Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 29, S. 36-45, Aralık 2021

Derleme Makale

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 29, pp. 36-45, December 2021

Review Article

Dağıtık Defter Teknolojileri ve Uygulama Alanları Üzerine Bir İnceleme

Emre Şafak[1*], Çağlar Arslan[2], Mesut Gözütok[3], Tacettin Köprülü[4]

[1] HAVELSAN A.Ş., ARGE TEKNOLOJİ VE ÜRÜN YÖNETİMİ BÖLÜMÜ, Ankara, Türkiye (ORCID: 0000-0001-7579-3410)
[2] HAVELSAN A.Ş., ARGE TEKNOLOJİ VE ÜRÜN YÖNETİMİ BÖLÜMÜ, Ankara, Türkiye (ORCID: 0000-0003-1856-9329)
[3] HAVELSAN A.Ş., ARGE TEKNOLOJİ VE ÜRÜN YÖNETİMİ BÖLÜMÜ, Ankara, Türkiye (ORCID: 0000-0002-5919-1951)
[4] HAVELSAN A.Ş., ARGE TEKNOLOJİ VE ÜRÜN YÖNETİMİ BÖLÜMÜ, Ankara, Türkiye (ORCID: 0000-0003-4395-6064)

(International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) 2021 – 21-23 October 2021)

(**DOI:** 10.31590/ejosat.1011289)

ATIF/REFERENCE: Şafak, E., Arslan, Ç., Gözütok M., Köprülü T. (2021). Dağıtık Defter Teknolojileri ve Uygulama Alanları Üzerine Bir İnceleme. *Avrupa Bilim ve Teknoloji Dergisi*, (29), 36-45.

Öz

Dağıtık defter teknolojisi verilerin dağıtık olarak saklandığı ve yönetildiği yeni bir yaklaşım sunmaktadır. Mevcut merkezi sistemler güvenlik, güvenilirlik ve kesintisiz çalışma konusunda sorunludur. Verilerin tek bir noktada tutulması sunucuların siber saldırılara açık bir merkez haline getirilmesine neden olmaktadır. Bunun yanında merkezi sunucuların yöneticileri veya saldırganlar verileri manipüle edebilmektedir. İnternete bağlı cihazların sayısının artmasıyla merkezi sunucuların tüm istekleri karşılayabilmesi giderek zorlaşmaktadır. Tüm bu problemleri gidermek için dağıtık defter teknolojisinin kullanıldığı çalışmalar artmaktadır. Dağıtık defter teknolojisinde veriler dağıtık olarak tutulduğu için tek bir saldırı noktası oluşmamakta ve veriler hiçbir katılımcı tarafından değiştirilememektedir. Katılımcılar birbirleri arasında merkezi bir sunucu olmadan aracısız işlem yapabileceği için işlem yoğunluğu ne kadar fazla olursa olsun sistem kesintisiz olarak çalışabilmektedir. Dağıtık defter teknolojisinin teknik olarak açıklandığı ilk makale 1991 yılında yayımlanmıştır. İlk yaygın kullanımı 2008 yılında ortaya çıkan Bitcoin kripto parasıdır. Bitcoin, küresel finans sisteminin çöktüğü 2008 yılında Satoshi Nakamoto tarafından geliştirilen aracısız ve güvenli ödeme sistemidir. Bitcoin kripto parasının popüler hale gelmesi ile birlikte arkasındaki dağıtık defter teknolojisi olan blok zinciri ile ilgili farklı sektörlere yönelik çalışmalar yapılmaya başlanmıştır. Yapılan çalışmalarda blok zinciri teknolojisinin hız ve ölçeklenebilirlik açısında yeterli olmadığının görülmesi nedeniyle Hashgraph, Tangle, Holochain ve Tempo dağıtık defter teknolojileri geliştirilmiştir. Bu makalede mevcut dağıtık defter teknolojileri ile savunma, siber güvenlik, sigorta, tedarik zinciri, dijital hak yönetimi, sağlık, enerji ve finans alanlarında nasıl kullanılabileceği açıklanmıştır.

Anahtar Kelimeler: Dağıtık Defter Teknolojisi, Blok Zinciri, Hashgraph, Tangle, Holochain, Tempo, Dağıtık Defter Teknolojileri Uygulamaları, Savunma, Siber Güvenlik, Tedarik Zinciri, Dijital Hak Yönetimi, Sağlık, Enerji, Finans

A Survey of Distributed Ledger Technologies and Application Areas

Abstract

Distributed ledger technology offers a new approach in which data is stored and managed in distributed. Centralized systems are problem in terms of security, reliability and uninterrupted operation. Data keeping in single point causes center servers to become open to cyber attacks. In addition administrators of central servers or attackers can manipulate data. With the increase in the number of devices connected to the Internet, it is increasingly difficult for central servers to answer all requests. In order to solve all these problems, studies using distributed ledger technology are increasing. Distributed ledger technology, there is no single point of failure because the data is kept in a distributed and data can't be changed by any participant. The system can operate uninterruptedly, no matter how high the transaction density as the participants can transact between each other without a central server. The first article describing the distributed ledger technology technically was published in 1991. The first widespread use is Bitcoin, which emerged in 2008. Bitcoin is without intermediary and secure payment system developed by Satoshi Nakamoto in 2008, when the global financial system collapsed. The popularization of Bitcoin cryptocurrency, studies on different sectors related to blockchain which is distributed ledger technology behind it have began. Blockchain technology due to the fact that is not sufficient in terms of speed and scalability, Hashgraph, Tangle, Holochain and Tempo distributed ledger technologies have been developed. In this article explains with existing distributed ledger technologies and defence, cybersecurity, insurance, supply chain, digital rights management, healthcare, energy and finance application areas.

Keywords: Distributed Ledger Technology, Blockchain, Hashgraph, Tangle, Holochain, Distributed Ledger Technlogy Applications, Defence, Cyber Security, Supply Chain, Digital Right Management, Health, Energy, Finance

[*] Sorumlu Yazar: HAVELSAN A.Ş., ARGE TEKNOLOJİ VE ÜRÜN YÖNETİMİ BÖLÜMÜ, Ankara, Türkiye, ORCID: 0000-0001-7579-3410, esafak@havelsan.com.tr

1. Giriş

Dağıtık defter teknolojisi ilk olarak 1991 yılında Stuart Haber ve W. Scott Stornetta tarafından yayımlanan "How to time-stamp a digital document" makalede açıklanmıştır (Haber ve Stornetta, 1991). Dağıtık defter teknolojisinin aşağıdaki yer alan sorunları çözebilme potansiyeline sahip olduğu için giderek önemli hale gelmektedir (Antal, Cioara, Anghel, Antal ve Salomie, 2021).

- Güvenilirliğini kaybeden merkezi otoriteler olmadan işlem yapılamamaktadır.
- Aracısız işlem yapılamamaktadır.
- Veritabanı yöneticileri veya siber saldırganlar merkezi verileri manipüle edebilmektedir.
- Anonim işlem yapılamamaktadır.
- Kullanıcılar verileri üzerinde tam kontrol sahibi değildir.
- Endüstri 4.0 ile milyarca cihazın işlem ağına katılması ile mevcut yöntemlerin işlem kapasiteleri aşılmaktadır.

Dağıtık defter teknolojisi birden çok düğüm ve birden çok katılımcı tarafından yönetilen merkezi olmayan bir veritabanıdır (Antal vd., 2021). Dağıtık defter teknolojisinde eşler arası ağ olmalı, katılımcılar bulunmalı, konsensüs mekanizmaları kullanılmalı ve değiştirilemezlik sağlanmalıdır (Kannengießer, Lins, Dehling ve Sunyaev, 2020). Eşler arası ağ, ağda bulunan taraflar merkezi bir otoriteye gerek kalmadan aracısız işlem yapabilmektedir. Merkezi sunucuların maruz kaldığı DDoS (Distributed Denial-of-Service) saldırılarının engellenmesi sağlanabilir. Katılımcılar, ağdaki işlemleri kaydeden, doğrulayan, paylaşan ve senkronize eden bilgisayarlardır. Konsensüs mekanizmaları, dağıtık defter teknolojisinde ağa veri ekleyen bir merkezi otorite olmadığı için veri ekleme için bir uzlaşma algoritması kullanılması gereklidir. Bu sayede ağdaki kötü niyetli kişilerin ağı bozma çabaları engellenmektedir. Değiştirilemezlik, dağıtık defter teknolojisine kaydedilen verilerin hiçbir katılımcı tarafından değiştirilemesidir. Dağıtık defter teknolojisinde iki genel sistem tasarımı vardır; herkese açık veya izinli dağıtık defterler. Herkese açık dağıtık defterler herkesin erişimine açık olarak tasarlanmıştır. Son kullanıcılar izinsiz olarak ağa katılabilir, ağı doğrulayabilir veya ağdan ayrılabilmektedir. İzinli defterler, genellikle belirli bir kullanıcı grubu için tasarlanırlar. Ağın fikir birliğine varmasında önceden belirlenen katılımcı grubu sorumludur. İzin verilen son kullanıcılar ağa katılabilir, ağı doğrulayabilir veya ağdan ayrılabilmektedir (Antal vd., 2021).

Lamport vd. (1982) tarafından yayımlanan Byzantine Generals Problem başlıklı makale ile mevcut durumda merkezi bir otorite olmadan taraflar arasında güvenin nasıl sağlanamadığı bir şehri kuşatan bizans generalleri üzerinden açıklanmıştır. Bizans generalleri problemi makalesinde şehri ele geçirmeye çalışan generaller arasında hainlerin bulunması durumunda şehre saldırmada zaferi garantileyen güvensiz bir sistemin nasıl geliştirilebileceği açıklanmaktadır. Bu problem dağıtık defter teknolojisinin geliştirilmesi için ilk gelişme olarak kabul edilebilir (Lamport, Shostak ve Pease, 1982).

Haber ve Stornetta (1991) tarfından yayımlanan How to time-stamp a digital document başlıklı makalede dijital belgelerde zaman damgasının nasıl gerçekleştirilebileceği açıklanmıştır. Dijital belgelerin zaman damgası ile imzalanmasındaki amaç belgenin oluşturulma veya değiştirilme tarihçesinin doğru bir şekilde takip edilebilmesini sağlamaktır. Güvenilir zaman damgası servisi için dağıtık defter teknolojilerinin temelini oluşturan hash ve dijital imza teknolojisi önerilmiştir. Hash fonksiyonu girdi olarak verilen farklı uzunluktaki anahtarın sabit uzunlukta bir çıktı vermesini sağlayan tek yönlü şifeleme yapılmasını sağlar. Bu sayede belgenin bütünlüğü sağlanmaktadır. Dijital imza ile ise işlemi yapan taraf ve onay tarihi ile dijital belgeye eklenmektedir (Haber ve Stornetta, 1991).

Mazieres ve Shasha (2002) tarafından yayımlanan makalede güvenilir olmayan bir sunucuda güvenilir bir ağ dosya sisteminin nasıl uygulanacağı açıklanmıştır. Önerilen yöntemde sunucu yalnızca bir kullanıcının diğerinin yaptığı tek bir değişikliği bile görmesini geciktirirse iki kullanıcı bir daha asla birbirinin değişikliklerini görmez. Bu sayede olası herhangi bir kurcalamanın engellenmesi amaçlanmaktadır (Mazières ve Shasha, 2002).

Nakamoto (2008) tarafından yayımlanan makalede herhangi bir merkezi otorite olmadan taraflar arasında düşük maliyetli ödeme yapılmasını sağlayan Bitcoin açıklanmıştır. Ardından kullanıcıların bu sistemi ticaret için kullanmaya başlamasıyla kripto para olarak kabul görmüştür. Bitcoin blok zinciri olarak adlandırılarak dağıtık defter teknolojisi türünün temelini oluşturmuştur. Bitcoin sisteminde veriler dağıtık olarak doğrulayıcı katılımcılarda bloklar içerisinde saklanmaktadır. Ağa veri ekleme işlemi doğrulayıcı düğüm olarak adlandırılan madenciler tarafından yapılmaktadır. Madenciler hash bulma problemini güçlü makineler ile çözmeye çalışır ve bu problemi ilk çözen madenci bloğu ağa ekler. Bu yöntem Proof of Work uzlaşma mekanizması olarak adlandırılmaktadır (Nakamoto, 2008).

Buterik tarafından 2013 yılında yayımlanan makalede Ethereum blok zinciri altyapısı ve kripto parası tanımlanmıştır. Ethereum, herkesin blok zinciri teknolojisinde çalışan merkezi olmayan uygulamaları oluşturmasına ve kullanmasına izin veren açık kaynak blok zinciri platformudur. Ethereum blok zinciri akıllı sözleşmeleri desteklemektedir. Akıllı sözleşmeler, geliştiricilerin blok zinciri ağında işbirliği yapan farklı kuruluşlar arasında temel iş süreçlerini yürütmesini ve varlıkların tanımlamasına izin veren programlardır. Ethereum ile ortaya çıkan akıllı sözleşmeler sayesinde blok zinciri teknolojisinin ilk kez farklı alanlarda kullanılabilmesi sağlanmıştır. İşlemler ağdaki madenciler tarafından blok zinciri ağına eklenmektedir ve uzlaşma algoritması olarak Proof of Work konsensüs algoritması kullanılmaktadır (Buterik, 2013).

Arslan vd. (2020) tarafından yapılan çalışmada nesnelerin interneti cihazlarında güvenliği ve gizliliği sağlayabilmek için geleneksel merkezi yaklaşımların yeterli olmadığı ifade edilmektedir. Bu nedenle güvenli, özerk ve güvenilir nesnelerin interneti platformu oluşturabilmek için dağıtık defter teknolojisinin kullanılması önerilmektedir. Dağıtık defter teknolojisi ile oluşturulan nesnelerin interneti platformu güvenlik, gizlilik ve merkezi olmayan çalışma sağlama potansiyeline sahiptir (Arslan, Jurdak, Jelitto, ve Krishnamachari, 2020).

Pandl vd. (2020) tarafından yapılan çalışmada yapay zeka ve dağıtık defter teknolojisinin birlikte kullanılması önerilmektedir.

Yapay zeka teknolojisi dağıtık defter teknolojisinin güvenliğini artırmak, akıllı sözleşmeleri iyileştirmek, gizliliği korumak ve sistemi daha otonom hale getirebilmek için kullanılabileceği belirtilmektedir. Yapay zeka ağdaki işlemleri sürekli izleyerek olası saldırıların gerçekleşmeden öngörülebilmesini sağlar. Bunun yanında özellikle herkese açık dağıtık defter teknolojilerinde madencilik işleminde çoğunluğun ele geçirelebilmesini önlemek için yapay zeka faydalı olacaktır. Kullanıcıların kötü niyetli akıllı sözleşemelerden korunması ve bu sözleşmelerin analiz edilmesi yapay zeka teknolojisi kullanılarak sağlanabilir. Yapay zeka dağıtık defter teknolojisinde kayıt ve doğrulama işlemlerini yerel bilgisayarlardan yapılmasını sağlayarak kişisel gizliliğin korunmasını sağlayabilir. Bu çalışma ile yapay zeka ve dağıtık defter teknolojisinin kaynaşması ile çok daha güçlü sistemlerin tasarlanması sağlanarak kullanım alanları artırılabilir (Pandl, Thiebes, Schmidt-Kraepelin ve Sunyaev, 2020).

Yapılan çalışmada ilk olarak dağıtık defter türleri açıklanmış ardından uygulama alanlarında bahsedilmiş ve son olarak sonuçlar tespit edilmiştir.

2. Dağıtık Defter Türleri

2.1. Blok Zinciri

Blok zinciri verilerin bloklar içerisinde tutulduğu ve her bir bloğun kendinden önceki bloğun hash bilgisini tuttuğu dağıtık defter teknolojisidir. Her bir blok başlık ve veri olmak üzere iki temel kısımdan oluşur. Başlık kısmında blok zincirinin içerisindeki verilerin kriptografik hash bilgisi ve kendinden önceki bloğun hash bilgisini tutulmaktadır. Bu sayede zincir şeklinde bir veri yapısı oluşmaktadır (Cagigas, Clifton, Diaz-Fuentes ve Fernández-Gutiérrez, 2021). Bloktaki verilerin hash bilgisinin hesaplanabilmesi için Merkle Ağacı yöntemi kullanılmaktadır. Merkle Ağacı yöntemi ile ilk olarak bloklarda yer alan işlemlerin hash bilgileri alınır. Ardından işlemlerin hash verilerine hash işlemi tekrar uygulanarak ara hash verileri elde edilir. Son katmanda ara düğümlerin hash bilgileri alınarak kök hash verisi elde edilmektedir. Blok zinciri teknolojisinden hash işlemi için SHA 256 algoritması kullanılmaktadır (Chen, Chou ve Chou, 2019). Katılımcılar blok zinciri ağına mesaj gönderirken asimetrik şifreleme ve dijital imza teknolojisini kullanırlar. Asimetrik şifrelemede şifreleyen ve çözen anahtar bilgileri farklıdır. Bir anahtar herkese açık diğeri sadece kullanıcıda bulunan anahtar çiftidir. Açık anahtar ile şifrelenmiş bir veri ancak ilgili özel anahtar ile çözümlenebilmektedir. Açık anahtardan özel anahtara ulaşmak çok yüksek hesaplama gücü gerektiğinden neredeyse imkansızdır (Qadir ve Varol, 2019). Dijital imza teknolojisi ile verinin bütünlüğünün bozulmadığının kontrolü yapılmaktadır. Gönderici mesajın hash bilgisini kendi özel anahtarı ile şifreler ve alıcı göndericinin açık anahtarı ile şifreyi açarak verinin bütünlüğünü kontrol etmektedir (Singh, Iqbal, ve Jaiswal, 2015). Blokların veri kısmında ise katılımcılar tarafından yapılan işlemler tutulmaktadır. Blokların kendinden önceki blokların hash bilgilerini tutması sayesinde bir bloktaki veri değiştirilirse sonrasındaki blokların da değiştirilmesi gerekeceği için blok sayısı arttıkça önceki blokların güvenliği sürekli olarak artmaktadır. Blokların yer aldığı zincir dağıtık olarak katılımcılarda yer almaktadır. Veriler bir blok zincirine işlendikten sonra kalıcıdır ve manipüle edilmesi neredeyse imkansızdır. Blok zinciri ağında bir kullanıcı bir işlem talep ettiğinde, bu işlemin detayları eşler arası bir şekilde tüm bu düğümlere yayınlanır. Her düğüm daha sonra işlemin geçerli olduğunu doğrular ve işlemin onaylanması için belirlenen konsensüs algoritması ile blok ağa eklenir (Wamba, Kamdjoug, Bawack ve Keogh, 2020). Blok zincirinde Proof of Work, Proof of Stake ve Practical Byzantine Fault Tolerance (PBFT) konsensüs algoritmaları kullanılmaktadır. Proof of Work konsensüs algoritmasında veriler ağa eklenmeden önce madenciler tarafından bir hash problemi çözülür ve ilk çözen madenci bloğu ağa ekler. Bu yöntemin dezavantajı oldukça fazla enerji tüketimine neden olmaktadır. Proof of Stake konsensüs algoritmasında blokları ağa ekleyecek madenci sahip olduğu kripto varlığa göre belirlenir. En fazla kripto paraya sahip madenci bloğu ağa ekleyebilmektedir. PBFT konsensüs algoritmasında ise iki aşamalı doğrulama vardır. İlk aşamada belirlenen kullanıcılar tarafından bloğun onaylanması gerekir. İkinci aşamada ağdaki tüm doğrulayıcı katılımcıların onayı gerekmektedir. Geliştirilen blok zinciri uygulamalarında bu algoritmalar aynen veya revize edilerek kullanılabilir (Bach, Mihaljevic, ve Zagar, 2018). Blok zinciri uygulamaları geliştirmek için Ethereum, Hyperledger ve Corda gibi altyapılar yaygın kullanıma sahiptir. Ethereum işlemleri doğrulmak ve kaydetmek için uygulamalar geliştirilmesini sağlayan açık kaynak blok zinciri uygulama geliştirme platformudur. Ether kripto parasına sahiptir. Ethereum akıllı sözleşmleri desteklemektedir. Akıllı sözleşmeler geliştirmek için Solidity dili kullanılmaktadır. Ethereum akıllı sözleşmleri Ethereum Sanal Makinesi üzerinde çalışmaktadır. Her gerçekleşen işlem için ücret ödenmesi üzerine kurgulanmıştır. Ethereum 2.0 ile konsensüs algoritması olarak Proof of Stake kullanılmaktadır. Hyperledger kurumsal blok zinciri uygulama geliştirmek için kullanılan açık kaynak blok zinciri uygulama geliştirme altyapısıdır. Linux topluluğu tarafından geliştirilmektedir. PBFT konsensüs algoritmasını kullanmaktadır. Hyperledger'ın kripto parası bulunmamaktadır. Hyperledger Fabric, Hayperledger Iroha ve Hyperledger Sawtooth en bilinen uygulama geliştirme altyapısıdır. Hyperledger altyapıları akıllı sözleşmeleri desteklemektedir. Hyperledger'da gelişmiş kimlik doğrulama, veri gizliliğini sağlar. Hyperledger ile Java, Go ve NodeJS dilleri kullanılarak geliştirme yapılabilir. Modüler mimariye sahiptir. Corda finansal uygulamalar geliştirmek için kullanılan açık kaynak blok zinciri altyapısıdır. Corda diğer blok zinciri altyapıları ile birlikte çalışabilmektedir. Corda altyapısı bulut ortamında bir servis olarak çalıştırılabilir ve docker entegrasyonu vardır (Şafak, Arslan ve Gözütok, 2020).

2.2. Hashgraph

Hashgraph hızlı ve güvenli işlemler için 2018 yılında Swirlds tarafından geliştirilmiş dağıtık defter teknolojisidir. Hashgraph ağında işlemleri doğrulamak için madenciler bulunmamaktadır. Bunun yerine işlemleri bloklara ayırmadan işlemleri zaman içerisinde ayırmayı sağlayan yönlendirilmiş graf kullanılır. Hashgraph ağında düğümler arasında bilgi göndermek için rastgele dedikodu protokolü kulllanılmaktadır. Rastgele dedikodu protokolü bilgileri bir düğümden başka bir düğüme zaman damgalı olarak rastgele aktarmak ve senkronize etmek için kullanılır. Bu protokol tüm verilerin ağın tüm üyelerine dağıtıldığından emin olmak için kullanılır. Rastgele dedikodu protokolü ile kullanıcılar yalnızca kendi işlemleriyle ilgili bilgileri paylaşmazlar aynı zamanda mevcut mesajına önceki işlemleriyle ilgili bilgileri de ekleyerek gönerirler. Hashgraph ağındaki her işlem olay olarak adlandırılmaktadır. Olay zaman damgalıdır. Olay içerisinde işlemler, olayı oluşturan ve rastgele seçilen diğer katılımcının hash bilgisi tutulmaktadır. Hashgraph işlemleri ağa eklemek için sanal oylama konsensüs algoritmasını

kullanmaktadır. Sanal oylama algoritması ile işlem sırasına göre fikir birliğine varılmaktadır. Sanal oylama ile Hashgraph ağının üçte ikisi tarafından kabul edilen işlemler geçerli sayılır ve her düğüm tarafından deftere kaydedilir. Sanal oylama çoğunluk sağlanmaması durumunda birkaç tur gerçekleşebilmektedir. Hashgraph, daha fazla olay gerçekleşirken yayılmak için daha az bilgi gerektirdiğinden daha yüksek işlem hızları sağlamak için rastgele dedikodu protokolü kullanır. Hashgraph ağında saniyede 10.000'den fazla işlem gerçekleştirebilir. Hashgraph ağında blok yapısı kullanılmadığı için aynı anda iki bloğun oluşturulmasından kaynaklı sorunlar da görülmemektedir. Her olay önceden rezerve edildiği için verimliliğin artırılması sağlanmıştır (Dolenc, Turk ve Pustišek, 2020). Hashgraph asenkron bizans hata toleransı ile uyumludur. Asenkron bizans hata toleransı ağın güvenilir düğümlerinin ağda güvenilmez katılımcılar olsa bile işlemin zamanlaması ve sıralaması konusunda uzlaşmaya varabilmesidir. Ağdaki düğümlerin üçte biri işlemi geciktirerek veya başka şekilde ağı bozmaya çalışırsa bile Hashgraph ağında fikir birliğine varılabilmektedir. 100 byte boyutunda kripto para transferleri kullanılarak yapılan testlerde saniyede 500.000 işlem gerçekleştirilebilmiştir. Akıllı sözleşmeler kullanılarak yapılan testlerde saniyede yapılan işlem sayısı 10 olarak gerçekleşmiştir. Dosya işlemlerinde ise saniyede yapılan işlem sayısı 10 olarak tespit edilmiştir. Hashgraph akıllı sözleşmeler ve dosya depolamayı desteklemektedir. Akıllı sözleşmelerin geliştirilebilmesi için Solidty dili kullanılmaktadır. Hashgraph dağıtık defter teknolojisi ile uygulama geliştirebilmek için Java ve Lisp dili kullanılmaktadır. Hashgraph altyapısı kullanılarak Hedera ve NOIA olmak üzere aktif iki ağ bulunmaktadır (Hedera, 2021). Hedera Hashgrap hızlı ve güvenli dağıtık defter teknolojisi ağıdır. Farklı türden merkezi uygulamalar geliştirebilmek için uygundur. İşlem ücretleri son derece düşüktür. Hedera Hashgraph ağına katılım herkese açıktır. Hedera Hashgraph kendi kripto parasına sahiptir. Bitcoin'de işlem ücreti $22.57, Ethereum'da işlem ücreti $19.55 iken Hedera Hashgraph ağında $0.0001'dır. Bunun yanında işlem süresi Bitcoin'de 10-60 dakika, Ethereum'da 10-20 saniye ve Hedera Hashgraph ağında 3-5 saniyedir. Bu nedenle Hedera Hashgraph mevcut popüler kripto parası bulunan blok zinciri altyapılarından daha avantajlıdır. Hedera Hashgraph'ın HBAR adında kendine ait bir kripto para birimi vardır. Eşler arası ödeme sistemleri, merkezi olmayan uygulamalar oluşturmak, mikro ödeme çözümleri geliştirmek ve ağı korumak için kullanılır. NOIA, yeni nesil hızlı ve güvenli internet altyapısı için düğümleri kullanan dağıtık çözümdür. Random Gossip protokolü sayesinde her paket şifreli olarak en uygun yol üzerinden yönlendirilir. NOIA ağına katılım herkese açıktır (Şafak, Arslan ve Gözütok, 2020).

2.3. Tangle

Tangle, birbirine oklarla bağlı olan düğümlerden oluşan herkesin kullanımına açık dağıtık defter teknolojisidir. 2015 yılında ortaya çımıştır. Her düğüm en az iki düğüme bağlı olmalıdır. Yeni bir düğüm oluşturmak için düğümün önceki iki düğümü doğrulaması ve geçerlemesi gerekir. Doğrulanmamış düğümlere ipuçları denir. Her düğüm bir dizi veri veya işlem belgesi içerir. Tangle, DAG veri yapısını kullanır. DAG veri yapısı işlemleri tek bir yöne işaret eden bir graf formatında saklayan ve geçmiş işlemlerin mevcut ve gelecekteki işlemleri doğrulayamayacağı şekilde dairesel olmayan bir defterdir. Tangle dağıtık defter teknolojisinde fikir birliği mekanizması her işlemin önceki iki işlemi onaylayarak doğrulanmasını gerektirir. Doğrulama işleminde bir algoritmaya dayalı olarak önceki iki işlem seçilir ve kriptografik problem çözülerek tamamlanır. Her düğüm bir madenci olduğundan Tangle dağıtık defter teknlojisinden madenci gerekmemektedir. Bu sayede yeni işlem eklemenin maliyeti sıfırdır (Saad ve Park, 2019). Tangle ağında eski işlemlere işaret eden bir işlem grafının oluşturduğu karmaşıklık sayesinde ölçeklenebilirlik artmaktadır. Konsensüs mekanizması her yeni işlemin yalnızca rastgele seçilen iki önceki işlemi onaylamasını gerektirdiğinden bir sonraki bloğu beklemek zorunda kalmadan birden fazla işlem hemen doğrulanabilir. Teorik olarak birden fazla işlemin aynı anda doğrulanmasına olanak verir. Tangle dağıtık defter teknolojisinde ağdaki kayıt sayısı arttıkça ölçeklenebilirlik artmaktadır. Tangle, diğer dağıtık defter teknolojilerine göre kuantum bilgisayarlara karşı en güçlü dağıtık defterdir (Živi, Kadušić ve Kadušić, 2019). Tangle dağıtık defter teknolojisinin zayıflığı birden çok düğüm arasında veri senkronizasyonunun sağlanması konusunda zorluklar yaşanmaktadır. Tangle, ağdaki kötü niyetli saldırıları önlemek için merkezi ve geçici bir fikir birliği mekanizması olarak hareket eden Koordinatör kullanır. Bir koordinatör düğümü kullanılması teknolojinin yeterince dağıtık olmadığı anlamına gelebilir. Tangle dağıtık defter teknolojisinin esas olarak IoT ve kurumsal ölçekte en önemli faydası tüm blok zinciri madenciliği sürecinin temel dayanağı olan madencileri tamamen ortadan kaldırmasıdır. Tangle ağında işlemleri doğrulamak için madencilere ihtiyaç yoktur. Tangle, madencileri denklemden çıkararak her işlemi madencilerden bağımsız hale getirir ve yalnızca önceki bir işleme dayanır (Bhandary, Parmar ve Ambawade, 2020). Tangle veri yapısını kullanan en önemli uygulamaları IOTA ve ByteBall'dır.

IOTA, nesnelerin interneti için tasarlanmış Tangle dağıtık defter teknolojisinin uygulaması ve kripto para birimidir. 2017 yılında ortaya çıkmıştır. IOTA kripto parasını depolamak için dijital cüzdanı bulunmaktadır. IOTA, işlemleri doğrulamak için madencileri kullanmaz. Bunun yerine işlemi yayımlayan düğüm önceki işlemi doğrulaması gerekir. Bu sayede milyonlarca cihazın yer aldığı ağda nesnelerin interneti ağında yüksek ölçeklenebilirlik ve hız sağlanmaktadır. IOTA ağında işlem ücreti yoktur. IOTA ağında IOTA kuruluşu tarafından işletilen bir koordinatör düğüm aracılığıyla fikir birliğine varılabilir. Özellikle ağa bağlanan cihazların sayısının artması ile birlikte işlemlerin hızlı ve güvenli bir şekilde yapılabilmesini sağlama potansiyeline sahiptir (Silvano ve Marcelino, 2020).

ByteBall, farklı sektörlerde kullanılabilen Tangle dağıtık defter teknolojisinin uygulamasıdır. ByteBall, Tangle defterinde tuttuğu verilerden bayt başına ücret talep etmektedir. ByteBall akıllı sözleşmeleri desteklemektedir. Akıllı sözleşmlerin kodlanmış kuralları değiştirilemezdir. Akıllı sözleşmeler geliştirici olmayanların bile sözleşme tanımlayabileceği ölçüde basitleştirilmiştir. ByteBall anonimlik için tasarlanımş kripto para birimine sahiptir. Bu kripto para BlackBytes olarak adlandırılmaktadır. BlackBytes şifreli mesajlaşma yoluyla iletişim kuran taraflar arasında gönderilebilir. Tangle dağıtık defter teknolojisi Blackbytes'ın önceki sahibinin artık ona sahip olmadığını kaydeder ancak yeni Blackbytes alıcısını kaydetmez. Bitcoin ağındaki tüm işlemler blok zincirinde depolandığından ve izlenebildiğinden bu kripto paranın Bitcoin'e göre bir takım avantajları vardır (Şafak vd., 2020).

2.4. Holochain

Holochain; güvenli, güvenilir ve hızlı eşler arası uygulamalar geliştirilmesini sağlayan açık kaynak dağıtık defter teknolojisidir. 2018 yılında ortaya çıkmıştır. Holochain her

katılımcının kendi yerel zincirini tutmasını esas almaktadır. Bu sayede ağ her düzeyde dağıtık hale getirilmiş ve ağ boyutunun azaltılması sağlanmıştır. Her katılımcı kendi zincirini tuttuğunda ağdaki tüm verilerin diğer katılımcılar tarafından bilinmesine gerek yoktur. Zincirlerin, mesajların ve doğrulama onaylarının kriptografik imzalanması kaynak ve hesap verilebilirliği korur. Katılımcılar kendi verileri üzerinde tam kontrrol sahibidir. Verilerin bütünlüğünün kontrolünün sağlanabilmesi için her zincirin hash bilgisi dağıtık hash tablosunda tutulmaktadır. Dağıtık hash tablosu katılımcılarda dağıtık olarak tutulmaktadır (Schueffel vd., 2017). Yerel zincirlerin doğruluğu dağıtık hash tablosu ile kontrol edilmektedir. Katılımcıda kayıt zincirinin tutulduğu cihaz zarar görürse bilgiler kaybedilebilir. Holochainn mevcut internet mimarisini dağıtık hale getirmeyi önermektedir. Mevcut internet mimarisinde uygulamalar merkezi sunucular üzerinde çalışır. Holochain ile dağıtık uygulamalar geliştirilerek güvenli sistemlerin geliştirilmesi sağlanacaktır. Kullanıcı verileri geleneksel internet mimarisinde merkezi sunucular üzerinden tutulmaktadır. Holochain dağıtık defter teknolojisi ile kullanıcı verilerin merkezi sunucular üzerinde tutulması yerine kendi cihazlarında tutabilmelerini sağlamaktadır. Kullanıcılar verileri üzerinde tam kontrol sahibi olacaktır. Blok zinciri gibi veri merkezli yapılarda ağdaki her düğüm onay sırasındaki işlemleri doğrular ve deftere kaydeder. Ancak veri boyutu arttıkça sistem yavaşlamaya başlar. Buna karşılık Holochain düğüm merkezli yapısı sayesinde kullanıcıların kendi geçmiş kayıtlarını tutmasını sağlar (Harris-Braun, Luck ve Brock, 2018). Holochain, geliştiricilerin Javascript programlama dilini kullanan dağıtılmış uygulamalar oluşturmasını sağlayan bir platform oluşturmuştur. Holochain'de fikir birliği mekanizmaların çalıştırmak için madencilik işlemi yapılmamaktadır. Dağıtılmış defterlerin yalnızca sürümünü korumak gerektiğinden daha düşük donanım kaynakları yeterli olmaktadır. Holochain ağında bir mobil cihazda birden fazla tam düğüm çalıştırabilir. Holochain ağında işlemler gecikme yaşanmadan anlık olarak gerçekleşir. Holochain ağıda sürüm kontrol özelliği sayesinde kullanıcılardan gelen verilerin kontrolü sağlanmaktadır. Kullanıcı gelecek verinin doğruluğunu verinin geldiği düğümün sürüm bilgisinin kontrolü ile sağlamaktadır. Bu sayede ağı bozmaya çalışan hareketler engellenmiş olacaktır. Katılımcılar kendi kişisel defterlerini sakladığı için ağ oldukça ölçeklenebilirdir. Holochain üzerinde uygulamalar geliştirebilmek için Rust programlama dili kulllanılmaktadır (Zia, Benbouzid, Elbouchikhi, Muyeen, Techato ve Guerrero, 2020).

Holo, yeni dağıtık internet mimarisine bir köprü olan Holochain uygulamaları (hApps) için dağıtılmış bir eşler arası uygulama adres barındırma platformudur. Holo dağıtık alan adı sistemi olarak tanımlanmaktadır. Holo, kullanıcılara yedek bilgisayar kapasitelerinden para kazanma fırsatı da sunar. Holo, dağıtılmış Holochain uygulamaları ile mevcut merkezi web arasında bir köprü görevi görür. Gerekli işlem gücü ve depolama alanı ağdaki isteyen katılımcılar tarafından yapılabilmektedir. Ağdaki herkes bilgisayarını holo uygulama depolayıcısına dönüştürebilir ve HoloFuel'den ödeme alarak uygulama barındıran kaynak olabilir. Holochain üzerine kurulu Holo uygulamasının amacı hApp'leri ana akım internet kullanıcıları için kolayca erişilebilir kılmaktır. Holo sayesinde kullanıcılar tarayıcılar üzerinden dağıtık uygulamalara erişim sağlayabilmektedir (Brock, Atkinson, Friedman, Harris-Braun, McGuire, Russell, Perrin, Luck, Harris-Brau, 2017).

2.5. Tempo

Tempo dağıtık defter teknolojisinde defter parçalama yöntemi kullanılarak katılımcılarda tutulmaktadır. Ağdaki defterin tamamı kullanıcılarda tutulmadığı için kaynak kullanımı açısından verimlidir. Her düğüm ağın tamamının bir alt kümesini tutmaktadır. Her alt kümenin alt kümeleri de yine farklı düğümlerde tutularak olası veri kayıplarının önüne geçilmektedir. Derfterin her alt kümesine parça adı verilir ve her bir alt kümenin bir kimliği vardır. Ağın parçalı olarak tutulması sayesinde ağın daha büyük miktarda veri kaydedilebilmesi sağlanır ve ölçeklenebilirlik artırılmıştır. Tempo dağıtık defter teknolojisi her parçanın kayıtlı olan verileri doğru sırayla içermesini sağlar. Her parçanın dağıtılmış defter hakkında güncel bilgilere sahip olduğundan emin olmak için dedikodu protokolü kullanılır. Bu protokol ile ağdaki düğümler birbirleriyle iletişim kurar ve parçalarına ilişkin bilgileri iletir. Dağıtılmış defter teknolojisinin özelliklerine ilişkin bu protokolün bu tür mimaride bilgileri yaymanın en etkili yollarından biri olduğu kanıtlanmıştır. Bu protokol ile ağdaki düğümler herhangi bir yeni yapılandırma hakkında ağa bilgi verir ve bilgileri diğer düğümlere iletir. Diğer düğümler daha sonra bilgileri optimize eder ve parçalarını buna göre senkronize eder. Düğümlerin ağda gerçekleşen yeni işlemleri doğrulamak için güncelleme parçalarına ihtiyacı olacağından bu işlem gereklidir. Dedikodu protokolü doğrudan bağlı oldukları diğer düğümler hakkındaki meta verileri de duyurabilir (Şafak vd., 2020). Tempo dağıtık defter teknolojisinde bir düğüm işlemleri doğrulamak istediğinde mantıksal saatler kullanılır. Dağıtılmış defter veritabanının olağan zaman damgası kendi başına fikir birliğine varamaz. Böylece meydana geldiği zaman eşleştirmek yerine kendisinden önce olanı görür. Önceki bir işlem A ise ve şimdi yeni bir B işlemi gerçekleştiyse, düğümler B'den önce A işleminin olup olmadığını görecektir. Dolayısıyla düğümler o olayın gerçek zamanı yerine olay sırasını kaydedecektir. Tempo dağıtık defter teknolojisinde her düğüm yerel olarak belirli düğümün tanık olduğu olayların toplam sayısını temsil edecek artan tamsayı değerine sahip bir mantıksal saat içerir. Mantıksal saat düğümün tanık olduğu olayların sayısını temsil eden artan tam sayı değeridir. Katılımcılar daha önce görmedikleri yeni bir olay gördüklerinde bu sayı artırılacaktır. Herhangi bir işlem kaydedilirken mantıksal saat numarası da beraberinde saklanacaktır. Düğümler daha önce görmedikleri yeni bir etkinlik gördüklerinde mantıksal saat numaraları artırılacaklar. Herhangi bir olayı kaydederken mantıksal saat numarasını da onunla birlikte saklanacaktır. Bu numara geçmiş işlemlerle yeni işlemlerin doğrulanmasına yardımcı olur. Tempo dağıtık defter teknolojisinin en önemli uygulaması Radix platformudur (Masood & Faridi, 2018).

Radix, Tempo dağıtılmış defter teknolojisi üzerine çalışmaktadır. Şirket piyasadaki diğer tüm dağıtık defter platformlarından daha ölçeklenebilir ve daha hızlı çalıştığını ifade etmektedir. Radix platformu herkese açıktır ve madencilik işlemi herkes tarafından yapılabilmektedir. Madencilik işlemi için akıllı telefonlar ve modem gibi düşük donanım kaynakları yeterli olmaktadır. Radix, Google Cloud altyapısını kullanarak yaptığı performans testinde 1.4 milyon TPS sayısına ulaşmıştır. Test için 17 ülkeye yayılmış 1.187 düğüm kullanılmıştır. Test verisi olarak 10 yıllık Bitcoin işlem geçmişi kullanılmış ve işlem bir saatten daha kısa sürede tamamlanmıştır. Toplam veri 2^64 parçaya bölünerek düğümlere dağıtılmıştır. Test sırasında parçalama düğümler arasında düşük miktarda parça %10 örtüşecek şekilde ayarlanmıştır. Radix dağıtık defter teknolojisi hala nihai olarak olgunlaşmamıştır ve henüz kararlı bir sürüm yayınlanmamıştır (Radix, 2020).

3. Dağıtık Defter Teknolojileri Uygulama Alanları

3.1. Savunma

Dağıtık defter teknolojisi ülkelerin savunma alanında dijital bütünlüğünün sağlanabilmesi için kullanılabilir. Savunma alanındaki veriler ülkelerin ulusal güvenliklerini doğrudan etkilediği için kritik öneme sahiptir. Dağıtık defter teknolojisi güvenlik özelliği ile öne çıkan bir teknolojidir. Dağıtık defter içerisine kaydedilen veriler değiştirilemez ve kullandığı güçlü kriptografik algoritmalar sayesinde yalnızca yetkili kullanıcıların erişimi sağlanabilmektedir. Veriler tek bir hata noktası yerine dağıtık olarak saklandığı için sistem olası siber saldırılara karşı da dirençlidir. Dağıtık defter teknolojisinde hiçbir katılımcı ağda değişiklik yapma yetkisine sahip değildir. Dağıtık defter içerisine kaydedilen veriler silinemez ve tahrip edilemez. Dağıtık defter ağı içerisine bir kayıt eklenebilmesi için belirlenen doğrulayıcı katılımcıların onayı gerekmektedir. Kritik veriler ile ilgili bir diğer zorluk bu verilerin güvenli olarak paylaşılabilmesidir. Dağıtık defter teknolojisi kritik verilerin güvenli olarak saklanması ve paylaşılmasını sağlamaktadır. İçerisinde gerekli kurumların yer aldığı kapalı bir savunma ağı ile kritik veriler dijital ortamda güvenli olarak saklanabilir, paylaşılabilir ve yönetilebilir (Sudhan & Nene, 2017). Dağıtık defter teknolojisi ile askeri tedarik zinciri süreçlerinin dijital ortamda güvenli olarak izlenebilmesi ve yönetilebilmesi sağlanabilir. Diğer birçok sektörde olduğu gibi savunma sektöründe de tedarik zinciri verileri için tek bir doğrulama noktası yoktur. Herkes kendi kayıtlarını tutmaktadır. Verilerin bu şekilde parçalı olarak tutulması tedarik zincirlerini izleme ve yönetmede hataların giderilmesini zorlaştırmaktadır. Tedarik zincirindeki taraflar arasındaki verilerin şeffaflığının yeteri kadar sağlanamaması güven eksikliğine neden olabilmektedir. Bu nedenle içerisinde askeri tedarik zinciri dahillerinin yer aldığı dağıtık defter altyapılı platform geliştirilerek tüm süreçler dijital olarak hızlı, güvenli ve şeffaf olarak gerçekleşebilecektir (Rahayu, RMN, Kamarudin ve Azahari, 2019).

Locheed Martin dağıtık teknolojisini kullanan ilk ABD savunma şirketidir. Temel amaç silah sistemindeki manipülasyon tehdidini engelleyerek veri bütünlüğünü sağlamaktır. Bunun yanında savunma alanında tedarik zinciri risk yönetimi için çalışmaktadır. Mevcut proje planlarının güvenliği sağlamak amacıyla dağıtık defter tabanlı sistemde depolamaktadır (Worth, 2018).

3.2. Siber Güvenlik

Dağıtık defter teknolojisi sistemleri siber güvenlik saldırılarına karşı güçlü bir şekilde koruma sağlama potansiyeline sahiptir. Siber saldırılar genellikle sistemin işleyişini bozma, verileri ele geçirme, verileri değiştirme, verileri silme ve kişilerin şifrelerini ele geçirme amaçlarıyla yapılmaktadır. Dağıtık defter teknolojisi ile geliştirilen uygulamalar bu amaçlarla yapılacak saldırılara karşı diğer sistemlere göre çok daha dayanıklıdır. Sistemin işleyişini bozmak için yapılan saldırıda amaç ağ trafiğini artırarak erişimi engellemektir. Bu saldırıların sistemi etkilemesinin nedeni sunucuların merkezi olmasından kaynaklıdır. Dağıtık mimari sayesinde tek noktadan kaynaklı hatalar engellenerek bu risk en aza indirilecektir. Bu sayede sistem çalışması kesintisiz olarak devam edebilmektedir. Veri günümüzde birçok sektörün gelişimi için en önemli bileşendir. Bu nedenle siber saldırganlar tarafından veriler açık hedeftir. Yapılan saldırılarda veriler ele geçirilebilir, silinebilir veya değiştirilebilir. Merkezi sistemler bu saldırıları engellemek amacıyla maliyetli önlemler alsa da çoğu kez bu saldırılardan etkilenmektedir (Mathew, 2019). Dağıtık defter teknolojisinde veriler dağıtık ve şifreli olarak saklanmaktadır. Bu sayede hiçbir katılımcı tarafından ağdaki veriler silinemez ve değiştirilemez. Ağa veri ekleme işlemi de fikir birliği algoritmaları ile sağlandığı için ağın onaylamadığı hiçbir veri ağa eklenemez. Siber saldırganlar sistemin güvenlik önlemlerini aşabilmek için kimlik doğrulama işlemlerinde kullanıcıların şifrelerini ele geçirmeye çalışırlar. Sistemlerde kullanılan basit kimlik doğrulamaları güvenlik açısından zayıflıklara neden olur. Bir kuruluş sistem güvenliği için ne kadar yatırım yaparsa yapsın çalışanların ve müşterilerin şifreleri ele geçirilirse bu çabalar bir anlam ifade etmez. Dağıtık defter teknolojisi cihazların ve kullanıcıların kimliklerini doğrulamak için dağıtılmış genel anahtar altyapısını kullanmaktadır. Dağıtılmış genel anahtar altyapısı kullanıcılara kimlik doğrulamak için şifre yerine SSL sertifikası sağlar. Sertifikaların yönetimi blok zinciri üzerinden sağlandığı için siber saldırganların sahte sertifikaları kullanması neredeyse imkansızdır. Dağıtık defter teknolojisinde kimlik doğrulama işleminde insan faktörünü ortadan kaldırdığı için siber saldırıların buradan gelmesini engeller (Taylor, Dargahi, Dehghantanha, Parizi ve Choo, 2020). NATO, IBM ve General Motor gibi firmalar siber güvenlik için dağıtık defter teknolojisinin kullanılmasına yönelik çalışmalar yapmaktadırlar.

3.3. Sigorta

Sigorta süreçleri mevcut durumda kağıt üzerinden yürütülmesi ve hatalara açık olması nedeniyle verimsizdir. Sigorta süreçlerinin dijital olarak izlenebilmesi ve dolandırıcılıkların engellenebilmesi için dağıtık defter teknolojisinin kullanılmasına yönelik çalışmalar yapılmaktadır. Sigorta süreçleri dağıtık defter teknolojisi ile güvenli, hızlı ve verimli hale getirilebilir. Dağıtık defter teknolojisi sigorta sektöründe talep yönetimi, dolandırıcılık tespiti, risk önleme ve aracısız sigorta sözleşmesi oluşturma amaçlı kullanılabilir. Sigorta işlemleri için talep oluşturmanın ve işleme almanın mümkün olduğunca kolay olması kullanıcılar için önemlidir. Dağıtık defter teknolojisi ile veriler dağıtık defter üzerinde değiştirilemez olarak tutulduğu için süreçler şeffaf olarak takip edilebilmektedir. Talep oluşturmak için gerekli süreçlerin dijital olarak yürütülmesi akıllı sözleşmeler aracılığıyla sağlanabilir. Talep oluşturmada bazı adımlar otomatik hale getirilebilir (Gatteschi, Lamberti, Demartini, Pranteda ve Santamaría, 2018). ABD'de sağlık sigortası dışındaki sigorta dolandırıcılığının toplam maliyeti 40 milyar dolardan fazladır. Sigorta sektöründeki süreçlerin karmaşık olması sahtekarlık yapmak için kullanılabilecek boşluklar oluşturur. Sigorta sektöründe sahtekarlıkların önüne geçilmesinde en büyük engel sigorta şirketlerinin birbirleri arasında veri paylaşımının yetersiz olmasından kaynaklanmaktadır. Dağıtık defter teknolojisi dolandırıcılık ile mücadele için sigorta süreci içerisindeki taraflar arasında daha iyi koordinasyon sağlar. Dağıtık defter altyapısı ile tasarlanmış sigorta sisteminde aynı zararın farklı sigorta şirketlerinde iki kez karşılanmasının önüne geçilmesi, güçlü kimlik doğrulama ile sahteciliklerin azaltılması ve prim sapmalarının engellenmesi sağlanabilir. Dağıtık defter teknolojisi sigorta sözleşmelerin akıllı olarak tasarlanabilmesini ve yürütülebilmesini sağlar. Akıllı sözleşmeler ile kullanıcılar aracısız olarak sigortalarını başlatabilir, yürütebilir ve yönetebilir. Kullanıcıların geçmiş verileri de sigorta şirketleri

tarafından şeffaf olarak görüntülenebildiği için kişiselleştirilmiş dinamik sözleşmeler oluşturulabilir. Bir sigorta olay talebi gerçekleşirse ödemeler aracısız ve hızlı bir şekilde tamamlanır (Chen, Xu, Shi, Zhao ve Zhao, 2018).

Fizzy, AXA tarafından geliştirilen gecikmeli uçuşlarda kullanıcılara tazminat ödenmesini sağlayan Ethereum ile geliştirilmiş sigorta uygulamasıdır. Fizzy platformunda uçuş gecikme sigortası alındığında işlem dağıtık deftere kaydedilir. Küresel hava trafik veritabanlarına göre sistem üzerinde iki saatten fazla gecikme görüldüğünde akıllı sözleşmeler tarafından tazminat ödemesi otomatik olarak yapılır. Veri setindeki görüntülerin %80'i eğitim ve geçerleme işlemi için kullanılırken %20'si test işlemi için kullanılmıştır. Bu neden Veri setindeki 34,684 görüntü eğitim/geçerleme, 8,672 görüntü test için kullanılmıştır. Veri seti 2,1 GB dosya büyüklüğüne sahiptir (Fizzy, 2017).

3.4. Tedarik Zinciri

Tedarik zinciri süreçlerinde tüm taraflar kendi yerel kayıtlarını sakladıkları için işlemlerin izlenebilirliği ve koordinasyonu konularında sorunlar ortaya çıkabilmektedir. Dağıtık defter teknolojisi kayıtların ortak veritabanında tutulması sayesinde tedarik zinciri süreçlerindeki izlenebilirlik ve koordinasyon sorunlarını önemli ölçüde azaltma potansiyeline sahiptir. Üretim, savunma, gıda, sağlık ve lojistik alanlarına tedarik zincirleri dağıtık defter teknolojisi ile dijital olarak tasarlanabilir (Moosavi, Naeni, Fathollahi-Fard ve Fiore, 2021). Dağıtık defter teknolojisi ürünlerin izlenebilirliğini artırarak daha hızlı ve düşük maliyetli şekilde teslim edilmesini sağlamaktadır. Tedarik zinciri süreçlerinde dağıtık defter teknolojisi şeffaflık, aracısız ödeme, denetlenebilirlik ve güvenilirlik sağlanmaktadır. Şeffaflık, ürünlerin tedarik zincirindeki tüm tarihçesinin görüntülenebilmesidir. Tedarik zincirlerinde işlemlerin izlenebilir olması olası sahtekarlıkların engellenmesini sağlayacaktır. Tedarik zincirindeki tüm işlemlerin yetkili katılımcılar tarafından görüntülenebilmesi ile denetlenebilirlik artırılacaktır. Tedarik zincirindeki katılımcılar sağlanan şeffaflık sayesinde banka gibi aracı bir kuruma gerek kalmadan ödeme işlemlerini yapabileceklerdir. Swift gibi uluslararası ödeme sistemleri yüksek maliyetlidir ve uzun sürebilmektedir. Tedarik zincirinde anlık ödemeler için bankalar doğrudan sisteme dahil edilebilir veya tedarik zinciri içerisinde geliştirilecek kripto para kullanılabilir. Dağıtık deftere eklenen veriler dağıtık olarak saklandığı için hiçbir katılımcı tarafından değiştirilemez veya silinemezdir. Hiçbir katılımcı ağın onaylamadığı veriyi ortak deftere kaydedememektedir (Azzi, Chamoun ve Sokhn, 2019).

Walmart, IBM ile birlikte gıda tedarik zincirinde şeffaflık sağlamak için Hyperledger Fabric altyapısını kullanarak IBM Food Trust çözümünü geliştirmiştir. IBM Food Trust ile ürünlerin tarihçesi görüntülenebilecek ve gıda kaynaklı bir hastalık meydana geldiğinde sorunun kaynağını bulmak kolaylaşacaktır (Kamath, 2018).

3.5. Dijital Hak Yönetimi

Değiştirilemez token (Non-fungible token – NFT) dijital hak yönetimi sağlamak için kullanılan dağıtık defter teknolojisinin bir uygulamasıdır. Değiştirilemez token varlıkların benzersiz sahipliğini temsil etmek için kullanılan belirteçtir. Dijital belirteçlerin kripto para birimlerinden farkı parçalanamaz olmasıdır. Kripto paralardan bir başka farkı da her bir varlığın değeri birbirinden farklıdır. Dijital varlığın yalnızca bir sahibi olabilir ve bu sahiplik dağıtık defter teknolojisi ile sağlanmaktadır. Ağdaki hiç kimse varlığın sahipliğini değiştiremez ve aynı belirteç tekrar kullanamaz. Dijital belirteçler genellikle sanat, müzik, oyun içi öğeler, spor ve videolar gibi gerçek dünyadaki nesneleri temsil edebilmek için kullanılırlar. Dijital belirteçler yalnızca dijital olarak tutulmaktadır. Geleneksel yöntemlerde bir dijital varlığın birebir kopyası alınabilmektedir. Dağıtık defter teknolojisi ile kayıtlı varlık değişitirilemez ve kopyalanamaz. Kopyalama işlemi ancak orjinal varlığın bir başka versiyonudur (Cornelius, 2021). Bu durum sanat eseri tablonun korunmasına benzetilebilir. Bir sanat eserinin kopyasına sahip olunabilir ancak değerli olan orjinalidir. Dijital belirteçler özellikle son dönemlerde ön plana çıkan içerik üreticiler için önemli fayda sağlayabilir. İçerik üreticileri içeriklerinin sahipliğini, içeriği yayınlamak için kullandıkları platformlara devretmediği yeni bir yaklaşım getirmektedir. Dijital belirteçler kullanılarak yapılan toplam satış 389 milyon dolara ulaşmıştır.

3.6. Sağlık

Sağlık gün geçtikçe ülkeler için daha kritik ve önemli hale gelmeye başlamaktadır. Salgın döneminde sahip olduğu önemi teyit ettirmiştir. Her alanda olduğu gibi sağlık alanında da gelişme sağlayabilmek için veriye ihtiyaç duyulmaktadır. Ülkeler sağlık verilerinin güvenliğini sağlarken bir yandan da geliştiriciler ile güvenli olarak paylaşabilmesi gereklidir. Sağlık sektöründe dağıtık defter teknolojisinin kullanımı verilerin güvenliğini sağlamak, güvenli veri paylaşımı, sağlık sigortası süreçlerin yönetimi, sağlık tedarik zinciri yönetimi ve genetik verilerin korunmasına yöneliktir. Sağlık verileri ülkeler için kritik öneme sahiptir. Dağıtık defter teknolojisi ile verilerin değiştirilemez ve tutarlı olarak saklanması mümkündür. Kullanıcılar kendi verileri üzerinde tam kontrol sahibi olabilir. Bu sayede verilerin kullanıcıların izni olmadan başkaları ile paylaşılması engellenecektir. Dağıtık defter teknolojisi ile sağlık sigortası sayesinde hastaneler, doktorlar, laboratuvarlar ve güvenlik ağı sağlayıcıları birbirine bağlanarak işlemlerin onaylanması için gerekli tutarlı sağlık verisi akışı sağlanabilir. Dağıtık defter teknolojisindeki veriler değiştirilemediği için işlemlerin tarihçesi de takip edilebilmektedir. Bu sayede sağlık tedarik zincirinde işlemlerin güvenli olarak yürütülebilmesi sağlanacaktır. Sağlık ekipmanları ve ilaçların üretimden son kullanıcıya ulaşana kadar olan tüm aşamalar dağıtık defter üzerinden yürütülebilir. Özellikle ilaç sektörü hastaların sahte ilaçlardan olumsuz etkilenmemesi açısından önemlidir. Dünya Sağlık Örgütü'ne göre sahte ilaç endüstrisinin ekonomik büyüklüğü 30 milyar doların üzerindedir (Thenmozhi, Dhanalakshmi, Geetha ve Valli, 2021). Hastaların genomlarının dizilenmesi, analizi ve yorumlanmasının gelecekte sağlık hizmetlerinin temelini oluşturacağı tahmin edilmektedir. Kişisel genom dizilimini genişletmenin önündeki kritik bir engel, genomik verileri güvenli ve yüksek bir bütünlük içinde saklama yeteneğidir. Bulut depolama bu tür verilere herhangi bir yerden ve cihazdan erişmek için çözümler sunarken, tek nokta arıza kayıpları gibi güvenlik, veri bütünlüğü ve sağlamlık açıkları henüz tam anlamıyla giderilmemiştir. Bu nedenle genetik verilerin saklanması ve işlenmesi için dağıtık defter teknolojisi kullanılabilir (Gursoy, Brannon, Wagner ve Gerstein, 2020).

Medicalchain, dağıtık defter teknolojisi kullanılarak geliştirilmiş elektronik sağlık kayıt platformudur. Medicalchain çeşitli kaynaklardan gelen hasta kayıtlarını birleştirdiği güvenli bir veri depolama sağlamaktadır. Dağıtık defter teknolojisinin

kullanılmasının amacı bir hastanın tıbbi verilerinin tek bir doğru versiyonunu korumaktır. Tasarlanan sağlık dağıtık defter ağında kullanıcılar verileri üzerinde tam kontrol sahibidir ve istedikleri kurumlarla paylaşabilecektir. Medicalchain MedCoin isimli kripto paraya da sahiptir. Bu sayede sağlık verilerinin alınıp satıldığı bir ticaret platformu oluşmaktadır (Medicalchain, 2021).

3.7. Enerji

Enerji sektörünün alternatif yenilenebilir enerji kaynaklarının artan kullanımına yönelik devam eden derinlemesine dönüşümü elektrik piyasasında merkezi olarak yönetilebilmesini zorlaştırmaktadır. Dağıtık defter teknolojisi ile enerji alım-satım işlemleri hızlandırılabilir ve mevcut enerji dağıtım süreçleri tamamen dönüştürülebilir. Dağıtık defter teknolojisinin enerji sektöründeki ilk kullanımı eşler arası mikro şebekelerin geliştirilmesidir. Mikro şebekeler iletim yoluyla kaybedilen enerji miktarını en aza indirir. ABD'de üretilen elektriğin tahmini %5'i geçiş sırasında kaybolduğundan dağıtık defter teknolojisi mikro şebekeler için verimli bir alternatif sunar (Jogunola, Hammoudeh, Anoh, Adebisi, 2020). Yeni enerji ticaret ağında enerji üreticileri ürettikleri enerjiyi aracısız olarak alıcılara satabileeceklerdir. Bunun için dağıtık defter teknolojisindeki akıllı sözleşmeler kullanılacaktır. Akıllı sözleşmeler tanımlanan süreçlerin dağıtık defter üzerinden otomatik olarak yerine getirilmesini sağlayan ve çok hızlı çalışabilen bilgisayar programlarıdır. Her satış işlemi için otomatik olarak akıllı sözleşmler çalışacak ve gerçekleşen işlem kaydı dağıtık deftere kaydedilecektir. Enerji ticaretine katılımın kolaylaştırılması yerel üreticileri teşvik ederek yenilenebilir enerji üretimini artıracaktır. Bu sistem enerjinin farklı ülkelere de satışını kolaylaştırarak enerji ihracatına katkı sağlayacaktır. Ayrıca bir kullanıcı hem üretici hem tüketici konumunda olabilecektir (Andoni, M., Robu, Flynn, Abram, Geach, Jenkins, McCallum ve Peacock, 2019). Dağıtık defter teknolojisinin enerji sektöründeki diğer kullanımı petrol, gaz ve yakıt teadrik zincirinin kontrol edilmesine yöneliktir. Dağıtık defter teknolojisinin enerji sektöründeki bir başka kullanımı üretilen enerjinin sertifikalandırılmasıdır. Bu sayede kullanıcılar tüketecekleri enerjinin nasıl üretildiğini tercih edebilir duruma gelecektir. Dağıtık defter teknolojisi kullanılarak mevcut enerji altyapılarının siber saldırılara karşı dayanıklı hale getirilmesi için de kulllanılmasına yönelik çalışmalar yapılmaktadır. Son olarak dağıtık defter teknolojisi enerji sektöründe kripto para amaçlı kullanılabilir (Brilliantova ve Thurner, 2019). Enerji alışverişinde kullanıma yönelik kripto para geliştirilebilir.

Brooklyn Microgrid, LO3 Energy ve Siemens işbirliği ile geliştirilen dağıtık defter teknolojisini kullanan pilot eşler arası enerji ticaret platformudur. Geliştirilen sistemde güneş panelleri olan kullancıılar fazla ürettikleri enerjiyi diğer kullanıcılara satabilmektedir. Brooklyn Mikrogrid şebekesi güneş panelleri kuranlara ve yerel üreticelere ekonomik olarak fayda sağlayarak iletimden kaynaklı enerji kayıplarının en aza indirilmesine katkıda bulunur (Brooklyn Microgrid, 2019).

3.8. Finans

Dağıtık defter teknolojisinin ilk yaygın kullanımı finans sektörüne yönelik geliştirilmiş Bitcoin kripto parasıdır. Başlnagıçta bir ödeme sistemi olarak tasarlansa da kripto para yönü daha çok öne çıkmıştır. Bitcoin'in ardından dağıtık defter teknolojisi kullanılarak yüzlerce kripto para geliştirilmiştir. Bu durum gelecekte paranın geçireceği inovasyonun ilk sinyallerini vermektedir. Para, teknolojinin gelişmesiyle birlikte sürekli değişime uğramıştır. Dağıtık defter teknolojisi finans sektöründe kripto para dışında farklı alanlarda da kullanılabilir. Mevcut küresel finans servisleri eski ve onlarca yıl önceki teknolojiler üzerinde kuruludur. Genellikle yavaş ve güvenlik riski yüksek sistemlerdir. Finansal servislerin kaleleri (bankalar vb.) tekelleri savunmakta ve yıkıcı inovasyonları bozmaktadır. Ayrıca mevcut finansal sistemler eski teknolojileri kullanır ve 19. yy düzenlemelerine göre yönetilmektedir (Ali, Ally, Clutterbuck ve Dwivedi, 2020). Dağıtık defter teknolojisi çoğu finansal servisi eski kuruluşların sınırlamalarından kurtarabilir ve inovasyon konusunda teşvik eder. Dağıtık defter teknolojisi finansal sistemlerin güveniliğini artıracak, işlemleri hızlandıracak ve maliyeteleri düşürecektir. Dağıtık defter teknolojisi taraflar arasında aracısız işlem olanağı sayesinde güven sağlamaktadır. Özellikle uluslararası ödemelerde hız artırılarak işlem maliyetleri düşürülecektir. Son olarak dağıtık defter teknolojisi borsaların yönetilmesi için kullanılabilir. Kullanıcılar istedikleri borsada aracı olmadan işlem yapabilir (Chen ve Bellavitis, 2020).

CHESS Avustralya Borsası tarafından işletilen ve menkul kıymetlerin alım satım işlemlerinin aracısız, güvenli ve hızlı bir şekilde yapılabilmesini sağlayan dağıtık defter tabanlı bir sistemdir. Günde 2 milyondan fazla işlem yapılmaktadır (Barbaschow, 2020).

4. Sonuç

Dağıtık defter teknolojisi; verilerin katılımcılarda dağıtık olarak tutulduğu, deftere veri kaydetme işinin belirlenen doğrulama algoritması tarafından yapıldığı ve verilerin hiçbir katılımcı tarafından değiştirilemediği veri saklama teknolojisidir. Geleneksel yaklaşımlarda veriler merkezi bir katılımcının kontrolünde olan sunuculardа tutulmaktadır. Bu yöntem başlangıçta kullanışlı olsa da teknolojideki gelişmeler ile işlevselliğini giderek yitirmektedir. Verilerin bir veya birkaç cihaz üzerinde tutulması ve yetkili kullanıcılar tarafından değiştirilebilmesi siber saldırılar için açık hedef haline gelmesine neden olmaktadır. Bunun yanında nesnelerin interneti teknolojisindeki gelişmelerle internete bağlanacak cihaz sayısının artmasıyla birlikte merkezi sunucuların bu işlem yoğunluğuna cevap vermesi mümkün değildir. Tüm bu problemleri ortadan kaldırmak için dağıtık defter teknolojisi ortaya çıkmışıtır ve üzerine çalışmalar yapılmaktadır. Bu makalede Blok Zinciri, Hashgraph, Tangle, Holochain ve Tempo dağıtık defter teknolojileri incelenmiştir. Bu teknolojiler arasında blok zinciri Bitcoin kripto parasında kullanılması nedeniyle oldukça popüler olsa da hız ve ölçeklenebilirlik açısından kullanımı kısıtlıdır. Yüksek işlem yoğunluğuna sahip uygulamalarda Hashgraph, Tangle, Holochain ve Tempo dağıtık defter teknolojileri tercih edilmelidir. Ancak işlem yoğunluğunun düşük olduğu sistemlerde kendini kanıtlamış blok zinciri dağıtık defter teknolojisinin kullanılması faydalı olacaktır. Dağıtık defter teknolojileri uygulamaları kripto paralar nedeniyle finans sektörü ile özdeşleştirilse de bir teknoloji olması sebebiyle ihtiyaçlar doğrultusunda birçok farklı sektörde kullanılabilir. Bu makalede dağıtık defter teknolojisinin kullanılabileceği Savunma, Siber Güvenlik, Sigorta, Tedarik Zinciri, Dijital Hak Yönetimi, Sağlık, Enerji ve Finans alanları incelenmiştir. İncelenen alanlarım tamamında dağıtık defter teknolojisinin dönüştürücü etkiye sahip olduğu tespit edilmiştir. Sonuç olarak dağıtık defter teknolojisi getirdiği güvenlik seviyesi sayesinde gelecekte birçok sektör ve teknolojiyi dönüştürme potansiyeline sahiptir. Dağıtık defter teknolojisi yeni bir felsefe de getirdiği

için teknik çalışmaların yanında gerekli regülasyon düzenlemelerinin yapılması ve toplumsal farkındalığın artırılması gelecekte teknolojinin gelişimini yakalayabilmek için faydalı olacaktır.

Kaynakça

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology. 3(2), 99-11.

Antal, C., Cioara T., Anghel I., Antal M., & Salomie, I. Distributed Ledger Technology Review and Decentralized Applications Development Guidelines (2021). Future Internet. 13(3):62. https://doi.org/10.3390/fi13030062

Kannengießer, N., Lins, S., Dehling, T., & Sunyaev, A. (2020). Trade-offs between Distributed Ledger Technology Characteristics. ACM Computing Surveys, 53(2), 37. https://doi.org/10.1145/3379463

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382-401. https://doi.org/10.1145/357172.357176

Mazières, D., & Shasha D. (2002). Building secure file systems out of byzantine storage. PODC '02: Proceedings of the twenty-first annual symposium on Principles of distributed computing. 108–117. https://doi.org/10.1145/571825.571840

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. (Erişim Tarihi: 15 Eylül 2021, https://bitcoin.org/bitcoin.pdf)

Buterik, V. (2013). Ethreum. (Erişim Tarihi: 15 Eylül 2021, https://ethereum.org/en/whitepaper).

Arslan, S. S., Jurdak, R., Jelitto, J., & Krishnamachari, B. (2020). Advancements in distributed ledger technology for Internet of Things. Internet of Things, 9, 1-5. https://doi.org/10.1016/j.iot.2019.100114

Pandl, K. D., Thiebes, S., Schmidt-Kraepelin, M., & Sunyaev A. (2020). On the Convergence of Artificial Intelligence and Distributed Ledger Technology: A Scoping Review and Future Research Agenda. IEEE. 8, 57075-57095. doi: 10.1109/ACCESS.2020.2981447

Cagigas, D., Clifton, J., Diaz-Fuentes, D., & Fernández-Gutiérrez, M. (2021). Blockchain for Public Services: A Systematic Literature Review. IEEE. 9, 13904-13921. doi: 10.1109/ACCESS.2021.3052019

Chen, Y-C, Chou, Y-P, & Chou, Y-C. (2019). An Image Authentication Scheme Using Merkle Tree Mechanisms. Future Internet, 11(7), 149. https://doi.org/10.3390/fi11070149

Qadir, A. M., & Varol, N. (2019). A Review Paper on Cryptography. 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 1-6. doi: 10.1109/ISDFS.2019.8757514.

Singh, S., Iqbal, S., & Jaiswal, A. (2015). Survey on Techniques Developed using Digital Signature: Public key Cryptography. International Journal of Computer Applications, 117(16). doi: 10.5120/20635-3272

Wamba, S. F., Kamdjoug, J. R. K., Bawack, R. E., & Keogh, J. G. (2020). Bitcoin, Blockchain and Fintech: a systematic review and case studies in the supply chain. Production Planning & Control, 31:2-3, 115-142. https://doi.org/10.1080/09537287.2019.1631460

Bach, L. M., Mihaljevic, B., & Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1545-1550. doi: 10.23919/MIPRO.2018.8400278

Dolenc, D., Turk, J., & Pustišek, M. (2020). Distributed Ledger Technologies for IoT and Business DApps. 2020 International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), 1-8. doi: 10.1109/CoBCom49975.2020.9174188

Hedera. (2021). (Erişim Tarihi: 15 Eylül 2021, https://hedera.com/learning/what-is-asynchronous-byzantine-fault-tolerance-abft)

Şafak, E., Arslan, Ç., & Gözütok, M. (2020). Blok Zinciri ile Yeni Nesil Dağıtık Defter Teknolojilerinin Karşılaştırılması. 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), 1-6. doi: 10.1109/ISMSIT50672.2020.9254311

Saad, A. & Park, S. Y. (2019). Decentralized Directed acyclic graph based DLT Network. COINS '19: Proceedings of the International Conference on Omni-Layer Intelligent Systems, 158-163. https://doi.org/10.1145/3312614.3312647

Živi, N., Kadušić, E., & Kadušić, K. (2019). Directed Acyclic Graph as Tangle: an IoT Alternative to Blockchains. 2019 27th Telecommunications Forum (TELFOR), 1-3, doi: 10.1109/TELFOR48224.2019.8971190

Bhandary, M., Parmar, M., & Ambawade, D. (2020). A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. 2020 5th International Conference on Communication and Electronics Systems (ICCES), 827-832, doi: 10.1109/ICCES48766.2020.9137858

Silvano, W.F., & Marcelino, R. (2020). Iota Tangle: A cryptocurrency to communicate Internet-of-Things data. Future Generation Computer Systems, 112, 307-319. https://doi.org/10.1016/j.future.2020.05.047

Schueffel, Patrick, Alternative Distributed Ledger Technologies Blockchain vs. Tangle vs. Hashgraph - A High-Level Overview and Comparison (December 15, 2017). https://ssrn.com/abstract=3144241 or http://dx.doi.org/10.2139/ssrn.3144241

Harris-Braun, E., Luck, N., & Brock, A. (2018). Holochain scalable agent-centric distributed computing DRAFT (ALPHA 1). https://github.com/holochain/holochain-proto/blob/whitepaper/holochain.pdf

Zia, M. F., Benbouzid, M., Elbouchikhi, E., Muyeen, S. M., Techato, K., & Guerrero, J. M., (2020). Microgrid Transactive Energy: Review, Architectures, Distributed Ledger Technologies, and Market Analysis. IEEE Access, 8, 19410-19432. doi: 10.1109/ACCESS.2020.2968402

Brock, A., Atkinson, D., Friedman, E., Harris-Braun, E., McGuire, E., Russell, J. M., Perrin, N., Luck, N., & Harris-Brau, W. (2017). Holo Green Paper. https://files.holo.host/2018/03/Holo-Green-Paper.pdf

Masood, F., & Faridi, A.R. (2018). An Overview of Distributed Ledger Technology and its Applications. International Journal of Computer Sciences and Engineering, 6(10), 422-427. doi: 10.26438/ijcse/v6i10.422427

Radix. (2020). Tempo - Consensus Lessons Learned. (Erişim Tarihi: 20 Eylül 2021, https://www.radixdlt.com/post/tempo-consensus-lessons-learned)

Sudhan, A., & Nene, M. J. (2017). Employability of blockchain technology in defence applications. 2017 International Conference on Intelligent Sustainable Systems (ICISS), 630-637. doi: 10.1109/ISS1.2017.8389247

Rahayu, S.B., RMN, N.J., Kamarudin, N.D., & Azahari, A.M. (2019). MILITARY BLOCKCHAIN FOR SUPPLY CHAIN MANAGEMENT. Journal of Education and Social Sciences, 13(1). https://www.jesoc.com/wp-content/uploads/2019/08/KC13_015.pdf

Worth, F. (2018). Lockheed Martin Partners With Guardtime Federal For Innovative Cyber Technology. (Erişim Tarihi: 20 Eylül 2021, https://news.lockheedmartin.com/2018-07-09-Lockheed-Martin-Partners-with-Guardtime-Federal-for-Innovative-Cyber-Technology)

Mathew. A.R. (2019). Cyber Security through Blockchain Technology. International Journal of Engineering and Advanced Technology (IJEAT), 9(1). doi: 10.35940/ijeat.A9836.109119

Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., & Choo, K.K.R. (2020). A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), 147-156. https://doi.org/10.1016/j.dcan.2019.01.005

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, & C., Santamaría, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?. Future Internet, 10(2). https://doi.org/10.3390/fi10020020

Chen, W., Xu, Z., Shi, S., Zhao, Y., & Zhao, J. (2018). A Survey of Blockchain Applications in Different Domains. ICBTA 2018: Proceedings of the 2018 International Conference on Blockchain Technology and Application, 17-21. https://doi.org/10.1145/3301403.3301407

Fizzy. (2017). AXA goes blockchain with fizzy. (Erişim Tarihi: 20 Eylül 2021, https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy)

Moosavi, J., Naeni, L.M., Fathollahi-Fard, A.M., & Fiore, U. (2021). Blockchain in supply chain management: a review, bibliometric, and network analysis. Environ Sci Pollut Res (2021). https://doi.org/10.1007/s11356-021-13094-3

Azzi, R., Chamoun, R.K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. Computers & Industrial Engineering, 135, 582-592. https://doi.org/10.1016/j.cie.2019.06.042

Kamath, R. (2018). Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM. The Journal of British Blockchain Association, 1(1), 1-12. doi: 10.31585/jbba-1-1-(10)2018

Cornelius, K. (2021). Betraying Blockchain: Accountability, Transparency and Document Standards for Non-Fungible Tokens (NFTs). Information 2021, 12(9), 358. https://doi.org/10.3390/info12090358

Thenmozhi, M., Dhanalakshmi, R., Geetha, S., & Valli, R. (2021). Implementing blockchain technologies for health insurance claim processing in hospitals. https://doi.org/10.1016/j.matpr.2021.02.776

Agbo, C.C., Mahmoud, Q.H., & Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019, 7(2), 56. https://doi.org/10.3390/healthcare7020056

Gursoy, G., Brannon, C., Wagner, S., & Gerstein M. (2020). Storing and analyzing a genome on a blockchain. biorxiv. https://doi.org/10.1101/2020.03.03.975334

Medicalchain. (2018). Medicalchain Whitepaper 2.1. (Erişim Tarihi: 20 Eylül 2021, https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf)

Jogunola, O., Hammoudeh, M., Anoh, K., & Adebisi, B. Distributed Ledger Technologies for Peer-to-Peer Energy Trading. (2020). 2020 IEEE Electric Power and Energy Conference (EPEC), 1-6. doi: 10.1109/EPEC48502.2020.9320061

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Renewable and Sustainable Energy Reviews, 100, 143-174. https://doi.org/10.1016/j.rser.2018.10.014

Brilliantova, V., & Thurner, T.W. (2019). Blockchain and the future of energy. Technology in Society, 57, 38-45. https://doi.org/10.1016/j.techsoc.2018.11.001

Brooklyn Microgrid. (2019). The Brooklyn microgrid: blockchain-enabled community power (Erişim Tarihi: 20 Eylül 2021, https://www.power-technology.com/features/featurethe-brooklyn-microgrid-blockchain-enabled-community-power-5783564)

Ali, O., Ally, M., Clutterbuck, & Dwivedi, Y.K. (2020). The state of play of blockchain technology in the financial services sector: A systematic literature review. International Journal of Information Management, 54. https://doi.org/10.1016/j.ijinfomgt.2020.102199

Chen, Y., & Bellavitis, C. (2020). Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights, 13. https://doi.org/10.1016/j.jbvi.2019.e00151

Barbaschow A. (2020). ASX's blockchain-based CHESS replacement pushed to April 2023. (Erişim Tarihi: 20 Eylül 2021, https://www.zdnet.com/article/asxs-blockchain-based-chess-replacement-pushed-to-april-2023)