ISSN: 2547-9725
Akademik İzdüşüm Dergisi
Journal of Academic Projection
2020; 5 (2); 172-182

Araştırma Makalesi / Research Article

Proof of Meet Konsensüs Protokolünün Gıda Taşımacılığı Üzerine Bir Uygulaması*

Sevda ÇAĞINDA**
Selçuk TOPAL***

Özet

Blokzinciri, merkeziyetsizliği şeffaf şekilde yansıtmayı ve üçüncü tarafları aradan çıkararak, gerek eşler arası (P2P) işlemleri gerekse değiştirilemez kayıtların elde edilmesini amaçlayan bir teknolojidir. Bir konsensüs protokolü, katılımcıları konsensüs kurallarının uygulanmasında işbirliği yapmaya zorlayarak blokzinciri üzerindeki kontrolü merkezsizleştiren bir algoritmadır. Çeşitli konsensüs protokolleri koşularak oluşturulan silinemez kayıtlar, şirketlerin, devletlerin ve bireylerin özel verileri olabilir. Blokzinciri platformu verileri saklar, korur ve hatta aracısız şekilde iletilmesini ve doğruluklarının ispatlanabilmesini sağlar. Her protokol ve blokzinciri platformu iş sahasına ve konusuna, proje yapısına ve kullanım fonksiyonlarının özelliklerine göre özelleştirilir. Son zamanlarda, blokzinciri kavramı pek çok iş sahasına uygulanmaya başlamıştır. Özellikle tedarik zinciri blokzinciri teknolojisinin odak noktalarından biridir. Gıda taşımacılığı ise tedarik zincirinin önemli bir ayağıdır. Bu araştırmada iletişim içinde olan iki ayrık zincire sahip HOX blokzincirinin ve üzerinde çalışan Proof of Meet (PoM) konsensüs protokolünün gıda taşımacılığı sektöründe nasıl kullanılacağı gösterilecektir. Ayrıca, herhangi bir enerji tüketimine ihtiyaç duymadan sektör çalışanlarının ve görevlilerinin çalışma performansı ve emeğine karşılık olarak adil ve merkezsiz şekilde ödüllendirildiği PoM modelinin diğer konsensüs protokolleriyle karşılaştırarak gıda taşımacılığı sektöründeki bir uygulaması verir.

Anahtar Kelimeler
Blokzinciri, Tedarik Zinciri, Gıda Taşımacılığı, Konsensüs Algoritması, Proof of Meet

An Application of the Proof of Meet Consensus Protocol on Food Transportation

Abstract

Blockchain is a technology that aims to obtain both peer-to-peer (P2P) transactions and immutable records by reflecting decentralization transparently and eliminating third parties. A consensus protocol is an algorithm that decentralizes control over the underlying blockchain by forcing participants to cooperate for applying consensus rules. Immutable records created under various consensus protocols may be private data of companies, governments and individuals. The blockchain platform stores and protects data, and even enables it to be transmitted and verified without intermediaries. Each protocol and blockchain platform is customized according to the business scope and subject, project structure, and usage functions. Recently, the concept of

* Bu makalede bilimsel araştırma ve yayın etiği ilkelerine uyulmuştur. / In this article, the principles of scientific research and publication ethics were followed.

** Lisans 4. sınıf öğrencisi, Bitlis Eren Üniversitesi, Sağlık Yüksekokulu, Beslenme ve Diyetetik Bölümü, Bitlis, Türkiye,sevdacgnd@gmail.com, ORCID: 0000-0001-8428-460X

*** Doç. Dr. Bitlis Eren Üniversitesi, Fen Edebiyat Fakültesi, Matematik Bölümü, Bitlis, Türkiye. s.topal@beu.edu.tr, ORCID:0000-0002-5829-5257

Atıf yapmak için / To cite this article: Çağında, S. & Topal, S. (2020). Proof of Meet Konsensüs Protokolünün Gıda Taşımacılığı Üzerine Bir Uygulaması. Akademik İzdüşüm Dergisi, 5(2): 172-182.

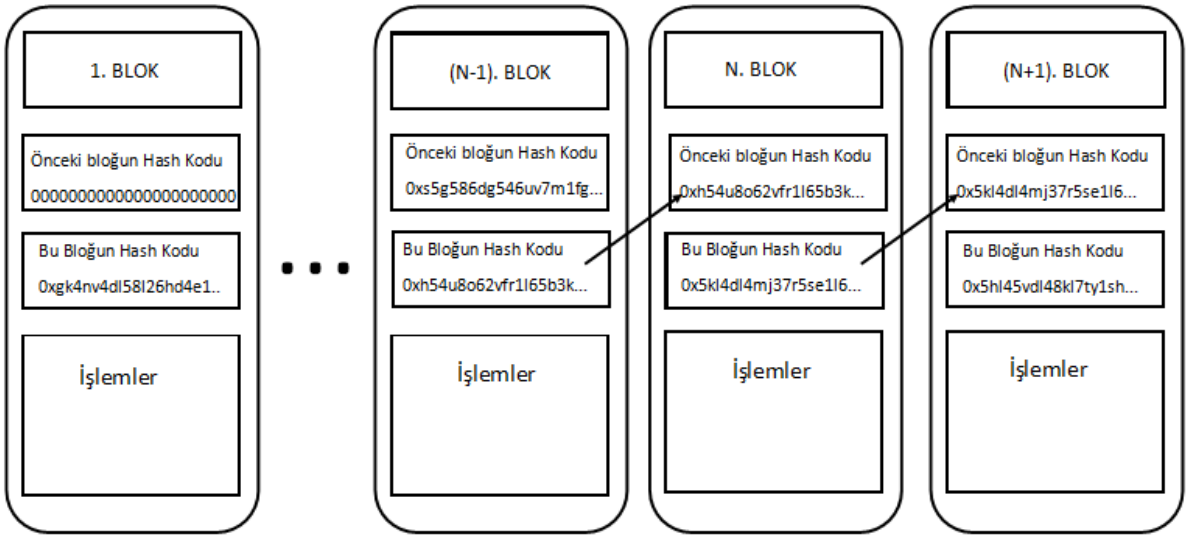
Başvuru tarihi/ Received: 12.09.2020 - Kabul tarihi/Accepted: 17.10.2020

blockchain has started to be applied to many business areas. In particular, the supply chain is one of the focal points of blockchain technology. Food transportation is an important part of the supply chain. This research shows use cases and how to use the HOX blockchain with two discrete chains in communication and the Proof of Meet (PoM) consensus protocol running on it in the food transportation industry. In addition, an application is given in the food transport sector by comparing the PoM model with other consensus protocols in which the sector employees and officials are rewarded fairly and decentralized for their work performance and labor without the need for any energy consumption.

Keywords
Keywords: Blockchain, Supply Chain, Food Transportation, Consensus Algorithm, Proof of Meet

GİRİŞ

Geçmişten bugüne alışveriş halinde olan insanlar ve ticari kurumların güven sorunlarını ortadan kaldırmak amacıyla üçüncü taraflar (bankalar) var ola gelmişlerdir. Güven sağlayan bu üçüncü taraflar hizmetlerinin karşılığında maliyeti arttırırlar ve alışverişlerin mali kayıtlarını veri depolarında tek bir merkezde korumaya çalışırlar. Ancak bu işlemler zaman kaybı ve maliyetlerin yükselmesi ile sonuçlanması sebebiyle hizmet satın alanları memnun etmez. Ayrıca tüm bu bilgilerin tek bir merkezde olması herhangi bir güvenlik açığı durumunda verilerin silinmesi veya değiştirilmesiyle çok büyük risk oluşturur. İlk olarak 2008 yılında Satahohsi Nakamoto (Nakamoto, 2008) tarafından 'Bitcoin: A Peer-to-Peer Electronic Cash System' adlı makale ile duyurulan blokzincir teknolojisi değiştirilemez veri kaydı, güvenliği ve şeffaflığıyla üçüncü tarafları elemine edebilecek niteliklere sahiptir. Bir blokzinciri, genesis bloğundan başlayarak, içine verilerin kayıt edildiği ve belirli veri sayısına ulaşıldığında yeni bloğun önceki bloğun bir hash kodunu da içerecek şekilde oluşturulduğu dağıtık bir veri tabanıdır. Konsensüs algoritmaları sayesinde bu dağıtık veri tabanı merkeziyetsizleştirilmeye çalışılır. Merkezsiz oluşu sayesinde korunur ve pratikte asla heklenemez. Kullanılan konsensüs algoritmalarıyla sağladığı güvenliğin yanı sıra ağda blok oluşturma ve blok ödüllerinin dağıtımını etkilediği için ağdaki her cihaz hash değerlerinin deşifrasyonu için rekabet eder. Bu rekabet kullanılan konsensüs algoritmasına göre bazen cihazın işlem gücüne (PoW), bazen sistemde hisselenmiş koin miktarına (PoS) göre belirlenir. Ağdaki cihazların çoğunluğu tarafından onaylanan blok artık hash kodu ile şifrelenmiş olarak zincire eklenir.



Şekil 1. Blokzincirinin Hash Kodlarıyla Birbirine Bağlanması

Böyle bir sistemde ağa yapılacak herhangi bir saldırı kendinden sonraki tüm blokların hash kodunu dolayısıyla kendinden sonraki tüm blok verilerini değiştireceğinden zincir yanlış bir

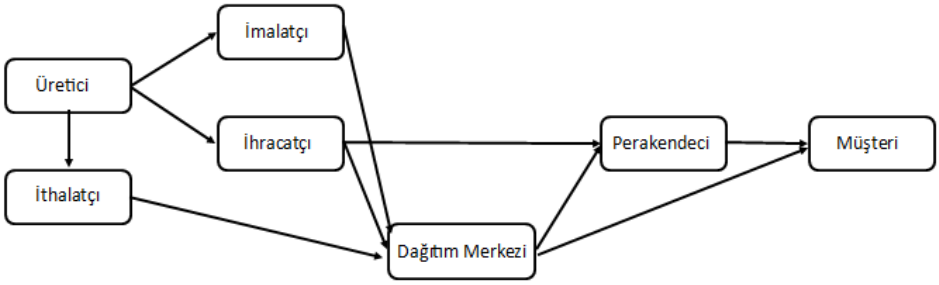
zincir olur ve atıl duruma düşer. Çünkü sistem ağdaki düğümlerin çoğunluğunun kabul ettiği zinciri esas zincir kabul eder. Yani ağa saldırı yapan bir düğümün ağdaki cihazların yarısından fazlasını aynı anda heklemesi ve değiştirmek istediği bloğu ve ondan sonraki tüm blokları doldurabilecek kadar zamana ihtiyacı olur. Ancak böyle bir durum pratik olarak imkânsızdır. HOX blokzinciri ise iki ayrık fakat iletişim içindeki zincirlerden oluşmaktadır. Bir zincir koin gönderisi ve alımı gibi işlem bilgilerini kayıt ederken diğeri ise akıllı sözleşmeler vasıtasıyla hem taşımacılık bilgilerini hem de bu operasyonlara karşılık gelen ödül hesaplarını içerir. Böylece platform ağır hesap yükü karmaşasından uzaklaştırılır ve etkin çalışan bir formata dönüştürülür. Blokzinciri teknolojisinin şimdiye kadar tarihinde iki devrim yaşadığını söyleyebiliriz; Bitcoin (Nakamoto, 2008) ve Ethereum (Wood, 2014). Bitcoin, blokzincir 1.0 olarak adlandırılan teknolojinin sadece veri kaydı ve güvenliği sağladığı dağıtık şeklidir. Bu şekliyle finans sektöründe önemli gelişmeleri sağladı. Ethereum ise Vitalin Buterin'in akıllı sözleşme kavramı çerçevesinde blokzincir alt yapısıyla oluşturulan ve blokzincir 2.0 olarak adlandırılan platformdur. Ethereum'un bu kadar önemli olmasının sebebi; tarihi BZT'den öncesine dayanan akıllı sözleşmeler için hem kolay uygulanabilir hem de güvenilir bir platform olmasıdır. Akıllı sözleşmeler blokzincirdeki hesaplar gibi akıllı sözleşme hesaplarına sahiptir. Sözleşmenin uygulayacağı algoritmalar ve yapacağı hesaplamalar gibi bilgilerin detaylarıyla kodlanarak Ethereum web sitesine yüklenmesi sonucu sözleşmeye dâhil olan her düğümün sözleşmenin şartlarına uyması sistem tarafından doğrulanır. Sözleşmenin doğru ve eksiksiz hazırlanması oldukça önemlidir. Aksi bir durumda DAO adlı projede olduğu gibi bir kullanıcı akıllı sözleşmenin herhangi bir açığından faydalanıp sözleşme hesabındaki parayı başka hesaba aktarabilir (Yıldız, 2019).

GIDA TEDARİK ZİNCİRİNDE (GTZ) BLOKZİNCİRİ TEKNOLOJİSİ

Tedarik zinciri, birçok paydaş arasında hammaddeden tüketiciye sunulacak ürünün tüm hareketlerinin kaydıdır. Tedarik zinciri yönetimi ise kaliteli son ürün için tedarik zinciri paydaşlarının etkili iletişimi ile sürecin ekonomik ilerlemesinin planlamasıdır. Bunun sağlanması için etkin bir lojistik ve gelişen teknolojiye uyum sağlamak şarttır (Keleş ve Ova, 2020). Tarımsal üretim, hasat, işleme, paketleme, taşıma, dağıtım gibi birçok aşamadan geçen ve özellikle mikroorganizmalar için ideal yaşam koşullarına sahip gıdaların tedarik zinciri ekstra önem taşır. Son 20 yılda ortaya çıkan at eti skandalı, yumurtada salmonella, hamburgerde Escherichia coli, peynirlerde Listeria gibi birçok gıda güvenliği (Tian, 2018) ve gıda sahteciliği uygulamaları tüketicilerin ve tedarik zincirindeki paydaşların satıcılara güvenmemesi sorununa yol açmıştır. Bu tür sorunların çözümü için GTZ'nin izlenelebilirliği içinde bulunduğu sorunların çözümünü kolaylaştırır (Gerdan vd., 2020).

Teknoloji her alanda olduğu gibi besinlerin tedarik zincirinde de etkisini göstermiş ve maliyet, zaman ve güven avantajı için bazı yazılımlar geliştirilmiştir. Bunların bazıları; elektronik veri değişimi (EDI), kurumsal kaynak planlaması (ERP), radyo frekanslı kimlik tanımlama (RFID), nesnelerin internetidir (IoT) (Keleş ve Ova, 2020). Ancak bu yazılımlar gıda şirketlerinin sadece kendi bünyelerinde gerçekleşen alışverişleri ve uygulamaları hızlandırır. İki şirket arasındaki alışverişler için yine üçüncü taraflara ihtiyaç duyar.

Şekil 2'de basit bir şekilde bir geleneksel GTZ şeması çizilmiştir. Burada oklar ile gösterilen her alışverişin kaydı yalnızca ilgili taraflar tarafından kaydedilip her şirket kendi bünyesinde gerekli gördüğü kadar veriyi saklar.



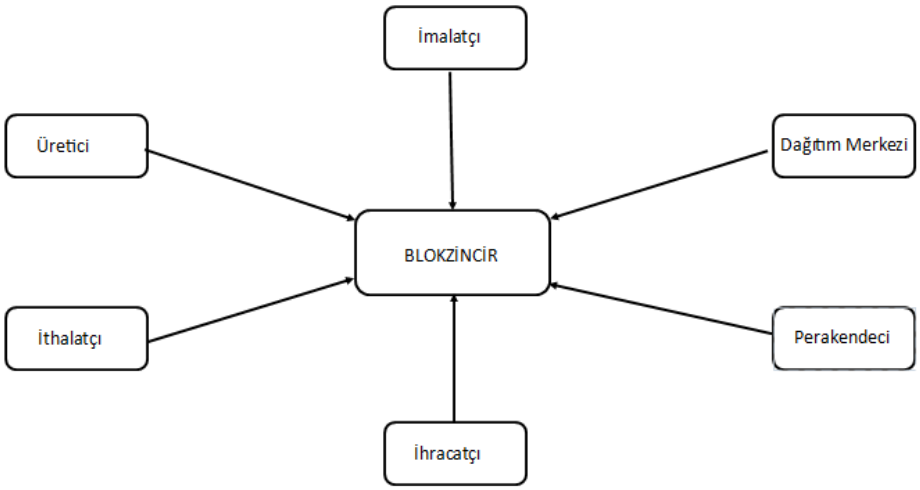
Şekil 2. Geleneksel Gıda Tedarik Zinciri Örneği

Böyle bir zincir, tüketicinin satın aldığı gıdanın takibi için herhangi bir mekanizmaya sahip değildir. Ayrıca farklı tedarik noktalarında birden fazla kez denetlenmesi ve vergilere tabi tutulmasından kaynaklı maliyet artması ve işlemlerin kabul edilmesi, paranın hizmet satana tahsis edilmesi ise zaman kaybı ile sonuçlanmaktadır.

Blokzincir teknolojisi (BZT), şimdiye kadar sıraladığımız tüm sorunlara aynı anda çözüm olma niteliğindedir. BZT'yi bir teknoloji olarak düşündüğümüzde sahip olduğu yenilikler sadece dağıtık ve güvenli bir veri kaydı sağlıyor olmasıdır. Ancak bu teknolojinin bu kadar etkili olması geliştirilen uygulamalarla farklı alanlarda kullanılıp özelleştirilerek farklı sorunlara çözüm bulmasıdır (Sultan vd., 2018). Farklı türlerinin olmasına karşın blokzincirinin genel olarak kamuya açık veya kapalı (özel), dağıtık bir veri tabanı olduğunu söyleyebiliriz. Ağa katılan her düğümün veri ekleyebileceği, okuyabileceği, onaylayabileceği ve asla değiştiremeyeceği hızla yayılan bir platformdur. Dolayısıyla sağladığı avantajlardan dolayı birçok uygulama alanı bulmuştur.

BZT'nin gelişim süreci üç kısımda incelenebilir: ilki para transferi, havale ve dijital ödemeler; ikincisi akıllı sözleşmelerin gelişmesiyle birlikte hisse senetleri, tahviller, vadeli işlemler, krediler, ipotek gibi piyasalar ve finansal işlemler; üçüncüsü maliye piyasalarının dışındaki hükümet, sağlık, bilim, kültür sanat alanlarındaki uygulamalarıdır (Taş ve Kiani, 2018). Bu sektörlerden özellikle finans, bankacılık, sağlık ve tedarik zinciri sektörlerinde gelişmeler hızla devam ediyor.

Blokzinciri geleneksel tedarik zincirindeki iletişimsizlik ve ürün geçmişine dair bilgi sorunu gibi sorunlara köklü çözümler sunar. Blokzinciri ağına tüm tedarik zinciri paydaşlarının katılımıyla oluşacak blokzincirinde hammaddeden son ürüne kadar kalıcı ve güvenli ürün geçmişini belgelemek mümkün olacaktır. Bu zincirin akıllı sözleşmesi ile her alıcı ürünü geçmiş bilgisini kontrol ederek alabilir.



Şekil 3. Blokzincir Uygulamalı Tedarik Zinciri

Şekilde de görüldüğü üzere, üreticiden tüketiciye her aşamada gıdanın tüm özellikleri tek bir zincirde ancak ağdaki her düğümde kaydedilir. Bu zincir hem güvenli hem maliyeti düşürür hem de zaman kazandırır. Bu aşamaların izlenebilirliği için geliştirilen blokzincir modellerinin işleyişini dile getirelim. Bir akıllı sözleşme dâhilinde oluşturulan blokzincir üzerinden müşteri ürün için talep oluşturur ve satıcı bunu onaylar ise MetaMask (2020 Ağustos, https://metamask.io/) üzerinden hesabından para kesilir, ret ederse alıcı bundan hemen haberdar olup yeni bir satıcıya talep oluşturabilir. Sonra satıcı ürünün taşıması için bir nakliye şirketi ile anlaşır ve nakliye sırasında ürünün güvenliği için belirli periyotlarla ürün ortamının nem ve sıcaklık değerleri ölçülüp kaydedilir. Ürün alıcıya ulaştığında alıcı bunu onaylar ve bloğa veri olarak kaydeder (Onay vd., 2019).

Günümüzde uygulama alanları bulmuş olan BZT devlet, hastane, şirket ve üniversite gibi kurumların tüm bilgi akışını kaydedebilir (Taş ve Kiani, 2018). Gıda tedarik sektöründe de bazı markaların dikkatini çeken BZT Skuchain, Provenance, Walmart, Everledger, Nestle, Carrefour gibi büyük markalar tarafından ürünlerinin tedarik zincirlerini daha iyi denetlemek ve daha çok sorunu daha etkili yollarla çözmek amacıyla kullanılmaya başlanmışlardır. Aşağıda bazı markaların blokzinciri kullanım şekilleri anlatılmıştır.

Wallmart, gıda ürünlerinin geçmişini ve sertifikalarını; Provenance, balıkların denizden ton balığına kadar ürünlerin izlenilebilirliğini (bu sayede yasadışı balıkçılık önlemlerini alabilmek) (https://impacttlimited.com/provenance-blockchain-innovators/); Intel Sawtooth Lake, balıkçılardan restorana kadar balıkla ilgili bilgileri (https://www.coindesk.com/intel-demos-seafood-tracking-sawtooth-lake-blockchain); Everledger, şarapların hareketlerini ve depo bilgilerini; Downstream, bira üretiminde mayalama yöntemleri ve bileşenlerini; Aldo Cozzi, makarnaların lojistik yönetimi ve kullanılan un kurutma tipi vb.; San Domenico Coffee, fidandan tüketiciye kadar kahvenin izlenilebilirliğini; jd.com, sahtecilikle mücadele için tüm perakende sürecini (https://www.ledgerinsights.com/jd-com-blockchain-traceability-asset-backed-securities/); Arc-net alkollü içkilerin tarım ürünleri, hasat ve damıtma bilgilerini; Ripe.io sensör bilgileriyle gıda kaynağı bilgilerini blokzincir sistemleriyle paylaştılar (Keleş ve Ova, 2020). Nestle müşterilerin ürün sürdürülebilirliği ve provenasını takip etmeleri için BZT kullandıklarını duyurdu (https://borsablockchain.com/nestle-blockchain-teknolojisine-basliyor/). Carrefour ve Nestle ortaklaşa kullandıkları BZT ile Mousline patates püresinin ürün geçmişini sadece bir QR kodu aracılığıyla müşterilere sundular (https://www.kriptoarena.com/nestle-ve-carrefourdan-blockchain-ortakligi). Et, süt ve meyvelerin ürün geçmişlerini paylaştıktan sonra satışların arttığını gözlemleyen Carrefour daha fazla ürünü blokzinciriyle paylaşacaklarını duyurdu (https://www.reuters.com/article/us-carrefour-blockchain/carrefour-says-blockchain-tracking-boosting-sales-of-some-products-idUSKCN1T42A5).

ABD' FDA tarafından reçeteli ilaçların takibi ve izlenilebilirliği için Merck, IBM, KPMG ve Walmart ABD Tedarik Zinciri Yasası'nı tanımlamak üzere her şirket ürünlerin izlenilebilirliğini sağlayacak şekilde blokzincirine paylaşım yapacaklar (https://bctr.org/kpmg-merck-ve-walmart-ilac-tedariginde-blockchain-kullanacak-9418/).

Literatürde blokzincir alt yapısıyla "tarladan çatala", "denizden sofraya" gibi GTZ'de önerilen birçok akıllı sözleşme önerisi var. Gelecekte tedarik zinciri ve daha birçok sektörde BZT'nin kilit nokta olacağına inanıyoruz.

BLOKZİNCİRİNDE KULLANILAN KONSENSÜS ALGORİTMALARI

Konsensüs algoritmaları blokzincirine kabul edilecek bloğun kabul edilmesi için ağdaki düğümlerin uzlaşma şeklini belirtir. Belirli sayıda verilerin girilmiş olduğu ve artık zincire

eklenmesi gereken yeni blok onaylamasını yapan ilk düğüm ağdaki diğer düğümlere şifreleri oluşturduğunu duyurur. Yeterli çoğunlukta düğüm bulunan değerlerin doğruluğunu kabul ederse blok zincire eklenir. Bu denklemde bloğu ilk onaylayan kişi blok ödülü ile ödüllendirilir. Ağdaki cihazlar da her yeni blok için yeni bir yarışa girerler. En çok kullanılan iki algoritma Proof of Work (PoW) ve Proof of Stake (PoS)'dir.

Kullanılan konsensüs algoritması, sistemin çıktı performansını büyük oranda etkiler (Feng vd., 2018). Bu sebeple geliştirilen bazı projeler blokzincirlerinde yeni oluşturdukları konsensüs algoritmalarını kullanırlar. Bu algoritmaların bazıları aşağıda açıklanmıştır.

- **Proof of Work (PoW):** İlk blokzinciri konsensüs algoritmasıdır. Madenciler nonce adı verilen değeri bulmak için yarışırlar. Bu yarışta donanımı güçlü olan, en çok kazım yapacağından başarı oranı yüksek olur. Ayrıca ağdaki her düğüm doğru nonce değeri için çaba sarf ettiğinden çok fazla elektrik tüketimi meydana gelir.
- **Proof of Stake (PoS):** Ağda hisselenmiş koin miktarı en yüksek olan düğümün bloğu oluşturması beklenir. Belirlenen bir süre boyunca blok onaylanmazsa ikinci en yüksek koin miktarına sahip olan düğüme hak verilir. Ethereum blokzinciri 3-4 büyük projede PoW'u kullandıktan sonra PoS'u kullanmaya başladı. Bu protokole göre en varlıklı düğümlerin sistemi kandırmayacaklarına inanılır.
- **Proof of Deposit (PoD):** İşleyiş mekanizması genel olarak PoS'a benzeyen bu protokol düğümün koinlerinden bir kısmını depozito olarak ayırdığı ve bunu harcayamayacağı bir algoritmaya sahiptir. Kullanıcılardan en çok depozito ayıran blok oluşturur (Yıldız, 2019).
- **Proof of Capacity (PoC):** Proof of space olarak da adlandırılan bu protokol PoW'da, her düğümün (cihazın) anlık iş oranın değişebilmesine karşın belleğin bir kısmını sadece kazı için ayırtır. Bu şekilde kazı için en çok enerji harcayan düğüm blok oluşturur ve blok ödülünü alır (Kumar vd., 2020).
- **Proof of Burn (PoB):** Madencilerin koin yakarak blok üretme hakkı elde ettikleri protokoldür. Ne kadar çok koin yakılırsa blok üretme şansı o kadar artar (Zheng vd., 2016). Yakılan paranın ağın kriptoparası olması gerekir, yeni bloklar oluştukça yakılan koinin etkisi azalır.
- **Simplified Byzantine Fault Tolerance (SBFT):** Belirlenmiş bir üretici düğüme paydaşlar mesaj atar. Üretici düğüm bu mesajları düzenler, periyodik bir şekilde sıralar daha sonra ağdaki diğer düğümlere onaylamaları için gönderir (Ataşen, 2019).
- **Pratical Byzantine Fault Tolerance (PBFT):** Ağdaki her düğümün birbiriyle iletişim halinde olduğu ve blokları oyladıkları bir sisteme sahiptir. Bir kullanıcı lider düğüme mesaj gönderir ve lider düğüm bunu diğer düğümlere gönderir. Düğümler kendilerine gelen mesajların hem göndericisini hem de mesajın değiştirilmediğini onaylamalıdır. Sistemdeki kötü amaçlı saldırı sorununa çözüm sağlar (Feng vd., 2018).
- **Proof of Importance (PoI):** Bir düğümün bloğa uygun olup olmadığının anlaşılması için hasat yapılır. En çok hasat yapılan bloğun zincire eklenmesi daha kolay olur. Düğümlerin hasat yapması için en çok hasat yapma oranına göre önem puanı hesaplanır ve önem puanı en yüksek olan blok ödülü alır (Eigelshoven vd., 2020).
- **Delegated Byzantine Fault Tolerance (DBFT):** Bu protokole göre blokzincirinde kullanıcılar üçe ayrılır; sıradan düğümler, temsilciler ve konuşmacı. Sıradan düğümler temsilcilere mesaj atar ve onlar arasında oylama yapar. Bu temsilciler arasında rastgele seçilen bir konuşmacı kendilerine gelen mesajları diğer temsilcilere yayar. Temsilcilerin üçte ikisinin bloğu onaylaması gerekir. Yeterli sayıya ulaşılmazsa yeni bir konuşucu seçilir ve aynı işlemler devam eder daha sonra blok zincire eklenir (Chiristofi, 2019).
- **Delegated Proof of Stake(DpoS):** Katılımcılardan seçilen bir grup temsilci arasında oylama yapılır ve oyu en yüksek düğüm blok oluşturur (Eigelshoven vd., 2020).
- **Leabsed Proof of Stake (LPoS):** Katılımcıların blok doğrulayabilmek için koin kiralayabildikleri konsensüs algoritmasıdır (Eigelshoven vd., 2020).

- **Proof of Activity(PoAc):** PoW ve PoS'un birleştirilmesiyle oluşmuştur denebilir. Madenciler PoW'da olduğu gibi tüm bloğu mine etmek yerine sadece blok başlığı ve kalıplarını kazım yaparlar (Zheng vd., 2016). Daha sonra rastgele bir grup doğrulayıcı seçilir ve blok doğrulayıcılar tarafından onaylanır.
- **Proof of Authority (PoA):** Kullanıcıların koin miktarına göre değil itibar değerlerine göre blok oluşturabildikleri algoritmadır (Kumar vd., 2020; Eigelshoven vd., 2020).
- **Proof of Weight (PoW):** Bu algoritma ağırlıklandırılmış faktörler ve PoS'da olduğu gibi koin miktarı ile hesaplamalar yapar. Bunun en büyük avantajı her sektör için özelleştirilebilir olmasıdır (Ataşen, 2019).
- **Proof of Elapsed Time (PoET):** Ağdaki katılımcılardan rastgele belirlenen zaman aralığını ilk bitiren düğüme bir blok oluşturma hakkı verilir. Blok oluşturduktan sonra tekrar rastgele beklemesi gereken zaman tanımlanır (Eigelshoven vd., 2020).

Bir bloğun kabul edilip ağa katılmasını sağlayacak bu algoritmalar ağın güvenliği ve devamlılığının sağlanması yanı sıra sahip oldukları bazı özelliklerden dolayı ağın merkezileşmesine sebep olmaktadır. Tablo 1'de bazı konsensüs algoritmalarını avantaj ve dezavantajlarıyla listeledik. Merkezileşme özelliği en kötü olasılıkları göz önünde bulundurarak merkezileşmesi mümkün protokoller tabloda belittik.

Tablo 1. 2009'dan beri geliştirilen başlıca konsensüs algoritmaları ve özellikleri

Yıl	Konsensüs Algoritması	Akıllı Sözleşme	Merkezileşme	Avantaj	Dezavantaj
2009	PoW	Yok	Mümkün	Güvenli	Yüksek enerji tüketimi
2015	PoS	Var	Mümkün	Düşük enerji tüketimi	Merkezileşme
2014	PoC	Var	Mümkün	Ucuz, Verimli	Merkezsizleştirme sorunu
2014	PoB	Yok		Enerji harcamamak	Ekonomik kayıp
2014	SBFT	Yok	Mümkün	İmza ile doğrulamadan dolayı güvenli	Açık blokzincirler kullanamaz
2015	PBFT	Var	Mümkün	Düşük enerji tüketimi	Büyük ölçekli blokzincirlere uygulanamaması
2015	PoI	Var	Mümkün	Adaletli, sahte işlemlerin tespiti	Yüksek enerji tüketimi, merkezsizleştirme sorunu
2016	DBFT	Var	Mümkün	Ölçeklenebilirlik	Zincirdeki çakışmalar
2016	DPoS	Yok	Mümkün	Demokratiktir, düşük enerji tüketimi, ölçeklenebilir, güvenili	İki kez harcama saldırısı, akıllı sözleşme özelliğinin olmaması
2016	LPoS	Var	Mümkün	Koinleri kiralayabilme	Merkezsizleştirme sorunu
2016	PoAc	Var		%51 saldırısını engeller	Yüksek enerji tüketimi
2017	PoA	Var	Mümkün	Düşük enerji kullanımı	Ağır blokzincirlerin kullanamaması
2017	PoWeight	Var	Mümkün	Özelleştirilebilirlik	Tanınmama
2017	PoD		Mümkün	Düşük enerji tüketimi	Merkezileşme
2018	PoET	Var		Katılım ucuzdur	Özellikli donanım

Sonuç olarak merkeziyetsiz olan blokzincir teknolojisi kullanılan konsensüs protokolüyle sözleşme ile ilgisi olmayan bir madenci tarafından kazanılabilir. Daha haklı bir rekabet ortamı için, her proje kendi için geliştirilen bir Proof of Meet (PoM) (Topal, 2020)

sistemi kullanılabilir. Yani zinciri en etkili ve aktif kullanan kişinin, tedarik edilen besinin uygun ve olabilecek en sağlıklı ve en kısa zamanda nakliyesi PoM ile denetlenip blok ödülü ile ödüllendirilebilir.

Bu makale blokzincir üzerinden talebi oluşturulmuş gıdanın takibi için PoM'u kullanmaya yöneliktir. PoM ise taşıma sırasında gıdanın en az zarar ve en kısa sürede tedarikçiye ulaşılması, bunun kayıt altında yapılması ve işini doğru veya yanlış yapan kişilerin verdiği emeğe, yaptığı işe göre blok ödülü ile ödüllendirilmesini hedeflemektedir.

PoM'UN GIDA TAŞIMACILIĞI ÖRNEKLEMİ

PoM, ilk kez HOX projesi (Topal, 2020) için PoS ve Blok Zinciri Tabanlı Konum Kanıtı (BTKK)'nın üzerine kurulmuş bir sistemdir. Bir kafe ve restoran gibi sabit bir konuma müşteri olarak giden kişilerin mobil cihazlarıyla bulundukları ortamda geçirdikleri süre ve buluştukları kişiler ile hem ağı kullandıklarını hem de bulundukları ortamın verisinin doğrulamasını yapmalarıyla blok ödülü ve indirim kazandıkları bir algoritmaya sahiptir. Ortamda en az iki müşteri (mobil cihaz, telefon vb.) ve bir sabit konum (Wi-Fi ağı) bulunmasını temel alan bu sistemde PoS ağa giriş için bir ön koşul, BTKK blok ödülü için gerçek çabayı simgeliyor.

PoM, blok ödülünü etkilemesinin yanı sıra gıdanın takip edilebilirliği dolayısıyla gıdanın daha güvenli taşınmasına olanak sağlar. Bu da BTKK ile hem gıdanın takibini sağlar hem de blok ödülü için haklı bir rekabete zemin hazırlar.

Hedefler:

- Blokzinciri işleyişinin kandırılmasını önlemek
- Emeğe göre ödüllendirilmek
- Alışverişte güvenliği ve sürekliliği sağlamak
- Haksız rekabeti önlemek
- Vergilendirmede kolaylık sağlamak

Ödüllerden sağlanacak faydaların oranları aşağıdaki metotlarla hesaplanır:

- En çok iş yapan (alım veya satım)
- Mesafeye göre en kısa sürede taşıma yapan
- En uygun koşullarda taşıma yapan-yaptıran
- En fazla kişiyle iş yapan

İnsan kaynaklı hataların ve haksızlığın önüne geçmek için elbette bunların hepsi sistem tarafından otomatik bir şekilde denetlenmelidir. Bunun sağlanması için her gıdanın taşıma için en uygun koşulları akıllı sözleşmelerde zaman damgalı olarak birer birer belirtilmeli ve ürünün gördüğü hasara göre ya alış-veriş iptal edilmeli ya da önceden belirlenen bir miktar fiyattan düşürülmeli. PoM için önerilen tedarik zinciri aşağıdaki gibidir:

C_1 ağdaki müşteri, C_2 ise satıcı olsun. C_1 zincir üzerinden talep oluşturup ürün istediğinde C_2' nin bunu onaylayıp satılan gıdayı karşı tarafa taşıması gerekir. Taşıma için ise bir nakliyeci (C_3) ile anlaşması gerekir. C_2'in doğru bir nakliye şirketi seçmesi kendi iş itibarı için ve sağlıklı bir alışveriş için önemli bir noktadır. Burada C_2 ve C_3 arasındaki iş ilişkisinin denetlemesini C_1 ürünü kabul ettiğinde yapar. Eğer taşıma doğru ve uygun şekilde yani akıllı kontrata uygun yapılırsa hem C_1 hem de C_2; C_3'den memnun olur ve bu alışverişin devamlılığı sağlanabilir. Çünkü PoM tarafından alışverişin değer kazanması 3 tarafa da gerek indirim gerek blok ödülü gerekse iş sadakati konularında avantaj sağlar.

Üç kısım ispat doğrulayıcı ve blok doğrulayıcı eşit ağırlıklandırılmış olarak rol oynarlar: C_1, C_2 ve C_3. En yüksek güce sahip olanlar her defasında bu kümelerden seçilir. Bu anlamda hem enerji (elektrik gibi) harcaması yönünden avantaj sağlar hem en çok çalışan en çok kazanır.

C_1 ve C_2 iki sabit konum (tarla, fabrika, market vb.) olup taşımayı yapan aracın şoförünün mobil cihazı ile C_1 ve C_2'nin konumlarında olduğu anlar takip edilir. Blok verisi; taşınan malın miktarını, özelliklerini, taşımayı yapan aracın şoförünün (C_3'ün) C_2'de olduğu son anın ve C_1'de olduğu ilk anın bilgilerini (BTKK-şoförün mobil cihazının Wi-Fi ağlarına bağlı olması ile), bu verilerden elde edilen nakliye süresi bilgilerini ve belirli periyotlarla ölçülmüş taşınma şartlarını (cihazlardaki özel sensörlerle ölçülen nem ve sıcaklık değerlerini) taşır. Bu şekilde gıdanın taşınması süresi takip edilmiş olup blok verisi en az 3 taraf tarafından onaylanmış olur. Konsensüs algoritmalarını domine edecek rollere göre hisse güçleri aşağıdaki gibi hesaplanır:

C_1 için hisse gücü $P_1(C_i)$ hesaplanması:

SC(C_i): C_i için hisselenmiş koin miktarı.

SB(C_i): C_i'nin son bir ay içinde birlikte iş yaptığı tedarikçi sayısı.

BN(C_i): C_i'nin son birkaç ay içinde yaptığı iş (yaptığı gıda talebi sayısı).

$P_1(C_i) = w_1\text{SC}(C_i) + w_2\text{SB}(C_i) + w_3\text{BN}(C_i)$, $\sum_{h=1}^{3} w_h$ öyle ki $0.1 < w_h < 1$

C_2 için hisse gücü $P_2(C_i)$hesaplanması:

SC(C_i): C_i için hisselenmiş koin miktarı.

SB(C_i): C_i'nin son bir ay içinde birlikte iş yaptığı tedarikçi sayısı.

BN(C_i): C_i'nin son birkaç ay içinde yaptığı iş (aldığı gıda talebi sayısı).

DB(C_i): C_i'nin en uygun koşullarda yapılan iş derecesi (doğru bir C_3 seçimi).

$P_2(C_i) = w_1\text{SC}(C_i) + w_2\text{SB}(C_i) + w_3\text{BN}(C_i) + w_4\text{DB}(C_i)$, $\sum_{h=1}^{4} w_h$ öyle ki $0.1 < w_h < 1$

C_3 için hisse gücü $P_3(C_i)$ hesaplanması:

SC(C_i): C_i'nin hisselenmiş koin miktarı.

SB(C_i): C_i'nin son bir ay içinde birlikte iş yaptığı tedarikçi sayısı.

BN(C_i): C_i'nin son birkaç ay içinde yaptığı iş (nakliye sayısı).

SD(C_i): C_i'nin yaptığı nakliyenin hız derecesi (mesafeye göre zaman).

DA(C_i): C_i'nin yaptığı nakliyenin en uygun normlara göre uygunluk derecesi.

$P_2(C_i) = w_1\text{SC}(C_i) + w_2\text{SB}(C_i) + w_3\text{BN}(C_i) + w_4\text{SD}(C_i) + w_5\text{DA}(C_i)$, $\sum_{h=1}^{5} w_h$ öyle ki $0.1 < w_h < 1$

Bu değerlerin oranları ağdaki istemcilerin blok ödülü ve iş yaptıkları kişilerden indirim kazanmalarını sağlar. Elbette kısa mesafeye alış veriş yapmak hem alıcı hem satıcı için bir avantaj olur. Ayrıca daha fazla talep oluşturup (büyük bir alışverişi küçük parçalara bölerek) daha fazla iş yapmış gibi göstererek sistem manipüle edilebilir. Bunun için akıllı sözleşmelerde bunu önleyecek önlemler niteliğinde maddeler bulunmalıdır. Alışveriş yapan firmaların üretim/ağdaki iş oranları (toplam iş kapasitesi oranı) sisteme dâhil edilebilir. Bu şekilde küçük firmalar da büyüklerle yarışabilecektir. Kurumsal ve uzun zamandır ağda olan bir düğüm ile ağa yeni katılan bir düğüm eşit haklara sahip olmayacağından yaptığı işin miktarı son bir veya birkaç ay ile sınırlandırılmalıdır. Taşıyıcı firma için çalışma saati/mesai saatleri taşıyıcı firmaların arasında daha fazla iş yapma katsayısı olarak kullanılabilir. Bir düğüm ağa ilk katıldığında ise önceden hisslenmiş koin miktarı ile ödül için bir şansı olabilir. Aynı zamanda vergilendirme için devlet açısından avantaj sağlar. Öte yandan, C_1, C_2 veya C_3'ün ürün fiyatını düşürmek için sistemi kandırmaya yönelik yanlış veri paylaştığı tespit edilirse sözleşmeye göre bir ceza alır ve ağdan atılır.

SONUÇ

PoW algoritmasının adı her ne kadar iş kanıtı olsa da ağa katılan kullanıcıların emeğine göre değil; cihazların işlem gücüne göre blok onaylar. Literatürde bu algoritmanın sorunları, yüksek enerji tüketimi ve merkezileşmedir. Bu makalede PoW'un bir başka sorununun haklı bir rekabet ortamı sunmaması olduğu açıklandı. Diğer bir algoritma olan PoS ise ağda hisselenmiş koin miktarı en fazla olan (en zengin) düğümün sistemi kandırma gereği duymayacağına inanılarak yine ağın merkezileşmesine ortam hazırlar. Ancak bu da adil bir durum değildir. Çünkü her seferinde belli bir kitle blok oluşturur, onaylar, blok ödülü kazanır ve ağı merkezileştirir. Ağın merkezileşmemesi için kullanılabilecek LPoS ve PoET gibi algoritmalar ise sadece blok ödülü amaçlı düğümler için bir zararı olmayan ama faydası olabilecek blokzincirleri sağlar. PoWeight gibi ağırlıklandırılmış bir algoritma ise istenildiği şekilde özelleştirilebilir olması bir avantaj olsa da ortada yapılan işin somut bir kanıtı olmadığı için sistemi kandırmak çok kolay olabilir. Tedarik zincirinde kullanılacak konsensüs protokolleri ağa katılabilecek yabancı düğümlerin ödüllerden faydalanması ya da her seferinde aynı kişinin ödülü kazanmasını önlemek, merkezileşmenin önüne geçmek ve ağı en aktif kullanıp işini doğru yapan kişilerin blok ödülü ve indirim kazanması için PoM tedarik zinciri için kullanılabilir.

KAYNAKÇA

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system, 20.06.2020 tarihinde https://bitcoin.org/bitcoin.pdf adresinden alındı.

Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum project yellow paper*. 151, 1-32.

Yıldız, B. (Kasım, 2019). Dijital dönüşüm Sürecinde blok zinciri teknolojisi ve akıllı sözleşmeler. Dijital Dönüşüm Trendleri. Filiz Kitabevi. 120-143.

Keleş, B. ve Ova, G. (2020). Gıda tedarik zinciri yönetiminde bilgi teknolojileri kullanımı. Adü Ziraat Dergisi, 17(1):137-143.

Sultan, K., Ruhi, U. ve Lakhani, R. (2018). Conceptualizing blockchains: characteristics & applications. *11th IADIS International Conference Information Systems*.

Tian, F. (2018). An information system for food safety monitoring in supply chains based on HACCP. *blockchain and internet of things* (Doctoral Thesis).

Gerdan, D., Koç C. ve Vatandaş, M. (2020). Gıda ürünlerinin izlenilebilirliğinde blok zinciri teknolojisi kullanımı. Tarım Makinaları Bilimi Dergisi, 16(2): 8-14.

Taş, O. ve Kiani, F. (Ekim, 2018). Blok zinciri teknolojisine yapılan saldırılar üzerine bir inceleme. Bilişim Teknolojileri Dergisi, Cilt: 11, Sayı: 4.

Onay, H., Cansı, K. İ., Temimhan, K., Yazıcı, H. ve Erten, M. (2019). Supply chain management using blockchain. 15.08.2020 tarihinde https://wwww.easychair.org/publications/preprint_download/GwGL adresinden alınmıştır. *EasyChair Preprint*.

Ataşen, K. (2019). Blokzinciri ve akıllı sözleşmeler: düzenli bir dijital sertifikasyon uygulaması Geliştirilmesi. Yüksek Lisans Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Zheng, Z., Xie, S., Dai, H. N. ve Wang, H. (2016). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services.* 14(4), 352-375.

Feng, L., Zhang, H., Chen, Y. ve Lou, L. (2018). Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain. *Mdpi, Applied Sciences, 8(10), 1919*.

Eigelshoven, F., Bender, B. ve Ullrich, A. (2020, Haziran). Public blockchain – a systematic literature review on the sustainability of consensus algorithms. *ECIS Proceedings, ECIS.*

Christofi, G. (2019). Study of consensus protocols and improvement of the Delegated Byzantine Fault Tolerance (DBFT) algorithm (Master's thesis, Universitat Politècnica de Catalunya).

Kumar, A., Sharma, D. K., Nayyar, A., Singh, S. ve Yoon, B. (2020). Lightweight proof of game (lpog): a proof of work (pow)'s extended lightweight consensus algorithm for wearable kidneys. *Sensors*, 20, 2868; doi:10.3390/s20102868.

Topal, S. (2020). A novel hybrid sharıng economy based blockhaın model (proof of meet*). Journal of New Theory*. Issue 32.