BLOKZİNCİRİ TABANLI BİR ÖZGÜN PAYLAŞIM EKONOMİSİ MODELİ (BULUŞMA KANITI)

Selçuk Topal
Matematik Bölümü
Bitlis Eren Üniversitesi
Bitlis, Turkiye
s.topal@beu.edu.tr

19.05.2020

ÖZET

Bu çalışma *Buluşma Kanıtı (PoM)* çalışmasının ilk bölümüdür. Bu bölüm, teknik detaylar vermek yerine model ve sistemine (kabaca) olan ihtiyaç üzerine odaklanmaktadır. İkinci bölümde, modelin tüm teknik detayları ve mimarisi tartışılacaktır. Model, fikir birliğine dayalı paylaşım (buluşma) ekonomi modeline odaklanmaktadır. Paylaşım (buluşma), bir yerde olanlarla o yere gidenler arasındaki ilişkiyi açıklar. Fikir birliği, bir sosyal faaliyet (konum ve eylem) üzerinde aktif istemciler (istemcinin herhangi bir konum değişimi) üzerine kurulmuştur. İki tip istemci vardır; birincisi bir amaç için bir yere giden (C_1 ler) ve ikincisi düzenli olarak bir amaç için bir yerde olanlardır (C_2 ler). C_1 en az iki ve C_2 en az bir istemciden oluşur. Bu makale, enerji tüketmi yapmaksızın merkezi olmayan bir blokzinciri oluşturmak için Hisseleme Kanıtı (PoS) ve Blokzinciri Tabanlı Konum Kanıtı'nın (BTKK) üstünde bir fikir birliği sistemi olan PoM'u önermektedir. Paylaşım ekonomisi modeli, önerilen blokzinciri modelinin uygulamalarından biridir. HOX adı verilen blokzincir sistemi, dinamik ulaştırma (lojistik) sisteminden dinamik büyük verilere kadar çok geniş alanlara, dağıtık defter sistemleri için kullanılabilir. HOX, PoM'un bir uygulama örneklemesidir. Sonuç olarak, önerilen model yasal kayıtlar çerçevesinde vergileri kaydetme, adil bir iş gücüyle kazanım ve blokzincirini günlük yaşamda aktif olarak kullanma fırsatı sunar.

***A*nahtar Kelimeler** Buluşma kanıtı · hisseleme kanıtı · blokzinciri · blokziniciri tabanlı paylaşım ekonomisi · konsensüs · konum tabanlı blokzinciri · dinamik büyük veri

1 Giriş

Bir blokzinciri genel olarak veri bloklarından oluşan ve dağıtık bir defter sistemine dayalı merkezsizlik adına oluşturulan bir kayıt sistemidir. Sistem bir genez bloğu ile başlar ve sonraki işlemler sırasıyla bloklar halinde kaydedilir. Kayıtlar silinemez veya değiştirilemez. Bloklardan belirli sayıda onaylanmış veri girildiğinde, sonraki bloğa geçirilir. Veriler hash ile kriptografik olarak şifrelenir ve bu şifrelerin dekripsiyunuyla yapılan işlemler onaylanır. Madenciler olarak adlandırılan düğümler, bu onayları yapmak için yani dekripsiylar için rekabet ederler. Bu rekabet, bazen cihazların işlem gücüne (PoW), bazen de (PoS) sistemde kilitli koin miktarına bağlı olarak sisteminde yapılır. Bu nedenle, yarışta ekipmanın daha güçlü veya madeni para miktarının daha yüksek olduğu bir mücadeledir. Bu makaledeki PoM sistemi buluşma tabanlı bir yapı önerir. Giderek daha fazla buluşan ve buluşmalarda daha fazla zaman harcayan istemcilerin, sistemin dinamiklerine dahil edildiği bir sistemden bahsedilir.

Blokzinciri ve merkeziyetsizlik fikri pratik anlamda hayatımıza girdiğinden beri yeni bir dijital macera için farklı entropiler yaşamaya devam ediyoruz. Bazı bilim adamları, insan toplulukları ve teknoloji severler bu konunuları sahiplenseler de, sıradan insanların ve çoğu yönetiminlerin (uzak ama kayıtsız kalamadan) kaçınma çabaları artan ivme ile devam etmektedir. Tabii ki, mesele sadece merkezsiz sistemde anlam bulmak değil, aynı zamanda pandemi günlerinin yaşandığı bu farklı tecrübe ortamında da anlam bulması, güvenli ve pratik bir dijitalleşmenin pek çok tartışmaya başladı.

Dijitalleşme ile amaç, dijital ödeme sistemlerinin günlük yaşama tamamen entegre olmasını sağlamak, sahtekarlığı ve üçüncü taraf kontrolünü sıfır seviyelere indirmektir.

Diğer ve en önemli konulardan biri de dijital varlıkların aktarım süreleri ve daha fazla veri işgaline neden olan şişen ve ağırlaşan bloklardır. Örneğin, Bitcoin blockchain [1] 100 GB veri kaydına sahiptir ve kazım çok fazla elektrik tüketilmesine neden olur. Öte yandan, merkezsizlik vurgusu ön plana çıkmış olsa da, madencilik sisteminde kazım yapan cihazların gücü sistemdeki en güçlü olanları belirler. Bu tür problemlerin çözümü için, özellikle enerji tüketimini en aza indirmek için birçok uygulama geliştirilmiştir ve özellikle Hisseleme Kanıtı (PoS) konsepti geliştirilmiştir. Şu anda, Ethereum cite eth sistemi PoS için hazırlık aşamasındadır. Günümüzün PoS tabanlı uygulamalarında, hissleme gücü, yani toplam dijital varlık içindeki dijital varlık sayısının baskınlığı olanların blok üreticisi, işlem onaylar olması nedeniyle sistemin merkezsizleşmekten uzaklaşmasına neden olmuştur. En çok sayıda koine sahip olanlardan rasgele blok yapıcılar ve işlem doğrulayıcıların (hisslenmiş koinler) seçimiyle bu baskınlık sorununun üstesinden gelinmeye çalışılsa da, sonuçta her zaman bir kitlenin kontrolüne terk edilmek zorunda kalınır.

Devlet yönetimleri tarafından önem merceğine alınan blokzinciri sistemleri, vergilendirme ve varlık takibi için yıpratıcı bir baskı faktörü oluşturur. Bunun ana nedeni, bankanın kontrolü altında olmayan dijital varlıkların günlük yaşam ekonomisine kaydedilememesidir.

Öte yandan, bir başka mesele ise sosyal işletmeler bunce blokzinciri ve benzeri dijital sistemlerin gelişmelerden ne kadar pay alabildikleri ve sistemlerden ne kadar faydalanabildikleridir. Çünkü sıfıra yakın. Çünkü dijital ödeme sistemleri (özellikle blokzinciri tabanlı) ile yapılan ödemeler devletlerin resmi mali kayıt ve göstergeleri için gayri resmi bir ekonomik durum olmaya devam ediyor. Doğal olarak, böyle bir dezavantaj ve sisteme katılım çatısı altında dijital para ve varlık sistemleri, işletmelerin gerçek ekonomisine ve reel ekonomiye direk katkı sağlamak hususunda asgari düzeyde kalmaya devam etmektedir.

Bu çalışmada önerilen model, model ekosistemdeki herkesin kazanacağı şekilde blokzincirinin nimetlerinden de faydalanarak kayıt dışı ekonomiyi en aza indirmeyi amaçlamaktadır. Model, PoS ve BTKK modelleri kullanarak geliştirilmiş bir sistem önerir. Öte yandan, bu sistem koin sayısının fazlalığından ziyade PoS sistemindeki blok-işlem doğrulayıcılarının ve blok oluşturucularının gerçek emek faktörlerinin ve $C_1 - C_2$'lerin aktivite oranlarının dahil edildiği daha adil ve paylaşılabilir bir tutum geliştirir.

2 Buluşma Kanıtı (PoM): HOX Örneklemi

PoM (Restricted to HOX) aims to blockchain as the follows:

Amoretti ve ark. [3] güvenilir bir LBS sistemi önerdiler. Sistem, konum aldatmacalarını ve yanıltmalarını merkezsiz (yani konumların doğru ve sistem içindeki düğümlerin birbirlerini bilmediği) Wi-Fi veya hücresel ağ arayüzü aracılığıyla internete bağlı mobil düğümleri olan ve Bluetooth gibi kısa menzilli iletişim teknolojileriyle komşu düğümlerle bilgi alışverişi yapabilen ağa odaklandılar. Bir ispatlayıcı (konum ispatlayan), komşularından (belli bir yarıçap içinde kalan) konum bilgisi toplamasını isteyen bir düğümdür. Bir İspatlayıcı için bir Şahit, İspatlayıcıya konum kanıtı sağlayan düğümdür. PoM sistemindeki kurgusal sistem aşağıdaki akışla sağlanır:

C_1 ler tek bir konum içinde (en az 2 adet C_1 olmalı) bir mobil telefon veya cihaz üzerinde (uygulama yoluyla bir Bluetooth türü işleviyle eşleşerek buluşur (ancak Bluetooth mobil cihazların pil ömrünü çok fazla tüketeceğinden, Wi-Fi'deki konuma dayalı mesafe belirli bir Zaman aralığında kontrol edilerek buluşma denetlenebilir). Wi-Fi veya hücresel ağ birimi aktif olduğu sürece C_1 lerin orada olduğunu ve konum bilgilerinin alındığını gösterir. Mevcut konumda oldukları bilgisi C_1 lerin mobil üzerinde parmak izi özelliğine sahip uygulama ile C_2 tarafından onaylanır. Daha sonra, mekanda harcanan toplam süre, C_2 tarafından buluşanların parmak izleri ile buluşmanın onaylanmasından ve vergi ödeme sistemine dahil edilmek üzere ödemenin onaylanmasından sonra C_2 tarafından onay süreci için blokzincirine gönderilir.

PoM (HOX'a indirgenmiş) aşağıdaki gibi bir blokzinciri hedefler:

1. Mevcut işleyişi aldatma ve kandırmaya karşı korumak için bir pozisyon ve buluşma sistemi oluşturmak.
2. Buluşanlar hem bugünün ödeme sistemindeki para hem de blokzincirinde koinlerle ödüllendirilir. Ödüllerden sağlanacak faydaların oranları aşağıdaki metotlarla hesaplanır:
    - En fazla buluşan. (koin darb metodu (mm))
    - En fazla kişiyle buluşan. (mm)
    - En uzun buluşma süresine sahip olma. (mm)
    - Alışveriş alanında indirimli olarak paypal veya benzeri bir sistemle ödeme yaparak uygulama üzerinden vergi ödemesine dahil edilme. (vergilendirme metodu (tm))

- C_2 nin toplantının başlangıcını ve bitişini (ticari olarak) onaylayarak, müşteri sadakati ve yoğunluğu kazanır ve ödemelerin vergiye kaydını sağlama. (mm+tm)

3. Blok oluşturma, toplantı kimliği (uygulama üzerinde harflerden ve rakamlardan oluşan bir karakter dizisi), başlangıç bitiş zamanı, buluşmadaki istemcilerin kimliği (C_1 grubundaki istemciler, uygulama üzerinde harflerden ve rakamlardan oluşan bir karakter dizisi), C_2 kimliği (Wi-Fi mac adresiyle kodlanmış karakter dizisi) gibi bilgileri içerir. Bu özellik sayesinde konum, zaman ve paydaşlar sistem havuzuna dahil edilir.
4. Modelde, karşılama kanıtlarını saklamak için özelleştirilmiş bir PoM kullanılır. İki kısım ispat doğrulayıcı ve blok doğrulayıcı eşit ağırlıklandırılmış olarak rol oynarlar: C1 ve C2. En yüksek güce sahip olanlar, her seferde bir kümeden rastgele seçilir. (mm)
5. C_1 için kamuya açık blokzinciri (PoM) nin konsensüs algoritmaları için ağdaki bir doğrulayıcı hisseleme gücü ($P_1(c_i))$)) aşağıdaki gibi hesaplanır:
   Bir C_1 istemcisi olan c_i nin doğrulayıcı hisseleme gücü $P_1(c_i))$ ile gösterilir.
   $SC(c_i)$: c_i nin hisselenmiş koin miktarı.
   $TC(c_i)$: c_i hisselenmiş koinlerinin saniye cinsinden hisseleme zaman periyodu.
   $CMN(c_i)$: c_i nin içinde bulunduğu vakte kadar buluştuğu toplam istemci sayısı.
   $MMN(c_i)$: c_i nin içinde bulunduğu vakte kadar toplam buluşma sayısı.
   $TMN(c_i)$: c_i nin içinde bulunduğu vakte kadar tüm buluşmalarda geçirdiği toplam sürenin saniye cinsinden değeri.
   $P_1(c_i) = w_1 SC(c_i) + w_2 TC(c_i) + w_3 CMN(c_i) + w_5 MMN(c_i) + w_5 TMN(c_i)$
   $\sum_{h=1}^{5} w_h = 1$ öyle ki $0.1 < w_h < 1$
6. C_2 için kamuya açık blokzinciri (PoM) nin konsensüs algoritmaları için ağdaki bir doğrulayıcı hisseleme gücü ($P_2(c_i))$)) aşağıdaki gibi hesaplanır:
   Bir C_2 istemcisi olan c_i nin doğrulayıcı hisseleme gücü $P_2(c_i))$ ile gösterilir.
   $SC(c_i)$: c_i nin hisselenmiş koin miktarı.
   $TC(c_i)$: c_i hisselenmiş koinlerinin saniye cinsinden hisseleme zaman periyodu.
   $CMN(c_i)$: c_i nin içinde bulunduğu vakte kadar ağırladığı toplam istemci sayısı.
   $TMN(c_i)$: c_i nin içinde bulunduğu vakte kadar ağırladığı toplam ağırlama süresinin saniye cinsinden değeri.
   $DMN(c_i)$: c_i nin içinde bulunduğu vakte kadar yaptığı toplam indirim miktarının yüzde (%) değeri.
   $P_2(c_i) = k_1 SC(c_i) + k_2 TC(c_i) + k_3 CMN(c_i) + k_4 MMN(c_i) + k_5 TMN(c_i)$
   $\sum_{t=1}^{5} k_t = 1$ öyle ki $0.1 < k_t < 1$

Açıklama 1 Sistemde, buluşulan (ağırlanan) istemci sayısına ve buluşma süresine bağlı olarak koin darbı (kazımı, minting) yapılır ve indirimler kazanılır. Bu katkılarla, istemciler aynı zamanda sistemin doğrulayıcıları haline gelirler, yani P_1 ve P_2 oranında blok ödülleri alırlar.

Açıklama 2 Bir C_1 ve bir C_2, C_2'nin yerinde buluşamaz. C_1 ve C_2 yalnızca sahip olmadıkları bir yerde buluşabilir.

Açıklama 3 Bir C_2, daha fazla hisse gücü kazanmak için indirimleri manupule ederek sistemi yanlış yönlendirmeye çalışırsa, sistemden atılır ve tüm hisselenmiş koinlerini kaybeder. C_2 istemcisi bu yasal olmayan yolu seçerse, doğal olarak, vergi sistemini aldatmış olur. Bunun da kanuni bir yaptırımı ortaya çıkacaktır.

Açıklama 4 Mobil uygulama, sağlayacağı ödeme sistemi ile ödenen tutarı kaydedebilir. Bu, indirim ile ilgili bir sahtekarlığı ve vergi kaçırmayı kolayca önleyebilir.

Konum bilgisiyle donatılmış dinamik büyük veri (KBDDBV) Elbette, ulaşım (nakliye, lojistik) sistemlerinde PoM kullanıldığında, varış noktasında daha az zaman harcanması bir avantaj olmalıdır. Bu anlamda, PoM sistemi, ödül oranı değişim süreci ile daha kısa bir zaman aralığı için daha fazla ödül verilen sistemle güncellenebilir. Buluşmada en az iki C_1 zorluğu nedeniyle, [3] deki sistem kullanılarak başka bir hibrit yapı kullanılabilir. Böylece, C_1 ve C_2 bir tane olduğu için konum şahitliği ve alan komşuluk özellikleri kullanılabilir.

Daha karmaşık veri sistemleri için, özellikle taşıma (nakliye, lojistik) işlemi de dahil olmak üzere dinamik veriler (işlem verileri), zaman boyutuna ve konum verilerine sahiptir. Bu veri kümeleri ve bunların analizleri finansal (siparişler, faturalar, ödemeler), iş (planlar, faaliyet kayıtları) ve lojistik (teslimatlar, depolama kayıtları, seyahat kayıtları) ile ilgilidir. İstemciler arasındaki olaylar, onların mekansal, nicel ve nitel veri değişiklikleri, veri analizi için statik olmayan

değerlendirmelere tabidir. Bu statik olmayan süreçlerin blokzinciri kaydıyla, şirket çalışanlarını ödüllendirmek ve şirketlerin iş geliştirme süreçlerini kalite kontrol teknikleri ile donatarak yapılan işin kalitesini iyileştirmek mümkündür. Sadece şirketlerin değil, kalite kontrol sistemleri çerçevesinde iş yapan şirketlerin de gelişmesine katkıda bulunabilir. PoM, özellikle veri kümelerinde zamansal ve konumsal değişikliklerin kullanılması ve değerlendirilmesinin gerekli olduğu iş kollarında, strateji belirleme, iş gücü kazanma oranı ve teşvik ödülleri açısından iş geliştirme için merkezsiz ve adil bir yaklaşım olarak kullanılabilir.

3 Sonuçlar

Blokzinciri çalışmaları ve tartışmaları çerçevesinde, devlet ve bankacılık sistemlerine karşı olumsuz argümanların ortaya konduğu ve zihinsel bir çatışma ortamı yaratma girişimlerinin var olduğu iyi bilinmektedir. PoM ile orta yol (el sıkışma, kucaklaşma) olarak adlandırılabilecek hibrit bir model tanıtıldı. Çünkü mevcut yasal ödeme sistemlerinin PoM'daki uygulamalarla hibrit alanı, koinlerin sistem içinde yasal bir ödeme aracı olmasını sağlayacaktır. Her ne kadar PoM tarafından sunulan hizmetler doğrudan bir ödeme aracı olmasa da, kayıtlı vergi sistemine dahil olma açısından avantajlar sağlarlar. Sistemin hem ölçeklenebilirlik hem de veri boyutu yönetimi açısından geliştirilmesi ve iyi bir test sürecinden geçmesi gerekir. Buluşma Kanıtı sistemi ile dinamik veriler içeren birçok uygulama iş yükleri, veri izleme, iş-çalışan ödülleri, konum verileri sahtekarlıkları ve vergi denetimi gibi pek çok mesele merkezsiz ve adil bir şekilde çözülebilir.

Bir sonraki makalede, tüm teknik detaylar açıklanacaktır.

Kaynakça

[1] Nakamoto S., "Bitcoin: A Peer-to-Peer Electronic Cash System," https://bitcoin.org/bitcoin.pdf, 2008.

[2] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 151(2014), 1-32.

[3] Amoretti, M., Brambilla, G., Medioli, F., & Zanichelli, F. (2018, July). Blockchain-Based Proof of Location. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 146-153). IEEE.