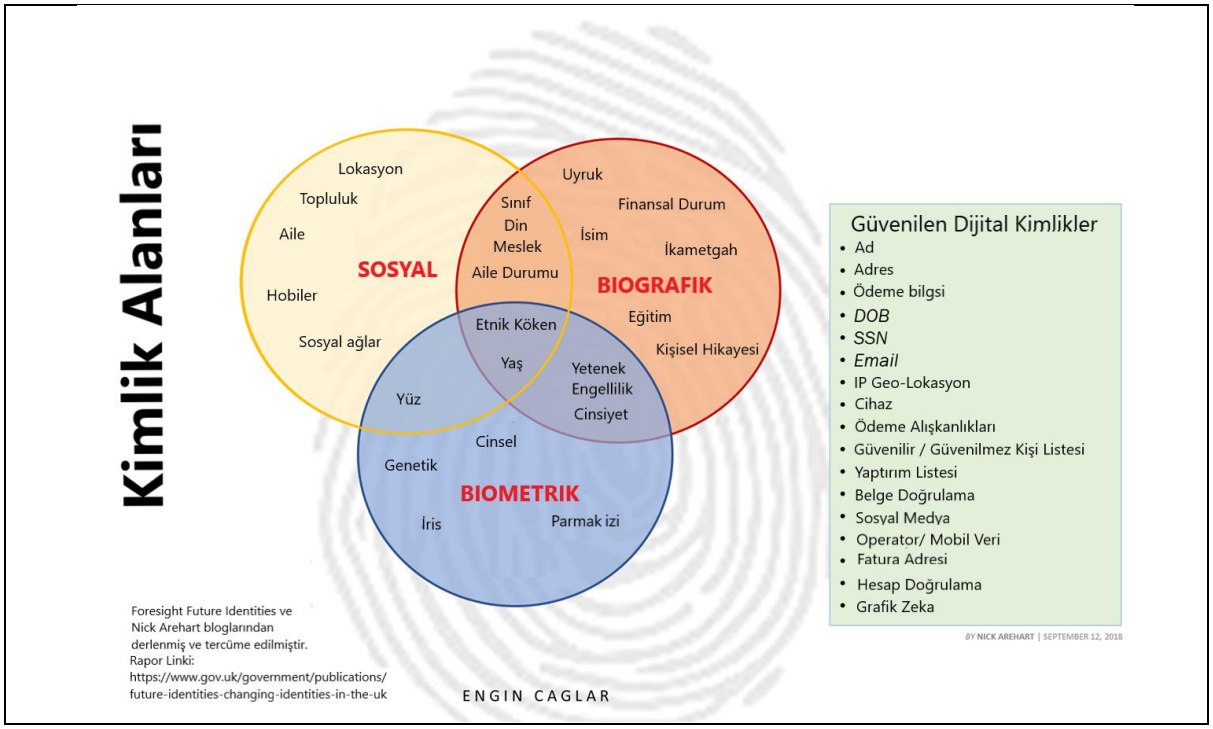
**YOLLARIN BAŞLANGICI: DİJİTAL KİMLİK VE BLOCKCHAIN**

*Bir bilgisayarda ilk password kullanıldıktan sonra başlayan süreç bizleri "dijital kimlik" kavramları ile tanıştırdı. Kullanıcı odaklı ve kullanıcıların kendi verileri üzerinde kontrol sahibi olabildikleri özerk kimlikler yoğun tartışmaların odağını oluşturuyor. Bu tartışmalara blockchain teknolojilerinin sağlayabileceği katkılar ve ortaya çıkarabilecek yeni sorular ise tartışmaları başka alanlara taşıyor.*




**İlk password ile başlayan dijital kimlik macerası:**

Bir bilgisayarda kullanılan ilk "password" 1961 yılında Massachusetts Institute of Technology (MIT) labaratuvarlarında CTSS isimli bir sistemde kullanıldı ([1]).

Üniversitedeki araştırmacıların birlikte kullandığı bu sistemde aynı dosyalara erişmek ve üzerinde çalışmak isteyen araştırmacılara yardımcı olabilmek için bir şifre kullanma fikri büyük bir ihtimal ile dijital kimlik kavramının ortaya çıkmasına neden olan en önemli oylardan bir tanesi.

1960'larda sadece bilgi işleme amacı ile kullandığımız bilgisayarlar artık ulaşım sistemlerimizi, fabrikalarımızı, elektrik, su ve doğalgaz şebekelerimizi yöneten, ameliyatlarımızı yapabilen, hatta silahlar kullanabilen sistemler haline geldi.

**Kimlik ve dijital kimlik**

Kanuni bir belge anlamında kullanılan "kimlik" ile "dijital kimlik" arasında birebir ilişki kurmaya çalışan sistemlerin oluşturduğu sağlıksız yapı nedeni ile bir çok kavram birbirine girmiştir.

Dijital dünyadaki kimliğimiz (çoğu zaman bir email ve şifre) ile **"doğrulama", "onaylama" ve "yetkilendirme"** yaptığımız bulunmaktadır.

Elektrik,su, doğalgaz, ulaştırma, bankacılık sistemlerimizi yöneten ya da ameliyatlarımızı yapan, dijital sistemler E-postamızı bilen ve bir kaç şifre deneyebilen başka insanlara ve "robot" yazılımlara da açabilmektedir.

Bu sistemler için "bizi biz yapan nedir?" ya da "sadece bir email ya da bir şifre midir?" tüm dünyada binlerce araştırmacı bu soruna farklı çözüm önerileri getirmeye çalışıyor.

**"Düşünüyorum, o halde şifremi çalabilirler"**

Pek çok internet sitesini ziyaret ettiğinizde kabul etmek zorunda olduğumuz kurallar ve ve ziyaret ettiğimiz site tarafından talep edilen bilgiler ciddi bir sorun.

Öyle bir hale geldi ki size okumanız için bir yazı gönderen bir şirket, okumanızı istediği yazı için sizden sitelerine üye olmanızı ve üye olurken de adeta tüm kimlik bilgilerinizi isteyebilmekte.

Ya da pek çok siteye en azından e-mailinizi vermeden,ve size dayatılan pek çok kuralı kabul etmeden girmek mümkün değil. Pek çok insanın okumadan kabul ettiği bu kurallar ile kendisine ait pek çok özel verinin kapılarını da bu sitelere açmış oluyor.

Sorunu daha da büyüten bir gerçek ise insanların ve hatta robot yazılımların birilerini taklit edebilmesinin kolaylığı. Internetteki güvenlik ihlallerini listeleyen BreachLevelIndex sitesine göre son 6 yılda 14 milyar'dan fazla ihlal gerçekleşmiş ([2])

1960'lı yılların akademik ortamında bilgisayar şifreleriyle başlayan dijital yolculuk o günlerde belki de hiç kimsenin beklemediği kadar büyük bir hızla tüm dünyaya yayıldı.

"Dijital Kimlik" kavramı ile ilgili tartışmalar ile geleceğin toplumunda bilgisayarların, robotların, otonom sistemlerin ve en önemlisi insanın nerede olacağı belirleniyor.

**Dijital kimliğin bilinen 4 aşaması:**

Dijital kimlik kavramının geçirdiği aşamaları kriptografi konusunun öncü isimlerinden Christopher Allen bloğundan yararlanarak aşağıdaki şekilde tablolaştırabiliriz ([3]):

| Aşama | Açıklama | Organizasyon Örnekleri | Sorunlar | Dönemin Çözüm Önerileri |
|---|---|---|---|---|
| **Birinci Aşama Merkezi Kimlik** | Tek bir otorite veya hiyerarşi tarafından idari kontrol | **IANA (1998)** The Internet Assigned Numbers Authority<br><br>**ICANN** The Internet Corporation for Assigned Names and Numbers<br><br>**Certification Authorities** (CAs) | Her nekadar organizasyonlar güvenilir olduğu varsayılan ve kar amacı gütmeyen kuruluşlar olsa da, kullanıcılar kimliklerini inkar edebilecek ya da sahte bir kimliği onaylayabilecek tek bir otoriteye teslim olmuşlardır.<br><br>İnternet büyüdükçe hiyerarşilerde biriken güç arttıkça kullanıcıları düzinelerce farklı hiyerarşide düzinelerce farklı kimliğe zorladılar. | 1991 yılında Philip Zimmermann "Pretty Good Privacy-PGP" adlı bir email şifreleme paketi önerdi. Aslen bir insan hakları aracı olarak tasarlanan yazılım, Zimmermann'ın Amerikan Hükümeti tarafından ihracat kısıtlamalarını ihlal ettiği gerekçesi ile 3 yıl süren bir soruşturmasına maruz kalmasına neden oldu. Buna rağmen, PGP en çok kullanılan e-posta oldu.<br><br>Carl Ellison,1996 "Establishing Identity without Certification Authority"<br><br>SPKI/SDSI Project, 1999 |
| **İkinci Aşama Federal Kimlik** | Çok sayıda federal otorite tarafından idari kontrol | **Microsoft's Passport** (1999)<br><br>**Liberty Alliance** (2001)<br><br>**Star Alliance** | Yüzlerce sitenin ortaya çıktığı bir dönemde aynı kimliğin kullanımı amacıyla ortaya çıktı, ancak her bir site otorite konumuna gelmeye başladı. | Kullanıcıların, üçüncü tarafların web sitelerine, uygulamalarına, mobil cihazlarına ve oyun sistemlerine mevcut kimlikleriyle giriş yapmalarını sağlayan, yani sosyal oturum açmayı sağlayan dijital kimlik platformları örneğin:<br>Microsoft account – Eski Windows Live ID<br>Google Account / Facebook – Login/Yahoo<br>Kullanıcılar bu sitelerdeki kimlikleri ile diğer sitelere girebilmeye başladılar. Bu firmaları: |

| | | | | |
|---|---|---|---|---|
| | | | | Twitter/<br>LinkedIn/PayPal/Foursquare/MySpace<br>AOLMozilla Persona (Kasım 2016'da kapandı) /Amazon/ GitHub<br>Not: Facebook Connect yetkilendirmeli bir kimliktir, federal kimlik değildir. |
| **Üçüncü Aşama: Kullanıcı Odaklı Kimlik** | Federasyon gerektirmeden birden fazla otorite üzerinde bireysel veya idari kontrol | **The Augmented Social Network-ASN** (2000)<br><br>**The Identity Commons** (2001-Günümüz)<br><br>**The IIW community**<br><br>**OpenID** (2005),<br>**OpenID 2.0** (2006),<br>**OpenID Connect** (2014),<br>**OAuth** (2010)<br>**FIDO** (2013)<br><br>Facebook Connect (2008) | Güçlü kurumlar bu oluşumların çabalarını destekledi ve hedeflerini tam olarak gerçekleştirmelerini engelledi. Liberty Alliance örneğinde olduğu gibi, günümüzde kullanıcı merkezli kimliklerin nihai mülkiyeti, onları kaydeden işletmelerde kalmaktadır.<br><br>Kullanıcı, uzun ömürlü ve güvenilir bir site seçerse, kendi kendine yeten bir kimliğin avantajlarının çoğunu kazanabilir - ancak kayıt kuruluşu tarafından herhangi bir zamanda elinden alınabilir!<br><br>Facebook'un son gerçek isimlerindeki tartışmalarda da görüldüğü gibi keyfi bir şekilde kapanmış hesapları var. | ASN grubu " "her bireyin kendi çevrimiçi kimliğini kontrol etme hakkına sahip olması gerektiği hedefini" Passport ve Liberty Alliance'ın ulaşamayacağını düşünüyordu. Onlara göre "iş temelli girişimler" bilginin özelleştirilmesine ve kullanıcıların tüketici olarak modellenmesine çok fazla önem veriyordu.<br><br>Identity Commons (2001'den bu yana) dijital kimlik konusundaki yeni çalışmayı ademi merkeziyete odaklanarak pekiştirmeye başladı.<br><br>IIW topluluğu, merkezileştirilmiş otoritelerin sunucu merkezli modeline karşı çıkan yeni bir terime odaklandı: kullanıcı merkezli kimlik. |
| **Dördüncü Aşama: Özerk Kimlik** | Herhangi bir sayıda otorite üzerinde bireysel kontrol<br><br>Kullanıcıların kimlik sürecinin merkezinde olmasını savunmak yerine, özerk kimlik, kullanıcıların kendi kimliklerini yöneten olmalarını gerektirir. | Sovereign Source Authority (2012)<br>Moxie Marlinspike<br><br>Open Mustard Seed (OMS) Framework (2012)<br>Patrick Deegan<br><br>The Windhover Principles For Digital Identity | Networke güvenmeyi gerektirir.<br><br>Yapay zeka ve makine öğrenimi kullanan sistemler, kimliğimize dayalı kararlar vermek için kullanılmaktadır. Bu sistemler önyargıyı ve ayrımcılığı güçlendirebilecek veriler üzerine kurulu olabilir. | Özerk kimlik aynı zamanda uluslararası politika alanına girmiştir.<br>Bu, büyük ölçüde Avrupa'yı besleyen mülteci krizinden etkilenmiştir.<br>Birçok kişinin kimlik bilgilerini veren devletten ayrılmalarıyla kabul edilmiş bir kimliğe sahip olmamasının sonuçlarından etkilenmiştir. Konu, uzun süredir devam eden uluslararası bir problemdir, çünkü yabancı işçiler, devlet tarafından verilen kimlik bilgilerinin eksikliğinden dolayı çalıştıkları ülkeler tarafından sıklıkla suistimal edilmektedir. |

1960'ların akademik ortamındaki bir tartışma ülkelerin kendi vatandaşlarının haklarını dijitaldünyada nasıl koruyabilecekleri bir noktaya gelmiştir.

Avrupa topluluğunun geliştirdiği yaklaşımlar Amerika ve dünyanın farklı ülkeleri ile karşılaştırıldığında daha fazla kişisel mahremiyet esası üzerine kurulmuştur.

Bir çoğuna Türkiye'nin de katılımı ile oluşturulan Avrupa Topluluğu'nun dijital kimlik çalışmalarının neticesinde ortaya çıkan düzenlemeleri aşağıdaki şekilde özetlenmiştir ([4])

| Düzenleme | Açıklama | İlave Bilgi |
|---|---|---|
| **eIDAS**<br><br>eIDAS Düzenlemesi 910/2014/EC<br><br>Elektronik Kimlik Belirleme ve Güven Hizmetleri Düzenlemesi | Avrupa için Sayısal Tek Pazarı (Digital Single Market) oluşturmak ve bu pazarda elektronik kimlikleri ve imzaları yasal bir statüye kavuşturmak amacı ile oluşturulan düzenlemeler.<br><br>Türkiye'de bu düzenlemelere iştirak etmektedir. | Üç çeşit elektronik imza tanımlanmıştır:<br><br>1.Elektronik İmzalar<br><br>2.Gelişmiş İmzalar (AdES)<br><br>3.Nitelikli Elektronik İmzalar (QES) |

| | | |
|---|---|---|
| **GDPR**<br><br>Avrupa Birliği Veri Koruma Yönergesi<br>(EU General Data Protection Regulation<br>(2016/679)<br>GDPR<br>(25 Mayıs 2018)<br>(95/46/EC yerini alır) | İşletmeler, Avrupa Birliği'ne üye ülkelerin vatandaşlarının ya da müşterilerinin verilerini, yönetmelikte belirtilen kurallar çerçevesinde güvenliğini sağlamalıdır.<br>Avrupa Birliği'ne üye 28 ülkede ve 28 ülkedeki vatandaşlarla iş yapan şirketler için geçerlidir. ve müşterilerin verilerini toplayan ve saklayan tüm şirketler GDPR'ye tabidir. | GDPR ne gibi gizlilik verilerini kapsıyor?<br>Temel kimlik bilgileri (isim, adres ve vatandaşlık numarası gibi)<br>- İnternet verileri (Konum, IP adresi, çerez veri ve radyo frekansı ile tanımlama etiketleri (RFID) gibi)<br><br>Sağlık ve genetik verileri<br><br>Biyometrik veriler<br><br>Etnik köken ve ırk verileri<br>Siyasi görüş verileri<br><br>Cinsel eğilim verileri |
| **PSD2**<br><br>Ödeme Servisleri Yönetmeliği (Payment Service Directive)<br><br>(PSD1'in yerini almaktadır). | Tüm Avrupa Topluluğu ülkeleri, Norveç ve Lihtenştayn'da geçerli olmak üzere aynı ödeme uygulamaları için aynı kuralların geçerli olduğu ve bankalar dışında yeni ödeme servis sağlayıcılarının tanımlandığı bir düzenleme. | PSD2 ile bu kurumlar güvenli API'ler (Application Programing Interface) ile kullanıcılarına ait verileri üçüncü partilerin kullanımına açacaklar. |

**Blockchain işin neresinde ?**

Blockchain veri tabanlarını standart veri tabanlarından ayıran en önemli özelliklerden bir tanesi her yeni kayıt, o kayıt için belirlenen şartlar sağanmadan kaydedilemiyor. Yani sisteme erişim yetkisi olan hiçbir "kişi" daha önce belirlenen belirlenen kurallara uyulmuyor ise yeni bir kayıt yaratmıyor ya da bir kaydı değiştiremiyor.

Dijital kimlikler açısından önemli bir başka blockchain özelliği ise verinin sahipliği kavramı.

Yazıyı kısa tutabilmek için bu konuyu sadece bir bitcoin örneği ile açıklamak yeterli olacaktır. Bitcoinlerin ya da onun en küçük birimleri olan sastoshilerin sadece tek sahibi olan kişinin onayı olmadan hiç kimse o "veriye" (sonuçta bitcoin bir veri ya da bir veri dosyasıdır) erişemez, işlem yapamaz.

Bu iki özellik bir araya geldiğinde "Self Sovereign Identity" adı verilen "özerk kimlik" için gerekenler büyük oranda blockchain tarafından karşılanıyor.

**Dijital Kimlik Blockchain ile Bitcoin arasındaki farkı belirginleştiriyor:**

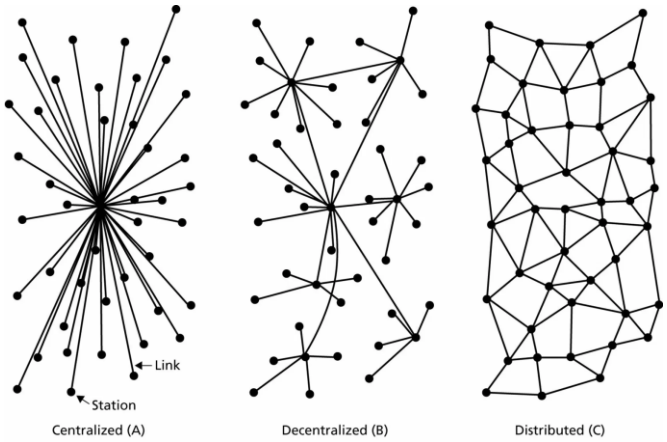
Dijital kimlik ile ilgili tartışmalar neden blockchain ve bitcoin farklı şeylerdir sorusuna da önemli katkılar sağlıyor.

Bitcoin tasarımı ile bir para olmayı hedeflemektedir. Bir akıllı sözleşme ya da dijital kimlik olarak kullanılmayı hedeflememiştir. Hedefini gerçekleştirmek için blockchain teknolojisinden yararlanmaktadır.

Blockchain teknolojileri tarafından kullanılan ağ yapıları 1960'larda Paul Baran tarafından ortaya atılan dağıtık ağ (distributed network) kavramınının bir uygulaması niteliğindedir ([5]).

Bu yıllarda askeri haberleşme ağlarının merkezi yapısının güvenlik açısından bu ağları daha "kolay hedef" haline getirmesi büyük bir sorun olarak görülüyordu. Bu sorununa bir çözüm önerisi olarak geliştirilen merkezi olmayan (decentralized) ve dağıtık (distributed) ağ yapıları bugün blockchain sistemleri ile yeni uygulama alanları bulmuştur.

Paul Baran: Centralized, Decentralized and Distributed networks (1964)




Bazı teknik kişişlerin ısrarla blockchain ve dağıtık defter (distributed ledger) kelimelerini ayrı ayrı vurgulayarak konuşmasının nedeni bu ağ yapılarından kaynaklanmaktadır.

Ağ yapıları, oyun teorsisi, kriptografi, dijital kimlik gibi farklı konularda çalışan bilim adamlarının para dışındaki pek çok akademik probleme de blockchain ile yeni bir cevap bulma imkanı çıkmıştır. Bu durum blockchain teknolojilerinin akademik çevrelerde büyük ilgi görmesine neden olmuştur.

Ağ yapılarının çeşitliliği bu ağlar içerisindeki "gerçek" ve " sanal" kişilerin ve bu bu kişilerin farklı ortamlardaki farklı kimliklerinin tanımlanması konusunda ortaya çıkan ihtiyaçlar yeni kavramlar yaratmıştır.

**Akıllı sözleşmeler Dijital Kimlikçileri heyecanlandırıyor**

Bitcoin her ne kadar bir para, para transfer sistemi ya da ödeme sistemi olarak tasarlanmış olsa da sonuçta bir dijital verinin kopyası olmadan transferini yapan ve bunu da içinde bulunduğu ağı bir doğrulama aracı olarak kullanan bir yapı.

Doğal olarak Bitcoin'in nasıl çalıştığını kavrayan pek çok akademisyenve teknik kişi para gibi farklı veri setleri için de dağıtık defter yapısını doğrulama amacı ile kullanabileceğini farketmekte geç kalmadılar. Bu konuda en dikkat çeken fikirlerden bir tanesi "akıllı sözleşme" oldu.

Akıllı sözleşmelerde veri sahibinin kendi verileri üzerindeki hakimiyeti doğal olarak dijital kimlik konusunda çalışanları etkiledi.Dijital kimlik projeleri kirptopara harici ilk uygulamalar arasında yer almaya başladı. Bunun ilk örneklerinden Uport projesi İsviçre'de Zug Kantonunda bir dijital kimlik prjesi olarak ortaya çıktı. Bunu farklı kantonlardaki ve ülkelerdeki projeler izledi.

**Gelinen noktada, mevcut blockchain projeleri "dijital kimlik" ile ilgili tüm ihtiyaçları karşılamakta mıdır?**

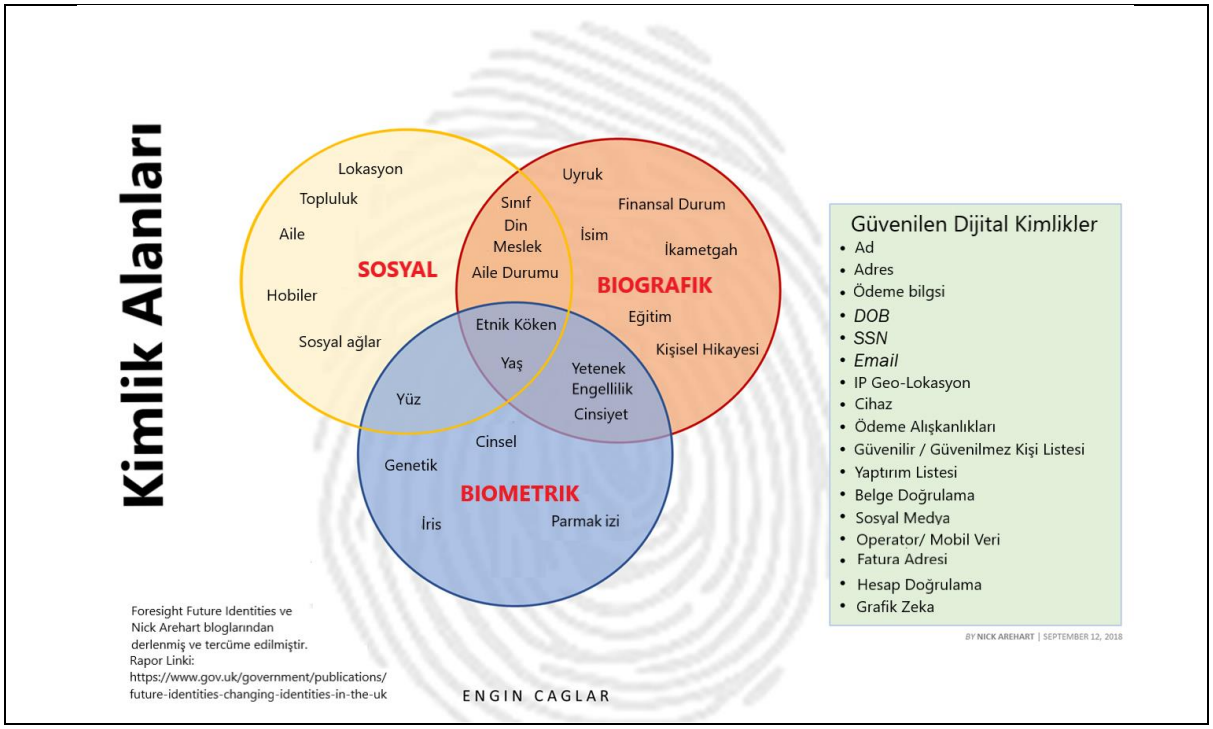
Kimlik kavramı belki yüzyıl önce bugün olduğu kadar hayati öneme sahip bir kavram değildi.

Bu yazıyı hazırlarken kimlik kelimesinin İngilizce'de kaç anlamı olduğundan yola çıkarak bugünkü tartışmaları özetleyebileceğimizi düşünmüştüm.( En popüler üç farklı sözlükte "identity" kelimesinin anlamlarına baktığımda açıkçası beklediğimden çok daha az açıklama ile karşılaştım).

Aşağıda İngilizce üç farklı sözlükten "Identity" kelimesi ile ilgili farklı anlamları görebilirsiniz:

| *Tanım* | *Sözlük* |
|---|---|
| ***Bireysel*** | |
| • *Bireyin ayırt edici karakteri veya kişiliği* | *Meriam Webster* |
| • *Bir kişi kimdir veya onu diğerlerinden farklı kılan kişi veya grubun nitelikleri.* | *Cambridge* |
| • *Kamuyunu bireyler hakkında belirli bir şekilde düşündüren kişi veya kuruluşun itibarı, özellikleri vb.* | *Cambridge* |
| • *Bir şeyin ne veya bir kişinin kim olduğu gerçeği.* | *Oxford* |
| • *Bir kişinin veya şeyin kim veya ne olduğunu belirleyen özellikler.* | *Oxford* |
| • *Bir insanı diğer insanlardan farklı kılan nitelikler kümesi* | *Merriam Webster* |
| ***Nesne*** | |
| • *(bir nesnenin) sahibinin, sahibinin veya kullanıcının kim olduğunu ve imza veya fotoğraf gibi diğer detayları sık sık taşıyarak kim olduğunu belirlemeye hizmet eder. Örnek: 'bir kimlik kartı'* | *Oxford* |
| • *Kim olduğunu, veya kim olduğunu ispatlayan bilgi, örneğin isimler ve doğum tarihleri* | *Cambridge* |
| ***Aynılık*** | |
| • *Farklı durumlarda esansiyel veya genel karakterin aynı olması* | *Merriam Webster* |
| • *Bir şeyin nesnel gerçekliğini oluşturan her şeyde aynılık* | *Merriam Webster* |
| • *Yakın bir benzerlik veya yakınlık.* | *Oxford* |
| ***Matematik*** | |
| • *A transformation that leaves an object unchanged.* | *Oxford* |
| • *Belirli bir ikili işlemle başka bir elemanla birleştirilirse, bu elemanı değiştirmeden bırakan bir kümenin elemanı.* | *Oxford* |
| • *Harflerle ifade edilen miktarların tüm değerleri için iki ifadenin eşitliği veya bunu ifade eden bir denklem; $(x + 1)^2 = x^2 + 2x + 1$.* | |
| • *Tanımlanan veya iddia edilenle aynı olma koşulu, çalınan malların kimliğini belirlemek* | *Merriam Webster* |
| ***Psikoloji*** | |
| • *Psikolojik tanımlama ile kurulan ilişki* | *Merriam Webster* |

Dijital kimlik tartışmalarının özüne indiğimizde aslında tartışmanın “kimlik” kavramından ziyade “güven” kavramı ile ilişkili olduğu ve bu nedenle blockchain teknolojilerinin yeniden “dijital kimlik” kavramını tartışılır bir hale getirdiğini görebiliriz.




Yukarıdaki grafikte sol tarafta kimlik alanları “sosyal, biyografik ve biometrik “ olarak özetlenmiş durumda. Sağ tarafta ise ise dijital sistemlerin sizi tanımak için kullandığı “veri” örnekleri var.

Pek çok şirket sağdaki bir ya da bir kaç veriyi sizinle ilişkilendirerek (bu verileri “kimliğiniz” haline getirerek) sizin sol taraftaki kimlik alanlarınızı tespit etmeye çalışıyorlar.

Milyonlarca hatta milyarlarca insan için bu eşleştirmeleri yapmak çok kolay değil. Bu nedenle de yapay zeka araçlarından ve algoritmalardan faydalanıyorlar.

Malesef işin içine “yapay” bir zeka girdiğinde de bu sistemler önyargıları ve ayrımcılıkları çok fazla güçlendirebilecek araçlara dönüşme riskine sahip.

**Merkezi sistemlerde ciddi bir sorun.**

Örneğin internette bir arama yaptığımızda karşımıza çıkan sayfalar internete bağlandığımız ülkeye göre ve bizimle ilgili tutulan kayıtlara göre farklılık göstermektedir. Arama motoru firmaları (örneğin google, yahoo, vs..) bilgiye erişimimiz üzerinde ciddi bir güce sahip.

Aynı şekilde bu durum sosyal medya ya da alışveriş siteleri için de geçerli. Aynı ürün için birden fazla arama yaptığımızda ürün fiyatlarının değişmesi örneğin uçak bileti için giderek sıklıkla karşılaşılan bir durum.

**Kelimeler algoritmalara dönüşüyor ve kaderimiz olmaya başlıyor**

Daha önce satın aldığımız bir ürün,  yaptığımız bir arama ya da oturduğumuz şehir ile ilgili tutulan bir kayıt sürekli bu kayıtlarla ilişkilendirilmemize sebep oluyor.

Daha da önemlisi bu ilişkilendirmeler, doğru veriler yerine manüple edilmiş verilere ulaşmamıze neden olabiliyor.

**Blockchain ya da “dijital kimlik” bu kadar büyük bir soruna çözüm olabilir mi?**

Teorik olarak evet.

Herhangi bir internet sitesini ziyaret ettiğimizde bizimle ilgili hangi bilgileri alabileceği konusunda “tarihte ilk kez” bir başka kişiye ya da kuruma güvenmek zorunda kalmadan blockchain bize bir kontrol “şansı” sunuyor.

Hatta akıllı sözleşmeler ile paylaşılan verilere ne kadar bir süre ile erişilebilir ve ne amaçla kullanılacağına karar verebiliyoruz.

**Yeni sorular:**

İlginç bir şekilde blockchain geçmişte yaşanan “dijital kimlik” tartışmalarındaki pek çok soruya yanıt verirken yeni soruların ortaya çıkmasına neden oluyor.

Bu yeni sorulardan kaç tanesini aşağıdaki şekilde sıralayabiliriz:

1. Bir kişi ya da kuruma güvenmiyoruz ama bu sefer de blockchain ağına güvenmek zorunda kalmıyor muyuz? (İyi tasarlanmamış bir blockchain projesi bir kabusa dönüşebilir.)
2. Bana ait verilerin kontrolü sadece bende olacaksa, örneğin sisteme giremeyecek kadar hasta olursam ne olacak?
3. Bana ait veriler hiçbir şekilde silinemeyecek ise uzun vadede yine ayrımcılık ve önyargılarla karşı karşıya kalmayacak mıyım?
4. Yapılan her işlem iki kişi ve network arasında ise kanuni otoriteler bu yapının neresinde olacak. Kanuni haklar sisteme nasıl uygulanacak. Örneğin : Dijital kimliğim ile elde ettiğim dijital varlıkları miras bırakabilecek miyim?
5. Sisteme ilk tanıtılan kimlik sonsuza kadar orada kalacaksa bu aşamadaki bir yanlışlık nasıl giderilecek?

Ortaya çıkan her yeni sorun yeni akademik çalışmaların ya da yeni iş fikirlerinin doğmasına neden oluyor. Farklı kulvarlarda yarışa başlayan blockchain ve dijital kimlik kavramlarının nasıl şekilleneceğini zaman bizlere gösterecek.

Bu yarıştan geri kalmamak için her biri ayrı uzmanlıklar gerektiren kavramları birarada geliştirebilen ekosistemler geliştirebilmek çok daha önemli olacak.

(1) https://www.wired.com/2012/01/computer-password/
(2) https://breachlevelindex.com/
(3) http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html
(4) https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en
(5) https://www.peacebiennale.info/blog/paul-baran-centralized-decentralized-and-distributed-networks-1964/