  - İhtiyaç duyulandan fazla bilgi paylaşmak
  - Bilgileri açık paylaşmaktan doğan güvenlik zaafiyeti
  - Gerekenden fazla bilgi paylaşmak
- Arıza Darboğaz noktası (Single points of failure), ölçeklenebilirlik sorunları
  - İhtiyaç duyulan bilgiye bazen/hemen erişememek
  - Aktör sayısı ve veri miktarı hızla artıyor (Bireyler, kurumlar ve Cihazlar)
  - Sınırlı tipte kimlik bilgisi paylaşımına ve doğrulamasına izin verir
  - Geri kalanları fiziksel olarak paylaşmak zor, güvenli değil, yavaş
- Birlikte çalışabilirlik (Interoperability)
  - Dokümantasyon, çoklu işlem veya fiziksel eylemin zahmeti ve zaman kaybı
  - Her yeni servise en baştan kimlik kanıtlama gerekliliği
  - Ayrı veritabanları, bilgi paylaşımını ve veri tutarılığını sağlamayı zorlaştırır
  - Verilere bütünleşik bakmak gereken senaryolara uygun olmayabilir

Geleneksel IDMS sorunları

- Veriler üzerinde kontrol
  - Bireyler, kendilerini kendi verilerinin kontrolüne sahip olmadığını düşünüyor
  - Toplanılan, paylaşılan bilgilerin akıbetinin ve saklanma süresi/koşullarının bilinmemesi
- Yönetim zorluğu ve maliyetleri
  - Saklanması ve taşınması gereken çok sayıda kimlik belgesi olması
  - Artan veri ve Karmaşıklaşan süreçler
  - Artan işletme maliyetleri

Diğer motivasyonlar

- Dijitalleşmenin getirdiği imkanlardan azami fayda sağlama motivasyonu
- Kişilerin çok fazla yerde kendilerini tanımlamaları ihtiyacı artıyor. Parçalılık ve entegrasyon ihtiyacı artıyor
- Yaygınlaşan dijitalleşme, başka süreçlerin de dijitalleşmesini mümkün kılıyor
- Artan entegrasyon ihtiyaçları (IoT, enterprise ID)

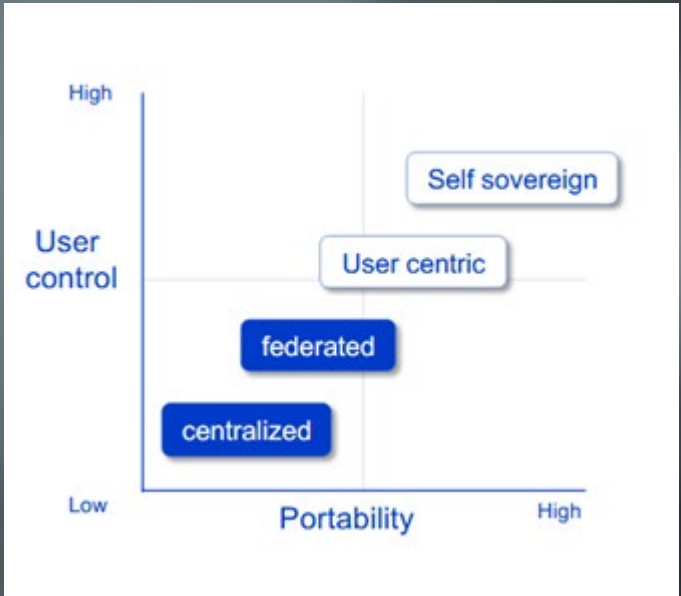
Diğer motivasyonlar
Artan Kişisel Veri ve Mahremiyet Regülasyonları

- Veri koruma kanunları, dijital kimliği yoğun olarak etkiler
- Regulasyonlar bireyleri güçlendiriyor, bilinçlendiriyor

- Ulusal kimlik sistemleri ve ülke içi kanunların yanı sıra uluslararası kanunlar
  - Avrupa eIDAS Regulation, üye ülkelerin, diğerlerinin kimliklerini tanıması
- EU GDPR (General Data Protection Regulation),
  - Hem fiziksel hem de dijital kimlik yönetiminde bireylerin kendi verilerini kontol edebilmesi,
  - En önemlileri: right to access, right to be forgotten, right to portability and right to data minimization
- ABD, California Consumer Privacy Act
- Filipinler, Data Privacy Act of 2012
- Güney Kore, Personal Information Protection Act

- Türkiye,
- 6698 sayılı Kişisel Verilerin Korunması Kanunu (**KVKK**), Nisan 2016, Türkiye
- 30224 sayılı ve 28 Ekim 2017 tarihli, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

Yeni Nesil Digital ID Yönetim (IDMS) Modelleri



- Kullanıcı rızası
- Taşınabilirlik
- Üçüncü taraflara bağımlı olmamak
- Güvenlik

Yeni Nesil Digital ID Yönetim (IDMS) Modelleri

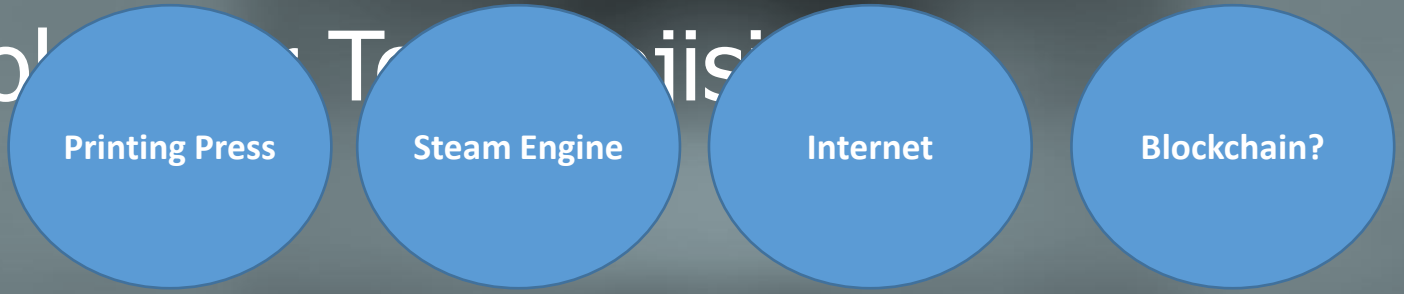
- Çözüm arayışları sürerken Blokzincir teknolojisi ortaya çıktı
- Blokzincir tabanlı IDMS, çözüm olarak adreslenmesi gecikmedi
    - Güvenlik, Mahremiyet, Hız,

Blokzincir nedir ve dijital ID yönetimi için önemi

Dijital Kimlik - Blokzincir ilişkisi

Yıkıcı teknoloji

Blo[illegible] T[illegible]jisi



* Strategy Paper On Blockchain

Blokzincirin Özellikleri

- Verileri izinsiz değiştirilmeye karşı korur
- Ademi merkezi yapıyla verilerin doğruluğuna, tutarlılığına güven sağlar
- Verinin erişilebilirliğini arttırmakta, paylaşımını kolaylaştırmaktadır
- Şeffaflık sağlar
- Birbirine güvenmeyen sistemlerin birlikte çalışmasına olanak sağlar

Blokzincirin IDMS için önemi

- Doğasındaki kontrol ve rıza (consent) özellikleri ile yeni veri sahipliği ve veri yönetişimi modellerini destekleyebilir. (Bireyler/kurumlar ve mahremiyet lehine)
- Bireylerin, kendi verilerini kontrol edebilmesini ve arzu ettikleri kişi/kurumlarla paylaşabilmesine olanak sağlar
- Dağıtık mimaride olduğu için kesinti olasılığı minimize edilir
- Geleneksel kimlik sağlayıcılara bağımlılığı azaltır.
- Kurumlar, bir sistem altyapısını işletme, kullanıcı verilerini depolama zahmeti olmaksızın süreçlerini, doğrulanmış kullanıcı bilgileri üzerine inşaa edebilir

Blokzincirin IDMS için önemi

- DKMS (ademi merkezi anahtar yönetimi) ve doğrulanabilir veriler (verifiable credentials) ile birleştirilen blokzincir, kullanıcı egemen kimlik modeline izin verebilir
- Güvenlik, ölçeklenebilirlik ve dayanıklılık özelliklerine güvenir.
- Kendi güvenlik ve mahremiyet özellikleri henüz sıkı analizlerden geçmiş değildir
- Gelecek vaadeden bir alan
- Çok sayıda blockchain-tabanlı kimlik yönetim modeli halen geliştiriliyor ve ticarileşiyor.

Dijital Kimlik ve Blokzincir Uygulama alanları ilişkisi


Blockchain
(Use Cases)
Source: GrowthPraxis
Proof of ownership and a marketplace for sales and purchase of digital assets
Company: MyPowers
Enables authenticity of a review through trustworthy endorsements for employee peer review
Company: TRST.im
Decentralized prediction platform for the share markets, politics etc
Company: Augur
Decentralized patient records management
Company – BitHealth (Healthcare IT)
Proof of ownership for digital content
Arts, pictures and images
Companies: Blockai, Bitproof, ascribe, Artplus
Other companies: Chainy.Link, Stampery
Digitizing assets: Improves anti-counterfeit measures
Consumer electronics, Automotive
Companies: The Real McCoy, ChainLink
Other companies: Everpass, BlockVerify
Degree Verification
Company: Degree Of Trust
Provides digital identity that protects consumer privacy
Internet, car locks: Onename
Customer identification: Trustatom
Elections Voting: Follow My Vote
Enables authenticity of a review
Helps users engage, share reputation and collect feedback
Company: The World Table
Through trustworthy endorsements
Company: Asimov
Decentralized internet and computing resources to every home and business
Company: ePlug
Digitizing company incorporations, transfer of equity/ownership and governance
Company: Otonomos
A smart contract IT portal executing order fulfilment in ecommerce/manufacturing
Company: UbiMS
Escrow/Custodian service
Gaming industry
Companies: PlayCoin, Bitnplay
Gaming industry and loan servicing
Company: New System Technologies
E-commerce
Company: Fundrs.org
Provides digital identity that protects consumer privacy
Companies: Sho Card, Uniquid
Decentralized IoT
Home automation: Chimera-inc.io
Industries: Filament
Decentralized storage using a network of computers on blockchain
Company: Storj
Digitization of documents/contracts and proof of ownership for transfers
Company: Colu (Colored Coins)
Digital security trading: ownership and transfer
Companies: Symbiont, Mirror, Spritzle, Secure Assets, BitShares, Coins-e, equityBits, DXMarkets, MUNA
Points based value transfer for ride sharing
Company – La'Zooz
Proof of ownership for digital content storage and delivery
Companies: Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN
Proof of ownership of modules in app development
Company: Assembly

- Blokzincir tabanlı Dijital ID Yönetim sistemi
  - Blokzincir için spesifik bir uygulama alanı mıdır ←EVET
  - Diğer blokzincir uygulama alanlarının (hepsini yatayda kesen) eksiklerini giderecek eksik parça mıdır? ←HENÜZ DEĞİL
    - Diğer blokzincir uygulamalarında gerçeklenecek süreçleri tamlama, transaction bağlantılandırma
    - Kripto paralarda, KYC, AML regülasyonları, STO ile kullanım
    - Blockchain yönetişiminde kullanım

Mevcut durum ve eksikler

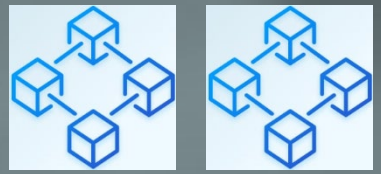
- Entegrasyon
  - Şimdilik Second Layer (off-chain) protokollerle
    - Ethereum tabanlı registries
    - Hyperledger Indy tabanlı çözümler
  - Entegrasyon iddiası
    - Cordentity Bridge
      - R3 Corda + Identity
      - Private Ledger düğümlerinde Credential işleme, issue etme yeteneği sağlayan CorDapp
- Mahremiyet konuları
  - On-chain DIDs, korelasyon riskleri
- Kullanıcı tarafında
  - Güvenli Kimlik Cüzdanları (diğer blokzincir uygulamalarını da destekleyen)
  - Kullanım kolaylığı
- Standartların gelişmesi (On-chain, off-chain)
- Mevcut dijital kimlik yapılarını da dışlamayan çözümlerin araştırılması

Mevcut durum ve eksikler

- **Universal Wallets*:***
  - Farklı mimari, bileşenler ve standartlar (Örneğin, ERC-1056, ERC-780, ERC-725, ERC-734, ERC-735), kripto para ve diğer dijital mülklerin de tutulabildiği, kullanıcı egemen kimlik cüzdanlarının geliştirilmesini, birlikte çalışmasını kolaylaştırabilir
  - Mutemet/Vekil cüzdanlar: üçüncü tarafların, bireylere ait bilgileri kontrol etmesine izin verebilir.
  - Secret sharing, threshold cryptograhy gibi teknolojilerin, biometrik bileşenlerle birlikte kullanılarak cüzdan güvenliğinin artırılması

IDMS'in diğer blokzincirle entegrasyonu

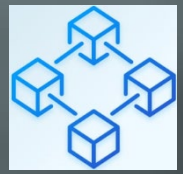
Universal DID Resolver



Cordentity, Hyperledger Indy yeteneklerine erişebilen Corda smart Contract (Corda ledger transactions Indy credentail ile bağlantılandırılabilir)

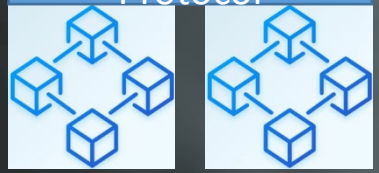
SecureKey Verified.me Hyperledger Fabric-based IDMS → Indy

Güvelik ve mahremiyet konuları



Birden fazla uygulama uzayına hizmet eden IDMS blokzincir

Second Layer Protocol



Blokzincir ile Dijital Kimlik çözme girişimleri, projeleri, dünyadaki ve ülkemizdeki durum

- Dünyadaki projeler
- Gelişen standartlar ve altyapılar

Blokzincir tabanlı IDMS projeleri

- Estonia (for electronic medical records),
- İsviçre, City of Zug, (UPort and ti&m) (Ethereum blockchain)
- Kanada, British Columbia ve Ontario şehirleri, Verifiable Organizations Network trusted şebeke(Sovrin blockchain).
  - The OrgBook, public verifiable business credential
- Finlandiya, TrsutNet
- İspanya, Alastria
  - Kar amacı gütmeyen konsorsiyum, ulusal blokzincir ekosistemi, SSI
- US, Illinois blockchain initiative
  - Doğum kayıt pilot projesi, SSI DIDs ve devlet ajansı doğrulanabilir dijital belge yayımlar (isim, cinsiyet, doğu tarihi, kan grubu)
- Sovrin, Global
- Belçika, Blockchain on the Move (Antwerp, Belgium)
  - Belediye hzimetleri seviyesinde SSI pilot projesi, devletin yayınladığı Doğrulaanbilir Belgelerin kullanımı.

Blokzincir tabanlı IDMS platformları ve altyapıları

- Uport (Ethereum)
- CIVIC (Ethereum)
- ShoCard (Bitcoin)
- Indy
- Sovrin (Indy)
- Verified.Me (Fabric)

Gelişen standartlar

- Standartlar, blockchain-based IDMSs :
  - Decentralized Identifiers and Verifiable Credentials (W3C)
  - Open Badges (Mozilla ve IMS Global)
  - Universal Resolver and Identity Hubs (Decentralized Identity Foundation (DIF)
  - Ethereum Request for Comments (ERCs)

Karşı görüşler ve sorunlar

Digital ID Karşı görüşler

- Faydalı ve Kötü amaçlı kullanılabilen teknoloji (Nükleer enerji, GPS gibi)
  - Örneğin, kullanıcı davranışları hakkında bilgi toplamak
- Kendi verilerinin kontrolünü almak istemeyen bireyler
- Kullanım zorlukları, kullanıcı hatalarından kaynaklı zaafiyetler
- Gizli ajanda eleştirileri
  - Dünya vatandaşlığı, devletlerin otoritesini zayıflatma, Kimlik ve bilgi hırsızlığının önünü açmak

Karşı görüşleri ve riskleri önlemek için yapılabilecekler

- Mahremiyet odaklı, kullanıcı egemen kimlik yönetimi
- Kullanıcıların yükümlülüklerini paylaşan Mutemet/Vekil mekanizmalarının geliştirilmesi
- Kullanım zorluklarını azaltıcı istemci taraf teknolojileri
- Dünya vatandaşlığı, devletlerin otoritesini zayıflatmak
  - Ülke çapında bir milli sistem
  - Otorite tarafından denetlenebilir nitelikte
  - Uluslararası sistemlerle birlikte çalışabilirlik için eklentiler, kontrollü ve ana omurgadan farklı bir sistem üzerinden

Çalıştay ana teması olarak seçme nedeni

Çalıştay kapsamında gerçekleşecek Dijital ID faaliyetleri

Ana tema

- Çözümler olgunlaşmaya devam ediyor
- Digital ID, devletler, bireyler ve özel kurumlar için çok büyük bir fırsat
- Dijital ID kullanımı içeren ve e-dönüşüm bekleyen pek çok süreç
  - Çok tarafın bir araya gelmesi gerekiyor
  - Kanun ve yönetmeliklerde eksikler
  - KVKK, mahremiyet, teknolojik entegrasyon engelleri
  - Süreçlerin çoğu, halen kamuya ait sistemlerde depolanan verilerin kullanılmasını gerektiriyor
  - Kamunun öncü rol oynaması gerekiyor

- TÜBİTAK
  - TC Ulusal Kimik Yönetim Sistemi tecrübesi
  - Blokzincir Farkındalığı → Dijital ID Farkındalığını artırmak
  - Dijital ID konusunda da sistemlerin gelişmesi için hızlandırıcı rolü oynamak
  - Geleceğe hazırlık adına işbirliklerin ve projelerin başlamasını sağlamak
  - İş birliklerini artırmak

Çalıştayın Dijital ID açısından içeriği

- Dijital ID konusunu irdeleyen sunuşlar
  - Teknolojik ve Hukuki yönünden
- BCTR Paneli
- DID, VerifiableCredential temelli sunuşlar, demo ve eğitimler
- Halihazırda çalışan evrensel çözümlerin tanıtımı, Sovrin

Ülkemizde yapılabilecekler

- Politik durum
  - Kanunlar ve düzenlemelerin olgunlaşması
- Digital altyapılar
  - Standartlar, Mevcut yapıların da kullanımı
- Güven
  - Türkiye SSI Önerisi
  - Güven verecek altyapı ve yönetişim modeli
  - Güvenlik gereksinimlerinden gerçeklemeye kadar şeffaflık ve güvenlik sertifikasyonu

Teşekkürler

Referanslar

- Digital Identity: the current state of affairs, Ana I. Segovia Domingo, A.M.Enriquez, BBVA Research Working paper, 2018
- Dijital Kimlik Raporu, BCTR, Nisan 2019
- The future of public service identity: blockchain, Accenture Consulting, Nov 2017
- NIST White Paper (Emerging Blockchain Identity Management Systems), July 2019