Merkez Bankası Dijital Para Birimi: Tasarım ve Protokol Mekanizmaları Bağlamında Karşılaştırmalı Bir Analiz

Literatür Makalesi/Review Article

Emircan YILDIRIM, Kerim Eser AFŞAR, Ramazan BEKTAŞ

İktisat Bölümü, Dokuz Eylül Üniversitesi, İzmir, Türkiye
emircnyld@gmail.com, eser.afsar@deu.edu.tr, ramazanbektasdeu1@gmail.com
(Geliş/Received:18.06.2022; Kabul/Accepted:16.01.2023)
DOI: 10.17671/gazibtd.1132632

Özet— Bitcoin ile başlayan kripto para ekosistemi ve büyük teknoloji şirketlerinin kendi ödeme sistemlerini kurma girişimleri, merkez bankalarının para üzerindeki tekel haklarını tehdit etmeye başlamıştır. Merkez bankalarının bu gelişmelere olan nihai tepkisi merkez bankası dijital parasıdır (CBDC). Bu çalışmada blok zinciri ağlarında kullanılan alternatif protokol mekanizmalarının, verimlilik, güvenlik ve mahremiyet bağlamında karşılaştırması CBDC literatürünü kapsayacak şekilde yapılmıştır. Çalışmanın amacı protokol ve tasarım özelliklerinin "yeni finansal mimari" içindeki işlevini analiz etmektir. Bu bağlamda çalışmada, CBDC tasarımında bahsi geçen protokollerin işleyişini ayrıntılandırıyoruz. Araştırma kapsamında blok zinciri teknolojisi uzmanlarıyla yarı yapılandırılmış mülakat tekniği kullanılarak veriler toplanmış ve karşılaştırmalı analize tabi tutulmuştur. Karşılaştırmalı analiz yöntemiyle elde edilen bulgulara göre CBDC tasarımında Proof of Authority (POA) protokolünün kullanılması, merkez bankalarına finansal sistemin tümü bağlamında bir gözetim yapabilme şansı tanıyarak bireysel mahremiyeti tamamen ortadan kaldırabilir. Çevrim dışı ödeme (OPS) protokolünün kullanılmadığı durumlarda CBDC'nin amaçlarından biri olan finansal kapsayıcılık işlevsiz kalabilir. Proof of Work (PoW) ve Proof of Stake (PoS) protokollerinin varyasyonlarının kullanılması ise ölçekleme probleminin ortaya çıkmasına neden olabilir. CBDC tasarımlarında kullanılan protokollerin güçlü yönleri dikkate alınarak hibrit bir protokol oluşturulabilir. Protokol yapısının güçlü olması para politikası bağlamında CBDC'nin işlevselliğini arttırabilir. CBDC protokolleri literatürde çoğunlukla verimlilik ve güvenlik boyutlarıyla tartışılmaktadır. Tartışmaya mahremiyet boyutunun da dâhil edilmesi gerektiğini iddia ediyoruz.

Anahtar Kelimeler— CBDC, konsensüs protokolleri, verimlilik, blok zinciri

Central Bank Digital Currency: A Comparative Analysis in the Context of Design and Protocol Mechanisms

Abstract— The ecosystem of crypto money that started with Bitcoin and the attempts of big technology companies to establish their own payment systems began to threaten the monopoly rights of Central Banks on money. The ultimate response of the Central Bank towards these developments is the central bank digital currency (CBDC). In this study, a comparison of an alternative protocol used in blockchain networks with respect to efficiency, security, and privacy that is compatible with the CBDC literature will be provided. The intention of this study is to analyze the function of protocol and design features in the "new financial architecture". In this context, we delve into the operation of the protocols mentioned in the CBDC design. Within the scope of this research, data were collected by using semi-structured interview technique with blockchain technology experts and subjected to comparative analysis. According to the findings obtained by the comparative analysis method, the use of the Proof of Authority (POA) protocol in the CBDC design can completely eliminate individual privacy by giving an opportunity to the central banks to oversee the entire financial system. In the absence of the offline payment (OPS) protocol, financial inclusion, one of the objectives of the CBDC, may become dysfunctional. Using variations of Proof of Work (PoW) and Proof of Stake (PoS) protocols might give rise to scaling problems. A hybrid protocol can be created by considering the strengths of the protocols used in CBDC designs. A strong protocol structure can significantly increase the functionality of the CBDC in the context of monetary policy. CBDC protocols are frequently discussed in the literature regarding their efficiency and security dimensions. We assume that the privacy dimension should also be included in the discussion.

Keywords— CBDC, consensus protocols, efficiency, blockchain

1. GİRİŞ (INTRODUCTION)

Dijital parayı madeni veya kâğıt paranın dijital hali olarak tanımlayabiliriz. 2008 yılında Bitcoin üçüncü bir taraf olmadan eşler arasında ödemeyi mümkün kılan yeni bir ödeme sistemi olarak tanıtılmıştır [1]. Kripto para, değişim aracı olarak, işlemlerin kriptografi temelinde güvence altına alındığı dijital paradır. Bitcoin'in alt yapısı olan blok zinciri teknolojisi ile eşler arasında işlemlerin mümkün kılınması, birçok alanda yeni projelerin ortaya çıkmasına neden olmuştur. Devletler başlarda kripto para birimlerine karşı yasaklayıcı bir tavır sergilerken blok zincirine yönelik araştırmalarını sürdürmeye devam etmektedir. Şimdilerde ise nakit kullanımının düşmesi ve dijitalleşme ile birlikte devletler blok zinciri teknolojisinin meydana getirdiği avantajlardan yararlanmak amacıyla CBDC[1]'ye yönelik araştırmalarını arttırmakta ve pilot uygulamaları hayata geçirmektedir [2]. Bu bağlamda Çin, Nijerya ve Bahamalar'ın yaptıkları çalışmalar CBDC alanındaki gelişmelere yol göstermektedir [3-5].

Bankacılık sisteminde para transferi, göndericinin hesabından gönderilen miktarın düşülüp alıcının hesabına aktarılması ile gerçekleşmektedir. Herhangi bir aracının olmadığı internet gibi güvenin sağlanmasının zor olduğu bir ortamda kişiler arasında işlemlerin gerçekleştirilmesinde kayıt sistemi önem kazanmaktadır. Bu ortamda tutulan kayıt defterlerine yeni işlemler eklenebilmeli, değiştirilemez olmalı ve işlemler silinmemelidir. Kayıt defterinin özgünlüğünün sağlanması için hash (özüt) değerinin olması gerekmektedir. Bu değer ile defterde meydana gelebilecek bir değişikliği görmek mümkündür. Bitcoin'in temeli de bu defter fikriyle hareket etmektedir. Dijital ortamda tutulan defterin bir merkeze bağlı olmadan dağıtık bir şekilde var olmasının öncü çalışmaları Bitcoin'den önce hayata geçirilmiştir. Bağlantılı zaman damgası ile veri yapısının oluşturulmasında Haber ve Stornetta'nın [6] çalışması Bitcoin'in ortaya çıkışı için önem arz etmektedir. PoW sisteminin temelleri ise spam mailler ile gerçekleştirilen saldırıların önüne geçmek için tasarlanmıştır [7]. Bitcoin'in bir diğer temeli olan anonimlik ise Chaum [8] tarafından detaylandırılmıştır.

Bitcoin ve diğer kripto para birimleri paranın bir takım özelliklerini taşımaktadır, ancak bir merkezin kontrolünde olmaması ve devletler tarafından tanınmaması nedeniyle fiat paralardan ayrışmaktadır. Aynı zamanda Facebook'un Libra olarak başlayıp Diem olarak değişen kripto para denemesi büyük şirketler tarafından devletlerin meşruiyetini sarstığı bir durumu ortaya çıkarmıştır. Facebook'un bu girişimi ile birlikte merkez bankaları dijital paralara yönelik araştırmalarını arttırmış ve pilot uygulamalarını hayata geçirmiştir. CBDC, finansal içerme, daha esnek bir ödeme sistemi, kamu mahremiyeti ve sınır ötesi ödemeleri daha etkin kılması gibi avantajları nedeniyle dijitalleşen dünyada merkez bankalarının geride kalmak istemediği yeni bir üründür. Uluslararası ödemelerde kullanılan SWIFT sistemi yavaş ve yüksek maliyete sahip olması nedeniyle kripto paralar ile birlikte kullanımı sarsılmaya başlamıştır. CBDC mimarisi bankaların kullandığı geleneksel yöntemlere yenilik getirerek daha hızlı ve daha düşük ödeme hizmeti sunabilir. Bununla birlikte kripto paraların yarattığı kaos ortamı CBDC ile kontrol edilebilir, geleneksel finans mimarisi için yeni bir alt yapı sunabilir, ödeme sistemlerini dengeleyebilir ve merkez bankalarının kendi meşruiyetlerini sağlayabileceği bir sistemi tekrar mümkün kılabilir.

CBDC'nin güvenli, hızlı ve daha düşük maliyetli bir ödeme sistemi sağlayabilmesi için tasarım içerisinde protokol tercihleri önem kazanmaktadır. Bashar vd. [9] blok zinciri teknolojisini destekleyen çeşitli konsensüs protokollerini ele almakta ve bunları hesaplama zorluğu, güvenlik açıkları, maliyet açısından nesnel olarak karşılaştırmaktadır. Blok zincirinde kullanılan protokollerin güvenlik ve performansı ile ilgili parametreler belirlenerek karşılaştırılması [10], PoW, PoS, DPoS, PBFT protokollerinin avantaj ve dezavantajlarının analizi [11], PoW, PoS, BFT, PoET ve FBFT protokolleri işlem kesinliği, işlem oranı, katılım maliyeti, blok zinciri, düşman saldırısı gibi parametreler ile karşılaştırılması [12], PBFT, PoW, DPoS, PoS ve Raft protokolleri verim, ölçeklenebilirlik ve doğrulama hızı üzerinden karşılaştırmalı olarak analizi [13] blok zinciri bağlamında literatürde yapılmıştır. Literatür içerisinde protokollerin karşılaştırılması blok zinciri teknolojisi üzerinden genel olarak güvenlik ve verimlilik üzerinden ele alınırken CBDC sisteminde kullanılan protokollerin karşılaştırılması literatürde henüz ele alınmamıştır. Ulusal literatürde ise yapılan çalışmalar genellikle CBDC'nin olası etkileri ve fırsatları üzerinden incelenmektedir [14-18]. Çalışmanın amacı blok zinciri teknolojisinde kullanılan protokollerin CBDC tasarımlarında verimlilik, güvenlik ve mahremiyet bağlamında karşılaştırmalı bir analizini yapmaktır. Çalışmada verimlilik, birim zamandaki işlem sayısına; güvenlik, protokollere yönelik siber saldırılara;

[1] İngiltere Merkez Bankası, Merkez Bankası Dijital Parasını ödeme sisteminde değer saklama aracı olarak kullanabilen, merkez bankasının elektronik fiat yükümlülüğü olarak tanımlamaktadır. Dar para arzı olarak belirlenmiş ve evrensel olarak erişilebilirdir. Bkz. J. Meaning, B. Dyson, J. Barker, E. Clayton, "Broadening narrow money: monetary policy with a central bank digital currency", Staff Working Paper No. 724, (2018).

mahremiyet, merkez bankasının kullandığı protokol yapısı ve sistem tasarımına bağlı olarak kişilerin dijital adreslerine ulaşması ve işlemleri takip etmesine göre temellendirilmiştir.

Merkez bankası dijital parası oluşturulurken tasarlanan mimari ve teknik alt yapı önem kazanmaktadır. Geleneksel blok zinciri sisteminin ölçeklenebilirlik problemi yaratması ve enerji verimliliğinin düşük olması nedeniyle bu alanda yeni tasarımlara ihtiyaç duyulmaktadır. Özellikle PoW protokolünün düşük işlem sayısına ve yüksek enerji maliyetlerine sahip olması nedeniyle CBDC mimarilerinde tercih edilmeyen konsensüs mekanizmasıdır. CBDC oluşturulurken mevcut bankacılık sisteminin mimari içerisindeki konumu ve rolü ise bir diğer tartışma konusudur. Bu bağlamda çalışmada, CBDC'nin tasarımı ve teknik alt yapısı için protokol yapıları karşılaştırmalı olarak analiz edilmektedir. Çalışmanın birinci bölümünde, CBDC'nin önemi ve genel tasarımı incelenmektedir. İkinci bölümde, literatürde yer alan CBDC tasarımları; üçüncü bölümde ise CBDC literatüründe tartışılan protokoller ele alınmaktadır. Dördüncü bölümde bu protokollerin karşılaştırmalı analizi yapılmakta ve çalışma sonuç kısmı ile sonlanmaktadır.

2. BLOK ZİNCİRİ VE CBDC (BLOCKCHAİN AND CBDC)

Bitcoin'in alt yapısı veya başka bir deyişle temel teknolojisi olan blok zinciri, Bitcoin'in ardından bir çok kripto para birimi tarafından benimsenerek yeni projelerin ortaya çıkmasına neden olmuştur. Dijital dünyanın hızla gelişmesi ile birlikte fiat paraların kullanımlarının azalması ve blok zincirinin sunduğu faydalardan kaynaklı olarak merkez bankaları, kripto paralardan esinlenerek kendi dijital paralarını çıkarmaya yönelik araştırmalara yönelmiştir. Merkez bankalarının CBDC'ye olan ilgisini Gerçek Zamanlı Brüt Ödemelerde (RTGS) meydana getirdiği avantajlar üzerinden ele alan Calle ve Eidan [19] 1970 yılında toptan ödemenin ilk örneği olan Fedwire'ın kurulmasından itibaren ödemelerin verimliliğini arttırmaya yönelik çalışmaların olduğunu, CBDC'yi de bu 50 yıllık sürecin son adımı olarak nitelendirmektedir. CBDC ile merkez bankaları daha güvenli ve verimli ödeme sistemlerine sahip olabilmektedir [20]. Elde bulundurulan nakit para faizi içermemektedir. Faiz içeren bir CBDC tasarımı ile merkez bankaları, para politikasını kontrol etme kabiliyetini arttırabilmektedir. Dolayısıyla faiz getiren bir CBDC, kısa vadeli devlet tahvilleri gibi diğer risksiz varlıklarla uyumlu bir getiri oranı ile güvenli bir değer deposu sağlayabilir [21]. Bu bağlamda faiz içeren bir CBDC para politikasının yürütülmesinde bir araç olarak kullanılabilir. Aynı zamanda CBDC sınır ötesi ödemelerde kolaylık, esneklik, erişilebilirlik, mahremiyet ve kullanım kolaylığı sunmalıdır [22]. Bununla birlikte CBDC'lerin ödeme sisteminde kullanılması nakit kullanımının yarattığı maliyetleri azaltabilir [23]. Merkez bankalarının dijital para birimleri yaygınlaştıkça artan dijitalleşmeye uyum sağlama süreçleri gelişecek ve meşruiyetini korumalarını sağlayacaktır. Aksi durumda CBDC'ye olan çekimser tavırlar uzun vadede merkez bankaları açısından olumsuz etkiler doğurabilecektir. Bunların başında özel şirketlerin kendi kurdukları ödeme sistemlerinde devletlere olan bağlılıklarının azalması gelmektedir. Örneğin eski adıyla Facebook'un (Meta) iptal edilen Diem projesi, merkez bankalarının para üzerindeki kontrolüne rakip olan en büyük projedir[2]. Bu bağlamda CBDC, şirketlerin sunduğu özel dijital paralara nazaran daha güvenli bir alternatif sağlayabilmektedir. Ancak CBDC'nin bu faydalarından yararlanabilmek için nasıl bir tasarıma sahip olması gerektiği önem kazanmaktadır.

Bir CBDC tasarlanırken veri tabanının seçiminde kullanılacak zincir yapısı ve tasarım biçiminin ne olacağına karar vermek gerekmektedir. CBDC sisteminde Dağıtık Defter Teknolojisi (DDT) ve DDT'nin bir türü olan blok zinciri kullanılırken merkezi veri sisteminin kullanılması da mümkündür. DDT ve blok zinciri teknolojisinde verilerin sisteme işlenmesinde farklılıklar bulunmaktadır. Blok zinciri teknolojisi kullanan mimarilerde veri girişinin ve kayıtların tutulması blok zinciri tipine göre değişmektedir. DDT'de ise veriler tek bir merkezden girilebilir ve kayıtlar dağıtık olarak tutulabilmektedir. Bu çalışma içerisinde blok zinciri veri tabanına ve DDT'ye sahip CBDC mimarileri incelenmektedir. Zincir tipi bakımından izinsiz (açık), izinli ve konsorsiyum olmak üzere üç zincir tipi bulunmaktadır [24]. İzinsiz blok zinciri, herhangi bir merkezin iznine tabi olmadan zincire katılmanın herkesçe mümkün olduğu bir zincir tipidir. Bu zincire kişisel donanım ile katılmak mümkündür. İzinsiz blok zincirinde sisteme dâhil olan herkes veri girişinde bulunabilmekte ve kayıtlar dağıtık olarak tutulmaktadır. İzinsiz blok zincirine örnek olarak Bitcoin ve Ethereum verilebilir. İzinli blok zinciri, bir merkez veya platform tarafından zincirin kontrol edildiği blok zinciri tipidir. Bu zincire madenci olarak katılabilmek için merkezin izin vermesi gerekmektedir ve zincirde düğüm (node) kontrolü merkezin elindedir. Dolayısıyla kayıtlar dağıtık olarak tutulurken veri girişleri bir merkezin kontrolünde ancak yine dağıtık bir şekilde yapılmaktadır. Konsorsiyum blok zinciri, izinli bir blok zinciri tipidir ancak ağın kontrolü bir

[2] Facebook (Meta) şirketinin Instagram, WhatsApp ve Facebook uygulamalarının kullanıcı sayısı 14.06.2022 tarihi itibari ile 2,93 milyardır. Şirketin kullanıcıların kişisel verilerine sahip olması nedeniyle dünya üzerindeki önde gelen merkez bankalarının para üzerindeki tekel hakkını tehdit etmesi nedeniyle finansal kurumlar ve üst düzey politikacılar Libra (Diem) projesine tepki göstermiştir. Bu konuda bkz. https://www.nytimes.com/2019/07/10/technology/fed-chair-facebook-cryptocurrency-libra.html

kuruluş yerine birden fazla kurum ve kuruluş tarafından sağlanmaktadır. Bu ağda yer alan her bir kurum yetkili olduğu düğümleri kontrol etmektedir.

CBDC'ler kullanım amaçlarına göre perakende ve toptan olmak üzere iki şekilde kategorize edilmektedir. Toptan CBDC, merkez bankası ve bankalarla doğrudan ilişkide olan kuruşların ödemelerini içermekte ve bankalar arasındaki ödemelere yeni bir altyapı oluşturmaktadır [25]. Bankaların kendi aralarında kredi riskinin artmasından kaynaklı olarak meydana gelen borçların sonlanması toptan CBDC ile sağlanabilmektedir. Perakende CBDC genel olarak bireyler ve işletmeler arasındaki ödemeler için kullanılmakta ve nakitin dijital bir biçimi olarak nitelendirilmektedir. Perakende CBDC, doğrudan, dolaylı ve hibrit olmak üzere kendi içinde üçe ayrılmaktadır [26]. Doğrudan CBDC, merkez bankası tarafından çıkartılan dijital paranın kişilerin hesaplarına merkez bankası tarafından aktarıldığı bu modelde kişilerin hesapları ve işlemleri merkez bankası tarafından tutulmakta ve kontrol edilmektedir. Son kullanıcılar merkez bankasından bir hesap açar ve işlemlerini gerçekleştirir. Bu haliyle model, klasik bankacılık sistemini dışlar. Dolaylı CBDC, geleneksel bankacılık sisteminin dijital hali olarak nitelendirilebilir. Merkez bankası tarafından ihraç edilen dijital para doğrudan kişilere aktarılmasından ziyade bu süreç finansal kurumların aracılığı ile gerçekleştirilir. Son kullanıcılar para talebinde bulunurken merkez bankasının yerine burada yer alan aracı finansal kurumlardan talepte bulunur. Burada hesapların ve işlemlerin kontrolü aracı olan kurumlar tarafından sağlanır. Hibrit CBDC, kullanıcıların işlemleri bu modelde hem merkez bankası hem de aracı kurumlar tarafından sağlanmaktadır. Bu modelde merkez bankası, perakende işlemlere ait defterleri kendi bünyesinde tutar ve kontrolünü sağlar.

Ödeme alt yapısı olarak CBDC'ler hesap tabanlı, token tabanlı ve semi token olmak üzere üçe ayrılmaktadır [27]. Hesap tabanlı CBDC, son kullanıcıya merkez bankası veya aracı kurumlar tarafından bir hesap tanımlanarak sisteme dahil edilmektedir. Bu sisteme dahil olmak isteyen kişiler kimlikleri ile hesaba sahip olmaktadır. Bu durumda blok zincirin anonimliğinden vazgeçilmektedir. Klasik bankacılık sistemindeki hesap sistemine benzer bir yapısı bulunmaktadır. Token tabanlı CBDC, kullanıcı özel ve genel anahtarı ile işlemlerini geçekleştirmektedir. Bu ödeme sistemi, nakit kullanımının bir versiyonu olarak nitelendirilebilir [28]. Kullanıcının sahip olduğu tokenlere dair anahtarı varsa transfer işlemlerini gerçekleştirebilmektedir. Bu yöntem ile anonimliği sağlamak mümkündür. Ancak anahtar çifti kimlik ile merkez bankası veya aracı kurumlar tarafından sağlanırsa anonimlikten yine vazgeçilmektedir. Semi token, hem token temelli hem de hesap temelli bir hesap yapısı sunmaktadır. Nakit kullanımı gibi küçük ödemeler token temelli yürürken daha büyük para transferleri hesap tabanlı gerçekleşmektedir. Burada token temelli yürüyen ödemeler tıpkı nakit kullanımı gibi kullanıcılara mahremiyet sağlamaktadır.

3. CBDC TASARIMLARI (CBDC DESİGNS)

CBDC literatüründe önerilen modellerin bir kısmı ölçeklenebilirlik sorununu çözmek için tasarlanmıştır. Practical Byzantine Fault Tolerance (PBFT) protokolü ile Panda modeli [29] olarak adlandırılan yeni bir dolaylı CBDC modeli önerilmektedir. Modelde geleneksel blok zincirinin meydana getirdiği ölçeklenebilirlik probleminin ortadan kaldırılması için Hesap (Account) Blok Zinciri ve İşlem (Trading) Blok Zinciri olmak üzere iki blok zincirli bir yapı sunmaktadır. Bu iki zincirin sadece bir işlevselliğe odaklanması nedeniyle model ölçeklenebilirdir. İzinli blok zinciri teknolojisi ve PBFT protokolü kullanılarak MBDC [30] adlı dolaylı CBDC modeli önerilmektedir. Model ödemelerin daha hızlı gerçekleşmesi ve ölçeklenebilirliğin iyileştirilmesi için çoklu blok zinciri mimarisi kullanmaktadır. Ölçeklenebilirliğin sağlanabilmesi için zincirler arası iletişim protokolleri tanımlanmaktadır.

Zang vd. [31] POA-BFT protokolü ile hibrit bir CBDC modeli önermektedir. Modelde, işlem hızının arttırılması, küçük-büyük ödemelerin yerleşimi, doğrulanması ve sorgulanması için dijital para birimlerini kayıt eden hesap şeması kullanılmaktadır. Dijital para birimlerinin kullanılabilirliğini iyileştirmek için Harcanmamış İşlem Çıktısı (UTXO) formu kullanılmıştır. Hesap şeması, banka hesapları gibi çalışmakta ve kullanıcıların bakiyesini kaydetmek için liste kullanmaktadır. PoW ve PoS protokollerinde, düğümler üretilen bloğu doğrulamaktadır, ancak kötü niyetli bir saldırı ile ağın yarısı kontrol edildiğinde sistem manipüle edilir. PBFT mekanizması daha kararlı ve verimli bir mekanizma iken düğüm sayısındaki artış performansı düşürebilmektedir. Delegated Proof of Stake (DPoS) ise CBDC'de kullanıldığında, sahte kimlik oluşturarak ağı kontrol etme girişimini (Sybil Saldırısı) engellemek için etkin bir mekanizmadır. Bununla birlikte geleneksel blok zincirinin dezavantajları göz önünde bulundurularak blok transfer etmek ve üretim sırasını belirlemek için PBFT yolunu kabul eden birkaç blok üreticisine oy veren DPoS-BFT konsensüsü kullanılarak POA-PBFT algoritması önerilmektedir. Bu protokole göre, defter tutan düğüm seçiminin yerini merkez bankası tarafından doğrudan atama ve yetkinin kaldırılması almıştır. Bu yöntem ile oylamadaki etkinsizlik ortadan kalkmaktadır. DPoS'ta blokların üretim sırası tüm düğümler tarafından görüşülürken önerilen protokolde, merkez bankası tarafından belirlenen bir düğüm ile numara bloğu üretilebilir. Bu durum çatallı zincirlerin oluşmasının da önüne geçebilmektedir.

Boston Federal Rezerv Bankası (Boston Fed) ve Massachusetts Teknoloji Enstitüsü'nün Dijital Para Birimi Girişimi (MIT-DCI) tarafından 2021 yılında Hamilton Projesi başlatıldı. Birinci faz raporunda, iki farklı CBDC mimarisi tasarlanmış ve temelde ölçeklenebilirlik üzerinde durulmuştur [32]. Modelde veri kayıtlarının işlenmesi ve konsensüsün sağlanması için Raft protokolü kullanılmıştır. Ağ performansının arttırılması için kripto paralarda kullanılan UTXO protokolünün tüm verilerini tutmak yerine UTXO'ya ait değer, seri numarası ve yükümlülük yükleminin hash fonksiyonu alınarak çekirdek işlemcisinde tutulur. Modelde her UTXO'ya seri numarası eklenerek "küresel benzersizliğe" ulaşılır ve çifte harcamanın önüne geçilir. Projede Atomizer ve İki Aşamalı Taahhüt (2PC) olmak üzere iki farklı mimari tasarlanmıştır. DDT kullanılarak oluşturulan modelde Atomizer tasarımı ile saniyede 170 bin işleme ulaşılırken 2PC tasarımı ile saniyede 1,7 milyon işlem gerçekleştirilmektedir.

Kripto paraların ortaya çıkması ile birlikte uluslararası para ödemeleri daha hızlı ve daha güvenilir bir duruma gelmiştir. Ülkelerin CBDC çalışmalarının artması ile birlikte farklı CBDC ağları arasında işlemlerin sağlanması için çalışmalar yapılmıştır. Jung ve Jeong [33] CBDC'ler arasında işlem yönetimini sağlamak, işlemleri kayıt etmek ve alışverişi mümkün kılmak için ISO/IEC 11.179 meta veri kaydına dayalı bir blok zinciri sistemi ve yönetimi önermektedir. Han vd. [34] birlikte çalışabilirliğin sağlanması için Blok Zincirler Arası İletişim (IBC) protokolü kullanılarak iletişimi sağlayan Cosmos blok zinciri tabanlı CBDC modeli önermektedir. Model, perakende CBDC olarak tasarlanmış ve gizliliğin sağlanması için "Grup Anahtar Yönetim Sistemi" önerilmiştir. Bu modelde konsensüs protokolü olarak BFT kullanılmıştır. Cos-CBDC ile heterojen blok zincirlerini bağlamak veya yan zincirler oluşturmak teorik olarak mümkündür. Bu sebeple, Cos-CBDC sınır ötesi ve toptan ödemede etkin bir şekilde kullanılabilir.

CBDC için bir diğer önemli unsur tasarımdır. Tasarım tercihi ise CBDC'nin yapısına göre değişmektedir. DDT tabanlı CBDC araştırmalarının perakende işlemler yerine genellikle toptan işlemlerin gerçekleştirilmesi üzerine yapıldığı [35] vurgulanarak toptan DDT sisteminde dağıtılan dijital para birimi veya tokenin bankalar tarafından sağlanan hesaplar aracılığı ile perakende kullanıcıların erişebildiği CBDC tasarımı önerilmektedir. Toptan CBDC bankalar arasındaki verimliliği ve dijital para dolaşımının kontrolünü arttırabilir. Ancak toptan CBDC'nin kullanıldığı bir durumunda perakende işlemlere erişim kısıtlanacak ve CBDC'nin avantajları kaybolacaktır. Bu sorunun çözümü için modelde, perakende işlemler için dijital paraları dağıtmak üzere ticari bankalarda DDT tabanlı toptan CBDC ağı ve DDT olmayan sistemleri entegre edecek bir tasarıma odaklanılmıştır. Benzer bir biçimde [36] iki katmanlı bir CBDC modeli önermektedir. Dağıtım katmanı, merkez bankası ve ticari bankalar arasındaki izinli blok zinciri ağına dayalı toptan CBDC'nin kayıtlarının tutulduğu zincirdir. Kullanıcı katmanında ise perakende CBDC kayıtları yer almaktadır. İki ayrı katmanın oluşturulması, ağ trafiğini azaltarak daha ölçeklenebilir bir sistem sunar.

Blok zinciri tarafından sağlanan hizmetler nedeniyle finansal kurumlar ve bankalar finansal sistemden dışlanabilir. Önerilen birçok CBDC modelinde bankacılık sisteminin dışlandığını vurgulayan [37] mevcut bankacılık sistemini etkilemeden uygulanabilecek dolaylı bir CBDC tasarımı önermektedir. İzinli bir blok zinciri mimarisinde tanımlanan CBDC modeli mevcut bankacılık sisteminde birkaç değişiklik yapmaktadır. Dijital ödemeler, ödeme ağları ve ödeme işlemcileri ile çevrimiçi olarak gerçekleşmektedir. Ancak son kullanıcının sisteme erişemediği veya erişim problemi yaşadığı durumlar söz konusu olmaktadır. Bu bağlamda [38] çevrim dışı ödemeleri (OPS) mümkün kılan bir CBDC modeli önermektedir. Dijital paranın güvenli bir şekilde transferinin sağlanması amacıyla sertifika yetkilisi olan merkez bankası, dijital imza oluşturmak için diğer finansal kurumlar ile ortak anahtar kriptografisi kullanarak iki katmanlı hiyerarşik bir anahtar alt yapısı oluşturmuştur. Bu güvenli anahtar yapısı, sertifika alt yapısını CBDC ödemelerinden ayırmakta ve bankalar gibi cüzdan sağlayıcılarının dijital para işlemlerini daha hızlı ve güvenilir bir şekilde gerçekleşmesine olanak tanımaktadır.

Literatürde yer alan CBDC tasarımlarında ölçeklenebilirlik problemlerinin çözümü için çift katmanlı yapılar ve birden fazla blok zincirin olduğu tasarımlar yer almaktadır. Buna göre merkez bankalarının etkin bir CBDC tasarlarken mevcut sorunların üstesinden gelebilmek için blok zinciri teknolojisini geleneksel yapılardan farklı bir biçimde ele almaları gerekmektedir. Bununla birlikte kripto paraların sunduğu mahremiyet, CBDC tasarımlarında genel olarak ihmal edilen bir meseledir. Merkezi olmayan kripto paralarda kullanıcılar sisteme açık (public) ve özel (private) anahtarları ile dahil olmaktadır. Merkezi bir yapıya sahip olan CBDC'lerde ise Müşterini Tanı (KYC), Sertifika Yetkilisi (CA) gibi uygulamalar ile kullanıcılar sisteme dâhil olmaktadır. Bu mimari içerisinde token tabanlı bir CBDC tasarımının tercih edilmesi kullanıcılara mahremiyet sağlayabilir. Ancak kullanıcıların açık ve özel anahtarlarını nereden ve nasıl alacağı burada önem kazanmaktadır. Merkez bankasının bu anahtarları verdiği bir durumda mahremiyet ortadan kalkacaktır.

4. CBDC TASARIMLARINDA ALTERNATİF PROTOKOL TASARIMLARI (ALTERNATİVE PROTOCOL DESİGNS İN CBDC DESİGNS)

Konsensüs protokolleri, sistem içerisinde yer alan üyelerin başarısızlıklardan kurtulup fikir birliği sağlanmasına olanak tanımaktadır. DDT'de ve blok zinciri teknolojisinde kullanılan protokoller temelde fikir birliğini sağlasa da işleyiş ve verimlilik bakımından farklılıklar ortaya çıkmaktadır. Blok zinciri teknolojisinde işlem verimliliği sistem içerisinde kullanılan konsensüs protokolüne göre değişiklik göstermektedir. PoW ve PoS protokollerinin düşük işlem hızı göz önünde bulundurulduğunda bir ülkenin CBDC tasarımı için protokol tercihi önem kazanmaktadır. Gün içerisinde milyonlarca işlemin onaylanması gerektiği bir durumda PoW protokolü gibi işlem hızının düşük olduğu protokol yapıları ölçekleme problemini ortaya çıkarmaktadır. Bununla birlikte kullanılacak protokolün enerji tüketimi açısından da verimli olması gerekmektedir. Bu bölümde CBDC tasarımlarında yer alan protokollerin (PoW, PoS, DPoS, PBFT, PoA ve Raft) teknik yapıları incelenmiştir.

PoW protokolünün ilk uygulaması Bitcoin olduğu için protokol, Bitcoin üzerinden ele alınmıştır. Bitcoin'de bir bloğun oluşturulması ortalama 10 dakikaya tekabül etmektedir ve ortalamadan sapması durumunda blok oluşturmak için istenen özütün zorluğu nonce[3] değeri ile algoritmik olarak ayarlanmaktadır. Bu süre içerisinde madenciler rekabete girerek bloğun nonce değerini bulmaya çalışmaktadır. Bloğun nonce değerinin bulunmasının ardından madenci özeti bulduğunu ağa bildirmektedir. Ağda bulunan düğümler bloğun doğruluğu konusunda konsensüs sağladığında blok zincirine eklenmektedir ve madenci oluşturduğu bloktan ödül olarak Bitcoin ve işlem ücretlerini almaktadır. Nakamoto'nun bu önerisi ile "Bizans Generalleri Problemi" çözülse de sistem hala saldırılara açıktır. Ağ içerisinde kötü niyetli olan kişilerin oranı %51 olduğunda sistemi manipüle etmek mümkündür[4].

PoS protokolü, cüzdanında para tutan her bir kullanıcının düğüm olduğu bir sistemdir. PoW protokolünün yarattığı yüksek enerji maliyetlerinin ortadan kaldırılması için geliştirilen bir modeldir [39]. Bu protokole göre, bir düğüm cüzdanında ne kadar çok kripto para tutarsa ve ne kadar erken sisteme dahil olursa bir sonraki bloğun oluşturulması için o kadar fazla şansa sahip olacaktır. Bu yüzden PoS'da yeni bir blok oluşturma hisse kanıtı ile ilişkilidir. Yeni blok oluşturmak için madenciler servetlerine göre seçilir. Bloğu oluşturan madenciler ödül olarak aldıkları servetlerin bir bölümünü paylaştıklarından güvenilir kabul edilmektedir [40].

PBFT protokolü dağıtık hesaplama sistemlerinde kullanılmakta ve Bizans Generalleri probleminin başarısızlığını belli bir düzeyde tolere etmektedir. HyperLedger sisteminde kullanılan bu konsensüs protokolü, kullanıcıların platforma daha önce kayıtlı olması nedeniyle izinli blok zinciri sistemlerinde kullanılmaktadır [41]. Bu protokolde her düğümün birer açık ve özel anahtarı bulunmaktadır ve düğümler birbirinin açık anahtar bilgisine sahiptir. Yeni bir blok oluşturulduğunda bloğu oluşturan düğüm diğer düğümlerden doğrulama yanıtını beklemektedir. Doğrulama yapan düğümler tüm düğümlerin içerisinde 2/3'e sahip olduğunda işlem onaylanıp üzerinde uzlaşma sağlandığı kabul edilerek blok, muhasebe defterine eklenmektedir. Bu protokol merkezi bir yapının izni ile yeni katılımcı kabul etmektedir. Bu sebeple izinsiz blok zinciri sisteminde kullanılmamaktadır.

PoS'un bir alt protokolü olan DPoS protokolü, iki katmanlı temsili demokrasi ve gerçek zamanlı oylama kullanmaktadır. DPoS'da oylama sistemi blok zincirin daha demokratik bir yapı sağlanmasına olanak sağlar. Bu protokolde, kripto parası olan güvenilir bir grup oylama ile seçilmektedir. Bu grubun kontrolü ile bloklar oluşturulmaktadır. Bu grubun dışında kalan diğer bir grup ise blokların oluşturulmasını sağlamakta ve bunun karşılığında ödül almaktadır.

2017 yılında Ethereum'un kurucu ortağı Gavin Wood tarafından tanıtılan PoA protokolü, blok zinciri sistemlerine verimlilik sunan fikir birliği algoritmasıdır. Bu protokolde PoS protokolünden farklı olarak düğümler hesaplarında token tutmak yerine kimlikleri ile sisteme dahil olmaktadır. Daha çok izinli blok zinciri yapısına uygun olan bu protokolde düğümler merkezin onayladığı bir komiteden oluşmaktadır ve sınırlı sayıda düğüm yer almaktadır. Aynı zamanda izinli zincirlerde PoA protokolü, performans ve verimlilik bakımından PoW protokolüne tercih edilir [42]. PoW'a göre sınırlı sayıda blok doğrulayıcısının olması sistemin daha ölçeklenebilir bir yapıya sahip olmasına olanak tanımaktadır. Bu sisteme dahil olmak isteyen doğrulayıcılar "kimlik kanıtı" DApp'ini kullanarak kimliklerini kanıtlamak zorundadır[5]. Ağ kurallarının bir madenci tarafından ihlal edilmesi durumunda ağda bulunan diğer katılımcılar sorunun çözümü için yasal haklara başvurabilecektir. Bir madenci ağa katılırken doğrulayıcılardan aldığı anahtarı üç

[3] Verilerin SHA-256 formatında özütü oluşturulurken başında 'n' adet sıfır olması istenmektedir. İstenen 'n' adet sıfır PoW mekanizmasının zorluğuna göre değişmektedir. Madenciler istenilen zorluğa sahip başında 'n' adet sıfır olan özüt değerine ulaşmak için nonce değerini kullanmaktadır. Tek kullanımlık sayı (nonce) değeri madenciler tarafından değiştirilerek istenilen özel özüt değer elde edilmeye çalışılır.

[4] Bu saldırıya "%51 saldırısı" adı verilir.

[5] https://github.com/PoAnetwork/wiki/wiki/POA-Network-Whitepaper

anahtarla değiştirmesi gerekmektedir. Bunlar, madencilik anahtarı, oylama anahtarı ve ödeme anahtarıdır.

Konsensüs algoritmalarında Leslie Lamport tarafından oluşturulan Paxos önemli bir konuma sahiptir ve çoğu konsensüs algoritması bu protokole dayanmakta veya ondan etkilenmektedir [43]. Paxos algoritması pratik sistemleri desteklemesi açısından oldukça karmaşık ve anlaşılması zor bir protokoldür. Bu karmaşadan hareketle daha işlevsel ve anlaşılması kolay olması amacıyla Raft protokolü hayata geçirilmiştir. Bu protokol, çoğaltılmış sıralı kayıtları yönetmek için kullanılan bir algoritmadır. Protokol içerisinde sunucular üç durumdan birindedir; lider, takipçi, aday. Protokolde ilk olarak küme içerisinde yer alan sunuculardan bir tanesi lider olarak seçilmekte ve lidere sıralı kayıtları yönetmesi için tam yetki verilmektedir. Lider, istemcilerden gelen sıralı kayıt girişlerini kabul eder ve bunları sunucularda çoğaltır. Bununla birlikte lider, sunuculara sıralı kayıtları durum makinelerine işlemenin ne zaman güvenli olduğunu söyler. Burada veri kayıtlarının tutarlı olması ve fikir birliği sağlanması için her sunucu aynı çıktıyı veren bir algoritma kullanmaktadır. Lider diğer sunucularla uzaktan prosedür çağrıları (RPC) ile iletişime geçmektedir. Bu protokol yapısında verilerin tek merkezden girilmesi fikir birliğinin daha hızlı olmasına dolayısıyla işlem hızının daha yüksek olmasına neden olmaktadır.

5. CBDC'DE KULLANILAN KONSENSÜS PROTOKOLLERİNİN KARŞILAŞTIRMALI ANALİZİ (COMPARATİVE ANALYSİS OF CONSENSUS PROTOCOLS USED İN CBDC)

Bu bölümde blok zinciri ve CBDC'de kullanılan protokollerin karşılaştırmalı analizi, iki sektör uzmanı ve üç akademisyenle yapılan görüşmeler sonucunda elde edilen verilerle yapılmıştır. Çalışmada yarı yapılandırılmış mülakatla on bir soru sorulmuş ve katılımcıların bir kısmı ile yüz yüze görüşmeler yapılırken bir kısmının görüşleri form ile alınmıştır. Çalışma kapsamında PoW, PoS, DPoS, PoA, PBFT ve Raft protokolleri analiz edilmiştir. Bu bağlamada verimlilik, blok zinciri türü, işlem hızı, iletişim karmaşıklığı ve enerji tüketimi parametreleri belirlenerek protokollerin verimlilik, güvenlik ve mahremiyet katmanları incelenmiştir.

Tablo 1. Protokol Yapılarının Analizi
(Analysis of Protocol Structures)

Protokol	Avantaj	Dezavantaj	Sınıflandırma
Proof of Work (PoW) – İş İspatı	-Yüksek Güvenilirlik -Adalet -Saldırılara Karşı Dirençli	-Enerji Maliyetleri -Yüksek CPU-GPU talebi -Düşük işlem hızı	Genellikle izinsiz blok zinciri ağlarında kullanılır (Bitcoin)
Proof of Stake (PoS) – Hisse Kanıtı	-Düşük enerji talebi -PoW'a göre madencilik düşük maliyetli -PoW'a göre ağa katılmak daha kolaydır	-Güvenilirliği düşük -Adaletsiz -Çatallaşma ihtimali yüksek	İzinsiz blok zinciri ağlarında kullanılır (Ethereum)
Delegated Proof of Stake (DPoS) – Temsili Hisse Kanıtı	-PoS'a göre daha adil -Çift katmanlı -Esnek uzlaşma	-Delege kartelleri oluşabilir -Merkezi bir hale gelebilir -Saldırılara daha az dirençli olabilir	Hibrit bir protokoldür ve izinsiz blok zinciri ağlarında kullanılır (BitShares)
Proof of Authority (PoA) – Yetki İspatı	-Kimlik temelli itibar sistemi -Mesajlaşma ağı hafiftir -Doğrulayıcılar itibarını korumak için güven oluştururlar	-Teşvik sistemi dengesiz olabilir -Merkezileşme sorunu ortaya çıkabilir -Sonuç olarak saldırılara açık hale gelebilir	İzinli veya izinsiz blok zinciri ağlarında kullanılır (VeChain)
Pratical Byzantine Fault Tolerance (PBFT) – Pratik Bizans Hata Toleransı	- Yüksek işlem hacmi -Delegeler oylama sistemine göre seçilir -Onaylama süresi kısadır	-Mesajlaşma ağı ağırdır -Ağ merkezi hale gelebilir -Ağ yeni delegeler için cazip olamayabilir	Genellikle izinli veya konsorsiyum blok zinciri ağlarında kullanılır (Hyperledger Fabric)
Raft Protokolü	-Yüksek işlem hacmi -Lider oylama sistemine göre seçilir -Doğrulayıcılığı yüksektir	-Sunucular arasında iletişim problemi yaşanabilir -Enerji kullanımı fazladır -Karar almada olası gecikme	DDT'lerde kullanılır

Tablo 1'de incelenen protokoller yarı yapılandırılmış mülakat ile elde edilen verilerle blok zinciri türüne göre sınıflandırılmış ve karşılaştırmalı analizde belirlenen parametreler bağlamında avantaj ve dezavantajları saptanmıştır.

PoW'da blok oluşturma hızı CPU ve GPU gücü ile doğru orantılıdır. Dolayısıyla Bitcoin'de işlem hızını ve verimliliği etkileyen üç unsur ortaya çıkmaktadır; blok boyutu, blok aralığı ve CPU gücü. PoW protokolünün verimliliğini Bitcoin üzerinden açıklayabiliriz. Bitcoin'in 10 dakikalık ortalama blok aralığı ve her blok için ortalama 1 MB boyutu göz önüne alındığında, verim 7 TPS ile sınırlıdır [44]. CBDC gibi yüksek işlem talebinin olduğu bir durumda saniyede 7 işlemin yapılması sistemde ölçekleme problemini ortaya çıkarabilmektedir. Buna ek olarak Bitcoin'de işlemlerin doğrulanması için özel donanım ve yüksek miktarda enerji gerektirmektedir [45]. PoW protokolü CPU gücü ile ilişkili olması ve blok oluşturmak için yüksek miktarda enerji gerektirmesi nedeniyle enerji kullanımı açısından da verimsiz bir sistemdir. PoW protokolünün güvenliği özel donanım ve elektrik gibi kıt kaynaklara bağlı olduğundan sistemi kaynak açısından verimsiz hale getirir böylece madenciler karını arttırmak için sürekli olarak daha fazla kaynak kullanmaya mecbur kalmaktadır [46]. PoW protokolünün bu verimsizliği nedeniyle CBDC tasarımlarında tercih edilmeyen bir protokoldür. Katılımcılara göre PoW protokolünde işlem sayısını arttırmak mümkün olsa da blok boyutunun sınırlı olması işlem sayısını belli bir yere kadar arttırmaktadır ve enerji verimliliği açısından etkin bir protokol değildir. PoW protokolü yapısı itibariyle tamamıyla merkeziyetsiz bir sistem sunmaktadır. Bu protokolde birkaç madenci ekosistemden ayrılsa da sistem işlemeye devam etmektedir. Bununla birlikte PoW protokolü %51 saldırısına açıktır. Kötü niyetli madencilerin yarısından bir fazlasına ulaşması durumunda sistem manipüle edilecektir. Katılımcılar, merkez bankalarının para üzerindeki tekel hakkını kaybetmemek için tamamıyla merkeziyetsiz bir sistem sunan PoW protokolünün tercih edilmeyeceğini düşünmektedir.

PoW'da enerji ve buna bağlı olarak ortaya çıkan verimlilik sorunu PoS protokolü ile çözülmeye çalışılır. PoS protokolünün temel mantığında kullanıcıların varlıklarını stake etmeleri yatmaktadır. Kripto para birimine olan güvenin ortadan kalkması durumunda kullanıcıların stakeleri değersizleşecektir. PoS protokolünün etkin bir şekilde çalışması için ekonomik bir teşvik gerekmektedir [47]. PoS protokolünün PoW'a göre fiziksel maliyetleri görece düşük olduğundan katılımcıların birincil maliyeti, ödülleri toplamak için teminat olarak stake etmektir [48]. Madenci faaliyetleri görece daha az enerji maliyetlerine yol açtığından PoS protokolünün PoW protokolüne göre daha verimli olduğu söylenebilir. Fakat PoS protokolünün daha çok izinsiz blok zincir türünde kullanılması merkez bankalarının CBDC tasarımında kullanımını zorlaştırabilir. Aynı zamanda PoS'un çatallaşma ihtimalinin olması CBDC için etkin bir protokol olmayabilir. Simülasyon deneylerinden elde edilen bulgulara göre [49]; PoS protokolü PoW protokolüne göre enerji tüketimini %75'ten fazla azaltabilmiştir. Aynı zamanda PoS protokolünün güvenilirlik ve adalet açısından düşük olduğu bulgularına ulaşmıştır. Karma protokol yapılarının enerji, güvenilirlik ve adalet açısından daha etkin olduğu gözlenmiştir. Böylece CBDC için de karma bir protokolün tercih edilmesi PoS'da ortaya çıkacak sorunların çözülmesini sağlayabilir. Katılımcılara göre verimlilik açısından PoS protokolü etkin bir sistem olsa da işlemleri onaylayanların stake miktarına göre işlem onaylama önceliğini elde etmesi adaletsiz bir yapı ortaya koymaktadır. PoW'a göre PoS protokolünün alternatif olarak ortaya çıkmasındaki temel unsurlardan biri çevreye verdiği zarardır. PoW'un yarattığı karbon emisyonu PoS mekanizması ile azaltılabilmektedir. Böylece PoS protokolü PoW'a göre daha etkin bir yapı sunarak çevreye olan etkileri bakımından daha duyarlı bir mekanizmaya sahiptir.

CBDC tartışmalarında genel olarak bir merkezin onayının gerektiği üzerine fikir birliği olması nedeniyle PBFT protokolü sıkça modellerde kullanılmıştır. PBFT protokolünün sıkça kullanılmasının bir diğer sebebi ise verim avantajı sağlamasıdır. Bununla birlikte PBFT protokolü ağ iletişim yükünün fazla ve sistem esnekliğinin düşük olması sorunlarına sahiptir [50]. Ağın iletişim yükünün fazla olması verimliliği olumsuz etkileyebilmektedir. Bu yüzden PoA ile kıyaslandığında PBFT'nin iletişim gücü verimsiz kalmaktadır. Dolayısıyla CBDC protokol tasarımları ele alınırken iletişim gücü ağ verimliliği açısından oldukça önemlidir. CBDC'ler ülke ekonomilerini kapsadığından iletişim yükünün fazla olduğu protokol yapıları verimliliği olumsuz etkileyebilecektir.

DPoS protokolü çift katmanlı ve esnek uzlaşı sağlaması ile PoS protokolünden farklılaşmaktadır. Dolayısıyla DPoS, PoW ve PoS'a göre daha hızlı işlem sağlamaktadır [51]. DPoS'un demokratik yapısı, ağ üzerinde kullanıcılara kontrol hakkına olanak tanıyarak blok zincirin verimliliğini arttırmaya çalışır. DPoS protokolü ağ üzerinde kullanıcılara kontrol hakkı sunabildiğinden PoW'a göre daha verimli bir ağ kullanıcılığı ve madencilik yapısı sunmaktadır [52]. Çünkü PoW protokolünde yalnızca madenciler ödüllendirildiğinden, gelirini maksimumlaştırmak için çabalayacaklardır dolayısıyla bu yapı madenciler ve para sahipleri arasında çatışmaya sebep olabilecektir. Aynı zamanda DPoS protokolü bakım

maliyetlerini azaltması nedeniyle blok zincirinin verimliliğini arttırmaktadır. DPoS, PoS protokolünün dezavantajlı yapılarına çözüm getirdiğinden CBDC tasarımlarında daha kullanışlı bir yapı sunabilir. Merkez bankalarının işlem hacminin yüksek olduğu, esnek uzlaşma ve iletişim yükünün hafif olduğu protokol yapılarını CBDC tasarımında tercih etme ihtimalleri yüksektir. Bu yüzden CBDC'nin protokol yapısında DPoS benzeri bir konsensüs mekanizması verimliliği arttırabilir ve bakım maliyetlerini azaltabilir.

PoA protokolünün izinli blok zincirlerde daha sık kullanılmasının sebebi mesajlaşma ağına daha az ihtiyaç duymasından kaynaklanmaktadır. Dolayısıyla mesajlaşma ağının daha hafif olması protokolün performansını arttırmaktadır [53]. PoA'nın daha düşük haberleşme ağına ihtiyaç duyması ve kimlik doğrulaması gerektirmesi izinli blok zinciri yapılarında verimliliği arttıracak potansiyele sahiptir [54]. PoA ve PBFT protokollerinin doğrulama mekanizmalarının sınırlı olması ağlarda merkezileşme sorununu ortaya çıkarabilir. Ağda merkezi yapını oluşmaya başlaması blok zinciri saldırılara daha açık hale getirebildiğinden bu yapıların merkezileşmemesi önem kazanmaktadır. PoA ve PBFT protokollerinin bu benzerlikleri dikkate alındığında CBDC tasarımını saldırılara açık hale getirme potansiyelleri barındırmaktadır. Dolayısıyla etkin bir CBDC tasarımının önemli kriterlerinden bir diğeri saldırılara karşı dirençli protokol yapısının sağlanmasından geçmektedir. Böylece merkez bankalarının tercih edecekleri protokol yapıları dikkate alındığında bu yapıların avantaj ve dezavantajları hakkında fikir sahibi olmaları önemlidir. Bununla birlikte katılımcılara göre PoA protokolüne dâhil olacak delegelerin kimliğiyle sisteme katılması, kötü niyetli saldırıların önüne geçmenin önemli bir unsurudur. PoA protokolünün bir diğer avantajı ise işlem sayısının yüksek olmasına bağlı olarak birim işlem maliyetlerini azaltmasıdır. İşlem sayısının yüksek olması ise ağda bulunan bütün onaylayıcılar yerine otorite tarafından seçilen onaylayıcıların büyük çoğunluğunun işlemin doğruluğunu kabul etmesi durumunda bloğa kaydedilmesinden kaynaklanmaktadır. İletişim sürecini kısaltan bu uygulama işlem hızını arttırmaktadır. Bu protokolün merkez bankası tarafından kullanılması, onaylayıcıların merkez bankası tarafından belirlenmesi anlamına gelmektedir. PoA protokolünün en büyük dezavantajı ise mahremiyeti ortadan kaldırması ve merkezi bir yapı statüsü sunmasıdır. Merkez bankası açısında bakıldığında para üzerindeki kontrolün merkezi olarak sağlanması için PoA protokolü işlevsel protokollerden biridir.

Raft protokolünde sunucuların lider, takipçi ve aday olması ve bu yapıda liderin oylama sistemine göre seçilmesi PoW ve PoS protokollerine göre daha demokratik bir yapı sunmaktadır. İşlemlerin lider eşliğinde gerçekleşmesi iletişim yükünü azaltarak işlem hızını arttırmaktadır. Ancak enerji ihtiyacının PoW'daki gibi yüksek olması protokolün önemli bir dezavantajıdır. Bununla birlikte Raft protokolünde oylama sisteminin olması, sisteme gelecek güncelleme ve yeniliklerde oy birliğinin sağlanması gerektiği durumlarda karar almada olası gecikmeler ortaya çıkabilir. Bu protokolün daha çok DDT'lerde kullanılması ve veri girişinin tek bir merkezden yapılması CBDC tasarımında mahremiyeti zedeleyebilir. Buna ek olarak veri girişinin tek merkezden yapılması merkez bankasını saldırılara karşı daha açık bir hale getirebilir.

6. SONUÇ (CONCLUSİON)

Merkez bankası dijital parası tasarımlarında ölçeklenebilirlik probleminin çözülmesi için genel olarak çift katmanlı yapılar ve birden fazla blok zincirinin kullanımı önerilmiştir. CBDC'de kullanılan protokollerin verimliliği ise ikincil planda tutulmuştur. CBDC'lerde kullanılan protokollerin karşılaştırmalı analiz sonuçlarına göre Raft protokolü ile yüksek işlem gücüne ulaşılsa da enerji kullanımı bakımından dezavantajlıdır [55]. Protokollerin verimliliğinin artmasında iletişim sürecinin kısa olması önemlidir. PoA protokolünde iletişimsel sürecin kısa olması işlem hızını arttırmaktadır. Bununla birlikte CBDC'lerin bir merkezin kontrolünde olacağı göz önünde bulundurulduğunda PoA protokolü hem yasal bir zemin sağlamakta hem de ağın genişletilebilir olması nedeniyle işlem hacminin yetersiz kaldığı bir durumda avantaj sağlamaktadır. Bankaların CBDC mimarisi içerisindeki konumu ise PoA protokolünde onaylayıcı olarak yer almasına fırsat sunmaktadır. Aynı zamanda PoA protokolünde bankalara yönelik teşvik sisteminin de verimliliği olumsuz etkilemeyecek yapıda olması gerekmektedir. Teşvik sisteminin asimetrik olması ağı saldırılara açık hale getirme ihtimalini ortaya çıkarabilmektedir. Bu yüzden sadece tek bir protokolün olanakları üzerinden tasarlanan CBDC, verimliliği olumsuz etkileyebilir.

PoW protokolünün genellikle izinsiz blok zinciri ağlarında kullanılması ve yüksek işlem hacmine ulaşmak için enerji tüketiminin fazla olması CBDC tasarımında bu protokolün etkin çalışmamasına neden olmaktadır. Bununla birlikte etkin bir CBDC tasarımında kullanılacak protokolün güvenli, işlem hacmi yüksek, ölçeklenebilir ve verimli olması gerekmektedir. Bu yüzden sadece bir protokolün olanaklarından faydalanmak yerine hibrit protokoller geliştirilerek oluşturulacak protokolün zayıf yönleri güçlendirilebilir. Karşılaştırmalı analize göre de elde edilen sonuçlardan biri CBDC tasarımlarında kullanılan protokollerin güçlü yönleri dikkate alınarak hibrit bir protokol oluşturulabilir. Protokol yapısının güçlü olması

dijital paranın etkinliğini arttırarak para politikası bağlamında CBDC'nin kullanılabilirliğini arttırabilir. Görüldüğü üzere yüksek performanslı, enerji ihtiyacı düşük ve verimli bir CBDC tasarımı için protokollerin yapısı CBDC tasarımlarında önemli bir unsurdur.

CBDC tasarımlarında göz ardı edilen bir diğer unsur ise mahremiyettir. Token tabanlı bir CBDC'nin tasarlanması durumunda bu problem çözülebilir. Bununla birlikte etkin bir CBDC tasarımı için izinli bir blok zinciri daha avantajlıdır. Böylece sisteme dahil olmak isteyen herhangi bir finansal kuruluş merkez bankasının onayı ile katılacaktır. İzinli bir blok zincirinin kullanılması aynı zamanda sistemi %51 saldırısına karşı daha dirençli hale getirebilir. Ancak bu durumda yine mahremiyet arka planda kalacaktır. Semi token tabanlı bir CBDC tasarımının tercih edilmesi ise kullanıcılara belli bir düzeyde mahremiyet sağlamaktadır. Bu bağlamda mahremiyet, CBDC tasarımında otoritenin tercih edeceği tasarıma göre değişmektedir.

Çalışma kapsamında verimlilik, blok zinciri türü, işlem hızı, iletişim karmaşıklığı ve enerji tüketimi parametreleri dikkate alınarak protokollerin karşılaştırmalı analizi CBDC literatürünü kapsayacak şekilde yapılmıştır. Bu bağlamda yarı yapılandırılmış mülakat ile elde edilen bulgular literatürle uyumludur. Gelecek çalışmalarda rakip tolerans modeli, gecikme ve bant genişliği gibi parametreler de eklenerek karşılaştırmalı analiz genişletilebilir. Buna ek olarak elde edilen bulguların ilerleyen çalışmalarda nicel olarak analiz edilmesi daha doğru sonuçlar üretecektir. Böylece CBDC'de kullanılacak protokollerin etkinliği, güçlü ve zayıf yönleri daha detaylı analiz edilebilir.

TEŞEKKÜR (ACKNOWLEDGMENT)

Bu çalışmaya görüşleri ile destek veren mfet.earth uzmanlarına ve değerli akademisyenlerimize teşekkürü borç biliriz.

KAYNAKLAR (REFERENCES)

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", *Decentralized Business Review*, 21260, 1-9, 2008.

[2] P. K. Ozili, "Central bank digital currency research around the World: a review of literatüre", *Journal of Money Laundering Control*, 2022.

[3] F. Allen, X. Gu, J. Jagtiani, "Fintech, cryptocurrencies, and CBDC: Financial structural transformation in China", *Journal of International Money and Finance*, 124, 102625, (2022).

[4] P. K. Ozili, "Central bank digital currency in Nigeria: opportunities and risks", Available at SSRN, (2021).

[5] S. L. Náñez Alonso, M. A. Echarte Fernández, D. Sanz Bas, J. Kaczmarek, "Reasons fostering or discouraging the implementation of central bank-backed digital currency: A review", *Economies*, 8(2), 41, 2020.

[6] S. Haber, W. S. Stornetta, "How to Time-Stamp a Digital Document", **In Conference on the Theory and Application of Cryptography,** Cilt 537, Editör: Menezes A. J., Manstone S. A., Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, 437-455, 1990.

[7] C. Dwork, M. Naor. "Pricing Via Processing or Combatting Junk Mail", **In Annual International Cryptology Conference**, Cilt 470, Editör: Brickell E. F., Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, 139-147, 1992.

[8] D. Chaum, "Security Without İdentification: Transaction Systems to Make Big Brother Obsolete", *Communications of the ACM, 28*(10), 1030-1044, 1985.

[9] G. Bashar, G. Hill, S. Singha, P. Marella, G.G. Dagher, J. Xiao, "Contextualizing Consensus Protocols in Blockchain: A Short Survey", **2019 First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)**, IEEE, Lahor-Pakistan, 190195, 1921 December, 2019.

[10] N. Chaudhry, M. M. Yousaf, "Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities", **In 2018 12th International Conference on Open Source Systems and Technologies (ICOSST)**, IEEE, Lahor-Pakistan, 5463, 1921 December, 2018.

[11] Q. Wang, J. Huang, S. Wang, Y. Chen, P. Zhang, L. He, "A Comparative Study of Blockchain Consensus Algorithms", *In Journal of Physics: Conference Series*, 1437(2020), 332-339, 2020.

[12] A. Baliga, "Understanding Blockchain Consensus Models", *Persistent*, *4*(1), 1-17, 2017.

[13] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, C. Qijun, "A Review on Consensus Algorithm of Blockchain" **In 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)**, IEEE, Banff, AB, Canada, 25672572, 0508 October, 2017.

[14] O. Demir, H. Odabaşi, "Merkez Bankası Dijital Para Sisteminin Avantaj ve Dezavantajları Neler Olabilir? *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, (61), 199-222, 2022.

[15] İ, Al, H. Akyazı, "Merkez Bankası Dijital Parası ve Para Politikasına Yansımaları", *Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 19(3), 573-593, 2019.

[16] K. Sebahattin, "Paranın Dijitalleşmesi ve Merkez Bankası Dijital Para Olasılığı", *Bitlis Eren Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Akademik İzdüşüm Dergisi*, 5(2), 196-204, 2020.

[17] N. Öztürk, A. Okan, "Paranın Dönüşümünde Yeni Bir Evre: Merkez Bankası Dijital Parası", *Uluslararası Muhasebe ve Finans Araştırmaları Dergisi,* 3(2), 85-104, 2021.

[18] Y. Toroman, "E-Para ve Tokenler (Dijital Türk Aakçesi) İle Borçlanma: Dijital Türk Lirası (DTL) Üzerine Bir Çalışma", *Bilge Uluslararası Sosyal Araştırmalar Dergisi,* 5(2), 124-134, 2019.

[19] G. Calle, D. Eidan, "Central Bank Digital Currency: An Innovation in Payments", *R3 White Paper*, 1-20, 2020.

[20] D. Priyadarshini, S. Kar, "Central Bank Digital Currency (CBDC): Critical Issues and the Indian Perspective", *Institute of Economic Growth Working Paper*, No. 444, 2021.

[21] M. D. Bordo, A. T. Levin, "Central Bank Digital Currency and the Future of Monetary Policy", *National Bureau of Economic Research*, Working Paper, No 23711, 1-30, 2017.

[22] R. Auer, R. Böhme, "The Technology of Retail Central Bank Digital Currency", *BIS Quarterly Review, March*, 85-100, 2020.

[23] S. M. Davoodalhosseini, "Central bank digital currency and monetary policy", *Journal of Economic Dynamics and Control*, 104150, (2021).

[24] G. Ünal, Ç. Uluyol, "Blok zinciri teknolojisi", *Bilişim Teknolojileri Dergisi*, *13*(2), 167-175, 2020.

[25] Zhang, T., & Huang, Z. (2021). Blockchain and Central Bank Digital Currency. *ICT Express 8*, 264–270, 2022.

[26] R. Auer, G. Cornelli, J. Frost, "Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies", *Bank for International Settlements Working Paper*, 1-42, 2020.

[27] N. Bilotta, F. Botti, **The (Near) Future of Central Bank Digital Currencies: Risks and Opportunities for the Global Economy and Society**, Bern, İsviçre, Peter Lang International Academic Publishers, 2021.

[28] İnternet: D. Niepelt, Central Bank Digital Currency: Considerations, Projects, Outlook, https://voxeu.org/article/central-bank-digital-currency-considerations-projects-outlook, 10.06.2022.

[29] W. Tsai, Z. Zhao, C. Zhang, L. Yu, E. Deng, "A Multi-Chain Model for CBDC", **2018 5th International Conference on Dependable Systems and Their Applications**, Dalian, China, 2534, 2223 September, 2018.

[30] H. Sun, H. Mao, X. Bai, Z. Chen, K. Hu, W. Yu, "Multi-Blockchain Model for Central Bank Digital Currency", **2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies,** Taipei, Taiwan, 360367, 1820 December, 2017.

[31] J. Zhang, R. Tian, Y. Cao, X. Yuan, Z. Yu, X. Yan, X. Zhang, "A Hybrid Model for Central Bank Digital Currency Based on Blockchain", *IEEE Access*, *9*, 53589-53601, 2021.

[32] J. Lovejoy, C. Fields, M. Virza, T. Frederick, D. Urness, K. Karwaski, N. Narula, "A High Performance Payment Processing System Designed for Central Bank Digital Currencies", *Cryptology ePrint Archive*, 1-35, 2022.

[33] H. Jung, D. Jeong, "Blockchain Implementation Method for Interoperability Between CBDCs", *Future Internet*, *13*(5), 133, 2021.

[34] J. Han, J. Kim, A. Youn, J. Lee, Y. Chun, J. Woo, J. W. K. Hong, "Cos-CBDC: Design and Implementation of CBDC on Cosmos Blockchain", **22nd Asia-Pacific Network Operations and Management Symposium,** Tainan, Taiwan, 303308, 0810 September, 2021.

[35] D. T. Sasongko, S. Yazid, "Integrated DLT and non-DLT System Design for Central Bank Digital Currency", **Proceedings of the 5th International Conference on Sustainable Information Engineering and Technology,** New York, United State,171176, 1617 November, 2020.

[36] S. Kumar, "Permission Blockchain Network Based Central Bank Digital Currency", **2021 IEEE 4th International Conference on Computing, Power and Communication Technologies,** Kuala Lumpur, Malaysia, 16, 2426 September, 2021.

[37] S. Maharjan, K. Ko, C. Kang, J. Woo, J. W. Hong, "A Study of CBDC Model Applicable for the Current Banking Environment", **KNOM Conference 2020**, Daejeon, South Korea, 5660, 2020.

[38] M. Christodorescu, W. C. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, M. Zamani, "Towards a Two-Tier Hierarchical Infrastructure: an Offline Payment System for Central Bank Digital Currencies", *arXiv preprint:2012.08003*, 1-21, 2020.

[39] F. Saleh, "Blockchain Without Waste: Proof-of-stake", *The Review of Financial Studies*, *34*(3), 1156-1190, 2021.

[40] E. Deirmentzoglou, G. Papakyriakopoulos, C. Patsakis, "A Survey on Long-Range Attacks for Proof of Stake Protocols", *IEEE Access*, *7*, 28712-28725, 2019.

[41] S. Kardaş, "Blokzincir Teknolojisi: Uzlaşma Protokolleri", *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, *10*(2), 481-496, 2019.

[42] C. N. Samuel, S. Glock, F. Verdier, P. Guitton-Ouhamou, "Choice of Ethereum Clients for Private Blockchain: Assessment from Proof of Authority Perspective", **2021 IEEE International Conference on Blockchain and Cryptocurrency**, Sydney, Australia, 15, 0306 May, 2021.

[43] D. Ongaro, J. Ousterhout, "In Search of an Understandable Consensus Algorithm", (extended version), 2013.

[44] Y. Gao, H. Nobuhara, "A Proof of Stake Sharding Protocol for Scalable Blockchains", *Proceedings of the Asia-Pacific Advanced Network*, *44*(1), 13-16, 2017.

[45] U. Gallersdörfer, L. Klaaßen, C. Stoll, "Energy Consumption of Cryptocurrencies Beyond Bitcoin", *Joule*, *4*(9), 1843-1846, 2020.

[46] O. Vashchuk, R. Shuwar, "Pros and Cons of Consensus Algorithm Proof of Stake. Difference in the Network Safety in Proof of Work and Proof of Stake", *Electronics and Information Technologies*, *9*(9), 106-112, 2018.

[47] C. Ganesh, C. Orlandi, D. Tschudi, "Proof-of-Stake Protocols for Privacy-Aware Blockchains", **Annual International Conference on the Theory and Applications of Cryptographic Techniques**, Darmstadt, Germany, 690719,1923 May, 2019.

[48] G. Fanti, L. Kogan, P. Viswanath, "Economics of Proof-of-Stake Payment Systems", *Working Paper*, 2019.

[49] R. Zhang, W. K. V. Chan, "Evaluation of Energy Consumption in Block-chains with Proof of Work and Proof of Stake". Journal of Physics: Conference Series, 1584(1), 2020.

[50] X. Zheng, W. Feng, "Research on Practical Byzantine Fault Tolerant Consensus Algorithm Based on Blockchain", Journal of Physics: Conference Series, 1802(3), 2021.

[51] S. M. S. Saad, R. Z. R. M. Radzi, "Comparative Review of the Blockchain Consensus Algorithm Between Proof of Stake (PoS) and Delegated Proof of Stake (DPoS)", *International Journal of Innovative Computing*, 10(2), 27-32, 2020.

[52] T. Do, T. Nguyen, H. Pham, "Delegated Proof of Reputation: A Novel Blockchain Consensus", **Proceedings of the 2019 International Electronics Communication Conference**, Okinawa, Japan, 9098, 0709 July, 2019.

[53] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone, "PBFT vs proof-of-authority: Applying the CAP Theorem to Permissioned Blockchain", **İtalian Conference on Cyber Security**, Milan, İtaly, 26 February, 2018.

[54] A. Avasthi, A. Saxena, "Two Hop Blockchain Model: Resonating Between Proof of Work (PoW) and Proof of Authority (PoA)", *International Journal of Information Systems & Management Science*, 1(1), 128-131, 2018.

[55] J. F. Paris, D. D. Long, "Pirogue, a lighter dynamic version of the Raft distributed consensus algorithm", **2015 IEEE 34th International Performance Computing and Communications Conference,** Nanjing, China, 18, 1416 December, 2015.