Blok Zinciri Teknolojisi

Semih Yazıcı-19011087

***Abstract*—Blockchain is a technology that allows data to be stored and exchanged on a peer-to-peer basis. Structurally, blockchain data can be consulted, shared and secured thanks to consensus-based algorithms. It is used in a decentralised manner and removes the need for intermediaries, or "trusted third parties".**

***Index Terms*—Blockchain, Distributed Ledger Technologies**

I. ÖZET

Blockchain, eşler arası verilerin depolanmasını ve paylaşılmasını sağlayan bir teknolojidir. Yapısal olarak, konsensüs tabanlı algoritmalar sayesinde blok zincir verileri sorgulanabilir, paylaşılabilir ve güvenceye alınabilir. Merkezi olmayan bir şekilde kullanılır ve aracılara veya "güvenilir üçüncü şahıslara" olan ihtiyacı ortadan kaldırır.

II. GIRIŞ

Blokzinciri teknolojisi son zamanlarda ulusal ve uluslararası basın, çeşitli uluslararası kuruluşlar, özel sektör ve kamu kurumları tarafından büyük ilgi görmekle birlikte bazı araştırmacılar tarafından potansiyel olarak Internet'ten daha güçlü bir teknoloji olarak ifade edilmektedir [1]. Allied Market Research tarafından yayınlanan raporda blokzinciri piyasasının 2016 yılında 228 milyon dolar olduğu ve 2023 yılına kadar 5.4 milyar dolar seviyelerine ulaşabileceği belirtilmiştir [2].

Blokzinciri sayesinde insanlar artık ürün veya hizmet transferi işlemlerinde güvenlik ve doğrulamayı sağlaması için üçüncü taraf bir aracıya ihtiyaç duymamaktadır. Blokzinciri ile oluşturulan "güven protokolü" güvenilir, şeffaf ve hesap verebilir bir ortam sunmaktadır. Blokzinciri, kullanıcılar için merkezi olmayan dağıtık veri yapıları sayesinde güvenliğin temeli oluşturmaktadır. [3].

A. Blok Zinciri Nedir?

Nakamoto' ya göre blokzinciri, yapılan her işlem bilgisinin ağdaki katılımcılar tarafından kaydedildiği ve paylaşıldığı dağıtılmış bir veri yapısıdır [4]. Beck' e göre ise blokzinciri, ağdaki çok sayıda düğüm tarafından güvenli ve tutarlı işlemlerin yapılmasını sağlayan bir veritabanıdır [5]. Zheng vd. blokzincirini, onaylanan tüm işlemlerin blok listeleri halinde depolandığı ve yeni bloklar eklendikçe büyüyen bir veri defteri olarak tanımlamıştır [6]]. Reyna vd. göre blokzinciri, işlemlerin güvenirliğinin ağdaki paydaşlar tarafından doğrulandığı dağıtılmış, şeffaf, değiştirilemez ve güvenli bir veri yapısıdır [7].

Sanal bir para birimi olan Bitcoin'in mucidi Satoshi Nakamoto 2008 yılında yaptığı çalışmada (A Peer-to-Peer Electronic Cash System) blok zinciri olarak isimlendirmeden blok zinciri teknolojisinden bahseden ilk kişidir. Nakamoto blok zincirinin çalışma prensibini kripto bir para birimi olan Bitcoin özelinde incelemiştir. Nakamoto çalışmasında kripto paranın kullandığı teknoloji, şifreli (kriptografik) olarak birbirine zincirlenmiş çok sayıda veri bloklarının oluşturduğu sistem olarak tanımlanmıştır. Blok zinciri merkezi olmayan kamuya açık bir kayıt platformudur. Bilgi ve varlık transferi sağlayan bu sistemde karşı taraftan kaynaklanan riskleri aşmak için herhangi bir otoriteye veya üçüncü bir kişiye ihtiyaç duyulmamaktadır.

Blok zinciri teknolojisinin temel bazı özellikleri aşağıda yer almaktadır.

1) Noterleşme: Dağıtılmış defteri yöneten zaman damgalı karma tabanlı algoritma nedeniyle, blok zinciri içinde kayıtlı tüm bilgiler noter gibi bir aracıya ihtiyaç duyulmadan otomatik olarak doğrulanmak ve onaylanmaktadır. İlgili taraflar, verilen bilgilerin belirli bir tarih ve saatte var olduğunu kesin olarak bilebilmektedirler. Bir blok zincirinde belgelerin saklanması gerçekliğini garanti etmekte ve olası izinsiz bilgi alımlarını önlemektedir.

2) Takas ve Ödeme İşlemleri: Potansiyel olarak, bir blok zinciri, özel / genel anahtar şifreleme ve dağıtılmış hesap defteri kullanarak işlemlerin verimli bir şekilde gerçekleştirilmesi ve işlenmesi yoluyla güvenilir üçüncü taraflara ihtiyaç duymaksızın her türlü dijital varlık veya varlık temsilinin transferine izin vermektedir. Nakit veya menkul kıymetler, gerçek zamanlı olarak hesaplanmaktadır. Çünkü blok zincirinde yapılan bir sonraki güncelleme onaylandığında işlem anlık tamamlanmaktadır. Bu sistem, uzlaşma döngüsü sırasında ticaret sonrası onaylama ve merkezi takas ihtiyacını ortadan kaldıracak ve uçtan uca süreci hızlandırarak veri hataları, ihtilaflar ve uzlaşma gecikmeleri kapsamını azaltacaktır.

3) Akıllı Sözleşmeler: Akıllı sözleşmeler, sözleşmeye dayalı ilişkilerin otomasyonuna izin vermekte ve dağıtılmış bir defterdeki varlıkların durumunu değiştirmektedir. Bu kavram, şirket işlemlerini ve nakit olaylarını otomatik olarak yürütme kapasitesine sahip olan menkul kıymetler olan "akıllı bonolar" fikrini geliştirmiştir (faiz ödemeleri, vade sonunda nominal tutarın geri alınması, ayrılma, olayların kapatılması vb.). Akıllı sözleşmeler para akışı harici bir olaya bağlanıp otomatikleştirilebilir. Örneğin, "eğer ürün teslim alınırsa, tedarikçi X firmasına 10.000 TL gönder yoksa geri al" şeklinde bir komut verilebilmektedir. Böylece BZT özelliklerinden birisi olan akıllı sözleşmeler ticari ilişkilerdeki karşılıklı riskin azaltılmasını veya ortadan kaldırılmasını sağlamaktadır.

4) Değişmez Veri Depolama: Zaman damgası oluşturma işlemleri sayesinde belgeler veya ağda depolanan ve depolan-

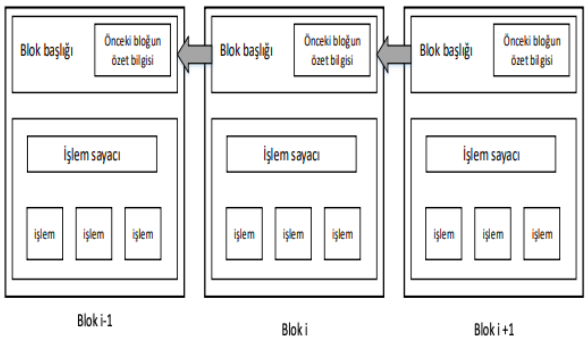
Identify applicable funding agency here. If none, delete this.

maya devam eden bir dijital zincirdeki herhangi bir varlık türü için değişmez bir veri depolama kapasitesi sağlamaktadır. Veriler katılımcılar arasında dağıtılmakta ve tek bir katılımcı bunları kaldıramamaktadır. Değişmez bir işlem geçmişi, tedarik zincirlerinde bir sahiplik zinciri sağlayabilmektedir. Değişmez işlem geçmişi katılımcılar için açık bir kanıttır ve alınıp satılan ürünlerin izlenmesine izin vermektedir.

5) Şeffaf Gerçek Zamanlı Veri: Wyman Euroclear (2016) tarafından yapılan bir çalışmaya göre, BZT'nin finansal alanda en büyük faydaları, bu teknolojinin şeffaf gerçek zamanlı veri sağlama yeteneğinden kaynaklanmaktadır. Blok zincirinin bu özelliği, veri zenginleştirme, uzlaşmalar ve diğer taraflar arasındaki anlaşmazlıkları ortadan kaldırabilmektedir. Katılımcılar, güvendikleri verileri, kendi değerlerinden daha fazla kesinlik sağlamak ve böylece risklerini azaltmak için işlem süresi öncesinde karşı tarafı seçerek gösterebilmektedirler [8].

B. Blok Zinciri Mimarisi

Blok zinciri, defteri kebir gibi gerçekleşen tüm işlemlerin kayıtlarının tutulduğu sıralı bloklardan oluşmaktadır. Şekil 1'de blokzinciri yapısının bir örneği gösterilmektedir. Bir blok sadece bir ana bloğa sahiptir ve her bloğun üst bilgisinde önceki bloğun özet bilgisi yer almaktadır. Blokzincirinin ilk bloğu, bir ana bloğu olmayan genesis blok olarak adlandırılır.



Şekil 1. Blok Zinciri Yapısı

Bir blok başlık ve bir gövdeden oluşmaktadır. Blok başlığında bulunan bilgiler şu şekildedir.

- Blok versiyonu, hangi blok doğrulama kurallarının uygulanacağını belirler.
- Merkle ağaç kökü özeti, bloktaki tüm işlem kayıtlarının özet değerini tutmaktadır.
- Zaman damgası, 1 Ocak 1970 tarihinden beri evrensel zamanda saniye olarak geçerli zaman bilgisini tutmaktadır.
- Nbit, geçerli bir blok özet değeri için eşik değer bilgisi içermektedir.
- Nonce, genellikle 0 ile başlayan her bir hesaplama için artan 4 byte boyutunda bir alandır.
- Önceki blok özet değeri alanında zincirde bir önceki bloğa karşılık gelen 256 bit boyutunda bir özet değer tutulmaktadır.

Örnek bir blok bilgisi Şekil 2'de gösterilmektedir.

Şekil 2. Blok Yapısı

C. Blok Zinciri Avantaj ve Dezavantajları

Blokzincirinin avantajlarını ve dezavantajlarını genel olarak aşağıdaki gibi sıralayabiliriz [9].

Blokzincirinin avantajları;

- Verilerin bir kopyası tüm paydaşlar tarafından kaydedilir, herkes bu verilere erişebilir ve yapılan işlemleri görebilir. Verilerin bu şekilde saklanması sayesinde veri kaybı ve veri tahribatı önlenir.
- Dijital imza ve doğrulamalar sayesinde aracılara ihtiyaç duymadan paydaşlarını birbirine güvenmesini sağlanır.
- Herkes hem kendi işleminin durumunu hem de blokzincirindeki tüm işlemlerin ayrıntılarını görebilir, bu şekilde şeffaflık sağlanmış olur.
- Blokzinciri üzerindeki veriler değiştirilemez veya silinemez.
- Merkezi bir otorite olmadan çalışabilir, bu dağıtık yapısı sayesinde kontrol edilemez, iptal edilemez veya kapatılamaz.
- Akıllı sözleşmeler sayesinde belirli faaliyetler otomatikleştirilebilir.

Blokzincirinin dezavantajları;

- Uzlaşma protokolü olarak proof of work (işin ispatı) kullanılan blokzincirlerinde çok fazla enerji tüketilmekte ve çok pahalı bilgisayar sistemleri çalıştırılmaktadır.
- Blokzincirindeki tüm veriler her bir düğümde ayrı ayrı saklanmaktadır ve her bir işlem sonrası bu düğümlerdeki verilerin tutarlılığı sağlanmaktadır. Örneğin zincire bir blok eklemek Bitcoin zincirinde 10- 60 dakika Ethereum zincirinde ise 15 saniye zaman almaktadır. Bu nedenle geleneksel veritabanları ile performans bakımından kıyaslandığında yetersiz kalmaktadır.
- Ağdaki her bir düğümün tüm verilerin bir kopyasını saklayabilmesi ve içeriğine erişebilmesi, kullanıcıların mahremiyetine zarar verebilir.
- Akıllı sözleşmeler bir kez oluşturulduktan sonra değiştirilemez ve blokzincirinde herkesin erişimine açık halde saklanır. Bu da akıllı sözleşmeleri kötü niyetli saldırılara karşı savunmasız bırakabilir

III. SONUÇ

Blokzinciri, şeffaflığı ve merkezi otoriteyi ortadan kaldıran dağıtık yapısı sayesinde bilgi teknolojilerinde yeni bir dönemin başlangıcı olarak ifade edilebilir. Basın, sosyal medya, uluslararası kuruluşlar özel sektör ve kamu kurumları blokzinciri konusuna büyük ilgi göstermektedir ve akademik çalışmalar incelendiğinde son birkaç yılda blokzinciri konulu çalışmaların sayısının hızla arttığı görülmektedir.

Blokzinciri teknolojisi iş dünyasının iş yapış şekillerini değiştirebileceği, ülkeler bağlamında sınırların kalkmasına ve ortak dili konuşma noktasında destek olacağı anlaşılmaktadır. Örnek olarak bankacılıkta bir ülkeden başka bir ülkeye para aktarmada (swift) ücret ödeme ve zorluğu varken dijital paralarla saniyeler içinde küçük masraflar ile aktarımının sağlanması gerçekleşmektedir. Blokzinciri gibi merkeziyetçi yapıları ortadan kaldıran şeffaf ve hesap verebilir teknolojilerin ortaya çıkması ve gelişimi sonrasında iş dünyasının bu değişime ayak uydurması, ülkelerin bunlara göre kendini, yönetimlerini, kanunlarını yeniden düzenlemesi gerektiği anlaşılmaktadır. Bu kapsamda eğitim müfredatlarında blokzinciri gibi yeni teknolojilere yer verilmesi, çağın yeterliklerine sahip insan kaynağının yetişmesi, bu teknolojilerin uygulama sahasının gelişmesine ve daha doğru anlaşılmasına katkı sağlayacaktır. Bu alanda yetişmiş insan gücü kurum/kuruluşların küresel ekonomide daha rekabetçi hale gelerek daha fazla katkıda bulunma imkânına sahip olacaktır.

KAYNAKLAR

[1] K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing Blockchains: Characteristics and Applications," in 11th IADIS International Conference on Information Systems, 2018, pp. 49–57.

[2] Blockchain Distributed Ledger Market Size by Type, End-User, Allied Market Research Report, 2017. [Online]. Available: https://www.alliedmarketresearch.com/blockchain-distributed-ledger-market. [Accessed: 14-Nov-2018].

[3] D. Tapscott and A. Tapscott, Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world, 2016.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf."

[5] R. Beck, "Beyond Bitcoin: The Rise of Blockchain World," Computer (Long. Beach. Calif)., vol. 51, no. 2, pp. 54–58, Feb. 2018.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, 2017, pp. 557–564.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Futur. Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018.

[8] Wyman O, Euroclear (2016) Blockchain in capital markets—the prize and the journey.

[9] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, "To Blockchain or Not to Blockchain: That Is the Question," IT Prof., vol. 20, no. 2, pp. 62–74, Mar. 2018.