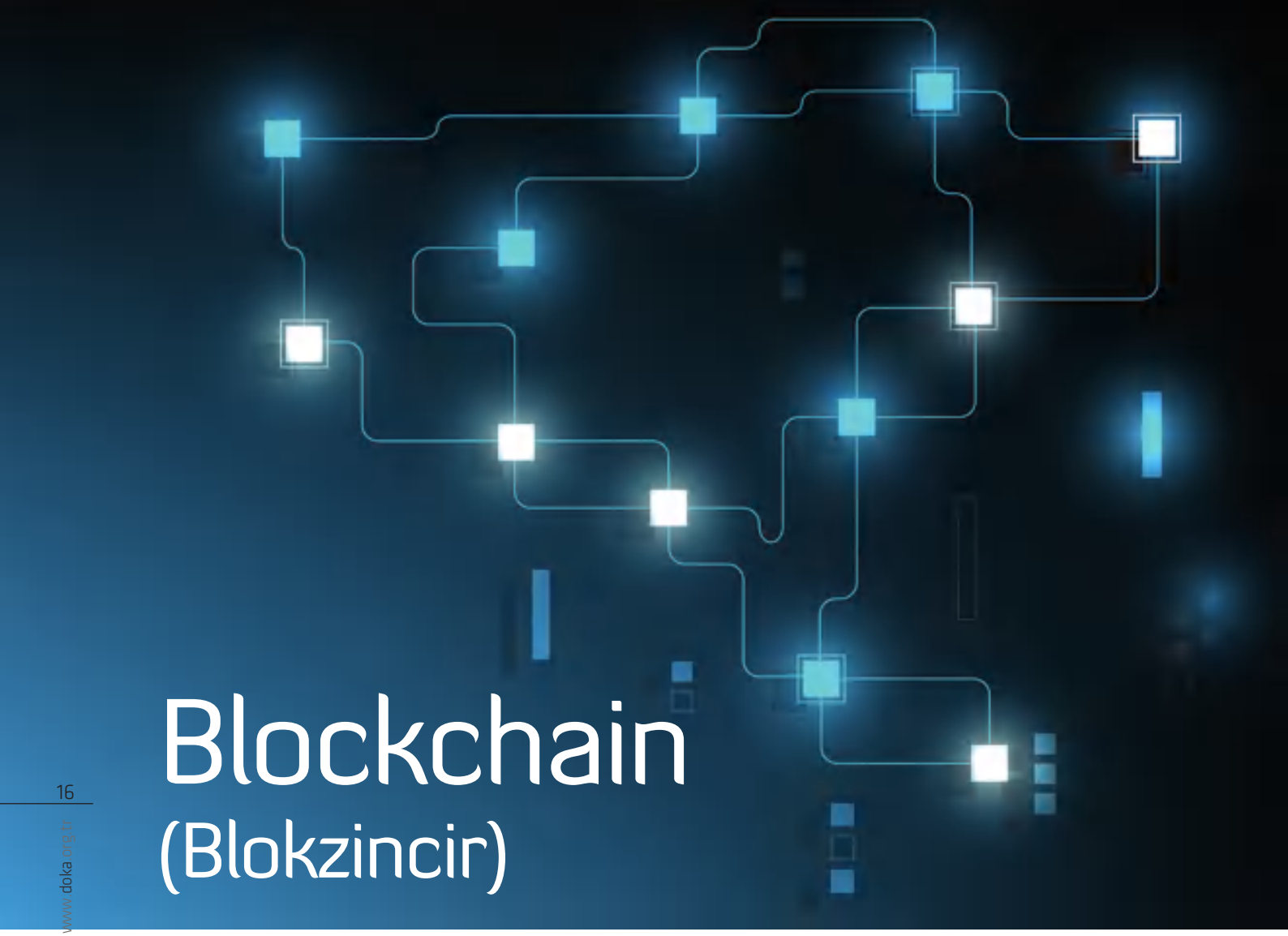

Blockchain
(Blokzincir)

Bilgi üretimi hiç olmadığı kadar hızlı bir şekilde artmaktadır. Şu andaki hızla dünyada her gün 2,5 kentrilyon bayt veri oluşturulmakta ve bu hız nesnelerin interneti (IoT) yardımı ile logaritmik olarak artmaktadır. Yalnızca son iki yılda, insanlık tarihi boyunca dünyada üretilen verilerin % 90'nın üretilmiş olması bu hızı bize açıkça göstermektedir.

Üretilen veri ve bilginin güvenli bir şekilde saklanması günümüz internet dünyasının en önemli problemleri arasında görünmektedir. Tek merkeze dayalı güven olgusunun yıkılması merkezi güven yapısının internet ortamında dağıtılması ihtiyacını ortaya çıkarmıştır. Bu ihtiyaç da **bilgi güvenliği, bilgi kodlama, bilgi-veri kriptolaması** gibi kavramlarını son yıllarda çokça konuşulan konular haline getirmiştir.

Adil SOLTAN / DOKA Uzmanı

Yeni tanışma fırsatı bulduğumuz ve bu yazıda değineceğimiz Blockchain (Blokzincir) konusu da adından anlaşılacağı gibi bloklardan oluşan zincire benzer bilgi yığınları anlamına gelmektedir. **Blokzincir teknolojisinin gelişmesi sonucu veriyi merkezi sistemlere kaydetmek zorunluluğu ortadan kalkmaktadır.** Sahip olduğumuz yüksek hızlı iletişim ağları verinin büyüklüğü ne olursa olsun istediğimiz her veri kümesinin dilediğimiz sayıda kopyasını çıkartarak ve bu kopyaları pek çok noktaya dağıtarak saklamamızı mümkün kılmaktadır.

Blokzincir şifrelenmiş işlem takibi sağlayan dağınık veri kayıt sistemi niteliğinde olup bir veri tabanı hüviyeti taşımaz. Her bir blokta kendinden bir önceki blok için bir işaretçi ve genellikle işlem bilgileri, zaman damgaları ve geçerliliği onaylamak için gerekli diğer meta verilerin bir kombinasyonu yer alır. Bloklara kaydedilen veri bir daha değiştirilemez veya silinemez. Bu özelliğini verilerin biriktirildikleri blokları aynı bir zincir gibi, birbirlerine şifreleme algoritmaları ile bağlayarak saklamasına ve bu zincirin birçok kişiyle dağıtık olarak paylaşılmasına borçludur.(1)

Blokzincir çalışma prensibine değinmeden önce düğüm kavramını tanımlamak gerekmektedir. Bazı kaynaklarda **Node** olarak ta ifade edilen **Düğüm**, bir blokzincirindeki katılımcı tarafından işletilen defterin kopyasını ifade etmektedir. Kullanıcı tarafından yeni işlem veya varolan bir işleme ait düzenleme, bir Blokzincir'e geldiğinde, genellikle bir Blokzincir uygulamasındaki düğümlerin çoğunluğu, önerilen tek tek Blokzincir bloğunun geçmişini değerlendirmek ve doğrulamak için algoritmalar yürütür. Eğer düğümlerin çoğunluğu tarihin ve imzanın geçerli olduğu konusunda bir fikir birliğine varırsa, yeni işlem bloğu deftere kabul edilir ve işlem zincirine yeni bir blok eklenir. Her bir işlem birbirine kriptografik olarak bağlanır. Zincire benzer yapısı nedeniyle Blokzincir ya da Blockchain ismi de buradan gelmektedir. Çoğunluk, defter girişinin eklenmesine veya değiştirilmesine katılmazsa, reddedilir ve zincire eklenmez. Dağıtılmış bu mutabakat modeli, blokzincirinin dağıtılan bir defter olarak çalışmasına izin verir; ve en önemlisi bunun için, hangi işlemlerin geçerli olduğunu ve hangilerinin bulunmadığını söyleyen bir merkezi otoriteye ihtiyaç duymuyor olmasıdır.(2)

Node

Düğüm

Blokzincirin verileri tutma mantığına bir de gerçek hayattan örnek vermek gerekirse, Ahmet Tufan Helvacı'nın şu örneği akıllarda yer edecektir. "Blokzincir bakkalların veresiye defterleri ile biraz benzerlik gösteriyor. Eskiden bakkaldan bir şey almaya giderken evin veresiye defterini de yanımıza alarak giderdik. Bakkaldan alışveriş yapıldığında hem bakkal kendi veresiye defterine yazar hem de biz evin veresiye defterine yazardık. Burada amaç bakkalın bizden habersiz veresiye defterinde değişiklik yapmasını önlemekti. İşte Blokzincir'de ki dağıtık ifadesi de bu mantığa çok benziyor. İşlemlerin kayıtlı olduğu blok zinciri ağ üzerindeki herkes ile aynı olacak şekilde tutulur. Eğer herhangi biri kendi defterinde diğerlerinin onayı olmadan bir şey eklemeye kalkarsa, diğer defterlerle çatışacağı için ağ dışında kalacaktır. "

Bu anlamda Blokzincir bizim değiştirilemez ve manipüle edilemez kayıtlar tutmamızı sağlar. Bu işlemlerin deftere kaydı ve ağa yayılması tamamen demokratik bir biçimde ağ üzerindeki bilgisayarlar tarafından yapılır. Ne kadar çok bilgisayar bu ağa katılırsa bu sistemin güvenilirliğini o derece de arttıracaktır.

Blokzincir Evrimi

Elektronik ve kripto para birimi olarak zikredilen Bitcoin'in de altyapısını oluşturan blokzincir teknolojisi gelecek vadeden bir teknoloji olmakla beraber bu teknolojinin tam bir olgunluğa erişmesi için kat edilmesi gereken adımlar vardır. Ancak, İsviçre merkezli Credit Suisse tarafından hazırlanan geniş çaplı bir rapora göre, blokzincir sadece dijital para birimleri veya finansal hizmetler için değil hali hazırda birçok alanda kullanılmaktadır. Dünya Ekonomik Forumu tarafından yapılan bir ankete göre, yöneticilerin %58'i küresel Gayri Safi Milli Üretimin %10'unu "2025'den önce blokzincirde bulunacak" şekilde bir tahmin yürütmektedir. Bu yıl rapora göre olgunluğa erişim yılı olarak belirtilmiştir. Şu anda bu teknoloji prototip ve deney aşamalarının arasında yer almaktadır.(3)

Âdemi merkeziyetçi veri işlemesine dayalı Blokzincir teknolojisi alanının 2021 yılında 10 milyar dolar civarında yeni yatırım alması beklenmektedir. Günümüzde finansal teknoloji girişimleri tarafından gelirleri tehdit altında olan geleneksel bankacılık sistemi Blokzincir'den faydalanma yoluna girmiş durumdadır. Bu teknoloji başta finans sektöründe olmak üzere özellikle dijital varlık transferinde hız ve işlem güvenliği sağlaması, merkezi birimlerin işlemlerin doğruluğuna onay verme ihtiyacını ortadan kaldırması ve hesap verebilirliği yüksek işlem kaydını kolaylaştırması açısından avantajlar sağladığı için önemini her geçen gün artırmaktadır. 2022 itibarıyla bankaların tamamının Blokzincir'i kullanması durumunda masraflarını 15-20 milyar dolar azaltabileceği öngörülmektedir. Blokzincir teknolojisinin aracıları ortadan kaldırdığı için mevcut sistemlere muhalif olduğu bilinmektedir. Ancak günümüzde bankaların haricinde farklı oyuncular da e-ticaret, dosya paylaşımı ve haberleşme gibi işlemler için Blokzincir keşfetmeye ve kullanmaya başlamıştır. (4)

Merkezsiz dağıtık yapıdan dolayı siber tehdit koruması, şifre işlemlerinin bulunmaması (sertifikaya dayalı işlem), veri depolamanın birbirinden farklı birçok yerde gerçekleştirilmesi gibi özelliklerinden dolayı **blokzincir uygulamaları siber saldırılara karşı kısmen dayanıklıdır.** Ancak yazılım/kod hataları, kimlik temelli saldırılar, kuantum bilgisayarından saldırılar ve dış veri kaynağına bağlı (işlemleri imzada kullanılan özel anahtar üzerinden) saldırılar blokzincir için siber güvenlik yönünden önlem alınacak alanlar olarak dikkat çekmektedir. Bunun yanında blokzincir için aslında daha önemli bir risk alanı olan mahremiyet-gizliliktir. İşlemlerin dağıtılmış ve umumi olması özel anahtar ya da cüzdan kimlik bilgilerine erişimi olan herhangi birinin tüm işlemleri elde edebilmesine yol açabilir. Diğer taraftan **blokzincir üzerinden** vergi toplama, kar dağıtımı, gayrimenkul ve varlık kaydı konularının yanında kamu güvenliği, sosyal güvenlik ve kimlik yönetimi alanlarında da kullanılacağından gelecekte milli güvenlik açısından önemli unsurlardan birini teşkil edecektir.

Kaynaklar

(1) https://medium.com/@finartz_com

(2) https://toptalent.co/

(3) (TÜBİTAK)

(4) https://multinet.com.tr/

(5) https://kriptokoin.com/