BİLGİSAYAR BİLİMLERİ VE TEKNOLOJİLERİ DERGİSİ
JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGIES
http://dergipark.org.tr/tr/pub/bibted

Araştırma Makalesi

Blockchain Mutabakat Protokollerinin Karşılaştırılması

İrem BEKMEZ*[1], Hakan GENÇOĞLU[2]

[1]İstanbul Sabahattin Zaim Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Bilgisayar Mühendisliği, İstanbul, Türkiye
[2]İstanbul Sabahattin Zaim Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği, İstanbul, Türkiye

Anahtar Kelimeler:
Blockchain
Mutabakat Protokolleri
Bitcoin

ÖZ

Kripto paralarla finans dünyasında popüler bir konuma ulaşan Blockchain teknolojisi, merkezi yapıyı sonlandıran, dağıtık bir sistem olarak ifade edilmektedir. Her ne kadar Bitcoin ile tanınmaya başlasa da bu teknoloji, her geçen gün yeni bir uygulama alanı ile adından söz ettirmektedir. Güvenliğin son derece önemli olduğu bir sistemdir. Bu sebeple blok zincir teknolojisinde yapılan her işlemin doğrulanması gerekir, bunun için de mutabakat protokolleri kullanılır. Bu çalışmada, en yaygın olarak kullanılan protokollerden kapsamlı bir şekilde bahsedilmiştir.

Comparison Of Blockchain Consensus Protocols

Keywords:
Blockchain
Consensus Protocols
Bitcoin

ABSTRACT

Blockchain technology, which has reached a popular position in the financial world with crypto currencies, is expressed as a distributed system that ends the central structure. Although it started to be known with Bitcoin, this technology is making a name for itself with a new application area every day. It is a system where security is extremely important. For this reason, every transaction made in blockchain technology must be verified, and consensus protocols are used for this. In this study, the most commonly used protocols are comprehensively mentioned.

***Sorumlu Yazar**

*(bekmez.irem@std.izu.edu.tr) ORCID ID 0000–0003–2523–2273
(hakan.gencoglu@izu.edu.tr) ORCID ID 0000-0003-2968-1615

e-ISSN: 2717-8579

Geliş Tarihi: 23/01/2024; Kabul Tarihi: 09/07/2024

1. GİRİŞ

Günümüzde teknolojinin hızla gelişmesi, teknolojinin kullanım alanlarını da önemli oranda genişletmektedir. Bu durum karşısında verileri güvence altına almak, kontrol etmek ve yönetmek büyük bir önem arz etmektedir.

Blockchain teknolojisi de bu ihtiyaca binaen ortaya çıkmıştır. Merkezi yapıyı sonlandıran dağıtık bir sistemdir. Verilerin kaydı her düğümde şeffaf bir şekilde tutulmakta ve geriye dönük doğrulanabilmektedir. Bu sebeple de güvenilir olarak kabul edilmektedir. Kripto para sistemleri ile tanınmaya başlamıştır. Blok zincir teknolojisi, merkeziyetsiz bir yapıda olduğu ve düşük maliyetlerle gerçekleştiği için, gıda güvenliği, reçeteli ilaçların takibi, nesnelerin interneti (IoT) gibi birçok alanda kullanıma elverişli bir yapıdadır(Ünal ve Uluyol, 2020).

Blockchain teknolojisinin açık ve şeffaf bir yapıda olması, Ethereum ağı aracılığıyla blok zincire dahil olan akıllı sözleşmeleri düzenlemeyi de çok daha kolay hale getirmektedir(Roy ve Yousuf,2022).

Dağıtılmış bir kayıt defteri olan Blockchain teknolojisi, bilinmeyen eşler arasında bir güven oluşturmaktadır. Yapılan her bir işlemi doğrulamak için ise, mutabakat algoritmaları kullanılmaktadır. Bu çalışmada bahsedilen algoritmalar ise şunlardır; Proof of Work, Proof of Stake, Proof of Space, Proof of Contribution.

Bu araştırmanın amacı, bu dört algoritmayı detaylı bir şekilde incelemek ve birbirleriyle kıyaslamaktır. Bu sebeple öncelikli olarak Blockchain teknolojisine değinilecek, akabinde ise mutabakat protokollerinden bahsedilecektir. Yapılan bu çalışma ile, blockchain mutabakat protokollerini kullanmak ve incelemek isteyen araştırmacılara bir kaynak oluşturulması hedeflenmiştir.

2. BLOCKCHAİN TEKNOLOJİSİ

Blockchain teknolojisi ilk olarak, 2000'li yılların başında bir fikir olarak ortaya çıkmıştır. Satoshi Nakamoto tarafından kaleme alınan "Bitcoin: A Peer-to-Peer Electronic Cash System" (Nakamoto & Bitcoin, 2008) makalesi yayımlanana kadar tam manasıyla bir ilgi görmemiştir. 2009 yılı itibariyle kripto para birimi ile tanınmaya başlamıştır. Blockchain teknolojisi, merkezi yapıyı sonlandıran dağıtık bir sistem olarak veri bütünlüğünü sağlamaktadır(Endurthi ve Khare, 2022). Böylece üçüncü taraflara olan ihtiyacı da ortadan kaldırmaktadır. Güvenlik ön plandadır. Şifrelenmiş ve geri dönüşü olmayan bir veri tabanıdır. Ayrıca, sistemin doğrulanabilir olmasına olanak sağlayan ve bu sistemde veri kaybını önleyen bir takım teknik özelliklere de sahiptir.

Verilerin değişmezliği ise blockchain teknolojisinin esas özelliğidir.

Blockchain'ler yapısı gereği kararlıdır ve Bizans hata toleransı ile dağıtılan bir bilgisayar sistemini biçimlendirmektedir. Yani hiçbir makine dağıtılmış bir sisteme karşı kötü niyetli olmayı başaramaz(Eklund ve Spasovski, 2017).

Blockchain'in güvenlik açısından yaklaşımları, açık anahtarlı kriptografinin kullanımını içermektedir. Depolanan veriler genel olarak bozulamaz ve değişmez bir bilgi bloğu olarak kabul edilmektedir. Verilerin saklanması blok olarak tanımlanmaktadır. Bir Blockchain veri tabanı ise bloklar ve işlemler olmak üzere iki çeşit kayıttan oluşmakta ve bir dizi madenci içermektedir. Blockchain, yeni bilgi bloklarının tasdik edilmesi için sunulan bir protokolle iş birliği yapan çiftler arası bir ağ tarafından gerçekleştirilmektedir. Bu paylaşılan verileri değiştirmek için ise, ağın %50'sinden fazlasının belirlenen bir blokta fikir birliği sağlaması gerekmektedir. Bir blokta yapılan değişiklikler sonucunda bu verilerin düzenlenmesi ve sonraki tüm bilgi bloklarına ise kaydedilmesi gerekmektedir.

Bloklar, Merkle Ağacı biçiminde kodlanmış bir yapıya sahiptir. Merkle Ağaçları, depolama için Blockchain verileri ve bir AVL ağacı kullanılarak gerçekleştirilen ortak bir veri yapısıdır. Normal ağaç tabanlı veri yapılarından farkı ise şudur: Ağaçtaki bir değer, seçilen düğümden ağacın köküne kadar olan bütün yol boyunca yeniden hash edilerek her zaman doğrulanabilmekte, bu da O (log n) süresini almaktadır. Her düğüm eklemede eklenen düğümün izi, kök düğüme kadar eklendiği yerden yeniden karıştırılmaktadır(Dorai ve Nair, 2021).Blockchain'de her bir işlemi doğrulamak için mutabakat algoritmaları kullanılmaktadır. Bu çalışmada bahsedilen mutabakat algoritmaları ise şunlardır; Proof of Work, Proof of Stake, Proof of Space, Proof of Contribution

3. MUTABAKAT PROTOKOLLERİ

3.1. Proof of Work (PoW)

PoW, Blockchain alanındaki en eski fikir birliğidir. Bir bloğun madenciliğinin hesaplanması oldukça zor bir durumdur. Çünkü bloğun ağ aracılığıyla "çözüldü" olarak onaylanması için SHA-256 (şifreleme algoritması) hash'inin hedeften daha düşük olması lazımdır. Başka bir ifadeyle, bir bloğun hash'inin belirli bir sayıda sıfır ile başlaması gerekmektedir. Bu sayıyı bulmak için, bilgisayarın yaklaşık 10^{21} hesaplama yapması gerekmektedir. İstenilen dizeyi veren bir nonce'u bulmak ise yaklaşık 10 dakika sürmektedir. Bu sebeple, bir Bitcoin'i tamamen işlemek ve blok zincirine kaydettirmek ortalama 10 dakika zaman almaktadır(URL-1).

Örneğin, Blok #304446 çözümü aşağıda verilmiştir:

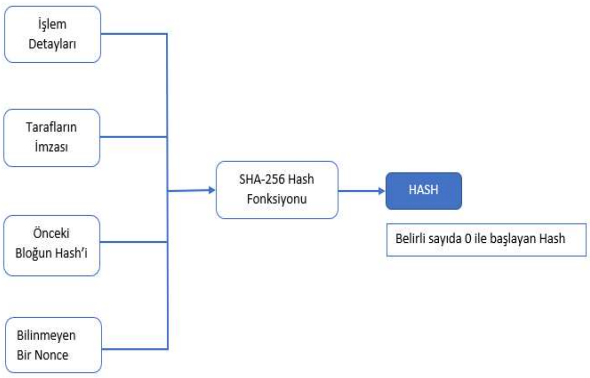
00000000000000002388679fe503d715603b

39ae7f965cdaec66dbe1de7071d4

Hash fonksiyonu, verilerin bilgisayar üzerindeki bir temsili olarak kabul edilmekte ve bu verilerin güvenli şekilde saklanmasına olanak sağlamaktadır. Bir blok zincirindeki hash'in aniden değişmesi işleri bütünüyle karıştırmaktadır. Blok zincirde, hiç kimse diğer kullanıcıların haberi olmadan herhangi bir değişiklik yapamamaktadır. Bitcoin işlemlerini ve kayıtlarını kurcalamalara karşı dirençli kılan özellik ise budur.

Yeni bir hash oluşturmak için her seferinde bir nonce arttırılır. Nonce, birden fazla madencinin benzer işlemlerden oluşan bir grup vasıtasıyla bir hash'i meydana getirmeye çalışmalarına ve farklı farklı değerler ortaya çıkarmalarına izin veren rastgele bir sayıdır.

Çözülmüş bir blok ise, zincirdeki bir önceki bloğun hash değerini, madencinin onayladığı işlemleri ve nonce değerini içermektedir. Önceki bloğun hash değerinin eklenmesi, zincirin Genesis bloğuna kadar her bloktan önce oluşturulmasını sağlamaktadır(URL-1).



Şekil 1. Hash fonksiyonu

Bitcoin'deki çoğunluğun fikir birliği, onu oluşturmak için en fazla emeği gerektiren en uzun blok zinciridir.

Proof of Work yapısında, bir madencinin gerekli oranda iş yaptığını ispatlayıp protokoldeki hakimiyetini ortaya koyması gerekmektedir. Düğümlerdeki bilgi işlem kaynaklarının çeşitliliğinden ötürü, zor olduğu belirtilen bu bulmacayı çözen ilk düğüm, yeni bloğu oluşturmak için bir hak kazanmış olur ve sistem tarafından ödüllendirilerek belirlenen bir tutarda Bitcoin alır.

Proof of Work, elektrik ve süper hızlı bilgisayarların maliyetinden ötürü pahalı bir yöntem olarak kabul edilmektedir. Bu algoritmada mevcut blokları işlemenin maliyeti de oldukça yüksektir.

Kripto para biriminde, bilgi depolamada ve sertifika oluşturma gibi çeşitli alanlarda yaygın olarak kullanılmaktadır(Ouyang vd., 2021).

3.2. Proof of Stake (PoS)

PoW protokolünün yüksek oranda elektrik enerjisi sarf etmesi, bilgi işlem gücünün büyük oranda harcanmasına sebep olmaktadır. PoS, Bitcoin ve Ethereum gibi mevcut blockchain protokollerindeki enerji ihtiyacı sorununu çözmek için önerilen en güçlü alternatiflerden biridir. Mutabakata varmak için madenciliğin gerekli olmadığı bir protokoldür. Blok oluşturmanın Proof of Work'e göre daha verimli olduğu bir algoritmadır. Buradaki pay, blok zincirinin kanıtını nasıl uyguladığına bağlı olarak değişkenlik gösterebilmektedir. Kripto para blok zincirlerinde, pay normalde bir düğümün tuttuğu madeni para sayısıdır. Kripto para birimi olmayan blok zincirlerinde ise, varsayılan bir hisse olmadığı için oylama gibi alternatif yaklaşımlar gerekmektedir(URL-2).

Proof of Stake'de kullanıcılar, blok zincirinde sahip oldukları hisselere binaen, kendilerine ait olan kripto para birimi oranında yeni bloklara oy verme hakkına sahiptir. Mevcut düğüme yeni bloklar ilave etmek ve nihai olarak ödül almak için ise bu hissedarlar arasından bir lider seçilmektedir. Proof of Stake'de Proof of Work'e göre hesaplama yükü çok daha azdır. Lakin, ademi merkeziyetçilik seviyesinin önemli oranda azalması sebebiyle "Hiçbir Şey Tehlikede Değil" ve "Uzun Menzilli Saldırı" problemlerinin ortaya çıkma ve çatallanma riski daha yüksektir.

Bitcoin'in yanı sıra Ethereum gibi kripto para sistemlerinde kullanılmaktadır(Ouyang vd., 2021). Ayrıca hesaplama gücü gerektirmediği ve yüksek işlem gücüne sahip olduğu için de Araçların İnterneti (IoV)' da da kullanılmaktadır(Nguyen vd., 2019).

3.3. Proof of Contribution (PoC)

PoC protokolü, blok zincir tabanlı bir uygulamadaki kullanıcı davranışlarını ve eylemlerini bir algoritma aracılığıyla hesaplanan katkı değerleri olarak ölçer. Her mutabakat turunda en yüksek katkı değerine sahip olan düğüm, bir sonraki yeni bloğu oluşturma hakkını elde eder. PoC, merkeziyetçilik ve sert çatallanmaya karşı direnç özelliklerini korur ve yüksek verimlilik göstererek son derece önemli özellikler sergiler. Katkı algoritması, farklı uygulama senaryolarına uyacak şekilde ayarlanabildiği ve optimize edilebildiği için iyi bir ölçeklenebilirliğe sahiptir. Bu mutabakat protokolünün en dikkat çekici kısmı ise, kripto para birimi içermeyi gerektirmeyen çok çeşitli uygulamalar için, Proof of Work gibi kripto para birimi tabanlı mutabakat mekanizmalarına iyi bir alternatif olmasıdır(Song vd., 2021).

Güvenilir olmayan makinelerin açık ve merkeziyetsiz bir ortamda güven sağlaması amacıyla tasarlanan PoC protokolü bunun yanı sıra

iExec ağına farklı katkılar sunarak ödemelerin her zaman için adil ve zamanında olmasını da sağlamaktadır(URL-3).

3.4. Proof of Space (PoSpace)

Proof of Space, 2013 yılında enerji ihtiyacı sorununu çözmek için ortaya konan ve Proof of Work'e benzer yapıda olan bir mutabakat protokolüdür. PoW'dan farklı olarak, kripto para kazanmak için hesaplamanın değil, depolamanın kullanıldığı bir algoritmadır.

Proof of Space protokolünde, bir doğrulayıcı bir kanıtlayıcıya davet göndermektedir. Kanıtlayıcı ise doğrulayıcıya belirlenen bir miktardaki depolama alanı için yer ayırdığını ispat etmektedir(URL-4).

Proof of Space protokolünün 3 bileşeni vardır:

3.4.1. Çizim

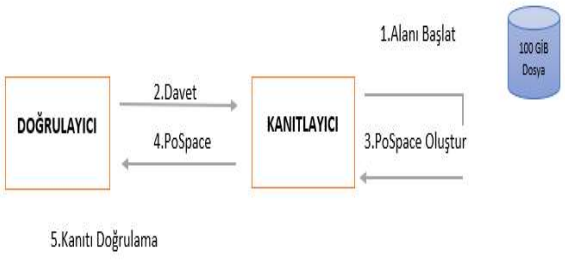
Çizim, çiftçi olarak adlandırılan bir kanıtlayıcının belirli bir miktardaki alanı başlatma işlemi olarak tanımlanmaktadır. Bir çiftçi olmak için gerekli olan şart, işlem yapılacak bilgisayarın en az 101.4 GiB alana sahip olmasıdır.

3.4.2. Kanıtlama / Çiftçilik

Çiftçilik, bir çiftçinin yasal olarak belirtilmiş bir depolama alanı ayırdığını ispatlamak için 256 bitlik sorgulama aldığı bir süreçtir. Çiftçi, her bir zorluğa cevap olarak arazilerini denetlemekte, bir kanıt oluşturmakta ve kazanan bu kanıtları doğrulama için ağa göndermektedir.

3.4.3. Doğrulama

Çiftçi başarılı bir şekilde Proof of Space'i meydana getirdikten sonra, birkaç tane sağlama gerçekleştirerek kanıttaki x değerleri arasında karşılaştırmalar yapmakta ve bu kanıtı doğrulanabilir kılmaktadır.



Şekil 2. PoSpace yapısı

Proof of Space'de kullanılan Chia ağı, Bitcoin'den bu yana ilk yeni Nakamoto fikir birliğidir. Çok daha fazla enerji verimliliğine sahiptir. Chia Network'ün Lisp işlevsel dilini temel alan ve akıllı para dili olarak ifade edilen Chialisp, akıllı paralar, akıllı sözleşme ve akıllı işlem yeteneklerini tek bir pakette sunmaktadır(URL-5).

4. SONUÇLAR

Kripto para birimi tabanlı bir algoritma olan Proof of Work, diğer mutabakat protokollerine göre nispeten daha güvenilir olmasına rağmen, Blockchain metodolojileri arasındaki en fazla enerjiyi sarf eden algoritmadır. Bu da PoW için dezavantajlı bir durumdur. Bu soruna binaen ise birçok algoritma önerilmiştir. Bunlardan biri ise Proof of Stake'dir. PoS, her ne kadar düşük enerji harcasa da adaletsiz seçim ve güvenlik gibi bazı konularda yetersiz kalmıştır. Proof of Contribution, PoW'un aksine kripto para birimi tabanlı olmayan bir algoritmadır ve çok çeşitli uygulamalar için iyi bir alternatif olmuştur. Proof of Space ise PoW'a benzer yapıda olan bir protokoldür. PoW'dan farklı olarak hesaplamanın değil, depolamanın kullanıldığı bir algoritmadır.

KAYNAKÇA

Gökhan, Ü. N. A. L., & Uluyol, Ç. (2020). Blok zinciri teknolojisi. *Bilişim Teknolojileri Dergisi*, *13*(2), 167-175.

Roy, T., & Yousuf, M. A. (2022, December). Secure E-commerce Trading Using Blockchain with Smart Contract Based on Proof of Work. In *2022 International Conference on Recent Progresses in Science, Engineering and Technology (ICRPSET)* (pp. 1-6). IEEE.

Endurthi, A., & Khare, A. (2022, March). Two-tiered consensus mechanism based on proof of work and proof of stake. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 349-353). IEEE.

Spasovski, J., & Eklund, P. (2017, November). Proof of stake blockchain: performance and scalability for groupware communications. In *Proceedings of the 9th International Conference on Management of Digital EcoSystems* (pp. 251-258).

Nair, P. R., & Dorai, D. R. (2021, February). Evaluation of performance and security of proof of work and proof of stake using blockchain. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 279-283). IEEE

URL-1: https://www.academia.edu/38268318/Proof_of_Work_Algorithm
[Erişim Tarihi: 15.01.2024]

Ouyang, Z., Shao, J., & Zeng, Y. (2021, September). PoW and PoS and Related Applications. In *2021 International Conference on Electronic Information Engineering and Computer Science (EIECS)* (pp. 59-62). IEEE.

URL-2: https://courses.cs.ut.ee/MTAT.07.022/2017 fall/uploads/Main/janno-report-f17.pdf [Erişim Tarihi: 08.03.2023]

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE access*, *7*, 85727-85745.

Song, H., Zhu, N., Xue, R., He, J., Zhang, K., & Wang, J. (2021). Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection. *Information processing & management*, *58*(3), 102507.

URL-3:https://protocol.docs.iex.ec/key-concepts/proof-of-contribution [Erişim Tarihi: 15.01.2024]

URL-4:https://docs.chia.net/proof-of-space [Erişim Tarihi: 15.01.2024]

URL-5:https://www.chia.net/wp-content/uploads/2022/07/Chia-Business-Whitepaper-2022-02-02-v2.0.pdf [Erişim Tarihi: 15.01.2024]