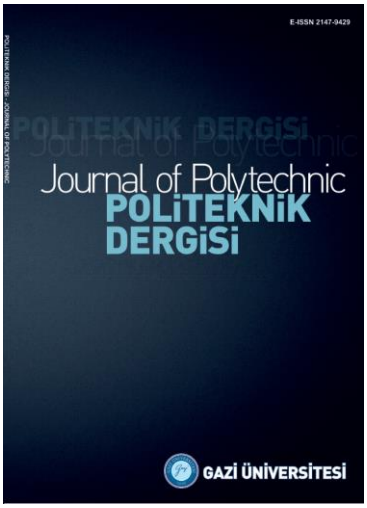


POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

Blok zincir altyapısı ile devlet desteklerinde mükerrerliğin önlenmesi için bir model önerisi

A model proposal for the prevention of duplication in state aids with blockchain infrastructure

***Yazar(lar) (Author(s))**: Kevser AÇIKALIN[1], İsmail ŞAHİN[2]*

ORCID[1]: 0000-0001-6222-3670

ORCID[2]: 0000-0001-8566-3433

To cite to this article: Açıkalın K., Şahin İ., "Blok zincir altyapısı ile devlet desteklerinde mükerrerliğin önlenmesi için bir model önerisi", ***Journal of Polytechnic***, 27(3): 1109-1119, (2024).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Açıkalın K., Şahin İ., "Blok zincir altyapısı ile devlet desteklerinde mükerrerliğin önlenmesi için bir model önerisi", ***Politeknik Dergisi***, 27(3): 1109-1119, (2024).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.1234605

Blok Zincir Altyapısı ile Devlet Desteklerinde Mükerrerliğin Önlenmesi için Bir Model Önerisi

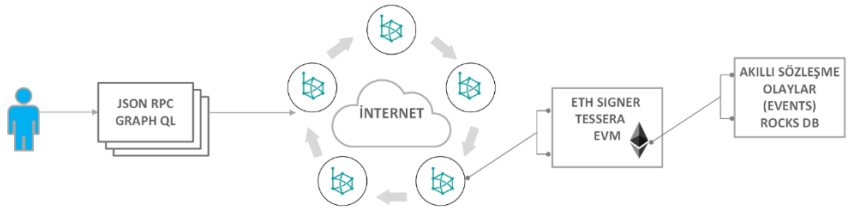
A Model Proposal for The Prevention of Duplication in State Aids with Blockchain Infrastructure

Önemli noktalar (Highlights)

- *Devlet Desteklerinde Mükerrerliğin Önlenmesi / Prevention of Duplication in State Aids*
- *Devlet Desteklerinin İzlenmesi Sürecinin İyileştirilmesi / Improving the Process of State Aids*
- *Blok zincir altyapısı ile Devlet Desteği izleyecek özel bir ağ modelinin geliştirilmesi Developing of a private network model to monitor State Aids with blockchain infrastructure*
- *Kurumların veri paylaşımında olası gizlilik endişelerinin giderilmesi / Elimination of possible privacy concerns in data sharing of institution*

Grafik Özet (Graphical Abstract)

Server-client web mimarisi yerine blok zincir altyapısı kullanılarak, özel ağ geliştirilmesi önerilmiştir. / Instead of server-client web architecture, it has been proposed to develop a private network using blockchain infrastructure.



Şekil. 1 Önerilen modelin yapısı / **Figure 1**. Structure Of The Model

Amaç (Aim)

Devlet desteklerinin takibi için kurulan Devlet Destekleri Bilgi Sistemi'nde fatura bazında takip yapılamadığı için desteğin mükerrer kullanılmasının önüne tam olarak geçilememektedir, ayrıca destek veren kurumların veri paylaşımı yaparken güvenlik endişesi taşımaları olağandır. Bu çalışmada bu sorunların önüne geçmek için blok zincir tabanlı bir model önerilmiştir. Bu model ile kurumların veri paylaşımında yaşayabilecekleri endişe giderilmiş olacaktır ve mükerrer destek alınmasının önüne geçilerek daha etkin destek sistemi kurulabilecektir./ Since it is not possible to follow up based on an invoice in the State Aids Information System established for the follow-up of state aids, it is not possible to prevent the duplicate use of the support, and it is normal for the supporting institutions to have security concerns while sharing data with each other. In this study, a blockchain-based model has been proposed to prevent this, and it is aimed to monitor more effective support with this model.

Tasarım ve Yöntem (Design & Methodology)

Devlet Desteklerinin izlenmesinde mevcut problemler derlendikten sonra çözüm önerisi olarak blok zincir altyapısında özel ağ üzerinde yeni bir model geliştirilmiştir./ After compiling the existing problems in the monitoring of State Aids, a new model was developed on the private blockchain infrastructure as a solution proposal.

Özgünlük (Originality)

Devlet desteklerinin izlenmesine yönelik olarak blok zincir tabanlı bir çalışma bulunmamaktadır. / There is no blockchain-based study for state aids monitoring.

Sonuç (Conclusion)

Önerilen yapı ile hem kurumların güvenlik endişesiyle veri gönderimindeki çekinceleri giderilmiş olacak hem de kötüye kullanımın önüne geçilerek, daha etkin bir destek izlemesi sağlanacaktır bu da yöneticilerin daha yerinde kararlar almasına yardımcı olacaktır. / With this proposed structure, both the reservations of the institutions in sending data due to security concerns will be eliminated and a more effective support monitoring will be ensured by preventing abuse, which will help the managers to make more appropriate decisions.

Etik Standartların Beyanı (*Declaration of Ethical Standards*)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları mateyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler. / The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Blok Zincir Altyapısı ile Devlet Desteklerinde Mükerrerliğin Önlenmesi için Bir Model Önerisi

Araştırma Makalesi / Research Article

Kevser AÇIKALIN[1*], İsmail ŞAHİN[2]

[1]Bilişim Enstitüsü, Adli Bilişim Bölümü, Gazi Üniversitesi, Türkiye
[2] Teknoloji Fakültesi, Endüstriyel Tasarım Mühendisliği, Gazi Üniversitesi, Türkiye

(Geliş/Received : 15.01.2023 ; Kabul/Accepted :03.03.2023; Erken Görünüm/Early View : 18.04.2023)

ÖZ

Birden fazla tarafın bulunduğu iş süreçlerinde merkezi bir doküman yönetim sistemi olmaması durumunda; dokümanların oluşturulma, değiştirilme ve erişilme aşamaları fiziksel olarak gerçekleştirilmektedir. Diğer taraftan merkezi bir sistem oluşturulsa dahi verilerin tek noktada tutulması, tek noktanın kırılganlığı riskinin fazla olmasından kaynaklı güvenlik endişesine neden olmaktadır. Bitcoin altyapısında bulunan blok zincir; dağıtık, anonim, güvenli bir veri saklama yöntemidir. Finansal ödeme sistemlerinin yanında tedarik sistemleri, Iot ve güvenilir üçüncü taraf aracılara ihtiyaç bulunan çeşitli alanlarda kullanılabilmektedir. Özellikle işlem takibinin gerektiği, çok sayıda tarafın katıldığı iş süreçlerinde kolaylık getirmektedir. Devlet desteklerinin takibi için kurulan Devlet Destekleri Bilgi Sistemi'nde fatura bazında takip yapılamadığı için desteğin mükerrer kullanılmasının önüne tam olarak geçilememektedir, ayrıca destek veren kurumların veri paylaşımı yaparken güvenlik endişesi taşımaları olağandır. Bu çalışmada bu sorunların önüne geçmek için blok zincir tabanlı bir model önerilmiştir. Bu model ile kurumların veri paylaşımında yaşayabilecekleri endişe giderilmiş olacaktır ve mükerrer destek alınmasının önüne geçilerek daha etkin destek sistemi kurulabilecektir.

Anahtar Kelimeler: Blok zincir, akıllı sözleşmeler, devlet desteklerinin izlenmesi.

A Model Proposal for The Prevention of Duplication in State Aids with Blockchain Infrastructure

ABSTRACT

In business processes with more than one party; The steps of creating, changing and accessing documents are physically performed in the absence of a central document management system. On the other hand, keeping a single point of data causes security concerns even if a central system is created. Blockchain infrastructure; is a distributed, anonymous, secure data storage method. Besides financial payment systems, it can be used in various fields where supply systems, Iot, and reliable third-party intermediaries are needed. It brings convenience, especially in business processes where transaction tracking is required and many parties participate. Since it is not possible to follow up based on an invoice in the State Aids Information System established for the follow-up of state aids, it is not possible to prevent the repetitive use of the support, and it is normal for the supporting institutions to have security concerns while sharing data with each other. In this study, a blockchain-based model has been proposed to prevent this, and it is aimed to monitor more effective support with this model.

1. GİRİŞ (INTRODUCTION)

Blok zincir (blockchain), kayıtların ya da işlemlerin (blok) arka arkaya zincir şeklinde ve birbiriyle kriptografik olarak ilişkili olarak tutulduğu, güvenilir merkezi bir otoriteye ihtiyaç duymayan, dağıtık ve açık bir veri saklama yöntemidir. Bu yöntem, dağıtık olarak tutulan verinin tutarlılığını ve şifreleme yapıldığı halde dışarıdan erişilebilmeyi garanti etmektedir, böylece veri doğrulamaya imkan tanır [1]. Bitcoin ile tanınırlığı artan blok zincirin temelleri 1990'lı yıllara dayanmaktadır [2]. Bitcoin (BTC), Satoshi Nakamoto mahlasıyla bir grup ya da kişi tarafından "Bitcoin: Uçtan Uca Elektronik Nakit Ödeme Sistemi" isimli yayınla [3] tanıtılan kripto paradır. Önerilen bu sistem 2009 yılı başında açık bir ağ olarak kullanıma sunulmuştur. Bitcoin ile herhangi bir üçüncü güvenilir tarafa ve merkezi otoriteye ihtiyaç duymadan güvenli bir şekilde kişiden kişiye para transferi yapılabilmektedir. Yapılan ödeme işleminin değiştirilmesi neredeyse imkânsızdır, böylece satıcıların korunması amaçlanmıştır. Sistemde alıcıların korunması amacıyla emanet mekanizmaları kolaylıkla uygulanabilmektedir.

Bitcoin ile tanınan blok zincirin uygulama alanları sadece kripto paralarla sınırlı değildir. Tedarik sistemleri, küresel ödeme sistemleri, dijital kimlik, bağış toplama ve yönetimi, seçim sistemleri ve telif hakkı kayıt sistemleri gibi çok farklı alanlarda kullanılmaktadır. [1].

Bu çalışmada; blok zincir teknolojisinin dokuman yönetim sistemlerinde nasıl yer alabileceği değerlendirilecektir. Ardından Devlet Desteklerinin İzlenmesi Sürecinin daha etkin hale gelmesi için blok

*Sorumlu Yazar (Corresponding Author)
e-posta : kevser.acikalin@gazi.edu.tr

zincir tabanlı model önerilmektedir. Bu çalışmanın alana katkıları aşağıdaki şekilde belirtilebilir;

- Devlet desteklerinde mükerrer desteğin önlenmesi için blok zincir tabanlı ilk modeldir.
- Önerilen model destek veren kurumların veri paylaşırken yaşayabilecekleri olası gizlilik endişesinin ortadan kaldırılacak yapıdadır.

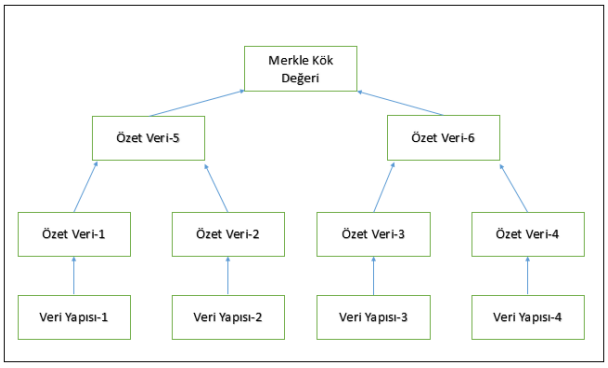
2. BLOK ZİNCİR BİLEŞENLERİ (ARCHITECTURE OF BLOCKCHAIN)

Blok zincir altyapısında özetleme algoritmaları, asimetrik şifreleme ve elektronik imza teknolojileri bulunmaktadır.

2.1. Özetleme Algoritmaları (Hash Functions)

Özetleme işlemi genel olarak bir mesajın ya da dosyanın özeti alınarak sabit uzunlukta bit serisi elde edilmesi olarak tanımlanmaktadır. Mesajda yapılan en ufak bir değişiklik olması halinde bile özet değeri değişmektedir. Tek yönlü olan özetleme algoritmalarında özetten mesaja ulaşmak imkânsızdır. Özet değerleri aynı olan iki farklı mesajın bulunması oldukça zordur [4]. SHA256 ve Keccak blok zincir altyapılarında kullanılan özetleme algoritmalarındandır.

Birden fazla unsurun doğrulanması amacıyla bütünü oluşan elemanların ikili olarak özeti alınarak tek bir özet değerin elde edildiği Merkle ağacı oluşturulmaktadır. 1979'da Ralph Merkle tarafından geliştirilen bu yapıda veri yığınları hızlı şekilde doğrulanabilmektedir [5]. Veri yığınındaki parçalar ikili bir ağaç yapısı oluşturularak en alt seviyeye yerleştirilir, daha sonra ikili özet değerleri alınarak tüm ağacın bir özet değeri elde edilir. Bu değer ağacın kök değeridir, yalnızca bu kök değerin karşılaştırılması ile tüm ağacın değiştirilmediğine dair doğrulama yapılabilir [1]. Örnek Merkle ağacı yapısı Şekil 1'de gösterilmiştir.



Şekil 1. Merkle Ağacı Yapısı (Merkle Tree)

2.2. Asimetrik Şifreleme (Asymmetric Encryption)

Asimetrik anahtarlı bir algoritmada şifreleme işlemi ve şifreyi çözmek için açık ve özel anahtar çifti kullanılır. Genellikle imza oluşturma verisi özel anahtarken imza doğrulama verisi açık anahtardır. Kullanılan yönteme göre özel anahtar ile açık anahtar aralarında matematiksel bir ilişki kurularak birlikte oluşturulur. Anahtarlardan biri kullanılarak oluşturulan şifre ancak diğer anahtar kullanılarak çözülür [6]. RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) ve Eliptik Eğri algoritmaları asimetrik şifreleme algoritmalarındandır. Blok zincir altyapısında Eliptik Eğri algoritması kullanılmaktadır. Eliptik eğriler, RSA'nın sağladığı güvenlik düzeyini daha düşük anahtar uzunluğu ile sağladığından tercih edilmektedir. Şifreleme için gereken süre de RSA'ya göre daha az olduğu için bellek ve işlemci kaynaklarının sınırlı olduğu mobil cihazlar, akıllı kartlar vb. cihazlarda tercih edilmektedirler [7].

2.3. Elektronik İmza (Digital Signature)

Gönderici tarafında elektronik bir dokümanı imzalama işlemi iki adımda gerçekleşmektedir. İlk olarak imzalanacak elektronik verinin özet değeri elde edilir. Ardından elde edilen özet bilgisi açık anahtarlı imza algoritmasıyla imzalanır. Bu iki adım sonucunda oluşan elektronik imza ile şifresiz haldeki açık elektronik veri karşı tarafa gönderilmeye hazırdır. Alıcı tarafında imzalı şekilde gelen elektronik verinin doğrulanması iki adımdan oluşmaktadır. İlki, şifresiz halde alınan elektronik verinin özet değerinin elde edilmesidir. Ardından alınan elektronik imza, açık anahtar kullanılarak açık anahtarlı imzalama algoritmasıyla deşifre edilir ve elektronik verinin özet değerine ulaşılır. İlk adımdaki özet değer ile ikinci adımdaki özet değer aynıysa elektronik verinin içeriği değiştirilmeden imzalanan kişi tarafından gönderildiği sonucuna ulaşılır [8].

2.4. Eşler Arası Ağ (Peer-To-Peer Network)

Eşler arası (Peer-to-peer/P2P), birden fazla bilgisayar arasında veri paylaşımı için kullanılan ağ protokolüdür. Katılımcı her bir eş, bir veriyi indireceği zaman elinde istediği veri bulunan diğer katılımcıları bulur ve onlardan veriyi indirir. Karşılığında da elinde bulunan veriyi o veriyi talep eden başka katılımcıların bilgisayarına aktarılacak şekilde yükler. BitTorrent ve eDonkey bu uygulamalara örnek verilebilir. Veri blok zincire benzer şekilde dağıtık şekilde tutulmaktadır ancak içerik şifreleme ve indirilen verinin istenilen dosya olduğundan emin olunamaması nedeniyle güvenli bir çözüm değildir [1].

Dağıtık tabanlı defter teknolojileri (DLT) bu probleme çözüm olarak ortaya çıkmıştır. Ağa veri ekleneceği zaman çalışan mutabakat yapısı ile merkezi bir sisteme ihtiyaç duymadan eşler/düğümler güncellemeleri alarak dağıtık bir şekilde güncel verileri tutmuş olur [1].

3. BLOK ZİNCİR ÖZELLİKLERİ (PROPERTIES OF BLOCKCHAIN)

Bitcoin'in yayınında blok zinciri öne çıkaran özellikler dağıtık mimari, kalıcılık, anonimlik ve denetlenebilirlik olarak belirtilmiştir [3]:

Dağıtık mimari (Decentralization): Geleneksel merkezi transfer sistemlerinde, her bir işlemin onaylanması için

merkezi, güvenilir bir yapıya ihtiyaç vardır (banka, noter vs.). Bu sistemlerde maliyet ve performansta darboğaz oluşması kaçınılmazdır. Blok zincirde üçüncü bir tarafa ihtiyaç yoktur, mutabakat yapıları ile dağıtık mimaride verilerin tutarlı bir şekilde tutulması sağlanır. Mutabakat yapısı örneğine bölüm 4.1.'de yer verilmiştir. Üzerinde mutabık kalınan veriler tek bir noktada tutulmak yerine dağıtık olarak birden fazla yerde bulunduğundan, tek bir merkezi noktanın kırılganlığına bağlı güvenlik açıklarından etkilenmeyecektir.

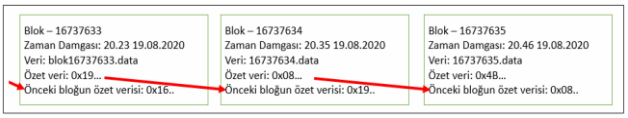
Kalıcılık (Persistency): Bloğa eklenen işlemlerin onaylanma süreci hızlıdır, geçerli olmayan işlemler güvenilir madenciler tarafından reddedilir. Blok zincire eklendikten sonra bir işlemi silmek veya geri almak neredeyse imkânsızdır. Böylece aynı paranın tekrarlı harcanmasının (double spending) önüne geçilerek dolandırıcılık önlenir.

Anonimlik (Anoniymity): Blok zincirde işlem yapacak kişi, bir cüzdan adresi üreterek işlemlerini yapabilir. Bunun için kişisel bilgilerini girmesine gerek yoktur. Yine de blok zincir tam olarak bir gizliliği iddia edemez, çünkü hem bu adreslerin oluşmasında kişisel bilgiler gerekir hem de bir zincir baştan sona incelendiğinde bir hesabın tüm işlemlerine ulaşılabilir.

Denetlenebilirlik (Auditability): Bitcoin özelinde açıklamak gerekirse, tüm kullanıcıların hesapları harcanmamış işlem çıktısı (Unspent Transaction Output, UTX-O) modeli ile tutulur. Bir işlem daha önce harcama yapılmayan başka bir işlemi referans göstermek zorundadır. Bloğa eklenen bir işlemin durumu harcanmamış işlemden harcanan işlem olacak şekilde değiştirilir. Böylece işlemler kolaylıkla doğrulanıp takip edilebilir.

4. BLOK VE MUTABAKAT YAPISI (STRUCTURE OF BLOCK AND CONSENSUS)

Blok zincir ağında verilerin en alt kademede saklandığı yapılar blok olarak adlandırılır. İlk blok (genesis) oluşturulduktan sonra zaman sırasına göre zincir olarak birbiriyle ilişkili olarak tutulur. İlk blokta önceki bloğun özet değeri 000..0 olarak bulunur. Bir blok kendinden önceki bloğun özet değerini de tutar, bu sayede arada bir bloğun dışardan müdahale ile değiştirilmesi durumunda o bloktan sonraki blokların da değiştirilmesi gerekir. Güvenliği sağlayan mekanizma bu zincir yapısıdır ve oluşturulduktan sonra değiştirilemez. Örnek blok yapısı Şekil 2'de gösterilmiştir.)



Şekil 2. Blok Yapısı (Block Structure)

4.1. Mutabakat Yapısı ve Süreci (Process of Consensus)

Dağıtık bir yapıda eklenen bloğun ağdaki tüm bilgisayarlar tarafından kabul edilmesi için mutabakat yapısına uygun olarak eklenmelidir. Böylece hatalı işlemlerin ya da geçerliliği olmayan işlemlerin önüne geçilebilir, bu şekilde birbirini tanımayan insanlar o ağa eklenmiş verinin güvenilirliğinden emin olur.

Bitcoin'de kullanılan İş-İspatı (Proof-of-Work (PoW)) en çok tercih edilen yöntemlerden biridir. Bu yöntemde, bir bloğun blok zincire eklenebilmesi için bir problem ortaya konulmuştur, bu problemi çözmek zaman almaktadır, denemelere dayanır ancak çözümün doğruluğu bir değerin özetini alacak kadar kısa sürede olmaktadır. Bu problemi çözme süreci madencilik olarak adlandırılır. Problem, zorluk değerine göre belirlenen karakterde 0 ile başlayan özet değeri bulmaya dayanır. Zorluk değeri arttıkça çözümü bulmak için gereken deneme sayısı da giderek artmaktadır. Olması istenen formatta özet değeri sağlayan ilk kişi, blok zincire yeni bloğu eklemeye hak kazanır.

Bir blok eklendikten sonra o bloğu değiştirmek isteyen kişi hem o bloğu hem de kendinden sonraki blokları değiştirmek zorundadır, blok zincir güvenliği bu şekilde sağlanmaktadır. Zamanla hızlanan donanımların bu sürece etkilerini düzenlemek için zorluk değeri değiştirilerek her zaman blok üretiminin belirli bir hızın üstüne çıkması önlenir [3].

4.2. İşlem Yapısı (Structure of Transaction)

Bitcoin özelinde işlem (trancation), ağa yayılan ve bloklar altında toplanan bir Bitcoin aktarımıdır. Yani Bitcoin'in bir yerden (input) diğer bir yere (output) transfer kaydıdır. Bir işlem, önceki işlem çıktılarını yeni işlemin girdisi olarak referans alır ve tüm Bitcoin girdi değerlerini yeni çıktılara dönüştürür. Şifrelenmedikleri için listelenmeleri ve bloklardaki tüm işlemlerin görüntülenmeleri mümkündür. İşlemler yeterli onay aldıktan sonra geri döndürülemezdir denilebilir. Standart bir işlemde çıktı olarak adresler gösterilir ve daha sonraki herhangi bir girdinin ödemesi ilgilinin imzasını gerektirir.

Tüm işlemler blok zincirde görülebilir ve bir hex editörü ile dışardan bir kişi tarafından görüntülenebilir. Blok zincir görüntüleyici (scan sayfaları) ile işlemler teknik ayrıntıları ile görüntülenip doğrulanabilir. Blok içindeki işlemlerin Merkle ağaç özeti tutularak değiştirilmemesi sağlanır [9].

5. BLOK ZİNCİR TÜRLERİ (TYPES OF BLOCKCHAİN)

Blok zincir, erişim ve katılım izinlerini belirleme ve yönetme özelliklerine göre üç grup altında incelenebilir:

Açık blok zincirler (Public Blockchains): Açık blok zincirde her katılımcı, ağdaki bilgiye erişebilir, mutabakat ve onay işlemlerine dahil olabilir. Kurallara uyan herkes, mutabakat yapısına katılarak maddi kazanç sağlayabilir. Tüm ağ açık olduğu için işlemler dışardan takip edilip görüntülenebilir. Dağınık yapının mutabakat yapısı ile senkron hale gelmesi onu güvenilir kılarken hızını yavaşlatır. Her bir bloğu eklemek için gereken hesaplamalarda çok fazla elektrik tüketilir. Bitcoin'i örnek olarak verebileceğimiz bu ağlar özel (private)

ağlara göre daha yavaştır [1]. Açık ağlarda geliştiren kişilerin dahi uygulama içindeki verileri değiştirmeye yetkisi yoktur.

Özel blok zincirler (Private Blockchains): Blok eklemeye erişim bir kurum/kuruluş tarafından koordine edilir ve ağa erişim herkese açık veya sınırlıdır. Aynı blok zinciri kullanırken bile mutabakat sağlamada güvenilir bir taraf gerektirir. Tek bir kurum içindeki veri tabanı yönetimi ve denetimi gibi konularda kullanılabilir [10]. Açık ağlara göre daha hızlıdır. Geth [11] ve Truffle [12] altyapıları özel blok zincirleri oluşturmaya olanak sağlar. Ayrıca HyperLedger Besu [13], Multichain [14], Hyperledger Fabric [15] , R3 Corda [16], Enterprise Ethereum [17] EOS [18] gibi ağların özel blok zinciri oluşturma desteği bulunmaktadır.

Konsorsiyum blok zincirler (Consortium Blockchains): Kısmen özel ağlardır. Açık ağlardaki gibi herkesin blok ekleyebileceği ya da özel ağlardaki gibi tek bir noktanın blok ekleyebileceği bir yapı yerine daha önceden tanımlanan birkaç noktanın ekleme yapabileceği yapılardır. Ethereum'un kurucusu, "Konsorsiyum blok zincirleri, daha az güvenilen açık ağlar ile yüksek güvenilirliğe sahip tek kurumun rol aldığı özel ağların karışımıdır "şeklinde tanımlamıştır [19].

6. AKILLI SÖZLEŞMELER (SMART CONTRACTS)

Vitalik Butalin, 2013 yılı sonlarına doğru Bitcoin üzerinde uygulama geliştirmek için komut dillerine ihtiyaç olduğunu savunarak Ethereum'u önermiştir [20]. Butalin'in bahsettiği akıllı sözleşmeler aşağıdaki özelliklere sahiptir:

-Mantıksal akış içeren bir kod bloğu vardır (if..then.. yapısı)

-Dağıtık bir altyapıda tutulur ve çoğaltılabilir.

-Bir ağ tarafından çalıştırılır.

-Doğrulaması bir ağ tarafından yapılır.

-Sözleşmeye bağlı bir sonucu icra edebilir, para transferi yapabilir, yeni bir sözleşme hazırlayabilir.

Taraflar anlaştıktan sonra sözleşmeyi kriptografik olarak imzalayarak akıllı sözleşmeleri ağa yüklerler. Sözleşme içindeki durumlardan biri oluşması halinde (kullanım zamanının bitmesi, işlem fiyatının belirli bir seviyeye gelmesi gibi) otomatik olarak anlaşma koşulları yürütülür. Bu işlemler bir transferi tetikleyebilir veya bilgilendirme yapabilir [1]. Akıllı sözleşmeler, bir blok zincir üzerinde, tarafların önceden belirlediği koşullar meydana geldiğinde otomatik olarak sonuçlarını icra edecek programlardır.

7.BLOK ZİNCİR TABANLI DOKÜMAN YÖNETİM SİSTEMİ (BLOCKCHAIN BASED DOCUMENT MANAGEMENT SYSTEM)

Bir iş sürecindeki belge ve bilgi alışverişinin sanal ortamda yapılmasıyla yazışma için harcanan maliyet en aza indirgenmektedir. Bir iş sürecindeki elektronik kayıtların oluşturulması, kullanılması, erişimin sürekliliği için gereken bakımın yapılması ve gerektiği şekilde sonlandırılabilmesinin yönetimini sağlayan sistemlere elektronik kayıt sistemi veya doküman yönetim sistemi denir [21]. Bu sistemlerle belgelere erişimler sınırlandırılabilir, bir belgenin değişimindeki iz takip edilebilir, belli standartlarda arşivlenerek fiziksel evrakların depolamasından kaynaklı sorunlar giderilir. Geleneksel yöntemlere göre oldukça hızlı ve etkindir aynı zamanda daha az insan kaynağına ihtiyaç duymaktadır.

Merkezi bir doküman yönetim sisteminin kurulması; farklı lokasyonlardan çok sayıda katılımcı olması gibi durumlarda uygulanamayabilir bu durumda blok zincir tabanlı doküman yönetim sistemleri göz önüne alınabilir [22].

E-devlet çözümleri gibi çok fazla kişisel kaydın tek bir merkezde tutulmasında ise güvenlik endişeleri ortaya çıkabilir. Kişisel bilgilerin doğrulanması ve paylaşıma izin verilmesinin kişinin onayına bağlı süreçlere gereksinim duyulabilir burada yine blok zincir tabanlı kriptografik çözümler devreye girecektir.

Ayrıca kişisel dosya ve klasörlerin dağıtık sistemlerde tutulması amacıyla geliştirilmiş blok zincir tabanlı uygulamaların olması dikkate değerdir [23, 24].

Dağıtık uygulamalarda (Distributed Applications (DApp)) elektronik dokümanların Dağıtık Defter Teknolojisi (Distributed Ledger Technology (DLT)) üzerinde saklanması için önerilen mimaride Hyperledger kullanılması önerilmiştir ve Erasure kodlama [25] kullanılarak ihtiyaç duyulan depolama alanının %25 oranında azaltılabileceği belirtilmiştir [26].

8.DEVLET DESTEKLERİNİN İZLENMESİ SÜRECİ (PROCESS OF MONITORING STATE AIDS)

Türkiye'nin Avrupa Birliği adaylık sürecinde uyması beklenen Avrupa Birliğinin İşleyişi Hakkındaki Antlaşma'da (TFEU - Treaty on Functioning of the Europan Union) bulunan 107.maddeye göre [27]:

"Bu antlaşmada aksine hüküm bulunmadıkça bir üye Devlet tarafından veya Devlet kaynakları vasıtasıyla herhangi bir şekilde yapılan ve belirli teşebbüsleri veya belirli malları kayırmak suretiyle rekabeti bozan veya bozmakla tehdit eden her türlü yardım, üye devlet arasındaki ticareti etkilediği ölçüde ortak pazarla bağdaşmaz."

Tanımda nelerin destek olmayacağı ifade edilmiştir, uygulamada verilen hukuki kararlarla fikir birliği sağlamak hedeflenmiştir.

Türkiye'de yasal olarak bu anlaşmaya uymak için 13.10.2010 tarihinde 6015 sayılı Devlet Desteklerinin İzlenmesi ve Denetlenmesi Hakkında Kanun yayımlanmıştır [28]. Kanun, Avrupa Birliği ile ülkemiz arasındaki anlaşmalara uygun şekilde devlet desteklerinin düzenlenmesini ve ilgili kurumlara bildirimini sağlamak için ilkelerin belirlenerek devlet

desteklerin izlenerek denetlenmesine ilişkin usul ve esasları tespit etmeyi amaçlamıştır.

8.1. Devlet Destekleri Bilgi Sistemi (State Aids Information Systems)

6015 Sayılı Kanun'da belirtilen desteğe konu işlemleri izlemek ve raporlayabilmek için Hazine Müsteşarlığı bünyesinde Devlet Destekleri Bilgi Sistemi (DDBS) geliştirilmiştir, bu sistemin kapsamı AB tarafında izlenecek desteklerden daha geniş tutulmuştur. DDBS'ye veri aktarımını düzenlemek için 30 Mayıs 2014'te "Devlet Destekleri Bilgi Sistemine Veri Aktarılması Hakkında Yönetmelik" yayımlanmıştır [29].

Yönetmelik gereğince hangi kurum ve kuruluşların DDBS'ye veri aktaracağı üç ayda bir güncellenen liste ile ilan edilmektedir. Listede yer alan yirmiden fazla kurumun (Ticaret Bakanlığı, Sanayi ve Teknoloji Bakanlığı, TÜBİTAK, KOSGEB vb.) her destek programına özgü veri seti oluşturulmuştur. Üç ayda bir destek veren kurumlar, web servisleri aracılığıyla veya sisteme girip Excel dosyası yükleyerek veri aktarımı yapmaktadırlar.

Bir kurumun hazırladığı veri setinde temel olarak, dört grup alan bulunmaktadır. Bunlar firma bilgisi, proje bilgisi, harcama bilgisi ve destek bilgisidir. Firma bilgisinde tekillik vergi kimlik numarası ile sağlanmaktadır. Proje bilgisinde tekillik o kuruma başvuruda verilen tekil proje numarası ile sağlanmaktadır. Harcama bilgilerinde o desteğe özel oluşturulan harcama kalemlerinin DDBS'de karşılığı olan harcama kodu, harcama tutarı ve harcama tarihi gönderilmektedir. Benzer şekilde destek bilgilerinde de o desteğe özel oluşturulan destek kalemlerinin kodu, destek tutarı ve destek tarihi gönderilmektedir. DDBS, Hazine ve Maliye Bakanlığı bünyesinde işleyişine devam etmektedir.

8.2. Karşılaşılan Sorunlar (Encountered Problems)

DDBS uygulamasında karşılaşılan sorunlar iki başlığa ayrılabilir. İlki, kurumların veri gönderiminde güvenlik endişesiyle titiz davranmalarıdır. İkincisi ise bir firmanın aynı harcama için birden fazla destek almasının önüne geçilmesinin zor olmasıdır.

Kurumların veri gönderiminde direnç göstermesinin önüne geçmek için 6015 sayılı Kanun'a ilave edilen ek madde ile veri gönderimi kanuni olarak zorunlu hale getirilmiştir. Ancak kurumların gizlilik endişesinin devam etmesi olağandır. Özellikle destek veren bir kurum tarafından yürütülen bir programda hem vergi indirimi hem de sigorta desteği bulunuyorsa bir kayıt üç farklı kurum tarafından oluşturulmaktadır. Burada tekilliği sağlayan proje numarasının üç kurum tarafından kullanılmasıyla kaydın tamamlanması sağlanmıştır.

Firmaların aynı harcama kalemi için birden fazla destek almasının önüne geçmek için DDBS'de bir ekran oluşturulmuştur. Burada veri girişi yapan kurumlar firma vergi numarası ile sorgulama yapabilmektedir, o firmanın daha önce aldığı destekler proje adı, harcama ve destek tutarı toplamı ile tarih bilgisi, detay bilgi vermeden özet şekliyle listelenmektedir. Böylece destek veren kurumdaki uzmana bir başvuru geldiğinde, ilgili firmayı sorgulatıp benzer proje bilgisinin olup olmadığını kontrol edebilmesi ve detayları hakkında firmadan bilgi talep edebilmesi hedeflenmiştir. Ancak bu ekranda bulunan verilerin, ticari sır niteliğine girme ihtimalinden dolayı sayfa kullanıma açılmamıştır.

Ayrıca aktarım üç ayda bir yapıldığından, sorgulama ekranı açılsa bile bir firmanın iki farklı kuruma aynı fatura ile yakın zamanlı başvurularını takip etmek mümkün değildir. Sisteme veri aktarımı anlık hale getirilmesi durumunda ise harcamaya konu faturalar sisteme dâhil edilemediği için mükerrerliğin önüne geçmek yine oldukça zor olacaktır.

Kolombiya'daki ambargo sistemi için önerilen blok zincir tabanlı çalışmada merkezi bir doküman yönetim sisteminin kurulmasının zor olduğu, birden fazla kurum ve/veya şahsın taraf olduğu ve sürecin aksamasının mali zararlara neden olduğu sistemler için blok zincir tabanlı doküman sisteminin kullanılmasının uygun olacağı ifade edilmiştir [22]. Hemen her iş sürecinde dokümanların bütünlüğünün tespiti ile zaman içinde üzerinde yapılan değişikliklerin izlenmesinin önemli olduğu düşünülmektedir.

Bu nedenlerle DDBS'ye veri gönderimi ve paylaşımında güvenlik endişesini gidermek ve mükerrer destek uygulamasının önüne geçmek için bu çalışmada blok zincir tabanlı bir model önerilmiştir. Bir sonraki bölümde modelde kullanılması önerilen HyperLedger Besu hakkında bilgi verilecektir.

8.3. HyperLedger Besu (HyperLedger Besu)

Ethereum istemci (client) uygulamaları Go, Javascript, Python gibi çok çeşitli dillerle bazı özelliklere uyularak geliştirilebilir. Her ne kadar Geth [11] gibi altyapılar ile bir Genesis dosyası oluşturulup özel bir ağ kolaylıkla oluşturulabilse de bu ağların kurumsal ihtiyaçları karşılaması zor olabilir. Bu problemi gidermek için Enterprise Ethereum Alliance (EEA); üyelerin izinlendirilmesi, yüksek performans ve bir işleme ait veriyi (transaction) sadece işleme katılanların görebileceği nitelikte özellikler gibi kurumsal ihtiyaçları karşılayacak şekilde geliştirilmiştir [30]. HyplerLedger Besu da Ethereum istemci uygulamalarından biridir, Java ile geliştirilmiştir. Bir Besu istemcisi hem Ethereum açık ana ağına (mainnet) hem de özel bir Ethereum ağına katılabilir.

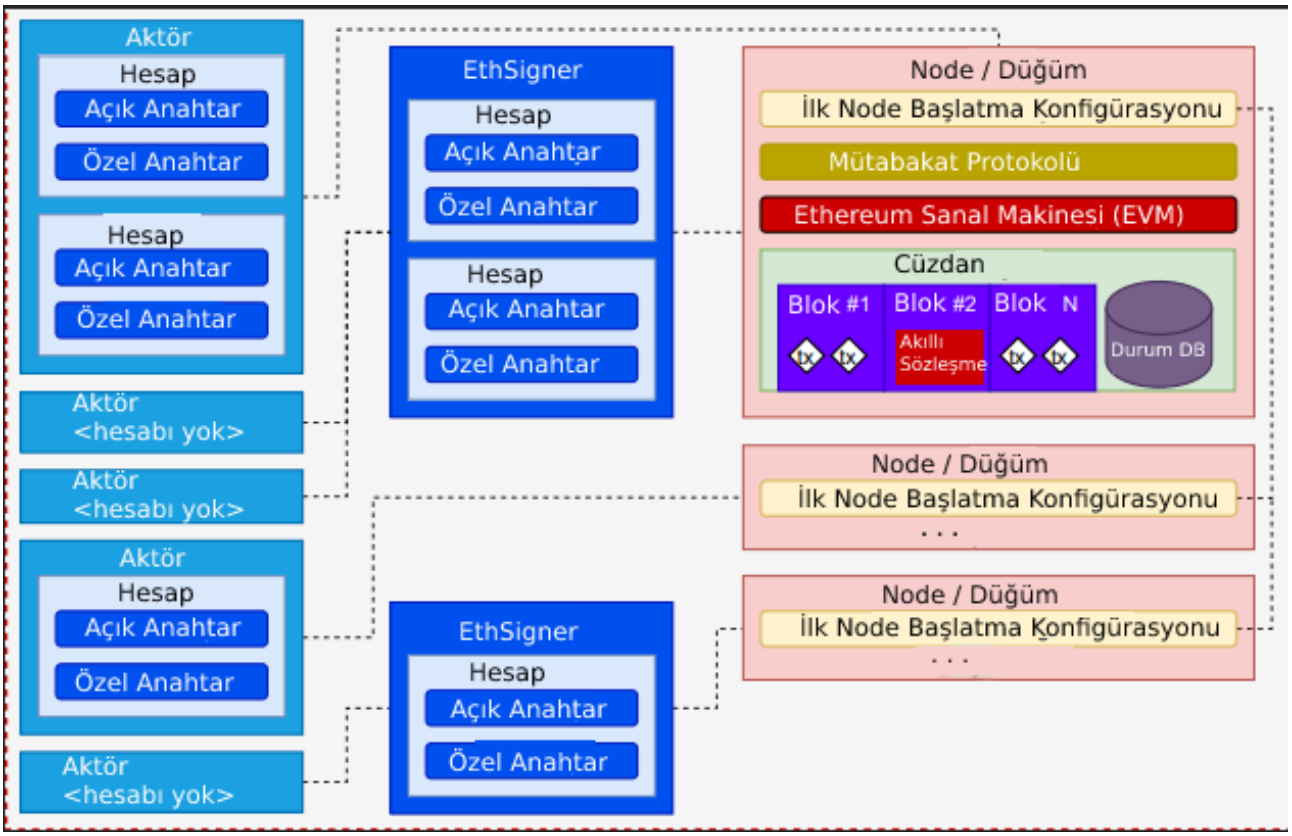
Özel ağ oluşturulacağı zaman, yapılandırma için bir akıllı sözleşmenin özel bir işlemde oluşturulması gerekir, bu özel işlemler ağa katılacak her düğüm tarafından tutulur, paylaşılır ve çalıştırılır. Her özel işlem için işlemin doğrulanmasını sağlayacak hash bilgisi ana blok zincire kaydedilir. HyperLedger Besu; QBFT, IBFT 2.0, Clique, PoS ve Ethash olmak üzere dört farklı mutabakat yöntemini destekler [31]. Hangi algoritmanın seçileceği minimum katılımcı sayısı, kayıt sıklığı gibi parametrelere bakılarak kararlaştırılmalıdır. HyperLedger Besu

mimarisi ve işlemlerin yapısı Şekil 3'te bulunmaktadır [32]. Mimaride görünen düğümler ağın altyapısını oluştururken hesaplar ağın içinde hareket eden varlıklardır.

Özelliklerine kısaca değinilen HyperLedger Besu'nun performans analizinin yapıldığı çalışmada, özellikle sistem yapılandırması ve zincir parametrelerinin performans metriklerine etkisine bakılmıştır [30].

ölçüsünü ifade eder. Bu ölçüm ağ veya düğüm boyutu arttığında verim ve gecikme ile belirtilir.

İlgili çalışmada HyperLedger Besu'nun performansını etkileyen en önemli faktörlerin yeni bir blok oluşturmak için gereken süre (blok süresi) ve blok boyutu gibi blok zinciri parametreleri olduğu ortaya çıkmıştır. Düğümün hesaplama gücü, işlemin karmaşıklığı (transaction complexity) ve yük dengeleme gibi parametreler



Şekil 3. HyperLedger Besu Mimarisi (Architecture of HyperLedger Besu)

İlgili çalışmada da değerlendirmeler için Hyperledger Caliper [33] kullanılmıştır ve performans metrikleri aşağıdaki gibidir;

- Verimlilik: Saniyedeki başarılı şekilde gerçekleştirilen işlem (transaction) sayısı (transactions per second (TPS)) veya saniyedeki sorgu işlemlerini ifade eder. İşlem sayısı ağ genelinde bakılır, sorgu sayısı ise bir düğümdeki TPS anlamına gelir.
- Gecikme: Bir işlemin etkisinin ağ genelinde kullanılabilir hale gelmesi için geçen süreyi ifade süreyi ifade eder, yayılma süresi ile mutabakat için gereken süreyi kapsar. Sorgu gecikmesi, okuma isteğinin gönderilmesi ile yanıtın alınması arasında geçen süredir.
- Kaynak tüketimi: Her bir düğümün harcadığı işlemci gücü (CPU) ve bellek (RAM) büyüklüklerini ifade eder.
- Ölçeklenebilirlik: Artan ağ katılımcılarını veya düğümlerin hesaplama kaynaklarını destekleme tarafından belirlenen işlem yürütme (transaction execution) ve blok zinciri durum güncellemelerinin HyperLedger Besu'nun performansını kötü etkilediği görülmüştür [30].

9. BLOK ZİNCİR TABANLI DDBS (BLOCKCHAİN BASED STATE AİD MONİTORİNG SYSTEM)

Önceki bölümde anlatılan DDBS'de karşılaşılan sorunları gidermek için önerilen model kamuda kullanılacağından erişim ve blok ekleme aşamalarında yetkilendirmeye ihtiyaç duyacaktır, bu da onun özel bir ağ (private blockchain) olacağını göstermektedir. Özel bir ağ kullanılacağı ve iş süreçlerinde yetkilendirilmeler farklı olacağı için Server-Client mimari tasarlanmıştır.

Platform olarak hem özel hem açık ağlarda kullanılabilen; HyperLedger Fabric [15], Ethereum ve R3 Corda [16] ile karşılaştırıldığında HeyperLedger Besu [34-35] kullanımının çok yönlü olması, gelişmiş gizlilik ve yüksek performans özelliklerine sahip olması sebepleriyle avantaj sahibidir [30]. Diğer taraftan HyperLedger Fabric ile HyperLedger Besu'nun farklı konfigürasyonlarla karşılaştırmasını HyperLedger Caliper [33] aracını kullanarak detaylı bir performans analiziyle yapan tez çalışmasında [32] farklı kriterlere göre sahip oldukları avantaj ve dezavantajlar görülmektedir. Bu çalışmada HyperLedger Besu'nun RocksDB'de [36] tutulan DLT'yi şifrelemek için eklenti sunması avantajı sebebiyle HyperLedger Besu kullanılacaktır. HyperLedger Fabric ile Hyper Ledger Besu'nun belirli özellikler için karşılaştırmaları Çizelge-1'de bulunmaktadır (kaynaktaki farklı tablolardan önemli görülenler birleştirilmiştir) [32].

Örnek bir senaryo şu şekildedir: Bir kurum, Client yazılımına kayıt için istek gönderir, sunucu bu isteği gerekli özetleme işlemlerinden sonra kurumlara dağıtarak kurumları mutabakat yapısına dâhil eder. Böylece gelen veri tüm kurumlara eşit olarak dağıtılmış olur. Daha sonra başka bir kayıt geldiğinde sunucu yeni kayıttaki faturanın numarasının özeti ile karşılaştırma için eriştiği düğümde bulunan verilerde aynı özete sahip fatura numarası varsa bu harcamanın daha önce yapıldığına dair uyarı gönderilir.

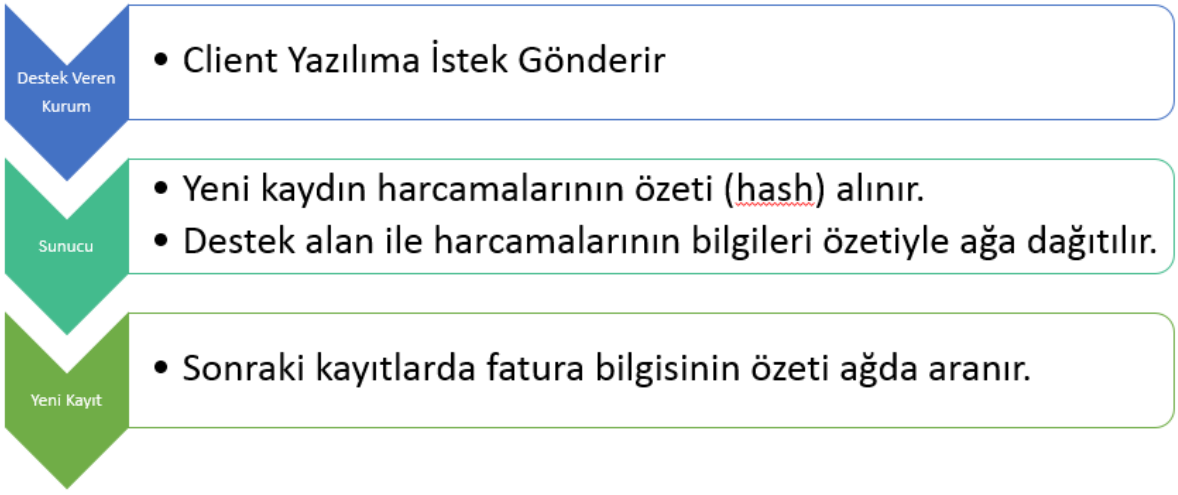
Önerilen modelin özellikleri aşağıda listelenmiştir:

- DDBS'de gönderim yapacak her kurumun ilgili birimi için ayrı kullanıcı vardır. Bu kullanıcıların gizli-açık anahtar ikilisi üretilerek ağda tutulacaktır.
- Gönderim yapılacağı zaman ilk adımda üretilen gizli anahtar kullanılarak imzalanacaktır.

Çizelge 1. HyperLedger Fabric ile HyperLedger Besu'nun Karşılaştırılması (Comparison of HyperLedger Fabric and HyperLedger Besu)

Özellik	HyperLedger Fabric	HyperLedger Besu
Ağ Yapısı	Heterojen (Farklı tipte düğümler olabilir)	Homojen (Tüm düğümler aynı tipte)
Düğüm konfigürasyonu	Yapılandırma için ileri uzmanlık gerekebilir.	İleri uzmanlık gerekmez, çoğunlukla izinler ve hangi Api'nin etkinleştirileceği seçilir.
Düğüm İzin Yönetimi	Kanalların organizasyonlarından türetilen dijital kimliklerle izinli listesi (white-list) tanımlanır.	Kullanıcılar kullanıcı adı-şifre ile izinlendirilebilir. Ayrıca İşlem gönderebilecek hesaplara göre, ağda bağlı olduğu düğümlere göre izinlendirilebilir.
Depolama Motorları (Storage Engines)	CouchDB/LevelDB	RocksDB, özel yapılandırma ile diğerleri eklenebilir.
Şifreli Depolama Alanları	Dosya sistemi şifrelemesi	RocksDB için şifreli depolama alanı eklentisi ve dosya sistemi şifrelemesi.
Geçmiş Durumların Okunması (World State)	Desteklenmiyor, işlemlerin takibi ile çıkartılabilir ancak uzun zaman alır.	Arşiv düğüm varsa doğrudan okunabilir ancak yoksa işlem geçmişinde yeniden yapılandırma gerekir.
Akıllı Sözleşme Dilleri	Genel amaçlı programlama dilleri (Golang, Java, Node.js)	Solidity, Vyper, Yul, Yul+

Gönderim işlemlerinde açık-gizli anahta ikilisi kullanılarak kimlik doğrulama yapılabilir. DDBS modelinde özet veriler üzerinden karşılaştırma yapıldığı için ticari sır paylaşımı endişesi giderilecektir ve aynı harcama için birden fazla yerden destek alımının önüne geçilecektir. Kullanım senaryosunun akışı Şekil 4'te gösterilmiştir.



Şekil 4. Blok zincir tabanlı DDBS Akış Şeması (Flowchart Of The Blockchain Based State Aid Monitoring System)

- Her kurumun ağa eklediği veriyi sadece kendisi ve DDBS yöneticileri görebilecektir. Ağ üzerinde tutulan verilerin özeti alınıp tutulursa sunucu özetten veriye dönüşüm yapamayacağı için raporlama yapamayacaktır. Bunun yerine şifreli bir şekilde tutulacaktır. Daha hızlı karşılaştırma yapılabilmesi için fatura tekil numarasının özeti tutulacaktır.
- Farklı kurumlardan gelen bloklardaki fatura tekil numarasının karşılaştırılması yapılacak böylece destekten mükerrer yararlanmanın önüne geçilecektir. Bu kısım için akıllı sözleşmeler ile ekleme esnasında düğümde bulunan verilerle karşılaştırma yapılıp, daha önce eklenmişse uyarı yapılabilecektir.

Yukarıda özellikleri belirtilen modelin yapısı Şekil 5'te gösterilmiştir. Burada gösterim kolaylığı olması için tüm destek veren kurumlara yer verilmemiştir.

Şekil 5'te önerilen modelde server-client mimari ile blok zincir altyapısının birlikte işleyebileceği bir yapı tasarlanmıştır. Bununla birlikte HyperLedger Besu başlangıç konfigürasyonunda hangi düğümlerin hangi izinlere sahip olacağı düzenlemesine izin veren esnek bir yapıya sahiptir. Bu nedenle sonraki evrelerde model, şekilde görünen sunucu tamamen kaldırılarak ve DDBS yönetimini yapan kurum ağa bir düğüm olarak katılarak güncelleştirilebilir. Modelde HyperLedger Besu'nun sağladığı blok zincirin mimari yapısının detayları ise Şekil 6'da bulunmaktadır. Burada JSON RPC, bir yazılımın HyperLedger Besu ile iletişim kurmasının Json veri formatı ile sağlandığı protokoldür. Graph QL ise API'ler üzerinde sorgu yapmaya olanak sağlayan, Facebook tarafından geliştirilen ve açık kaynak olarak açılan bir sorgulama dilidir [37].

HyperLedger Besu'nun yapılandırma aşamasında her düğümün hangi izinlere sahip olacağı ve kimlerin işlemdeki verileri hangi izinlerle görebileceği belirlenebilir. Başka kurumlar tarafından geliştirilen uygulamaların verilerini yalnızca izlemek isteyen kurumlar HyperLedger Besu altyapısının sağladığı bu avantajdan faydalanabilir. İlgili kurum başka herhangi bir ek sunucu maliyetine katlanmadan ağa düğüm olarak eklenip ağdaki verileri izleyebilir. Özellikle denetleyici düzenleyici kurumlar tarafından, piyasa izleme gibi işlevler için kullanılabilecek blok zincir altyapısıyla geliştirilecek bu uygulamaların etkinliği arttıracağı ve maliyeti düşüreceği

Eth Signer, Ethereum istemciler tarafından işlemleri (transaction) imzalayıp ağa göndermek için kullanılan araçtır [38]. Tessera ise Apache 2.0 lisansı altında geliştirilmiş ve Java dili ile geliştirilmiş, açık kaynaklı bir özel işlem yöneticisidir (private transaction manager) [39]. HyperLedger Besu içinde bu ihtiyaç için daha önce Orion [40] kullanılırken artık Tessera kullanılmaktadır.

Evm Ethereum'un sağladığı sanal makineyi ifade etmektedir. Ethereum altyapısında çalışan akıllı sözleşmelerin içindeki olaylar (events), kod içinde tanımlandıktan sonra, belirlenen şartlara bağlı olarak tetiklenecekleri yerler ilgili koşul içinde belirtilir. Akıllı sözleşme ağa dağıtıldıktan sonra tetikleme gerçekleştiğinde işlemin loglarında (transaction logs) olay tanımında bulunan değerler görüntülenebilir. Solidity dilinde örnek bir olay oluşturma ve onun tetiklenmesi aşağıdaki gibidir [41].

```
event OlayAdi(uint a);
emit OlayAdi(10);
```

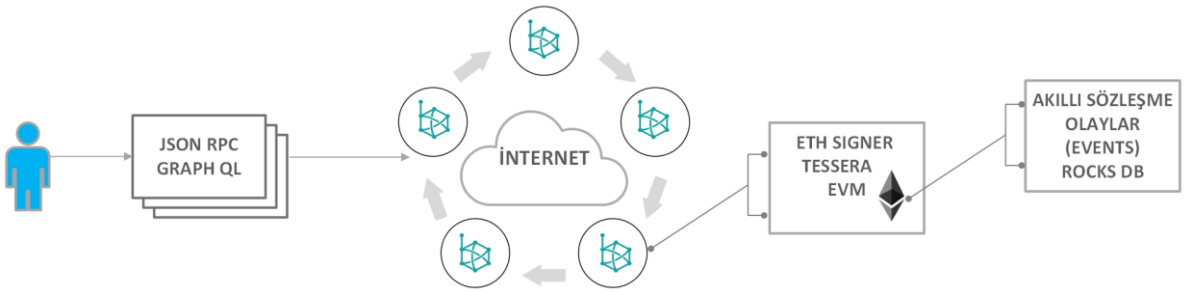
değerlendirilmektedir. Kamu kurumlarında blok zincir altyapısında modellerin uygulamaya geçirilmesi için kurumların teknoloji hakkında bilgilendirilmelerine, gerekli insan kaynağını sağlamak için eğitimlerin

Şekil 5. Önerilen modelin yapısı (Structure Of The Model)

verilmesine ve ilgili üst kuruluşlar tarafından test ortamlarının kurulmasına ihtiyaç bulunmaktadır. Bununla birlikte her projenin blok zincir altyapısına geçirilmesi gibi bir algının oluşması doğru değildir, var olan teknolojiler incelendikten sonra mevcut projelerdeki problemleri giderebileceği görülüyorsa uygun altyapı seçilerek test ve canlı ortamlarda sistemler tasarlanmalıdır.

Bu çalışmada, devlet desteğinden yararlanan firmanın mükerrer destek almasının önüne geçilebilmesi için blok zincir tabanlı bir model önerilmiştir. Bu yapı ile hem kurumların güvenlik endişesiyle veri gönderimindeki çekinceleri giderilmiş olacak hem de kötüye kullanımın önüne geçilerek daha etkin bir destek izlemesi sağlanacaktır bu da yöneticilerin daha doğru kararlar almasına yardımcı olacaktır.

Gelecek çalışmalarda, önerilen model uygulamaya geçirilebilir, uygulamaya geçirilirken farklı platformlar kullanılarak performans değerlendirmesi yapılarak zenginleştirilebilir.



Şekil 6. Modelin Mimari Yapısı (Architecture Of The Model)

10. SONUÇ (CONLUSIONS)

Finansal ödeme sistemleri ile tanınan blok zincir teknolojisinin çok farklı alanlarda yenilik getireceği düşünülmektedir. Özellikle her türlü belgenin etkin, daha düşük maliyetle, güvenilir ve esnek bir yapıda tutulmasına olanak verdiği için bu teknoloji önem arz etmektedir. Kamunun sadece ödeme sistemleri bakış açısıyla değil, doküman yönetimi ve benzeri alanlarda da blok zincir teknolojisini tanımasının faydalı olacağı açıktır.

ETİK STANDARTLARIN BEYANI (DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazarları çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

Kevser AÇIKALIN: Verilerin toplanması, uygulama ve yazım.

İsmail ŞAHİN: Makale konseptinin belirlenmesi ve sonuçların doğrulanması.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur.

KAYNAKLAR (REFERENCES)

[1] A. Usta , S. DOĞANTEKİN "BlockChain 101 v2," ***BKM*** , Türkiye, 2019.

[2] N. Szabo , "Smart Contracts: Building Blocks for Digital Markets",1996, (Erişim 30 Ocak 2020).

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009, (Erişim 30 Ocak 2020).

[4] S.T. Bartkewitz , R.U. Bochum, "Building Hash Functions from Block Ciphers, Their Security and Implementation Properties",2009.

[5] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," ***Advances in Cryptology CRYPTO '87***, Santa Barbara 369-378, 16-20 Ağustos 1987.

[6] W. Diffie and M. Hellman, "New directions in cryptography," (in en), ***IEEE Transactions on Information Theory***, 22(6), 644-654,1976.

[7] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," in ***IEEE Wireless Communications***, vol. 11, no. 1, pp. 62-67, Feb. 2004, doi: 10.1109/MWC.2004.1269719.

[8] R. L. Rivest, A. Shamir, ve L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", **Commun. ACM**, c. 26, sy 1, ss. 96-99, Oca. 1983, doi: 10.1145/357980.358017.

[9] Bitcoin Wiki https://en.bitcoinwiki.org/wiki/Block, (Erişim 30 Ocak 2020).

[10] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," ***Int. J. Web and Grid Services***, 14(4), 352-375, (2018).

[11] Geth documents, "Welcome to go-ethereum", go-ethereum. https://geth.ethereum.org/docs (Erişim 01 Ocak 2023).

[12] "Truffle Documentation - Truffle Suite". https://trufflesuite.com/docs/ (Erişim 01 Ocak 2023).

[13] "Besu Ethereum Client". Hyperledger, "https://github.com/hyperledger/besu", (Erişim 3 Ocak 2020).

[14] Getting Started With MultiChain: "https://www.multichain.com/getting-started/", (Erişim 30 Ocak 2020)

[15] WG. Hyperledger, "Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf" . Erişim: 01 Ocak 2023. Erişim adresi: https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf

[16] "R3 Documentation", R3 Documentation. https://docs.r3.com/ (Erişim 01 Ocak 2023).

[17] "EEA Community Projects", GitHub. https://github.com/eea-oasis (Erişim 01 Ocak 2023).

[18] "EOSIO", GitHub. https://github.com/EOSIO (Erişim 01 Ocak 2023).

[19] E. Foundation, On Public and Private Blockchains, https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains, (Erişim 30 Ocak 2020)

[20] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.", 2014.

[21] D. V. Bowen , G. P. Johnston, "The benefits of electronic records management systems: a general review of published and some unpublished cases," **Records Management Journal**, 15(3), 131-140, 2005

[22] J.S.Rivera, A.V. Zemanate, C. Cobos, J. A. C. Lopez, T. Velasco, "Document Management System Based on a Private Blockchain for the Support of the Judicial Embargoes Process in Colombia, ***Advanced Information Systems Engineering Workshops,*** Tallin, Estonya, 126-137,11-15 Ocak, 2018

[23] Filecoin, https://filecoin.io/, (Erişim, 30 Ocak 2020)

[24] MaidSafe https://maidsafe.net , (Erişim, 30 Ocak 2020)

[25] Babu, B.S.; Krishnan, M.N.; Vajha, M.; Ramkumar, V.; Sasidharan, B.; Kumar, P.V. Erasure coding for distributed storage. an overview. Sci**.** ***China Inf. Sci.*** 2018, 61, 1–45.

[26] O. Hammoud, I. Tarkhanov, ve A. Kosmarski, "An Architecture for Distributed Electronic Documents Storage in Decentralized Blockchain B2B Applications", **Computers**, Kas. 2021, doi:10.3390/computers10110142.

[27] Avrupa Birliği Antlaşması ve Avrupa Birliği'nin işleyişi hakkında antlaşma. https://www.ab.gov.tr/files/pub/antlasmalar.pdf, (Erişim, 30 Ocak 2020)

[28] 6015 Sayılı Kanun http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6015.pdf, (Erişim, 30 Ocak 2020)

[29] Devlet Destekleri Bilgi Sistemine Veri Aktarılması Hakkında Yönetmelik. Mevzuat Bilgi Sistemi: http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.19724&MevzuatIliski=0&sourceXmlSearch=Devlet%20Destekleri, (Erişim, 30 Ocak 2020)

[30] C. Fan, C. Lin, H. Khazaei, ve P. Musilek, "Performance Analysis of Hyperledger Besu in Private Blockchain", içinde ***2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS)***, Ağu. 2022, ss. 64-73.

[31] "Consensus protocols - Hyperledger Besu". https://besu.hyperledger.org/en/stable/private-networks/how-to/configure/consensus/ (Erişim 05 Ocak 2023).

[32] M. Soelman, "Permissioned Blockchains: A Comparative Study A Deep Dive into Hyperledger Fabric and Hyperledger Besu", University of Groningen, **Master** of Science in Computer Science, 2021.

[33] "Hyperledger Caliper", Hyperledger Caliper. https://hyperledger.github.io/caliper/ (Erişim 04 Ocak 2023).

[34] G. Hartley, "Hyperledger Besu: An Overview", ConsenSys, 2020.

[35] R. Dawson, PegaSys, M. Baxter, ve PegaSys, "Announcing Hyperledger Besu – Hyperledger Foundation". https://www.hyperledger.org/blog/2019/08/29/announcing-hyperledger-besu (Erişim 03 Ocak 2023).

[36] S. Dong, A. Kryczka, Y. Jin, ve M. Stumm, "RocksDB: Evolution of Development Priorities in a Key-value Store Serving Large-scale Applications", ***ACM Trans. Storage***, c. 17, sy 4, s. 26:1-26:32, Eki. 2021.

[37] "GraphQL | A query language for your API". https://graphql.org/ (Erişim 09 Ocak 2023)

[38] ConsenSys, "Install binary distribution - EthSigner - latest". https://consensys.net/docs/ethsigner/en/latest/HowTo/Get-Started/Install-Binaries/ (Erişim 09 Ocak 2023).

[39] "Tessera Private Transaction Manager". https://docs.tessera.consensys.net/en/stable/ (Erişim 09 Ocak 2023).

[40] ConsenSys, "Orion". ConsenSys, 08 Eylül 2022. Erişim: 09 Ocak 2023, Erişim adresi: https://github.com/ConsenSys/orion/blob/0c000637da565f16fbc8632467933d55c9e6e401/CHANGELOG.md

[41] "Contract ABI Specification — Solidity 0.8.4 documentation". https://docs.soliditylang.org/en/v0.8.4/abi-spec.html#events (Erişim 13 Ocak 2023).